



NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS

SCHOOL OF SCIENCES

DEPARTMENT OF INFORMATICS AND TELECOMMUNICATIONS

**POSTGRADUATE PROGRAMME "COMPUTER, TELECOMMUNICATIONS AND
NETWORK ENGINEERING "**

MSc Thesis

**Evaluation of Websites with Respect to Security and Privacy
Services**

Ilias D. Chountalas

Supervisor: **Limniotis Konstantinos**, External Tutor

ATHENS

FEBRUARY 2025



ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

**ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ "ΜΗΧΑΝΙΚΗ ΥΠΟΛΟΓΙΣΤΩΝ,
ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΔΙΚΤΥΩΝ"**

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

**Αποτίμηση Ιστοσελίδων ως προς
Υπηρεσίες Ασφαλείας και Ιδιωτικότητας**

Ηλίας Δ. Χουντάλας

Επιβλέπων: Λιμνιώτης Κωνσταντίνος, Διδάσκων εκτός Τμήματος

ΑΘΗΝΑ

ΦΕΒΡΟΥΑΡΙΟΣ 2025

MSc THESIS

Evaluation of Websites with Respect to Security and Privacy Services

Ilias D. Chountalas

S.N.: 7115122300016

SUPERVISOR: **Limniotis Konstantinos**, External Tutor

THESIS COMITEE: **Kostantinos Limniotis**, External Tutor
 Nikos Passas, Laboratory Teaching Staff
 Dimitrios Katsianis, External Tutor

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αποτίμηση Ιστοσελίδων ως προς τις Υπηρεσίες Ασφάλειας και Ιδιωτικότητας

Ηλίας Δ. Χουντάλας

A.M.: 7115122300016

ΕΠΙΒΛΕΠΩΝ: **Λιμνιώτης Κωνσταντίνος, Διδάσκων εκτός Τμήματος**

ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ **Κωνσταντίνος Λιμνιώτης, Διδάσκων εκτός Τμήματος**
Νίκος Πασσάς, ΕΔΙΠ
Δημήτριος Κατσιάνης, Διδάσκων εκτός Τμήματος

ABSTRACT

In today's digital era, ensuring website privacy and security has become a critical concern for both users and organisations. This thesis aims to evaluate the privacy and security practices of a targeted selection of websites, focusing on two key areas: compliance with GDPR cookie regulations, with emphasis to those rooted in the ePrivacy Directive and adherence to mainstream security standards.

The analysis is divided into two distinct parts. The first part examines the level of compliance with cookie regulations. In this case, primarily online stores and news websites were, as these types of sites tend to engage heavily in user tracking and data collection for advertising purposes. On the other hand, the second part of the analysis evaluates the security configurations of websites related to critical infrastructure sectors, based on NIS2 guidelines. In both cases only free tools were used to conduct this analysis.

As the findings reveal several privacy and security misconfigurations, this thesis highlights the need for continuous improvement in web privacy and security standards and lays the groundwork for future research. Through this work, the broader landscape of web privacy and security is better understood.

SUBJECT AREA: Website Security and Privacy

KEYWORDS: Cookies, GDPR, NIS2, ePrivacy, Websites

ΠΕΡΙΛΗΨΗ

Στη σημερινή ψηφιακή εποχή, η διασφάλιση του απορρήτου και της ασφάλειας των ιστοσελίδων αποτελεί κύριο μέλημα τόσο για τους χρήστες όσο και για τους οργανισμούς. Η παρούσα διπλωματική εργασία αποσκοπεί στην αξιολόγηση των πρακτικών προστασίας της ιδιωτικότητας και της ασφάλειας μιας στοχευμένης επιλογής ιστότοπων, εστιάζοντας σε δύο βασικούς τομείς: τη συμμόρφωση με τους κανονισμούς για τα cookies στο πλαίσιο της οδηγίας ePrivacy και κατ' επέκταση του GDPR, καθώς και την τήρηση των κύριων καθιερωμένων προτύπων ασφαλείας για ιστοσελίδες.

Η ανάλυση χωρίζεται σε δύο μέρη. Το πρώτο μέρος εξετάζει το επίπεδο συμμόρφωσης με τους κανονισμούς για τα cookies. Στην προκειμένη περίπτωση, η ανάλυση αφορά κυρίως ηλεκτρονικά καταστήματα και ειδησεογραφικούς ιστότοπους, καθώς αυτοί οι τύποι ιστοσελίδων τείνουν να εμπλέκονται σε μεγάλο βαθμό στην παρακολούθηση χρηστών και στη συλλογή δεδομένων για διαφημιστικούς σκοπούς. Από την άλλη, το δεύτερο μέρος της ανάλυσης αξιολογεί τις διαμορφώσεις ασφαλείας των ιστότοπων που σχετίζονται με τομείς κρίσιμων υποδομών, με βάση τις κατευθυντήριες γραμμές της οδηγίας NIS2. Και στις δύο περιπτώσεις χρησιμοποιήθηκαν μόνο δωρεάν εργαλεία για τη διεξαγωγή της ανάλυσης.

Τα ευρήματα αποκαλύπτουν αρκετές ευπάθειες και προβλήματα στις ρυθμίσεις που σχετίζονται με το απόρρητο και ασφάλεια των ιστοσελίδων. Έτσι, η παρούσα διατριβή τονίζει την ανάγκη συνεχούς και περαιτέρω βελτίωσης της συμμόρφωσης των ιστοσελίδων και θέτει τις βάσεις για επιπλέον μελλοντική έρευνα.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Ασφάλεια και Ιδιωτικότητα Ιστοσελίδων

KEYWORDS: Cookies, GDPR, NIS2, ePrivacy, Websites

ΕΥΧΑΡΙΣΤΙΕΣ

Πρωτίστως, θα ήθελα να εκφράσω τις ειλικρινείς μου ευχαριστίες στον επιβλέποντα μου, κ. Κωνσταντίνο Λιμνιώτη, για την ανάθεση της παρούσας διπλωματικής εργασίας και την πολύτιμη υποστήριξή του καθ' όλη τη διάρκεια της συγγραφής της.

Επιπλέον, θα ήθελα να ευχαριστήσω την οικογένεια μου και ιδιαίτερα τους γονείς μου Δημήτριο Χουντάλα και Αγγελική Γεωργίου για την αμέριστη υποστήριξη τους καθ' όλη τη διάρκεια των σπουδών μου.

CONTENTS

1. Introduction.....	18
1.1 Problem Statement.....	18
1.2 Thesis Scope	18
1.2.1 Research Questions	18
1.2.2 Research Approach.....	18
2. Overview of Website Security.....	20
2.1 Encryption and Secure Communications (SSL/TLS)	20
2.1.1 The Evolution of SSL/TLS	21
2.1.2 SSL/TLS Certificates.....	22
2.1.3 SSL/TLS Vulnerabilities	24
2.2 Authentication Mechanisms and Access Control	27
2.2.1 Multi-Factor Authentication (MFA).....	27
2.2.2 OpenID Connect	28
2.2.3 CAPTCHA and Bot Protection	29
2.3 DNSSEC and PCI DSS	30
2.3.1 DNSSEC.....	30
2.3.2 PCI DSS.....	30
2.4 Vulnerability Management and Scanning for Websites	31
2.4.1 Passive Scanning.....	31
2.4.2 Active Scanning	32
3. Overview of Website Privacy.....	34
3.1 Cookies by Category.....	35
3.1.1 Strictly Necessary Cookies	35
3.1.2 Performance and Functionality Cookies.....	35
3.1.3 Targeting Cookies	36
3.2 Cookies by Security	36
3.2.1 HttpOnly Cookies	36
3.2.2 SameSite Cookies	36
3.2.3 Secure Cookies.....	37
3.3 Advanced Tracking Mechanisms	37
3.3.1 Session-only Tracking Mechanisms	38
3.3.2 Storage-Based Tracking Mechanisms	39
3.3.3 Cache-based Tracking Mechanisms	40
3.3.4 Web Fingerprinting	41
4. Legal and Regulatory Frameworks in Website Security and Privacy	43
4.1 The European Regulatory Framework	43
4.1.1 Data Protection Directive 95/46/EC	43
4.1.2 ePrivacy Directive 2002/58/EC.....	43
4.2 The GDPR Framework	44
4.2.1 Definitions and Fundamentals	44
4.2.2 The Impact of on Websites and Global Data Practices	44
4.3 Cookie Consent and GDPR Compliance	45
5. Used Tools	47
5.1 Tools for Cookie Compliance Evaluation	47
5.1.1 CookieYes	47
5.1.2 ImmuniWeb Privacy Test.....	51
5.1.3 Cookie-Editor	53
5.2 Tools for Website Security Evaluation.....	54
5.2.1 ImmuniWeb Website Security Test and SSL Security Test.....	55
5.3 Honourable Mentions.....	57
5.3.1 Qualys SSL Labs.....	58
5.3.2 Webbkoll by dataskydd.net	58
6. Examining Websites in Practice	60

6.1	Evaluation Framework and Approach	60
6.1.1	Standards for Assessing Cookie Non-Compliance and deviation from best practises	60
6.1.2	Standards for Assessing Website Security	61
6.2	Methodology	62
6.2.1	Website Selection Criteria	62
6.2.2	Websites Under Examination	63
6.2.3	The Procedure	63
6.2.4	Practical Evaluation and Analysis on Cookie Compliance	65
6.2.5	Case Study 1: www.plaisio.gr (Extended)	65
6.2.6	Case study 2: www.tovima.gr	73
6.2.7	Case Study 3: www.public.gr	82
6.2.8	Case study 4: www.notos.gr	86
6.2.9	Case Study 5: www.atticadps.gr	92
6.2.10	Case Study 6: www.kathimerini.gr	97
6.2.11	Case Study 7: www.lifo.gr	104
6.2.12	Case study 8: www.cnn.gr	110
6.2.13	Case Study 9: www.protothema.gr	115
6.2.14	Case Study 10: www.factoryoutlet.gr	120
6.3	Practical Evaluation and Analysis on Website Security	127
6.3.1	Case Study 1: www.gov.gr	127
6.3.2	Case study 2: www.dei.gr	129
6.3.3	Case study 3: www.nbg.gr	131
6.3.4	Case study 4: www.oasa.gr	133
6.3.5	Case study 5: www.nis.gr	135
6.3.6	Case Study 6: www.eydap.gr	137
6.3.7	Case Study 7: www.alphabank.gr	139
6.3.8	Case Study 8: www.aegeanair.com	141
6.3.9	Case Study 9: www.helpe.gr	143
6.3.10	Case Study 10: www.ert.gr	145
7.	Additional Analysis	148
7.1	Supplementary Website Cookie Evaluations	148
	To carry out the cookie evaluation for the rest of the websites, the same methodology was consistently applied throughout. This time however, the results from the ImmuniWeb Privacy scanning tool are not included in this instance, as the websites fully blocked the tool's access.	
	148	
7.1.1	Gov.gr	148
7.1.2	Dei.gr	150
7.1.3	Nbg.gr	154
7.1.4	Oasa.gr	157
7.1.5	Nis.gr	159
7.1.6	Eydap.gr	160
7.1.7	Alpha.gr	162
7.1.8	Aegeanair.com	164
7.1.9	Helpe.gr	165
7.1.10	Ert.gr	168
7.2	Supplementary Website Security Evaluations	171
7.2.1	Plaisio.gr	171
7.2.2	Public.gr	172
7.2.3	E-shop.gr	173
7.2.4	Factoryoutlet.gr	175
7.2.5	Notos.gr	175
8.	Findings summary	177
8.1	Privacy Evaluation Results	177
8.2	Security Evaluation Results	178
8.3	Observations on the Additional Analysis	179
9.	Conclusions and Future Work	180
10.	BIBLIOGRAPHY	181

LIST OF FIGURES

Figure 1: Evolution of SSL/TLS.....	22
Figure 2: SSL Certificate Structure.....	23
Figure 3: HTTPS Detected on Browser.....	23
Figure 4: The Workflow of SSL Certificates.....	24
Figure 5: SSL Layered Representation	25
Figure 6: Client - Server Communication during Handshake Phase	26
Figure 7: Authentication Methods Evolution.....	28
Figure 8: OIDC Protocol Workflow	29
Figure 9: CAPTCHA Flowchart	30
Figure 10: OWASP Top 10 Vulnerabilities	32
Figure 11: Overview of Tracking Mechanisms	38
Figure 12: Cookie Acceptance Rate Example.....	45
Figure 13: Example of a Maliciously Configured Cookie Banner.....	46
Figure 14: Example of a Correctly Configured Cookie Banner.....	46
Figure 15: CookieYes Plan Options	48
Figure 16: CookieYes Scanner UI.....	48
Figure 17: CookieYes Scan Execution.....	49
Figure 18: Example of a CookieYes Scan Report 1/2	49
Figure 19: Example of a CookieYes Scan Report 2/2	50
Figure 20: ImmuniWeb Community Edition Tools	51
Figure 21: ImmuniWeb Scanner UI.....	52
Figure 22: ImmuniWeb Privacy Scan Report Example (1/3)	52
Figure 23: ImmuniWeb Privacy Scan Report Example (2/3)	53
Figure 24: ImmuniWeb Privacy Scan Report Example (3/3)	53
Figure 25: Cookie-editor Usage Example	54
Figure 26: ImmuniWeb Security Scan Report Example (1/5)	55
Figure 27: ImmuniWeb Security Scan Report Example (2/5).....	56
Figure 28: ImmuniWeb Security Scan Report Example (3/5).....	56
Figure 29: ImmuniWeb Security Scan Report Example (4/5).....	57
Figure 30: ImmuniWeb Security Scan Report Example (5/5).....	57
Figure 31: Qualys SSL Labs Scan Output Example.....	58
Figure 32: Webkoll Scanner UI	59
Figure 33: Security Testing Procedure Flowchart	64
Figure 34: Privacy Testing Procedure Flowchart.....	65

Figure 35: ImmuniWeb Scan plaisio.gr (1/4)	66
Figure 36: ImmuniWeb Scan plaisio.gr (2/4)	66
Figure 37: ImmuniWeb Scan plaisio.gr (3/4)	67
Figure 38: ImmuniWeb Scan plaisio.gr (4/4)	67
Figure 39: CookieYes Scan Results for Plaisio.gr	68
Figure 40: Overview of plaisio.gr Cookie Banner	70
Figure 41: Expanded Cookie Banner - plaisio.gr (1/2)	71
Figure 42: Expanded Cookie Banner - plaisio.gr (2/2)	71
Figure 43: rr_rcs Searched on Cookiepedia.....	72
Figure 44: ImmuniWeb Scan tovima.gr (1/4).....	73
Figure 45: ImmuniWeb Scan tovima.gr (2/4).....	73
Figure 46: ImmuniWeb Scan tovima.gr (3/4).....	74
Figure 47: ImmuniWeb Scan tovima.gr (4/4).....	74
Figure 48: CookieYes Scan tovima.gr.....	75
Figure 49: Overview of vima.gr Cookie Banner.....	78
Figure 50: Expanded Cookie Banner - tovima.gr (1/2)	79
Figure 51: Expanded Cookie Banner - tovima.gr (2/2)	79
Figure 52: Cookie-Editor Output - tovima.gr with Reject All option.....	80
Figure 53: _cb Searched on Cookiepedia	81
Figure 54: Cookie-Editor Output - tovima.gr with Accept All option.....	81
Figure 55: ImmuniWeb Scan - public.gr (1/4).....	82
Figure 56: ImmuniWeb Scan - public.gr (2/4).....	82
Figure 57: ImmuniWeb Scan - public.gr (3/4).....	82
Figure 58: ImmuniWeb Scan - public.gr (4/4).....	83
Figure 59: CookieYes Scan public.gr	83
Figure 60: Overview of public.gr Cookie Banner	85
Figure 61: Expanded Cookie Banner - public.gr.....	85
Figure 62: ImmuniWeb Scan - notos.gr (1/4)	86
Figure 63: ImmuniWeb Scan - notos.gr (2/4)	86
Figure 64: ImmuniWeb Scan - notos.gr (3/4)	87
Figure 65: ImmuniWeb Scan - notos.gr (4/4)	87
Figure 66: CookieYes Scan - notos.gr	87
Figure 67: Cookie Banner Overview - notos.gr	91
Figure 68: Extended Cookie Banner - notos.gr (1/2).....	91
Figure 69: Figure 68: Extended Cookie Banner - notos.gr (2/2).....	91
Figure 70: cpab Searched on cookiepedia.....	92
Figure 71: ImmuniWeb Scan - atticadps.gr (1/4).....	92

Figure 72: ImmuniWeb Scan - atticadps.gr (2/4).....	93
Figure 73: ImmuniWeb Scan - atticadps.gr (3/4).....	93
Figure 74: ImmuniWeb Scan - atticadps.gr (4/4).....	93
Figure 75: CookieYes Scan - atticadps.gr	93
Figure 76: Cookie Banner Overview - atticadps.gr	95
Figure 77: Expanded Cookie Banner - atticadps.gr (1/2)	95
Figure 78: Expanded Cookie Banner - atticadps.gr (1/2)	96
Figure 79: Revoke Consent Option - atticadps.gr	96
Figure 80: ImmuniWeb Scan - kathimerini.gr (1/4).....	97
Figure 81: ImmuniWeb Scan - kathimerini.gr (2/4).....	97
Figure 82: ImmuniWeb Scan - kathimerini.gr (3/4).....	97
Figure 83: ImmuniWeb Scan - kathimerini.gr (4/4).....	98
Figure 84: CookieYes Scan - kathimerini.gr	98
Figure 85: Cookie Banner Overview - kathimerini.gr	103
Figure 86: Expanded Cookie Banner - kathimerini.gr	103
Figure 87: Cookie-editor Output - kathimerini.gr	104
Figure 88: ImmuniWeb Scan - lifo.gr (1/4)	105
Figure 89: ImmuniWeb Scan - lifo.gr (2/4)	105
Figure 90: ImmuniWeb Scan - lifo.gr (3/4)	105
Figure 91: ImmuniWeb Scan - lifo.gr (4/4)	106
Figure 92: CookieYes Scan - lifo.gr	106
Figure 93: Cookie Banner Overview - lifo.gr	109
Figure 94: Expanded Cookie Banner - lifo.gr	109
Figure 95: Cookie-editor Output - lifo.gr	110
Figure 96: Revoke Consent Option - lifo.gr	110
Figure 97: ImmuniWeb Scan - cnn.gr (1/4)	111
Figure 98: ImmuniWeb Scan - cnn.gr (2/4)	111
Figure 99: ImmuniWeb Scan - cnn.gr (3/4)	111
Figure 100: ImmuniWeb Scan - cnn.gr (4/4)	111
Figure 101: CookieYes Scan - cnn.gr	112
Figure 102: Cookie Banner Overview - cnn.gr	114
Figure 103: Expanded Cookie Banner - cnn.gr	114
Figure 104: Cookie-editor Output - cnn.gr	115
Figure 105: ImmuniWeb Scan - protothema.gr (1/4).....	115
Figure 106: ImmuniWeb Scan - protothema.gr (2/4).....	116
Figure 107: ImmuniWeb Scan - protothema.gr (3/4).....	116
Figure 108: ImmuniWeb Scan - protothema.gr (4/4).....	116

Figure 109: CookieYes Scan - protothema.gr	117
Figure 110: Cookie Banner Overview - protothema.gr	119
Figure 111: Expanded Cookie Banner - protothema.gr	119
Figure 112: Cookie-editor Output - protothema.gr	120
Figure 113: Revoke Consent Option - protothema.gr	120
Figure 114: ImmuniWeb Scan - factoryoutlet.gr (1/4).....	121
Figure 115: ImmuniWeb Scan - factoryoutlet.gr (2/4).....	121
Figure 116: ImmuniWeb Scan - factoryoutlet.gr (3/4).....	121
Figure 117: ImmuniWeb Scan - factoryoutlet.gr (4/4).....	122
Figure 118: CookieYes Scan - factoryoutlet.gr	122
Figure 119: Cookie Banner Overview - factoryoutlet.gr	124
Figure 120: Extended Cookie Banner - factoryoutlet.gr (1/3)	125
Figure 121: Extended Cookie Banner - factoryoutlet.gr (2/3)	125
Figure 122: Extended Cookie Banner - factoryoutlet.gr (3/3)	126
Figure 123: Cookie-editor Output - factoryoutlet.gr	126
Figure 124: ImmuniWebSec Scan - gov.gr	127
Figure 125: Qualys SSL Labs Test - gov.gr (1/4)	128
Figure 126: Qualys SSL Labs Test - gov.gr (2/4)	128
Figure 127: Qualys SSL Labs Test - gov.gr (3/4)	128
Figure 128: Qualys SSL Labs Test - gov.gr (4/4)	129
Figure 129: Partial Scan Blockage - dei.gr	129
Figure 130: Qualys SSL Labs Test - dei.gr (1/3)	130
Figure 131: Figure 130: Qualys SSL Labs Test - dei.gr (2/3)	131
Figure 132: Figure 130: Qualys SSL Labs Test - dei.gr (3/3)	131
Figure 133: ImmuniWeb TLS Test - nbgr.gr (1/2).....	132
Figure 134: ImmuniWeb TLS Test - nbgr.gr (2/2).....	132
Figure 135: Partial Scan Blockage - oasa.gr	133
Figure 136: Qualys SSL Labs Test - oasa.gr (1/3).....	134
Figure 137: Qualys SSL Labs Test - oasa.gr (2/3)	134
Figure 138: Qualys SSL Labs Test - oasa.gr (3/3).....	135
Figure 139: Qualys SSL Labs Test - nis.gr (1/2)	136
Figure 140: Qualys SSL Labs Test - nis.gr (2/2)	137
Figure 141: ImmuniWeb TLS Test (1/2) - eydap.gr	138
Figure 142: ImmuniWeb TLS Test (2/2) - eydap.gr	139
Figure 143: ImmuniWeb Security Scan - alphabank.gr	139
Figure 144: Qualys SSL Labs Test - alphabank.gr (1/3)	140
Figure 145: Qualys SSL Labs Test - alphabank.gr (2/3)	140

Figure 146: Qualys SSL Labs Test - alphabank.gr (3/3)	141
Figure 147: ImmuniWeb Security Test - aegeanair.com	142
Figure 148: Qualys SSL Labs Test - aegeanair.com (1/3)	142
Figure 149: Qualys SSL Labs Test - aegeanair.com (2/3)	142
Figure 150: Qualys SSL Labs Test - aegeanair.com (3/3)	143
Figure 151: ImmuniWeb TLS Test - helpe.gr (1/4)	144
Figure 152: ImmuniWeb TLS Test - helpe.gr (2/4)	145
Figure 153: ImmuniWeb TLS Test - helpe.gr (3/4)	145
Figure 154: ImmuniWeb TLS Test - helpe.gr (4/4)	145
Figure 155: Partial Scan Blockage - ert.gr	145
Figure 156: Qualys SSL Labs Test - ert.gr (1/3).....	146
Figure 157: Qualys SSL Labs Test - ert.gr (2/3).....	147
Figure 158: Qualys SSL Labs Test - ert.gr (3/3).....	147
Figure 159: CookieYes Scan Gov.gr.....	148
Figure 160: ai_user searched on cookiepedia.....	149
Figure 161: Cookie Banner gov.gr	150
Figure 162: Cookie-Editor gov.gr	150
Figure 163: CookieYes scan gov.gr	150
Figure 164: Cookie banner dei.gr.....	152
Figure 165: Expanded cookie banner dei.gr	153
Figure 166: Cookie-Editor dei.gr	153
Figure 167: CookieYes scan nbg.gr	154
Figure 168: Cookie banner nbg.gr.....	156
Figure 169: Expanded cookie banner nbg.gr	156
Figure 170: Cookie-editor nbg.gr	157
Figure 171: CookieYes scan oasa.gr	157
Figure 172: Cookie banner oasa.gr.....	157
Figure 173: Cookie-editor oasa.gr.....	158
Figure 174: Revoking consent option oasa.gr	158
Figure 175: CookieYes scan nis.gr	159
Figure 176: Cookie-editor nis.gr.....	159
Figure 177: CookieYes scan eydap.gr	160
Figure 178: Cookie banner eydap.gr.....	161
Figure 179: Expanded cookie banner eydap.gr.....	161
Figure 180: Cookie-editor eydap.gr.....	162
Figure 181: CookieYes scan alpha.gr	162
Figure 182: Cookie banner alpha.gr.....	162

Figure 183: Expanded cookie banner alpha.gr.....	163
Figure 184: Cookie-editor alpha.gr.....	163
Figure 185: CookieYes scan aegeanair.com.....	164
Figure 186: Cookie banner aegeanair.com	164
Figure 187: Expanded cookie banner aegeanair.com	164
Figure 188: Cookie-editor aegeanair.com	165
Figure 189: CookieYes scan helpe.gr	165
Figure 190: Cookie banner helpe.gr.....	166
Figure 191: Expanded Cookie banner helpe.gr.....	167
Figure 192: Cookie-editor helpe.gr.....	167
Figure 193: CookieYes scan ert.gr.....	168
Figure 194: Cookie banner ert.gr	170
Figure 195: Expanded cookie banner ert.gr	170
Figure 196: Cookie-editor ert.gr	170
Figure 197: SSL Scan rating plaisio.gr.....	171
Figure 198: SSL configuration plaisio.gr.....	171
Figure 199: TLS cipher suites plaisio.gr	172
Figure 200: SSL scan rating public.gr	172
Figure 201: SLL configuration public.gr.....	173
Figure 202: SSL scan rating e-shop.gr.....	173
Figure 203: SSL configuration e-shop.gr.....	173
Figure 204: TLS cipher suites e-shop.gr	174
Figure 205: SSL scan rating factoryoutlet.gr	175
Figure 206: TLS configuration factoryoutlet.gr.....	175
Figure 207: SSL scan notos.gr.....	175
Figure 208: TLS configuration notos.gr	176
Figure 209: Cookie Violations by Percentage	178

LIST OF TABLES

Table 1: Common SSL/TLS Vulnerabilities	27
Table 2: Website Selection for Privacy Evaluation	63
Table 3: Website Selection for Security Evaluation	63
Table 4: Cookies Detected on plaisio.gr	68
Table 5: Cookies Detected - tovima.gr	75
Table 6: Cookies Detected - public.gr	83
Table 7: Cookies Detected - notos.gr	88
Table 8: Cookies Detected on atticadps.gr	94
Table 9: Cookies Detected on kathimerini.gr	98
Table 10: Cookies Detected - lifo.gr	107
Table 11: Cookies Detected on cnn.gr	112
Table 12: Cookies Detected on protothema.gr	117
Table 13: Cookies Detected on factoryoutlet.gr	122
Table 14: Software Related Vulnerabilities - dei.gr	130
Table 15: Software Related Vulnerabilities - oasa.gr	133
Table 16: Software Related Vulnerabilities - nis.gr	136
Table 17: Software Related Vulnerabilities - eydap.gr	137
Table 18: Software Related Vulnerabilities - helpe.gr	144
Table 19: Cookie Violations Summary	177
Table 20: Security Evaluation Results	179
Table 21: CookieYes Cookies gov.gr	149
Table 22: CookieYes Cookies dei.gr	151
Table 23: CookieYes cookies nbg.gr	154
Table 24: CookieYes cookies nis.gr	159
Table 25: CookieYes cookies eydap.gr	160
Table 26: CookieYes Cookies helpe.gr	166
Table 27: CookieYes cookies ert.gr	168

1. Introduction

1.1 Problem Statement

Ensuring website privacy and security is a continuous and growing challenge in the World Wide Web. User tracking, personal data collection or potential data leakage and theft are major concerns, since websites and third-party organisations leverage tracking technologies and other advanced services to personalize content, such as advertisements and other user experiences. This along with the increase in cyberattacks and the commercialization of user data, have further highlighted the need for strict privacy laws and security protocols. Even though regulations such as the ePrivacy directive [1] are intended to safeguard users, the environment continues to present difficulties. Numerous websites, whether intentionally or not, use configurations that could violate user rights, such as unclear consent processes, using "dark patterns" to deceive users into accepting cookies, or having insufficient security settings that place them at risk of attacks.

The General Data Protection Regulation (GDPR) [2] is the main legal instrument in Europe for data privacy, mainly because of its wider applicability and more strict enforcement measures. Apart though from the GDPR, there also exists the ePrivacy Directive that focuses on online and electronic communications, such as cookies and marketing practices. It should be pointed out that its effectiveness is limited due to the varying levels of enforcement in different EU countries, while, on the other hand, the GDPR establishes more thorough and enforceable regulations for safeguarding personal data, which are applicable worldwide to every business providing services to EU residents and on top of that includes substantial penalties in case of compliance failure. Thus, the GDPR provides a stronger framework for managing data protection and user privacy in the digital realm. However, the ePrivacy is applicable as "lex specialis" legislation in specific fields (which includes the use of cookies).

Apart from privacy, website security plays a crucial role in protecting users from common threats such as data breaches, identity theft, and malware attacks. The rise of cyberattacks and vulnerability exploitation in website infrastructures has pointed out the importance of adhering to strong security standards like those outlined in the Network and Information Systems 2022 (NIS2) Directive [2]. Implementing complex encryption protocols, secure configurations, and protection against common vulnerabilities, such as SQL injections [3] and cross-site scripting (XSS) [4] are essential to maintaining the integrity and safety of websites and in turn protect user data.

In conclusion, both privacy and security are vital components in the protection of users on the World Wide Web. While the GDPR strengthens privacy rights with enforceable laws, website security standards continue to evolve to handle the growing complexity of cyber threats. Together, these regulations and measures create a safer and more transparent digital environment for users and service providers alike.

Thus, this study highlights the current security and privacy compliance gaps of websites providing a foundation for future research and potential improvements.

1.2 Thesis Scope

The scope of this thesis is to evaluate and analyse the privacy and security practices of popular websites, with a focus on compliance with cookie regulations and adherence to security standards. Since privacy and security, while interrelated, are two very broad sectors that require separate evaluation methods, the analysis was split into two distinct

parts. Additionally, only free tools were utilized for both assessments, which allowed for an accessible and replicable analysis, though also presented limitations in the depth of the findings.

Through a detailed analysis of target selected websites, this thesis aims to offer insights into the current landscape of web privacy and security practices. Regarding the privacy part, the evaluation targeted media and news websites, where cookie compliance is critical. In terms of security, websites from sectors related to the NIS2 Directive, such as transport, banking, and other critical infrastructures, were selected for evaluation.

The main goal is to shed light on the current state of web privacy and security practices, recognize common issues and to showcase opportunities for improvement. Additionally, this study seeks to establish the groundwork for future research, by identifying the most common issues in these sectors, creating a foundation for further in-depth analysis.

1.2.1 Research Questions

This work aims to answer several critical research questions regarding website privacy and security.

First, it seeks to explore how compliant websites are with cookie best practises and regulations, mainly set in the ePrivacy Directive and the GDPR. Moreover, it tries to collect statistical data regarding the most common misconfigurations and/or violations. However, the most crucial question, is to investigate how common violations of cookie compliance are across websites, regardless of the existing regulatory frameworks and irrespective of the potential fines and penalties. Thus, showcasing the extent to which these violations persist despite regulatory efforts aimed at ensuring user consent and privacy.

Secondly, it strives to investigate the security compliance levels of websites that fall under the umbrella of the NIS2 directive. This is a pressing issue that has garnered significant attention. By 2025, it is estimated that over 100,000 public and private sector organizations will be required to comply with NIS2 [5]. Failure to comply could result in sanctions, including administrative fines for both private and public sector entities, temporary suspension of relevant service certifications, and potential bans on individuals responsible for managerial functions.

By shedding light into these critical matters, this research offers a detailed insight into website compliance practices, the obstacles to achieving full regulatory adherence, and the effectiveness of existing regulatory frameworks in both privacy and security.

1.2.2 Research Approach

The research methodology is very straightforward. As already discussed, only free tools are used to conduct the assessment.

Regarding the privacy and cookie evaluation a set of custom rule checks has been developed. These checks are designed to evaluate how well websites adhere to privacy and cookie regulations. By applying these checks, key aspects of website behavior are examined in an attempt to ensure compliance with relevant privacy laws and standards, always emphasizing on the ePrivacy Directive and the GDPR. In accordance a custom website selection list was created, containing online stores and news websites as these types of sites tend to engage heavily in user tracking and data collection for advertising purposes.

For the security assessment, the focus was on websites covered by the NIS2 Directive. These sites were scanned using a specialized tool to evaluate their security configurations. The checks included an analysis of TLS configurations, PCI DSS compliance, outdated software, and other critical security aspects. This approach provided a quick yet effective way to assess the security posture of these websites, ensuring they meet essential standards for safeguarding user data and maintaining secure operations.

Lastly, the project's methodology is furtherly analysed in a dedicated section later in this thesis.

2. Overview of Website Security

In today's digital landscape, websites serve as fundamental platform for communication, data exchange and transactions for both individuals and organizations. However, with the growing reliance on the internet, websites have become primary targets for cyberattacks, data breaches and other malicious activities. As a result, website security has become a major concern for ensuring the confidentiality, integrity and availability-often referred as the CIA triad-of sensitive data, along with the principle of non-repudiation.

The standardized term for describing website security refers to the protection of personal and organizational public websites from cyberthreats [6]. It includes a wide range of practices and technologies designed to protect websites from potential threats and vulnerabilities. One of the foundational components of this protection is encryption, particularly through the well-known protocol of SSL/TLS, which establishes an encrypted network connection between web browsers and websites, to prevent unauthorized interception of sensitive data [7]. Alongside encryption, authentication mechanisms are essential for ensuring that only legitimate users can access sensitive areas of the website, protecting accounts from unauthorized access. There are numerous different ways to achieve authentication, such as Cookie and Token based authentication or third-party access like OpenID connect [8]. Additionally, access control systems, such as Role-Based Access Control (RBAC), limit user permissions to necessary actions, preventing unauthorized users from accessing sensitive resources. Lastly, there are two well-established security standards / protocols that are used in most websites, namely Payment Card Industry Data Security Standard (PCI DSS), which mainly protects cardholder data and DNSSEC (Domain Name System Security Extensions), which is designed to secure information provided by the DNS.

Other crucial pillars of website security are vulnerability management and gap analysis, which focus on finding and fixing system flaws to stop potential attacker exploitation. This requires doing frequent security assessments, deploying patches and following industry-standard best practices to mitigate security threats. Because cyber dangers are always changing, maintaining website security requires constant work and adjustment.

This chapter will focus on the fundamental parts of website security alongside with vulnerability management, especially a part of this process, called vulnerability scanning, as these are more relevant to the main scope of this thesis. However, it will also provide a high-level overview regarding authentication and access control, in an attempt of indicating how these components cooperate to protect user data and online identities from new and developing threats.

2.1 Encryption and Secure Communications (SSL/TLS)

Transport Layer Security (TLS) and Secure Sockets Layer (SSL), commonly referred in the wider literature as SSL, are cryptographic protocols designed to safeguard client-server communications over insecure network connections. Specifically, the protocol establishes the authentication of the members involved in the communication, transmitted information confidentiality and on top of that integrity checks.

While the process of establishing a transaction takes place, asymmetric cryptography systems are used to authenticate the connections of the participants exchanging a symmetric key, which is often referred to as a session key. Moreover, participants are authenticated by using the so-called X.509 certificates. On the other hand, the session key exchanged is parsed into one the approved symmetric algorithms, encrypting the data exchanged between the two members. This process results in covering the security principles of authentication and ensuring the confidentiality of the exchanged information.

Lastly, to be considered suitable and complete for key applications, the protocol has data integrity control mechanisms that are also implemented through symmetric cryptography with Message Authentication Codes (MACs) [9].

These security measures provide a strong foundation for secure communications and data exchange over potentially insecure networks, mitigating common dangers such as eavesdropping, tampering, and forgery. By combining authentication and data integrity checks the TLS/SSL protocol has become a crucial baseline in safeguarding sensitive data transferred between users and services, therefore securing modern web applications.

2.1.1 The Evolution of SSL/TLS

In the 1990s, SSL was introduced by Netscape in an attempt to secure online communications and transactions for both commercial use and professional organizations. It was designed to operate in-between the Application Layer and Transport Layer of the fundamental networking communication OSI model. The first version, namely 1.0, was never released due to major security concerns. On the contrary the second version 2.0 was officially launched later, in 1995. This version also had plenty of serious vulnerabilities that led to its replacement by version 3.0 in 1996. This version, implemented by Netscape engineers, became historically significant, with RFC 6101 published by the Internet Engineering Task Force (IETF).

By November 2014, SSL version 3.0 was deemed insecure due to its susceptibility to the POODLE attack [10], particularly when using block ciphers. While the RC4 algorithm, a stream cipher, was immune to POODLE, it had its own security flaws, leading to the official retirement of SSL 3.0. After that, Google announced plans to enforce updates by suspending websites still using version 3.0 from search results, thereby encouraging website owners to further invest into website security and user data protection.

After the retirement of SSL version 3.0, a new protocol was launched in 1999, this time named as Transport Layer Security (TLS). This protocol was set in motion as an improvement over SSL latest version standardized in RFC 2246. While TLS 1.0 and SSL 3.0 differences weren't dramatic, they were significant enough to prevent interoperability between the two versions. Essentially, TLS 1.0 could even be considered an unofficial continuation of SSL 3.1. However, vulnerabilities in many implementations of TLS 1.0 lead to the escalation of downgrade attacks, driving website sessions to SSL 3.0, thus compromising security. Eventually, this version was further weakened by the BEAST (2011) and Lucky 13 (2013) attacks [11], which exposed additional critical weaknesses.

In April 2006, following seven years of TLS 1.0 usage, TLS 1.1 was launched, standardized in RFC 4346. The key enhancements included protection against attacks on CBC (cipher-block chaining) algorithms, achieved by explicitly using initialization vectors (IVs) and suppressing decryption failed messages when padding errors occurred. These changes enabled the protocol to counter malicious activities that treat servers as decryption oracles. Additionally, this version introduced the standardization of the so-called IANA parameters, which handle IP distribution and protocol parameter management. Despite having these improvements, TLS 1.1 was still vulnerable to the aforementioned attacks such as Lucky (2013) and also included weaknesses from the RC4 algorithm exploitation. [12].

A newer version of TLS, namely TLS 1.2 standardized in RFC 5246 in August 2008, introduced significant changes by improving the flexibility and variety of the cryptographic algorithm selection. A key innovation was the ability for servers or clients to choose the hash and digital signature algorithms which they want to accept, removing previous

limitations. Additionally, more stringent controls were implemented for verifying the "EncryptedPreMasterSecret" versions. TLS 1.2 was regarded as the only fully secure version, utilizing next-generation algorithms like Authenticated Encryption with Associated Data (AEAD) and Galois Counter Mode (GCM), which enhanced both encryption and data integrity [13].

Constant growing concerns regarding the security of TLS 1.2 and the need to deprecate outdated algorithms in order to improve privacy, and reduce latency, resulted in the IETF's TLS working group developing the latest version of TLS, namely 1.3 in 2014. After extensive research and security analysis, the finalized version was standardized in RFC 8446, published in August 2018. This version came in with key cryptographic updates, like encrypting handshake messages, signing the handshake transcript, and using different keys for handshake and application data encryption. The protocol also got rid of older and insecure algorithms and methods, like the RSA key transport, SHA-1, and CBC mode, adopting modern AEAD schemes for data protection [14].

TLS version 1.3 comes different handshake modes. Most importantly, the 1-RTT handshake, which uses public-key certificates for server and optional client authentication. It also establishes several session keys to secure the handshake and application data. The name comes from the fact that after one round trip, the client can send application data. There is also the PSK mode, used for session resumption. This mode relies on pre-shared keys for authentication, and it optionally supports 0-RTT key establishment, allowing immediate encrypted data transmission alongside the initial handshake.

A brief visual representation of the evolution of SSL/TLS is presented below:

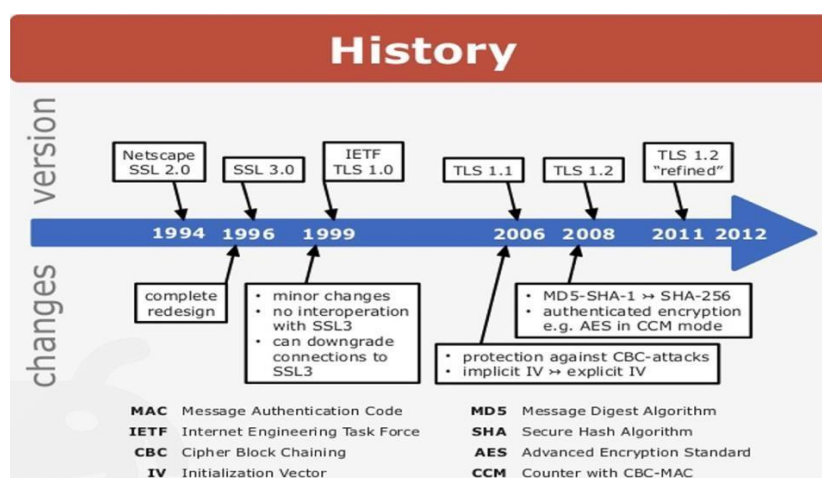


Figure 1: Evolution of SSL/TLS

In conclusion, SSL/TLS is the most used security protocol for encrypting communications over the internet. It consists of two main components: The TLS Handshake Protocol, which manages the authentication of the parties involved and the establishment of encryption keys and the TLS Record Protocol, which leverages these keys to ensure the CIA triad of the data exchanged, between the client and the server [15]. More details regarding these protocols will be discussed later in this chapter.

2.1.2 SSL/TLS Certificates

A crucial part of the SSL/TLS protocols are its certificates. The use of the more secure HTTPS on websites is made possible via SSL/TLS-or simply SSL certificates. By definition, a data file stored on the origin server of a website is referred to as an SSL certificate. In terms of functionality, they hold the public key and identity of the website,

together with other relevant data enabling the aforementioned SSL/TLS encryption. Appliances trying to communicate with the origin server will reference this file to obtain the public key and verify the server's identity. The private key is always kept secret and in case of leakage the security is considered as compromised.

It is crucial to understand how these certificates work. A high-level description regarding their structure and operation is presented below [16]:

SSL certificates include the following information in a single text file:

- The domain name of the certification's issue
- The source of issue
- The certificate authority (CA) of issue
- The CA's digital signature
- Associated subdomains
- Issue date of the certificate
- Expiration date of the certificate



Figure 2: SSL Certificate Structure

The certificate is stored on a webpage's origin server and is sent to any devices that request to load the website. It is also important to note that most web browsers enable users to view the SSL certificate, while visiting a webpage.

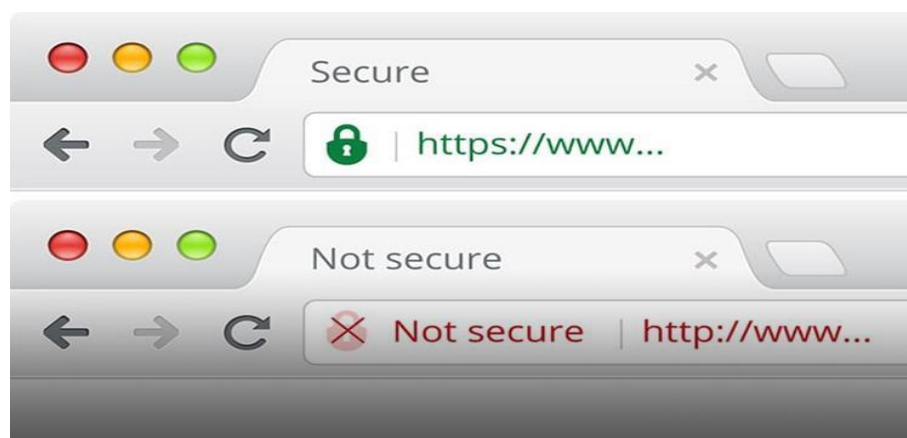


Figure 3: HTTPS Detected on Browser

Regarding their operation, the SSL certificates workflow is split in the following steps:

1. **Initiating secure connection:** A user proceeds to open a website that is protected with an SSL certificate.
2. **Certificate presentation:** The webserver replies by loading its SSL certificate to the browser that issued the request.
3. **Certificate validation:** The user's browser checks the SSL certificate for several attributes. The most significant of them are the expiring date, the Certificate Authority (CA), and the certificate's digital signature.
4. **Root trust verification:** Checks are performed by the browser, to validate if the SSL certificate is signed by a trusted root certificate.
5. **Key exchange process:** If the SSL certificate is valid and trusted, the server and browser start a process called "key exchange." The server forwards its public key to the browser, which in turn generates a symmetric session key and transmits it to the server using its public key cryptography.
6. **Establishing a secure connection:** At last, the browser encrypts the session key using the server's public key, establishing a secure connection.



Figure 4: The Workflow of SSL Certificates

In summary, SSL certificates play a critical role in ensuring website security by validating a website's identity and encrypting data transmissions. Without a valid SSL certificate, websites are flagged as "unsafe" by major browsers, often preventing access entirely, therefore establishing SSL as a key trust signal for users. Additionally, they offer an SEO advantage, as search engines rank secured websites higher, and some may not even display results from unsecured sites. Thus, SSL certificates are essential for securing a website, enhancing its online visibility and establishing user trust.

2.1.3 SSL/TLS Vulnerabilities

As already discussed, the first main scope of this thesis is to evaluate website security, an aspect directly interconnected with SSL/TLS vulnerabilities. However, to dive into the examination of those vulnerabilities it is crucial to first assess and comprehend the structure of the SSL/TLS protocol.

The protocol is split into two main layers, including several distinct subprotocols. The first one, namely the lower layer, is positioned adjacent to the transport layer in the OSI

reference model and includes the SSL/TLS Record Protocol, which manages the encapsulation and encryption of the data. The second layer, referred to as the upper layer sits just above the Record Protocol and includes the SSL/TLS Handshake Protocols, specifically: the Handshake Protocol, ChangeCipherSpec Protocol, and Alert Protocol. These handshaking protocols are responsible for initiating and managing the secure connection during the client-server communication [17]. A visual representation is shown on the image below, followed by a deeper analysis regarding the protocols on display:

SSL handshake protocol	SSL cipher change protocol	SSL alert protocol	Application Protocol (eg. HTTP)
SSL Record Protocol			
TCP			
IP			

Figure 5: SSL Layered Representation

The Record Protocol focuses on the transmission of data blocks between the two entities in communication. It takes messages from the upper layer of the OSI model, splits them into smaller, manageable fragments, optionally compresses the data, applies a Message Authentication Code (MAC), encrypts the output and finally transmits it. The security parameters used are established during handshake phase. **The Handshake Protocol** is the main operating pillar of SSL/TLS, since it is responsible for authenticating both parties involved in the communication. It also manages the negotiation of security parameters, such as the encryption keys and algorithms, which are responsible for securing the transmission of encrypted data while the communication takes place.

The ChangeCipherSpec Protocol is responsible for informing both entities in communication, to switch the session conditions the agreed-upon security parameters and transition to a secure mode of data exchange.

The Alert Protocol is utilized to signal any errors encountered during communication between the two parties. For instance, it can be used to indicate error events, such as that a connection is being terminated or that a message could not be decrypted. During the handshake phase, all cryptographic elements required for protecting the connection are established. The client server communication during the handshake phase follows a predefined set of messages, as shown on the image below:

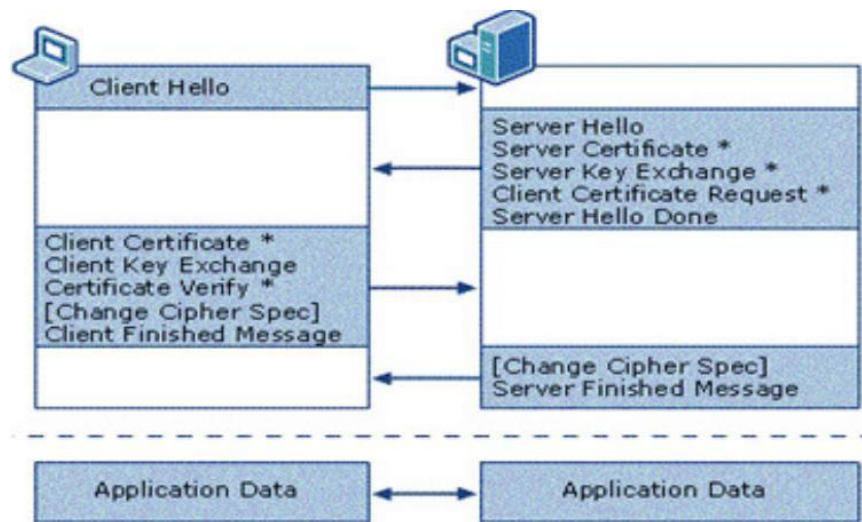


Figure 6: Client - Server Communication during Handshake Phase

Some of the typical messages exchanged include:

- **Client Hello:** This message is sent by the client to notify the server about the supported security parameters, including the protocol version, session ID, cipher suites, compression methods and other policies that it wishes to use.
- **Server Hello:** In response to the clientHello message, the server replies with this to specify the security parameters that will be used.
- **Certificate:** This message always contains the server's certificate and, optionally, the client's certificate in case of mutual authentication required.
- **ServerKeyExchange:** Following the ServerHello message, this optional message is sent when anonymous negotiation is used or when the server's certificate lacks sufficient information required for the client to continue with the key exchange.
- **CertificateRequest:** The server uses this message to request a certificate from the client. This step is also optional and deeply depends on the authentication requirements that were previously established.
- **ServerHelloDone:** The server sends this message to indicate that all necessary information has been sent to the client. From now on, the server no longer has any involvement with the establishment of the communication.
- **ClientKeyExchange:** This message contains the premaster secret generated by the client, which is encrypted using the server's public key. It will be used to derive the session's encryption keys.
- **CertificateVerify:** The client uses this message to prove possession of the private key corresponding to its public key if a client certificate was provided. This message is optional.
- **ChangeCipherSpec:** This message informs the other party that the agreed security parameters are established, meaning that every form of communication will be encrypted from now on.
- **Finished:** This message is sent by both parties to finalize the process and confirm the establishment of secure communication.

Once the negotiation is over and the required keys are generated, the Record Protocol takes the application-level data and divides it into smaller fragments. In turn, these are optionally compressed, run through a hash function, then encrypted with the agreed algorithm and at last transmitted via the transport layer to the other party.

In conclusion, while this protocol is considered the de facto standard in securing data transmissions on the internet, it is by no means immune to vulnerabilities. Over the years, attackers have discovered several weaknesses in SSL/TLS, particularly in the Handshake Protocol, but also in other of its key components. The most well-known attacks are listed on the table below:

Table 1: Common SSL/TLS Vulnerabilities

Cipher Suite Rollback Attack
Drop ChangeCipherSpec Attack
Version Rollback Attack
Key Exchange Algorithm Confusion
Bleichenbacher Attack on PKCS#1
RSA-Based Session Attacks in SSL/TLS
Timing Attack
Cross-Protocol Attack via ECC Key Exchange
New Bleichenbacher Side-Channel Attacks
SKIP-TLS Attack
FREAK Attack
Logjam Attack

2.2 Authentication Mechanisms and Access Control

The Internet and particularly websites have become one of the most popular and accessible platforms for information exchange. However, today's Internet faces numerous challenges, with one of the most critical being the need for robust security. Ensuring authentication through suitable mechanisms is a complex task. As with other network-based applications, security concerns have become central issues that need to be addressed. Among these concerns, authentication and access control are key areas that must be tackled to safeguard information and computing systems from unauthorized access [18].

There is a wide variety of website related authentication techniques, the most well-known and related to this thesis are: Multi-Factor Authentication (MFA), OpenID, Captcha and Bot Protection, password best practices and lasty session management and Cookies, which however will be analysed in depth in a later section.

2.2.1 Multi-Factor Authentication (MFA)

Most websites, especially when safety requirements are higher than usual, are MFA enabled, since it is a fundamental safeguard against bots and illegitimate access. Based on the current standards, three types of factor groups enable an individual to establish a connection to these websites [19]:

1. A **knowledge factor**, which refers to something the user knows, such as a password or a secret phrase.
2. An **ownership factor**, which involves something the user possesses, such as a card, smartphone, or other physical tokens.
3. Finally, the **biometric factor**, that refers to the physical characteristics of the user themselves, such as biometric data (e.g. fingerprints, or behavioural patterns).



Figure 7: Authentication Methods Evolution

Incorporating MFA into website security protocols adds an additional layer of protection against common cyberthreats like password theft or brute force attacks. By implementing more than one form of authentication, MFA reduces reliance on passwords alone, which are often vulnerable, especially by social-engineering attacks. This approach ensures that even if one authentication factor is breached, the other factors, such as possession of a physical device or biometric verification, provide additional security layers. As more online services adopt MFA, it becomes a crucial measure for safeguarding sensitive information and ensuring more robust security for both users and organisations.

2.2.2 OpenID Connect

Single Sign-On (SSO) services for the web, such as the well-known Google Sign-In are operating based on the OpenID Connect (OIDC) protocol. This protocol enables websites-relying parties to outsource user authentication to third-party identity providers. As one of the most recent and widely adopted SSO standards it has become a critical part of web authentication frameworks. To clarify, instead of creating a new username and password for each website, users can log in once and then leverage the authentication from the third-party provider.

This protocol is not going to be covered in detail in this thesis, however it is important to keep in mind the following high-level overview:

The OIDC protocol enables user authentication to Relying Parties (RPs) using their existing accounts at Identity Providers (IdPs). A fundamental pillar of OIDC is the ID token, an encrypted and signed document, which is generated by the user's IdP and validates the user's identity to the RP.

The basic procedure involves the user sending a login request at an RP by providing their email address. The RP retrieves necessary operational information for the protocol flow (known as discovery) and registers itself with the IdP. The user is then redirected to the IdP, to complete the authentication process. After successful authentication, the IdP issues an ID token to the RP, either relayed through the user's browser or directly fetched by the RP. This token contains config-like details such as the issuer (the IdP) and a unique user identifier, both signed by the IdP. The RP verifies the token to confirm the user's identity and may then set a session cookie in the user's browser to allow continuous access to its services [20].

This process is presented in the following figure:

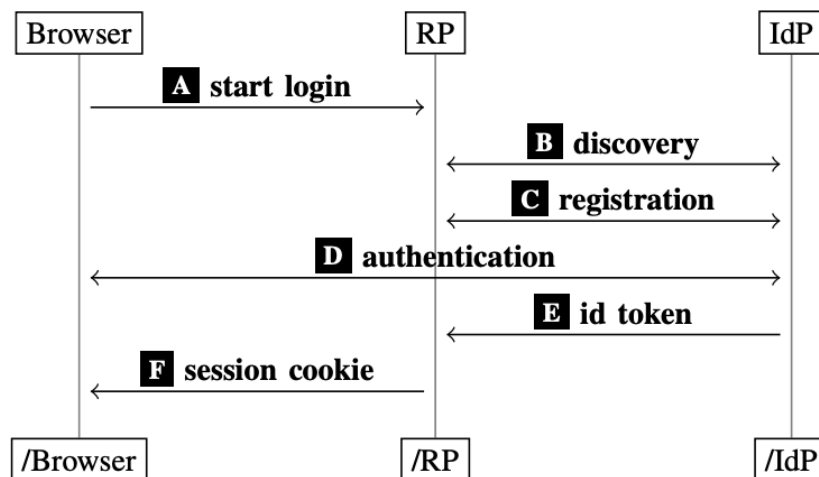


Figure 8: OIDC Protocol Workflow

2.2.3 CAPTCHA and Bot Protection

Completely Automated Public Turing Test to tell Computers and Humans Apart (CAPTCHA), was initially created in 2000 by Luis Von Ahn, Manuel Blum, Nicholas J. Hooper, and John Langford at Carnegie Mellon University (CMU). It works as a reverse Turing Test. On the other hand, the CAPTCHA application works as a judge, while the user is considered the participant. If the test is successfully carried out by the users, that means they are most likely human; otherwise, they are persuaded as bots. The system is designed in such way that it prevents automated bots from misusing online services like email providers, wikis, and blogs. Thus, CAPTCHA is a type of Human Interaction Proof (HIP) system that helps secure web-based applications by distinguishing between human users and bots through challenge-response tests [21].

For a test to be considered as CAPTCHA, it must fulfil the following:

- It should be easy enough for humans to complete successfully.
- It should be simple for the system to generate and evaluate.
- It should be difficult for automated bots to solve.

There is a wide variety of different types of CAPTCHAS, however this is beyond of the scope of this thesis. Thus, only the basic logic of this HIP system is presented in the flowchart below:

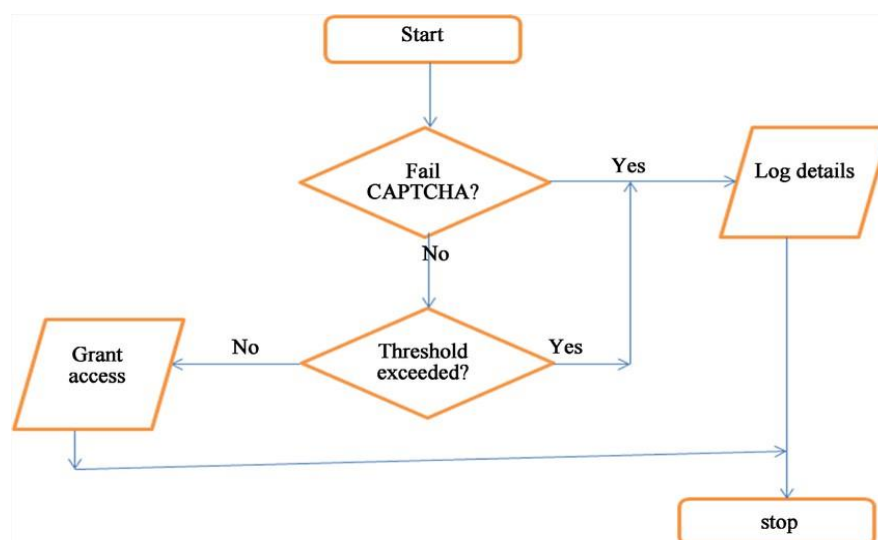


Figure 9: CAPTCHA Flowchart

This operation holds a crucial role in maintaining the integrity of online environments by filtering out bots, while ensuring that legitimate users easily interact with web services.

2.3 DNSSEC and PCI DSS

2.3.1 DNSSEC

DNSSEC was designed to settle many vulnerabilities and security concerns of DNS. It can be considered as a set of security extensions or even a separate protocol. Its main operation is to ensure data integrity and verification of the authentication of data origin, primarily by using pre-generated digital signatures for each piece of information stored in the DNS database. These signatures confirm that the data has not been altered and comes from a legitimate and trusted source-server. In case the data is not present on the server an authentication denial is produced [22].

However, no protocol comes without security flaws. The most important and well-know are listed below:

- Man in the middle (MITM) attacks: Packet Sniffing, Transaction ID Guessing
- Caching poisoning Problems
- Distributed Denial of Service (DDoS) Attacks

2.3.2 PCI DSS

Most websites support or even require online transactions. As already stated, websites are targets for cyberattacks and sensitive data theft, for example credit card information. PCI DSS is a data security standard specifically designed for organizations that carry over online card transactions. What it does, is that it ensures the security of storage, processing and transmission of cardholder data. To achieve compliance with this standard however, an organization must demonstrate that it meets all the required standards, either through internal assessments or by using third-party services [23]. Meaning, that depending on the organization's specific structure and circumstances, it may be eligible to complete a self-assessment or, alternatively, it might require a formal external audit conducted by a qualified entity.

In conclusion, the PCI DSS is well-respected and of great importance in the cybersecurity field. In this study we won't dive into detail about how it works, but we will try to examine if certain websites are compliant with this standard, since it is directly correlated to the overall security and privacy of websites that fall under the supervision of the NIS2 directive.

2.4 Vulnerability Management and Scanning for Websites

One of the primary objectives of this thesis is to conduct vulnerability analysis using open-source tools, focusing on a process referred to as a "Scanning Activity." It is essential to clarify that only passive website scans will be performed in this study. This decision is twofold. Firstly, the focus is on SSL/TLS certificates, protocol versions, cipher suites, and the usage of additional security measures like HTTP Strict Transport Security (HSTS), PCI DSS and DNS records. These aspects do not require intrusive, active scanning. Secondly, performing penetration testing on commercial websites without explicit permission is considered illegal [24].

Passive scanning, unlike active scanning, gathers information from public data and network traffic, without directly interacting with the target system in a disruptive way. This approach enables the detection of vulnerabilities, while minimizing the risk of impacting website performance or violating ethical and legal boundaries.

In the following sections, we will explore the types of reconnaissance scanning, including both passive and active methods. Furthermore, we will highlight the most common vulnerabilities that each type of scan is capable of detecting, focusing more on the active scanning, since most of the vulnerabilities related to the passive one have been already covered in previous sections.

At a first glance, web application vulnerability scanners appear to be user-friendly, often promoting their ability to detect numerous vulnerabilities with minimal setup – typically requiring just the base URL of the target application as input. However, in practice, using these tools effectively can be much more complex than it initially seems.

2.4.1 Passive Scanning

A passive scan conducts non-intrusive assessments, merely observing elements to assess whether they are vulnerable. This method can be visualized as encountering a door but refraining from touching it to check whether it is open or locked. If the door appears closed, the investigation stops at that point. This is particularly useful for detecting misconfigurations or outdated security protocols without risking disruption to the network or violating ethical and legal boundaries [25].

Data packets are intercepted and examined during passive vulnerability scanning to find known vulnerabilities, configuration errors, or possible attack routes. This could entail keeping an eye on network traffic in wired environments to make sure that only the most recent, secure versions of communication protocols, like TLS (Transport Layer Security), are being used, or monitoring traffic over the air in wireless networks to search for unauthorized or rogue Wi-Fi Access Points. It can also assist in locating out-of-date SSL/TLS certificates, inadequate encryption techniques, missing critical security headers like HTTP Strict Transport Security (HSTS) or weak cypher suites. In conclusion, passive vulnerability scanning can detect plenty of website vulnerabilities, without disrupting their normal daily operations or causing legal implications.

We will dive into more details regarding passive scanning or reconnaissance later on, as in this thesis various active scans took place, in a number of different websites.

2.4.2 Active Scanning

On the other hand, active scanning involves direct interaction with a target system by sending requests and analysing the responses to uncover vulnerabilities. Web application scanners do not have access to the source code and therefore detect vulnerabilities by mimicking potential attack patterns. With this approach, scanners can identify a wider range of vulnerabilities, including application-layer issues such as cross-site scripting (XSS), SQL injection, Cross-Site Request Forgery (CSRF) and a variety of insecure configurations. This operation is often called Penetration testing, and, in most cases, it is performed by third-party organizations, to detect security flaws in an organisation's website and therefore prevent potential attacks. Except from the vulnerabilities already mentioned there are a lot more, which can be detected from tools like vulnerability scanners, however the most emphasis is given on the so-called, Open Web Application Security Project (OWASP) Top 10 Vulnerability Types. The latest version established in 2021 is presented on the table below [26]:

No	Vulnerability Type	10	13	17	21	Description
1	Injection	✓	✓	✓	✓	The injection is a vulnerability in the application that allows user input data to be taken as a command. This allows the system to execute the unwanted command without requisite authorization and exposes the database to the attacker
2	Cross-Site Scripting (XSS)	✓	✓	✓		Cross-site scripting (XSS) is a computer vulnerability of web applications. It injects the attacker's script into the web application. When the user opens the web page, the script gets executed, allowing the attacker to change the web page, deface the web page or redirect the user to bad sites [63], [87], [65].
3	Cross-Site Request Forgery (CSRF)	✓	✓			Cross-Site Request Forgery (CSRF) tricks the user into taking undesired action after the user logs into an application. The user is tricked by malicious email or link that sends the forged request to the web server. The attack may change the user's password or transfer money from his account or steal data etc.
4	Broken Authentication and Session Management	✓	✓	✓		This vulnerability occurs due to improper security implementation of the web application as well as users' carelessness in the use of the system. In this, the attackers get access to the user's credentials if these are stored without encryption or the user is careless about the password, closes the browser without logging out, etc.
5	Broken Access control			✓	✓	This vulnerability happens due to improper implementation of access control of the website. It allows the attacker to get into the system where regular access is not permitted. Having gained access, attackers can steal information and create havoc
6	Insecure Direct Object References	✓	✓			The websites allow the user to access the system by putting a direct reference to the database in the URL. Insecure Direct Object References is a vulnerability of the system that enables an attacker to modify the URL containing direct reference to the database and access the location that regular user is not authorized to access
7	Missing Function Level Access Control		✓			This vulnerability happens due to improper functional level access rights given by developers to the user. The attacker changes the URL to access the unauthorized area by trial and error. This allows attackers to get inside the application without proper authorization if proper protection is not in place
8	Security Misconfiguration	✓	✓	✓	✓	Once a system is installed, it needs to be configured properly to plug all loopholes and remove all vulnerabilities. In the case system is not configured correctly, the attacker can exploit the system and make it vulnerable to attacks
9	Insecure Cryptographic Storage	✓				The sensitive data such as user credentials need to be stored in encrypted form so that in case of attacks, the attacker is unable to access the sensitive information. The encryption level should be as per norms to make stored data secure
10	XML External Entities (XXE)			✓		XML (Extensible Markup Language) is used by many web service and applications. XML parser or processor is used for the interpretation of XML data. If the XML processor accepts the XML entity without proper verification, then the attacker can push unwanted content that XML processor is unable to process and causes the denial of service

Figure 10: OWASP Top 10 Vulnerabilities

In summary, active vulnerability scanning-penetration testing can detect a wider range of vulnerabilities in contrast to passive scanning. However, it can lead to serious implications. Depending on the system's configuration and the intensity of the scan, it

may cause performance degradation, trigger security alarms, or even disrupt services. Furthermore, conducting active scans on websites or networks without explicit permission is illegal in many jurisdictions. Since active scans often mimic attack patterns, they could be viewed as malicious behaviour by the target, leading to potential legal action. Thus, these actions are beyond the main scope of this thesis and are not going to be discussed or tested in the following chapters.

3. Overview of Website Privacy

The second topic that this thesis focuses on, is Website Privacy and specifically Web Cookies. Designed in 1994 their main role was to maintain the state between clients and servers. A cookie is a small text string stored on a client's browser, which accesses a server, and it is sent back to the server with subsequent requests. Early support for cookies was available in the pre-1.0 Mosaic browser in 1994, and the first cookie standard was established in 1997. Since then, cookies have remained essential to the web, evolving with website and application needs.

First-party cookies, set by the domain in the browser's address bar, are commonly used in e-commerce for tasks like maintaining shopping cart data. Third-party cookies, set by domains other than the one being visited, are often used by data brokers, advertisers and tracking services such as Google Analytics. While vital for web applications, cookies raise significant privacy concerns, as data brokers and advertisers use them to collect detailed user information for targeted advertising. This has led to widespread concerns in the media, research, and regulatory bodies, prompting the development of tools for managing cookies and laws protecting user privacy.

Each time a user visits different websites, they are typically prompted to either accept or reject cookies. This is because cookies can store user preferences, such as a username or language settings for a specific period, thereby enabling the monitoring of online behaviour and the collection of personal data. Additionally, cookies can be utilized to gather anonymized statistical information regarding the browsing experience across various websites [27] [28].

A web cookie is a formatted string made up of key-value pairs separated by semicolons. In this study, the terms "web cookie" and "cookie" are used interchangeably. Other types of cookies, such as flash or zombie cookies, are not discussed here. A typical cookie might look like this:

Name=Value; Host=example.com; Path=/account; Expires=Tue, 1 Dec 2024 14:12:08 UTC; Secure;

- **Name:** Contains the cookie's unique identifier, which is sent by a particular server.
- **Value:** Holds the data transferred between the client and server. Though it can be in plain text, it is often encrypted or obfuscated for privacy and security.
- **Host:** Specifies the server from which the cookie originates. Also, it takes care of the cookie being sent back to the appropriate server and helps to sort first party and third-party cookies.
- **Path:** Checks when the cookie should be returned to the server, based on whether the path in the URL matches the value of the path attribute.
- **Expires:** Defines the date and time when the cookie becomes invalid. This attribute distinguishes between session and persistent cookies.
- **Secure:** A flag indicating that the cookie must be transmitted over secure protocols, for example HTTPS.
- **HttpOnly:** Works as a flag, which limits client-side access to the cookie, preventing it from being accessed by third party scripts.
- **isDomain:** A flag (specific to Firefox) that indicates whether the cookie should be sent to any subdomain of the original site, based on the host attribute.

This condensed version provides a clearer overview of the key aspects of cookies while reducing unnecessary detail.

Lastly, it is important to note that all types of cookies can be placed in two main groups, with respect to origin or lifespan, specifically [29]:

Based on origin

- **First-party cookies** are set by the website that the user is visiting and are recognizable only by that specific site. The site may also leverage external services, which can place **third-party cookies** e.g. cookies from another domain, often used for tracking and advertising purposes.

Based on lifespan

- **Persistent cookies** are stored on the user's device and remain there even after the browser is closed. However, they have an expiration date and will eventually be removed. In contrast, **session cookies** are temporary and are automatically deleted when the browser is closed, as they do not have an expiration date.

In the following sections dive into a deeper analysis of cookies, breaking down the aforementioned groups.

3.1 Cookies by Category

There are many different cookie categories. Each one of them is analysed on the following subsections.

3.1.1 Strictly Necessary Cookies

Strictly necessary cookies are essential for navigating a website and using its key features, such as gaining access to secure areas. For example, they enable online shopping carts to retain items while a user continues browsing. These cookies are typically first-party session cookies and do not require user consent. However, it is important to clearly inform users about the function of these cookies and why they are indispensable for the website's operation [30]. Lastly, essential cookies enable users to swap between websites without losing their previously performed actions.

3.1.2 Performance and Functionality Cookies

Performance cookies are designed to gather data about how users interact with a website, allowing the site owner to enhance its performance. These cookies track information such as page load times, user navigation, and any errors encountered, all of which are used to optimize the user experience. Functionality cookies, on the other hand, are responsible for remembering user-specific preferences, such as language settings or geographic location, allowing the website to offer a more personalized experience during future visits.

As a result, they help website owners understand which pages are the most and least popular and track how visitors navigate through the website. All data collected is encrypted and anonymized, ensuring that no specific user can be directly identified. If a user disables this service, the website provider will not be able to determine when the user has visited the site, nor will they be able to monitor the site's performance [31].

3.1.3 Targeting Cookies

Targeting cookies are used to deliver tailored advertisements to users, often by tracking their browsing activity across different websites. These cookies can also be shared with other advertisers to track the effectiveness and reach of the ads, helping monitor and measure their performance. By collecting data and building user profiles, targeting cookies allow websites to present ads that are more relevant to individual users, thereby driving ad revenue.

These cookies are typically third-party cookies, meaning they are placed by external domains rather than the website being directly visited. Targeting cookies often follow users from one site to another, enabling advertisers to display ads to users even after they have left the original site, by showing ads on other websites based on the user's previous interactions.

In case the user decides to reject this type of cookies, he will probably continue to watch ads during surfing the web, however these won't be entirely adjusted to his interests and preferences.

3.2 Cookies by Security

Cookies can also be categorized based on their security levels. Website owners should be aware that cookies offer varying degrees of security. Thus, from a security perspective, cookies are classified into three main types: HttpOnly, SameSite, and Secure cookies.

3.2.1 HttpOnly Cookies

In an effort to improve the security of cookies, the HttpOnly attribute was added. The HttpOnly attribute restricts cookies to be used only in HTTP requests, meaning they are attached only when an HTTP request is made by the client. Introduced in 2002, this attribute was designed to defend against content injection attacks, such as Cross-Site Scripting (XSS), which attempt to steal authentication cookies by exploiting server vulnerabilities. By setting this attribute, cookies are limited to HTTPS requests, preventing JavaScript from accessing them and blocking their use in non-HTTP APIs. However, while it helps protect against the theft of authentication cookies, it does not fully eliminate the risks posed by XSS attacks [32].

3.2.2 SameSite Cookies

First, it is important to clarify that SameSite cookies are not perceived as separate cookies on their own, but they act as a cookie attribute. The SameSite attribute defines three cookie policies. The Nonpolicy allows cookies to be included in all outgoing requests, including cross-site requests, which was the default behaviour before the SameSite attribute existed. The Strict policy, on the other hand, limits cookies strictly to same-site requests, meaning they will not be included in any cross-site requests. Lastly, the Lax policy is now the default for cookies and permits cookies to be included in same-site requests and top-level navigation requests (e.g., when a user clicks a link) using safe HTTP methods. However, for cross-site requests using unsafe HTTP methods, browsers will exclude cookies [33].

3.2.3 Secure Cookies

Finally, some cookies have a secure attribute, which ensures that they can only be transmitted over secure channels, such as HTTPS, when an HTTP request is made. This attribute helps maintain the confidentiality of the cookie by preventing its transmission over unsecured connections. However, while the secure attribute enhances privacy, it does not provide full protection against active network attacks. Also, Secure cookies are created using established cryptographic methods, including message digests, digital signatures, message authentication codes, and encryption. The specific process varies depending on how these techniques are applied to secure cookies and the web services they are used with. In some cases, secure cookies can also be issued by one entity for enhanced security [34].

3.3 Advanced Tracking Mechanisms

Nowadays, there are tracking mechanisms that represent more covert or advanced approaches to monitoring user activity, posing significant privacy concerns because they can be harder for users to control, or block compared to standard cookies. The most well-known are [35]:

1. Session-only tracking mechanisms
2. Storage-based tracking mechanisms
3. Cache-based tracking mechanisms
4. Fingerprinting
5. Other tracking mechanisms

Each of those 5 categories contain some sub-mechanisms that as shown on the image below [35]:



Figure 11: Overview of Tracking Mechanisms

Covering every single one of them is beyond the scope of this thesis, however in this chapter a short high-level overview is presented.

3.3.1 Session-only Tracking Mechanisms

As shown on the previous image, there are three distinct session-only tracking mechanisms, namely Session identifiers stored in hidden fields, explicit web-form authentication and window.name DOM property.

Session identifiers stored in hidden fields

This mechanism relies on passing an identifier from one website to another in the URL or in a hidden field in a web form, leveraging the technology of the Web-server session. Typically, this identifier is a session ID, which is transmitted between the client and server and used to track the user's interactions with the site. Additionally, this technique may pose a security risk if the identifier is exposed in URLs, as it can be intercepted through methods like URL sharing, browser history, or logging, making it vulnerable to session hijacking or replay attacks. Proper encryption and securing the session ID are essential to prevent such exploits.

Explicit web-form authentication

Firstly, it requires a user to log in to a website before using its resources, leveraging once again a web-server session, to manage the user's identity across different pages during their session. Also, it ensures secure access to protected resources and keeps

unauthorized users from accessing sensitive content. However, security features like HTTPS, encryption, and session timeout are required to safeguard the user's session.

Window.name DOM property

Window.name DOM property uses a special Document Object Model property to store up to 2 MB of data, which can be then shared among different visited parties, utilizing HTML5 and JavaScript. On top of that, by using a JSON stringifier, multiple variables can be compressed into a single string, which can then be saved on the user's device. The window.name property is persistent across page reloads and is accessible by other domains, allowing third-party content to share information with the first-party site or even other third-party entities.

3.3.2 Storage-Based Tracking Mechanisms

The next group of tracking mechanisms, called Storage-Based depend on explicit storing data on the users' computers. These methods seem to be the most used ones. They always require explicit user permission, and they generally arise more security concerns than the session-only mechanisms. Thus, all modern browsers give the ability to clear these storages on user's request.

The most well-known tracking mechanisms are presented and analysed below, except from Internet explorer related storage, since it is outdated and HTTP cookies, which have already been discussed [36].

Flash cookies and Java JNLP PersistenceService

Local Shared Objects (LSOs), also known as Flash cookies, are used by Adobe Flash to store data on a user's device. By default, they can store up to 100 KB of data, making them more efficient for tracking than traditional HTTP cookies, which are limited to 4 KB. Additionally, LSOs are more difficult for users to delete and are accessible across all browsers installed on the system, as Flash plugins share the same storage directory. This allows LSOs to track users across different browsers. Unlike HTTP cookies, Flash cookies do not expire by default and are stored as .sol files on the user's device.

Flash LocalConnection object

The LocalConnection object in Flash allows for communication between different SWF files running on the same machine simultaneously. This feature enables SWF files to exchange data and communicate, even if one is running in a normal browsing window and the other in a private browsing session. The ability to share values between these instances makes LocalConnection a versatile tool for facilitating data exchange across different environments.

Silverlight Isolated Storage

Silverlight provides a way to store data in the client browser plugin cache. This storage can be used to save user-specific data across browsing sessions. However, it cannot be used while on private browsing mode.

HTML5 and Web SQL Storage

HTML5 provides several client-side storage options. Local Storage allows for persistent data storage without an expiration date, ensuring data remains available even after the browser is closed. Session Storage operates similarly but clears its data once the browser session ends. Additionally, HTML5 IndexedDB offers a more advanced solution for structured data storage by creating databases directly on the client side. It has largely

replaced the older Web SQL Database, offering more flexibility and better support for complex data operations.

3.3.3 Cache-based Tracking Mechanisms

Cache-based tracking mechanisms, which rely on Web, DNS and operational caches are covered in this subsection.

Web caching refers to the storage of web documents, such as HTML pages, images, and JavaScript, in a location closer to the user (such as in the browser or on a proxy server). Thus, allowing user requests for the same content to be delivered faster, without requiring the server to regenerate or reload the resource.

On the other hand, DNS caching stores recent DNS queries results locally, either in the browser or on an ISP server. This results to the DNS resolution step being skipped, speeding up access, in case a user revisits a website.

Lastly, operational cache refers to temporary storage used by applications to speed up repetitive data retrieval and improve performance. It stores frequently accessed data, reducing the need to fetch it from slower, more permanent storage systems like databases or file systems.

Web cache and DNS cache

While beneficial, there are many ways that a Web cache can be exploited in a malicious way leading to unauthorized access to a user's Web browsing history. One of the most common techniques leverages browser caching. When a user visits a website, objects like images are downloaded and stored in the cache for faster access on future visits. If the object is retrieved from the cache during a revisit, the website can determine if the user has visited before. This method also allows advertisers with objects on multiple websites to compare cached versions and deduce which pages were visited.

There are several ways to exploit web cache tracking [37]:

1. **Embedding Identifiers:** By embedding unique identifiers in cached HTML files, websites can retrieve user data by reading the cached file's properties during the user revisits.
2. **Loading Performance Tests:** Websites tend to run JavaScript to measure the loading time of cached objects like images. Faster loading times than normal, indicate that the object is cached, suggesting a prior visit. This also applies on DNS caching.
3. **ETags and Last-Modified Headers:** ETags and Last-Modified headers store unique identifiers in HTTP requests. When a browser revisits, these headers are sent to verify if the cached version is up to date. ETags can store unique user identifiers and can be used for tracking.

Clearing the browser cache or blocking JavaScript can prevent these methods, but even during private browsing, the cache persists until the session ends.

Operational Caches

Operational caches store web browser-related information such as permanent redirects, authentication credentials, and domains that enforce HTTP Strict Transport Security (HSTS).

For instance, the **HTTP 301 redirect cache** stores information when a resource has been permanently moved to a new URL resulting in future requests automatically using the

new URL. This mechanism can also be exploited, enabling tracking users by attaching unique identifiers to the redirected URLs.

The **HTTP authentication cache** stores user credentials after login, allowing automatic re-authentication on subsequent requests. Certain methods enable JavaScript to trigger authentication without user interaction.

The **HSTS cache** enforces HTTPS for all future visits to a domain, but it can also be misused for tracking by encoding user identifiers into subdomains, which are stored in the HSTS cache and can be queried later.

Lastly, the **TLS session resumption cache** stores session IDs to resume secure connections without repeating the full handshake, but this can also be used for tracking if not properly managed.

These techniques can be mitigated through clearing browser caches and using special browsers that have addressed such issues.

3.3.4 Web Fingerprinting

Web-Browser Fingerprinting works by collecting and analysing numerous data points from a visitor's browser and device to generate a unique identifier for that user. This technique carefully distinguishes the subtle variations in browsers, even among users with similar devices or operating systems.

The strength of browser fingerprinting lies in its ability to create a highly distinctive identifier, known as a high-entropy profile. This profile is generated by combining multiple data points, which form a unique fingerprint that differentiates one user from millions. Even when users share the same operating system, factors such as browser settings, installed plugins, and hardware variations ensure that each profile remains unique. It is important to point out that this tracking mechanism arises high concerns and it very different to cookies for example, since it is almost undetectable.

The main techniques to create a user's digital fingerprint are listed below:

Network and Location Fingerprinting

Commonly, HTTP request headers reveal a user's global network address, and their approximate location based on the IP address, along with details such as the domain name and ISP. Proxy servers can often be detected or bypassed to reveal the real IP address. JavaScript and Flash can gather additional data like internal IP addresses, connection performance, and more. However, Tools like VPNs help mask real IPs and enhance user privacy.

Device Fingerprinting

The device fingerprinting method, often using only JavaScript relies on passively collected data like the first two octets of the IP address, OS version, screen resolution, time zone, and system fonts. This technique provides browser and plugin independence, allowing tracking across different browsers or domains as long as the IP address comes from the same pool. Additionally, returning users become identifiable despite making changes in screen resolution, time zone, or even their IP address.

Another method, based on clock skew detected via TCP timestamps, tracks devices regardless of location or network type. However, this approach struggles with uniqueness and as a result with accuracy, especially when time synchronization protocols like NTP are in use.

Operating System instances Fingerprinting

This technique is mainly based on the use of JavaScript and Flash, which can both detect the version and architecture of the operating system. JavaScript can also determine system and user-specific language, local time zone, and precise date and time. Installed fonts can also be identified, which is commonly taken advantage of by major fingerprinting companies like BlueCava, Lovation, and ThreatMetrix.

Additionally, they are able to detect settings like colour depth and screen dimensions, while along with assessing audio functions, camera and microphone permissions, and whether access to printing and hard disk has been restricted. Java applets can open, read, and save files on the client's system, bypassing typical security sandboxing for privileged applets, which have greater access to system information.

Browser Version Fingerprinting

In early stages Web browser detection, was mainly done through the UserAgent string of HTTP Headers. Nowadays, this method is not reliable, since various programs can hide the targeted string. For this reason, new methods of fingerprinting through CSS and HTML5 fingerprinting were developed. HTML5 fingerprinting is based on the differences between the way web browsers implement the template, while the CSS method is based on the differences between the way that various functions are implemented in a browser.

Browser Instance Fingerprinting using Canvas

Canvas fingerprinting is a technique that uses the browser's canvas API to generate unique identifiers by drawing invisible graphics. The images or text rendered by the canvas vary slightly based on the user's system configurations (such as browser, OS, and hardware). These differences allow websites to create a unique fingerprint for tracking purposes. The produced graphics can be retrieved and analysed using advanced methods, which convert the canvas content into a format that can be hashed to generate a unique identifier-fingerprint for a user.

Browser instance fingerprinting using web browsing history

According to various studies, there are serious indications that browsing history can lead to fingerprinting the users. For example, Research on over 368,000 internet users showed that web browsing history can be used to fingerprint 42% of users by checking visits to 50 pre-defined websites. This percentage rises to 70% when testing against 500 websites, drawn from top Alexa and Quantcast rankings. Researchers found that 88% of the browsing history profiles were unique, and even after clearing browser data, 38% of profiles remained identical [38].

In conclusion, the evolution of tracking methods has shifted from relatively user-controllable tools like HTTP cookies, which can be easily deleted, to far more invasive techniques such as fingerprinting and ISP-inserted identifiers. These newer methods are difficult for average users to avoid, posing greater challenges to privacy. As tracking technologies continue to evolve, they have the potential to become even more intrusive, raising concerns about user control over their online privacy.

In the next chapter, we will cover the legal frameworks surrounding online privacy, focusing on regulations such as the General Data Protection Regulation (GDPR). We will examine how these laws aim to protect user data and what responsibilities websites and service providers using tracking techniques need, in order to ensure compliance. Although, the main emphasis will be on cookies and the legal framework and regulations surrounding them.

4. Legal and Regulatory Frameworks in Website Security and Privacy

The management and protection of personal data have become key considerations for businesses and organizations when selecting software, service providers and thus websites. To ensure that personal data is kept secure, various laws and regulations have been introduced across the globe, establishing standardized data protection frameworks [39]. As a result, organizations that handle personal data are obligated to meet strict privacy and security baselines to ensure compliance with these regulations. A range of methodologies and tools has been developed to help organizations, such as the PCI DSS that was previously covered, to identify and implement the legal requirements for compliant software and services, primarily based on regulatory laws, directives and frameworks such as ePrivacy Directive and the General Data Protection Regulation (GDPR) in the EU and similar regulations in the US. Since this is a very complex and large topic, this chapter aims to just cover the tip of the iceberg, emphasizing on the basics of the ePrivacy Directive, GDPR and the overall compliance measures, that apply to website security and privacy.

4.1 The European Regulatory Framework

European legislation has long aimed to safeguard privacy and personal data, especially concerning citizens' communications. This is reflected in foundational documents like the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union, as well as regulations such as the GDPR and the ePrivacy directive. Article 8 of the ECHR guarantees the right to private and family life, while the EU Charter's Article 7 focuses on the respect for privacy, and Article 8 ensures the protection of personal data.

4.1.1 Data Protection Directive 95/46/EC

Directive 95/46/EC, adopted in 1995, aimed to protect personal data and ensure its free distribution. It was repealed and replaced on 25.05.2018 by Article 94 [40] of the GDPR. The GDPR, adopted in April 2016 by the European Parliament, took direct effect in all Member States, overriding any conflicting national laws. In Greece, the GDPR was incorporated through Law 4624/2019 [41] (Government Gazette A' 137/29.08.2019). Additionally, Directive 2016/680 was transposed, regulating the processing of personal data in criminal investigations by law enforcement authorities [42].

4.1.2 ePrivacy Directive 2002/58/EC

Directive 2002/58/EC [1], known as the ePrivacy Directive, was adopted to protect privacy and personal data in electronic communications. It was incorporated into Greek law through Law 3471/2006 and laid the foundation for data protection in this sector, covering communications via fixed and mobile telephony and the Internet. As a *lex specialis*, the ePrivacy Directive provides specific rules for privacy in the electronic communications sector, complementing broader data protection laws. The GDPR, in Article 95, specifies that it does not impose additional obligations on entities already subject to the ePrivacy Directive. However, rapid technological advancements, including new communication methods (e.g., messaging apps), the Internet of Things (IoT), and artificial intelligence.

4.2 The GDPR Framework

4.2.1 Definitions and Fundamentals

In 2018, the European Union authorities introduced the General Data Protection Regulation (GDPR), labelling it as a unified legal framework aiming to both simplify and reduce costs for businesses operating within the EU. However, existing literature suggests that early reactions to GDPR were marked by concerns over the complexity of its implementation and uncertainties in its interpretation. Organizations around the world, particularly those handling the personal data of EU residents, have been pivotal in transforming these regulatory principles into practical measures [43]. In turn, the framework of GDPR resulted in seriously influencing various aspects in the field of information technology, such as: User profiling through data collection-analysis, business impacts, management and compliance, personal competences, authorisation, authentication and data storage.

According to Art. 4 GDPR [44], for the purposes of the regulation the following parameters are explicitly defined:

- **Personal Data:** Is equal to any information that relates to an identified or identifiable individual ("data subject"). An identifiable person is one who can be recognized, either directly or indirectly, through identifiers such as a name, identification number, location data, online identifiers, or other factors related to the person's physical, physiological, genetic, mental, economic, cultural, or social characteristics.
- **Processing:** Refers to any action or series of actions carried out on personal data, whether automated or not. This includes activities such as collecting, recording, organizing, structuring, storing, modifying, retrieving, consulting, using, disclosing through transmission, disseminating, combining, restricting, deleting, or destroying personal data.
- **Controller:** Is defined as the natural or legal person, public authority, agency or other body which, alone or jointly with others determines the purposes and means of processing of personal data.
- **Personal Data Breach:** Refers to a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data that is transmitted, stored, or otherwise processed.

Taking these definitions into account, Art. 25 GDPR [45] requires organisations (data controllers) to implement appropriate technical and organisational measures to ensure that data protection principles are embedded into the design of systems and processes from the outset.

Lastly, Art. 32 [46] & 34 [47] of the GDPR focus on ensuring the CIA triad and general protection of personal data. Specifically, Article 32 requires organizations to implement appropriate technical and organizational measures, like encryption and regular testing, to safeguard data. Article 33 mandates that data controllers notify supervisory authorities about data breaches within 72 hours. Article 34 requires notifying affected individuals if a breach poses a high risk to their rights and freedoms, detailing the breach's nature and mitigation measures. Together, these articles mainly establish proactive, reactive, and corrective measures in response to a data breach.

4.2.2 The Impact of on Websites and Global Data Practices

Organizations, particularly in websites, have been pivotal in implementing GDPR principles. As a result, all data controllers, including those who process personal data

through websites, have adjusted their processes for handling and storing user personal and sensitive data. The GDPR not only states how and what kinds of data should be stored by service providers but also ensures users have a transparent way to access the data collected, along with the ability to export it easily [48]. The regulation applies to any entity that tracks or monitors behaviours within the European Union, regardless of whether they offer a direct service in the region. Article 15 [49] outlines one of the core rights: users can request a copy of all personal data that a website has collected about them. These right aims to give users greater control and awareness over their personal information, whether they have knowingly shared it or not. On the other hand, GDPR also takes care of some security aspects, by demanding organisations and websites to use encryption during data transmission (such as HTTPS), implementing strong authentication controls, and ensuring that stored data is appropriately secured.

In summary, the GDPR regulations extend to any entity that monitors behaviour within the EU, highlighting its broad scope and impact on global data practices.

4.3 Cookie Consent and GDPR Compliance

With the EU regulations forcing organisations to comply with the GDPR standards, cookie consent and allowance became significantly noticeable for every user browsing the web. Popups and banners on websites often ask visitors to give consent regarding the collection of personal data, tracking, and the placement of cookies in their browsers, typically organized based on specific use purposes. While these consent prompts may indicate that users have control over their privacy and data rights, many websites employ malicious practices and patterns to manipulate or mislead users into giving consent. Additionally in many cases some websites disregard users' privacy choices altogether [50].

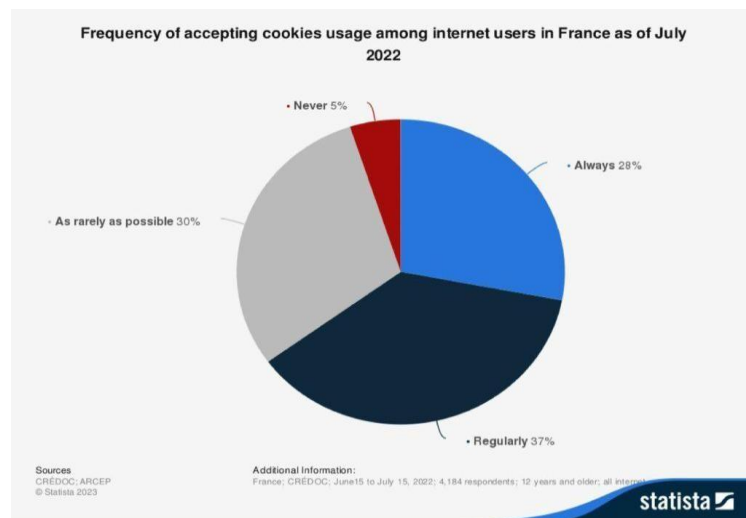


Figure 12: Cookie Acceptance Rate Example

To proceed in collecting personal user data or tracking, websites must establish a legitimate legal basis as required by the GDPR. The recognized legal bases under Article 6(a-f) [51] of the GDPR include: (a) obtaining user consent, (b) fulfilling a contractual obligation, (c) complying with legal obligations, (d) protecting vital interests, (e) performing tasks in the public interest, and (f) legitimate interests pursued by the controller or third parties. Among these, consent and legitimate interest are the most frequently used as justifications and enablers for data collection.

Consent notices are specifically designed to obtain clear, affirmative agreement from users regarding data collection. As outlined in Article 7 [52] and Recital 32 [53] of the

GDPR, valid consent must be freely given, specific, informed, and unambiguous. The use of pre-checked boxes or inactivity is by no means considered as valid consent. Consent must be sought before cookies are set, and the request must be clearly worded and easily accessible. The data controller must also keep records proving that consent was indeed granted.

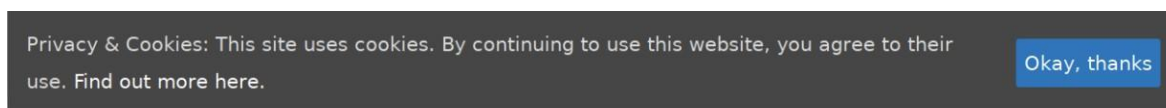


Figure 13: Example of a Maliciously Configured Cookie Banner

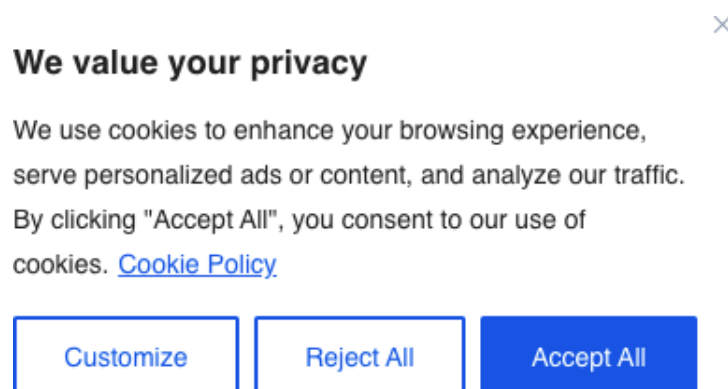


Figure 14: Example of a Correctly Configured Cookie Banner

If any consent requirements are breached, the consent is considered invalid, and organizations may face serious penalties. According to Article 83 [54], fines can build up to 20 million Euros or 4% of the company's annual global turnover. Additionally, the GDPR has extra-territorial reach, meaning it applies to any website, even those outside the EU region, that processes or store the personal data of EU residents.

The GDPR involves all cookies that store unique identifiers and not just those that process sensitive data. Recital 30 [55] clarifies that online identifiers, such as IP addresses and cookie identifiers, can be linked to individuals and used to build profiles. In some regions, consent is required for all cookies except those deemed strictly necessary for a service to function, as outlined by the ePrivacy Directive. This directive, which was replaced by the GDPR, mandates that users must provide clear consent for data storage and access unless the cookie is essential for the service requested by the user. Wrongfully categorizing cookies as strictly necessary can leave website operators liable for violations. Add the following at the end: Therefore, the proper use of cookies is defined by the e-privacy directive and is the following: if the cookie is strictly necessary then it can be installed without the user's consent (but with information provided), otherwise explicit informed user's consent is required (and the notion of consent is the same as in the GDPR).

In conclusion, the issue of cookie consent and allowance is undoubtedly complex. While GDPR sets forth a series of stringent standards, there are still various loopholes and dark practices that some organizations and websites exploit to coerce users into tricking users into giving consent. In this study, the scanning tools used, will highlight real-world examples, illustrating the challenges and grey areas within this landscape. These findings will shed light on the ongoing issues of consent manipulation and the broader implications for data privacy.

5. Used Tools

In conducting the research and analysis for this study, a range of tools were employed to evaluate both the security and privacy aspects of the websites under scrutiny.

This chapter includes a short overview of the utilized tools. The tools were chosen based on the following key characteristics: Being free of charge, effective and lastly easy to use. By combining these tools, the evaluation of the selected websites as to their security and privacy services was made possible, while emphasizing on the identification of key security vulnerabilities along with ensuring GDPR compliance in terms of cookie management.

The tools presented in this chapter are split into two main categories: The ones that are responsible for the examination of the website security and those focused on privacy – cookie compliance.

In summary, by performing systematic analysis with these tools, the study gathered detailed data and insights, forming the foundation for the results and conclusions that follow. The following sections will explore each tool in detail, outlining their specific purposes and how they were utilized to achieve the goals of this thesis.

5.1 Tools for Cookie Compliance Evaluation

5.1.1 CookieYes

CookieYes is a very popular and widely used tool, mainly used for addressing cookie consent and privacy related matters. It is trusted by roughly 1.5 million businesses worldwide, such as: Forbes, Renault, Toyota and many other large companies [56]. These companies choose CookieYes, due to offering the following at a very high level:

- **Customizable cookie banner:** Choose from various templates and tailor the banner according to company's preferences.
- **Cookie list and preference centre:** Correctly and clearly listing cookies, allowing users to provide consent for specific categories.
- **Geo-targeting and translation:** Display the banner based on visitor location and their predefined browser language.
- **Automated scans:** Schedule monthly scans to detect and categorize cookies for GDPR or other regulation standards compliance.
- **Cookie Auto-blocking:** Prevent non-necessary cookies from being installed without user consent.

At this point however, it is important to clarify that all utilities mentioned above are by no means free of charge. To use these CookieYes advanced features and ensure privacy-cookie compliance for a website someone owns; a premium plan must be selected as shown on the image below.

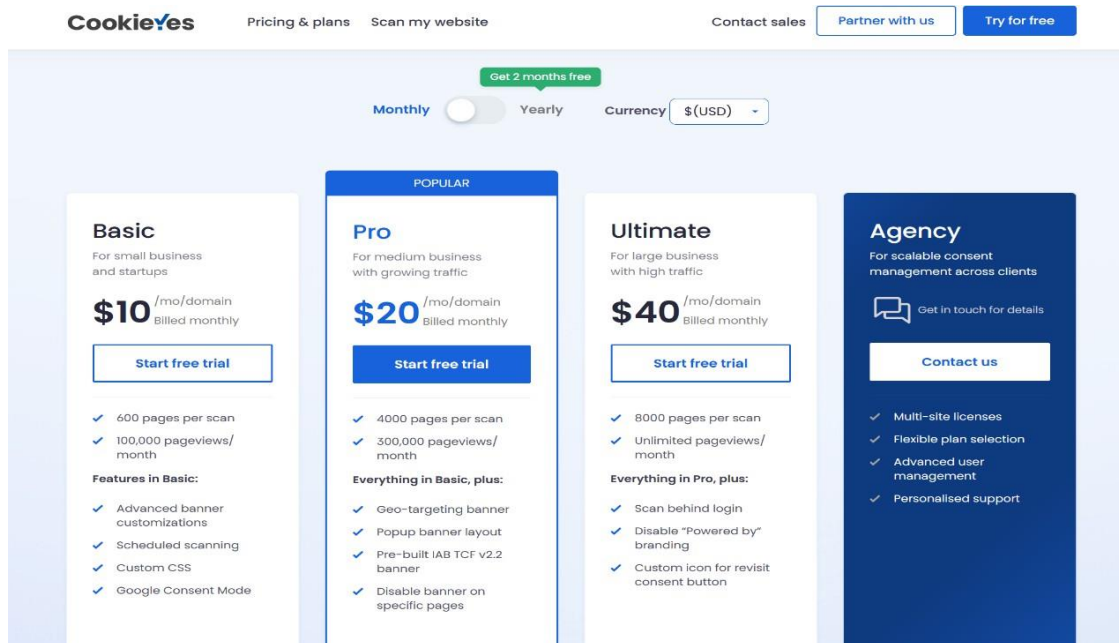


Figure 15: CookieYes Plan Options

Regarding the scope of this thesis, using any of these premium plans serves no purpose. Firstly, we want to use a free of charge tool and secondly even if that wasn't the case, these premium plans of CookieYes and of other similar cookie consent management tools are created for website owners or administrators. Thus, in this study we only leverage the commercial and free of charge feature of CookieYes, which is accessed by clicking the "Scan my website" text on the image above and navigating to the following section of the website.

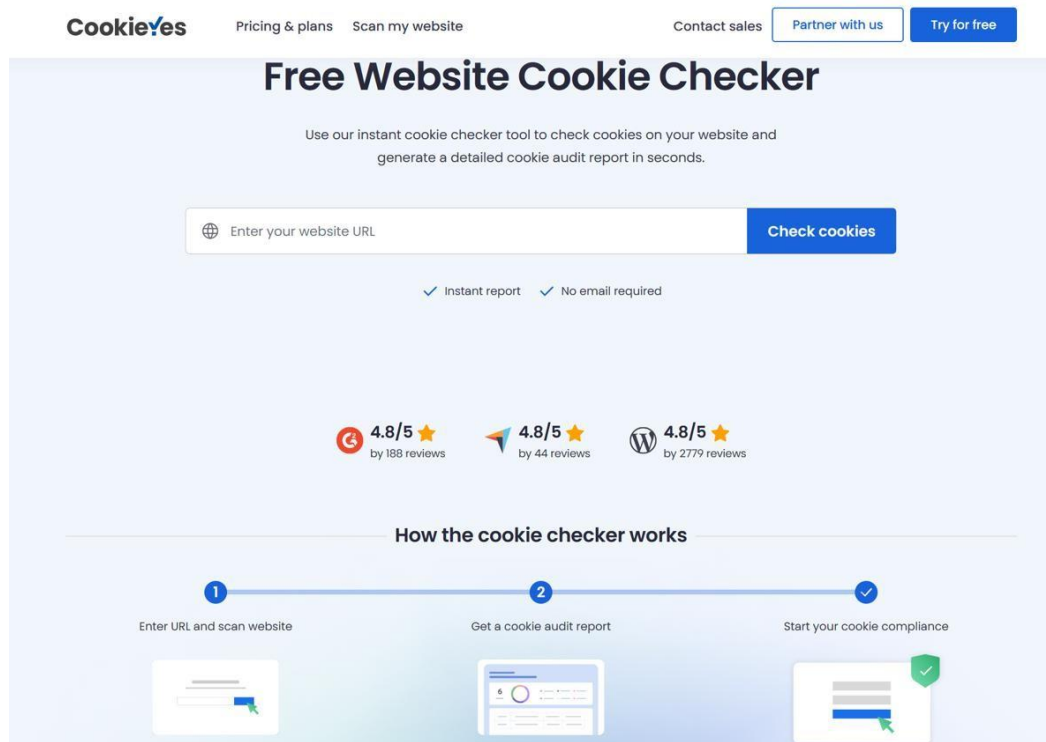


Figure 16: CookieYes Scanner UI

This free feature offered by CookieYes is called “Free Website Cookie Checker”. It offers great functionality and at the same time it is very easy to use. All the user has to do is enter a valid website URL and then click the “Check Cookies” button.

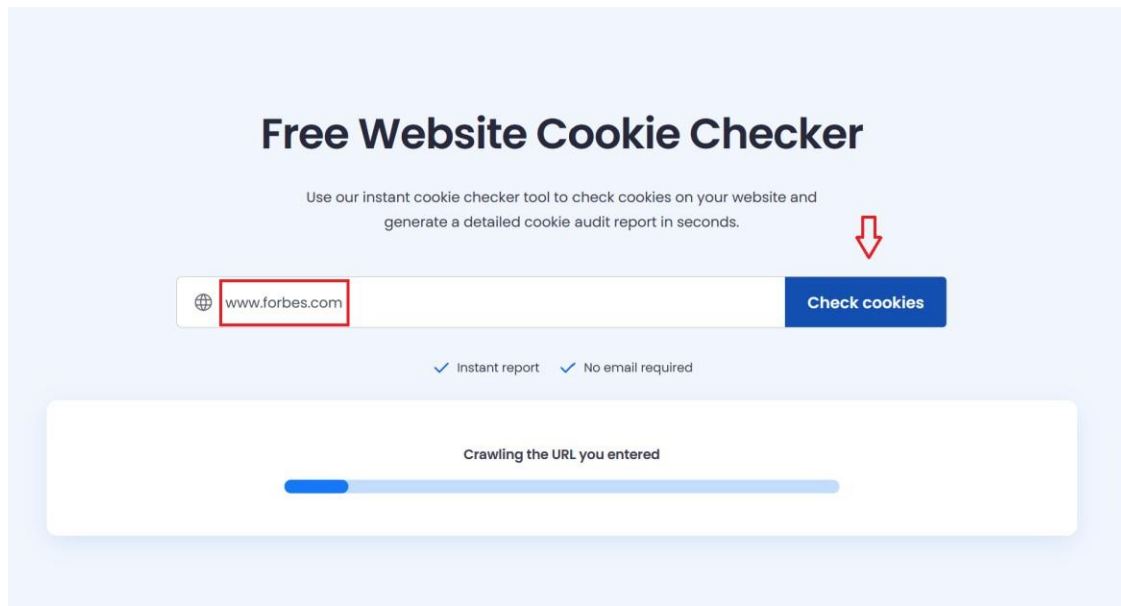


Figure 17: CookieYes Scan Execution

After a short time, averaging from a few seconds to a few minutes a detailed scan report is generated as shown on the images below.

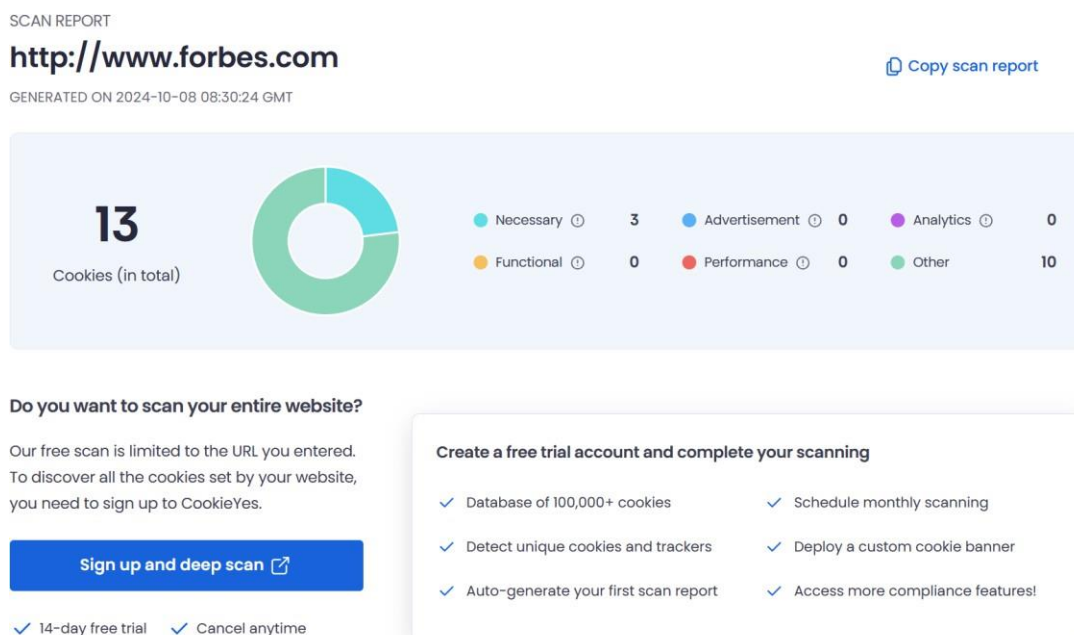


Figure 18: Example of a CookieYes Scan Report 1/2

Evaluation of Websites with Respect to Security and Privacy Services

Cookie	Domain	Description	Duration	Type
datadome	.forbes.com	This is a security cookie set by Force24 to detect BOTS and malicious traffic.	1 year	Necessary
VWO	www.forbes.com		1 year 1 month 4 days	Other
notice_gdpr_preferences	.forbes.com	No description available.	1 year	Other
client_id	.forbes.com	This cookie is used for passing authentication information.	1 year 1 month 4 days	Necessary
addtlConsent	.forbes.com		1 month	Other
usprivacy	.forbes.com	This is a consent cookie set by Dailymotion to store the CCPA consent string (mandatory information about an end-user being or not being a California consumer and exercising or not exercising its statutory right).	1 month	Necessary
us_privacy	.forbes.com	No description available.	1 month	Other
_swb	.forbes.com	No description available.	1 year 1 month 4 days	Other
_swb_consent_	.forbes.com		7 days	Other

Figure 19: Example of a CookieYes Scan Report 2/2

Even though it is a free scanner tool it offers a comprehensive overview of the cookies detected on the website URL. The scan categorizes cookies into various categories that were previously covered, such as necessary, analytics, advertising, and other, ensuring that each cookie's purpose is clearly defined. Furthermore, it provides a short description of each cookie (when there is one available in its database), along with their predefined lifetime.

Despite being a great free tool CookieYes free website scanner also has some limitations. The most noticeable one is that it only tracks and categorizes cookies without checking if the website is compliant with privacy regulations, in our case the ePrivacy directive and the GDPR. This means that by using this tool alone without further or manual investigation it is not enough for the purpose of this thesis, however it creates a great foundation for further analysis and investigation. Lastly, another limitation of this scanner, which also applies to every free version of scanner tool, is that it only scans the entered URL, meaning the front page of the website and not the whole website. This limitation is often foreshadowed or misunderstood by users.

In this case however, scanning only the entered URL is not of great importance. The scope of this work is to point out what it takes for a website to ensure cookie compliance by presenting examples. That by no means requires to scan whole websites, a process that is very time consuming and complex and often meaningless for education purposes, since in case there is website incompliance it terms of cookies this should be detected by the frontpage already. The frontpage of the website is the first point that most users interact with, therefore viewing the cookie banner and giving consent for the installation of the website's cookies. Also, scanning a whole website takes an excessive amount of time, which is a limitation when considering scanning a large number of websites.

In conclusion, this is the main tool that was used in this thesis in order to collect information regarding cookies on the websites under investigation, targeting the website's frontpage only. Thus, please keep in mind that while this is enough for the scope of this

thesis, these tools are by no means capable of enabling users to detect all cookies contained in a website.

5.1.2 ImmuniWeb Privacy Test

As already mentioned, while CookieYes free scanner offer great functionality, it is limited to only working as a cookie collector and analyser. Therefore, in order to dive deeper into examining websites for privacy compliance with emphasis on cookies a second tool was selected, namely ImmuniWeb a well-established tool use by over 1000 customers in 50 different countries [57]. In this thesis for simplicity and clarity purposes we refer to ImmuniWeb as a tool, however it is more like a whole platform offering several different products and services for different use cases. Once again, most services are not free of charge, since they offer advanced features like excessive penetration testing, law compliance and more. However, ImmuniWeb offers a community edition sub-platform containing several free tools as displayed on the image below.

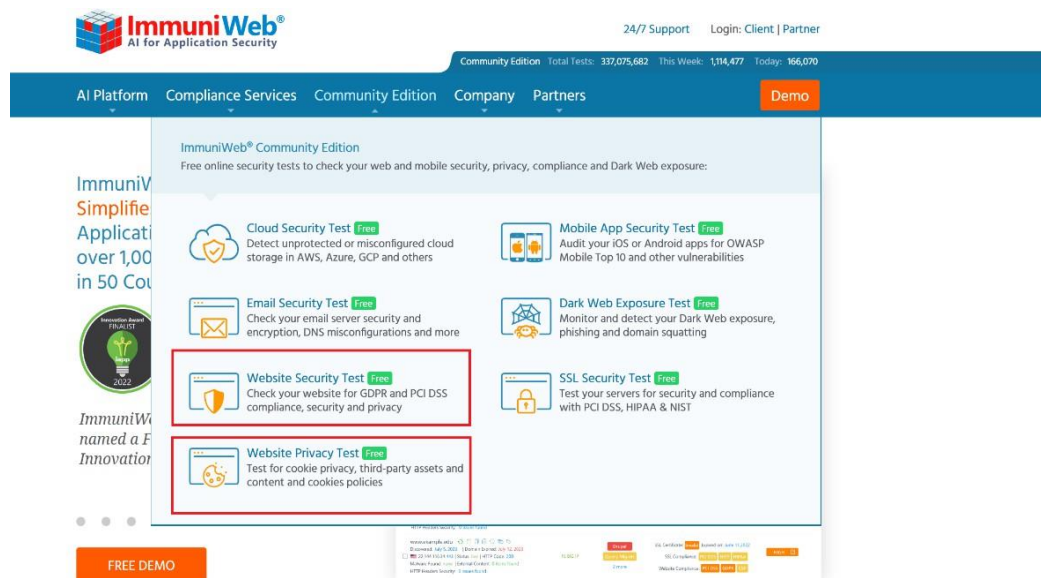


Figure 20: ImmuniWeb Community Edition Tools

The highlighted services are the ones that are relevant to cookie compliance. The one used for the privacy section of this study is the “Website Privacy Test”, since it emphasizes more on cookies, while the “Website Security Test” was used for evaluating website security and is analysed in a different subsection.

By selecting the “Website Privacy Test”, just like previously with CookieYes we are transferred into a friendly user interface. The user is only required to enter a valid website URL and click the start button to initiate the scan.

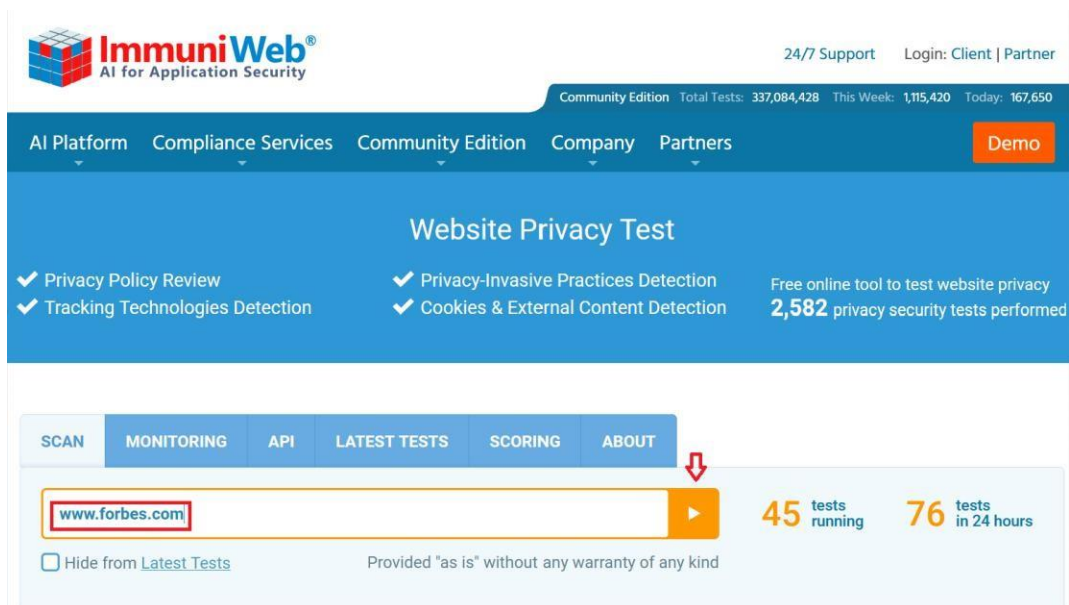


Figure 21: ImmuniWeb Scanner UI

After a short period of time, typically some minutes a report is generated containing valuable information, some of which we will filter out since it is not relevant to cookie compliance.

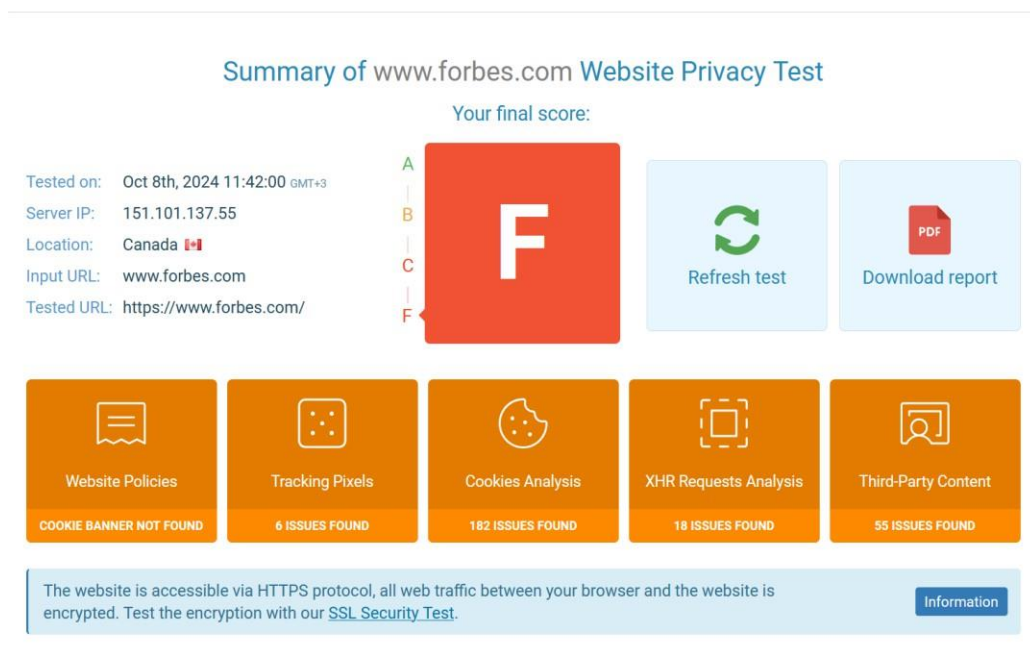


Figure 22: ImmuniWeb Privacy Scan Report Example (1/3)

Cookies Analysis of www.forbes.com								
Cookies are small files that websites save on your computer or mobile device to remember your preferences, such as website language or search history. However, cookies, especially third-party cookies, can be used for user tracking across different websites and collection of personal data for targeted advertising.								
First-Party Cookies								
There are 21 first-party cookies without a Secure flag						Misconfiguration or weakness		
There are 28 first-party cookies without an HttpOnly flag						Misconfiguration or weakness		
Name	Value	Domain	Path	Expires	Samesite	Secure	HttpOnly	
VWO	54.700	www.forbes.com	/	Nov 12th, 2025		No	No	
client_id	7470bb576fc8e ... 9ceacaa6c3ee7	.forbes.com	/	Nov 12th, 2025		No	No	
lux_uid	172838413881235015	www.forbes.com	/	Oct 8th, 2024	Lax	No	No	
pushly. ... r_puuid	fkZFo1cqdd4P6 ... bPUapdAlbeRLI	.www.forbes.com	/	Apr 6th, 2025	Strict	No	No	
_pnss	none	.www.forbes.com	/	Apr 6th, 2025	Strict	No	No	
SHOW 23 MORE								

Figure 23: ImmuniWeb Privacy Scan Report Example (2/3)

Third-Party Cookies	
+ 25 Cookies	pubmatic.com [United States] 🇺🇸
+ 14 Cookies	media.net [United States] 🇺🇸
+ 6 Cookies	intentiq.com [United States] 🇺🇸
+ 5 Cookies	adnxs.com
+ 5 Cookies	rubiconproject.com [United States] 🇺🇸
SHOW 63 MORE	

Figure 24: ImmuniWeb Privacy Scan Report Example (3/3)

While this tool is also able to detect and categorise cookies, CookieYes provides a more accurate and well-structured analysis, at least for this study's purposes. Nevertheless, this ImmuniWeb provides some information that CookieYes could not detect. The most critical is the existence of a cookie banner, a parameter very critical for ensuring that a website is compliant. Furthermore, it can categorise cookies as first- party, third-party even samesite, secure and HTTPOnly. Even though that is great in this study we will only take into consideration the information for the cookie banner and some information for first/third party cookies.

In summary, this is the second main tool that is used to examine website regarding compliance with the ePrivacy Directive and GDPR. Of course, more details regarding the methodology and the set of standards used will be covered on the next chapter.

5.1.3 Cookie-Editor

Using scanning tools like the ones previously mentioned to check for cookies and ensure compliance with the aforementioned regulations is a great and common practice, however it comes with its own limitations. Cookie-Editor, along with some manual checks

is also used to verify some of the results of these scanning tools and to capture all the dynamic aspects of cookies.

It is a very simple software and is installed as a web browser extension. All it does is capture cookies deployed in real time while browsing the web. An example of its operation is displayed on the image below.

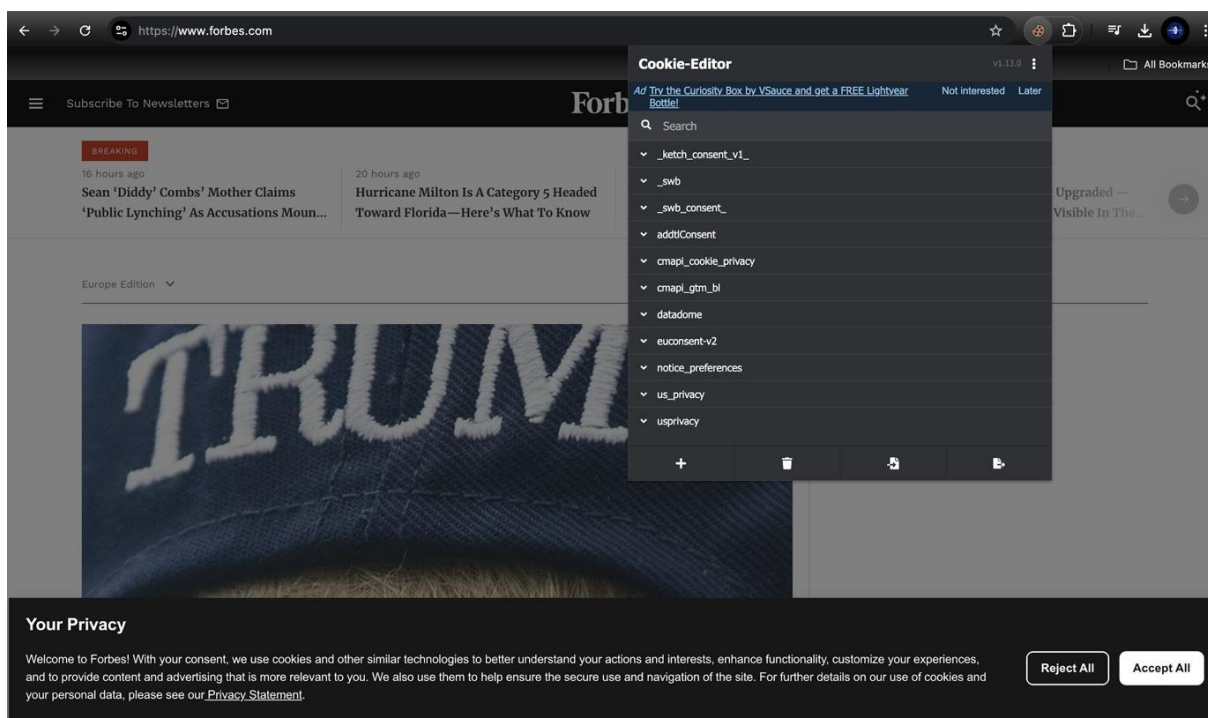


Figure 25: Cookie-editor Usage Example

There is a variety of different extensions like Cookie-Editor, but they tend to be browser specific. Since Cookie-Editor supports the majority of well-known web browsers like Chrome, Mozilla and Safari it was considered as the top choice in this study.

Using this software, provides a deeper and more accurate understanding of the cookies that are being set during user interactions. By using Cookie-Editor, it is possible to identify any discrepancies between what is declared and what is actually set, ensuring a more thorough compliance evaluation.

In short, this software is very straightforward yet useful for our study. We will delve deeper into how it was utilized in the next chapter.

5.2 Tools for Website Security Evaluation

While including multiple tools often adds value to a study, this is not exactly the case with free website security scanners. First, as previously discussed in the section dedicated to vulnerability scanning, we are restricted to implementing passive scanning only, meaning that the amount of information that can be collected is limited.

Most free scanning tools scan for the exact same things resulting in redundant data if multiple scanners are used, without necessarily adding significant depth to the analysis. Since most free tools primarily focus on scanning surface-level vulnerabilities that we already discussed, such as SSL/TLS configurations, HTTP security headers and basic website weaknesses, using more than one tool could lead to an overlap in findings rather than discovering new insights. Moreover, these tools often don't offer comprehensive vulnerability scanning in areas like server configuration or web application logic, which are typically covered by more advanced and by no means free tools.

As a result, it is more efficient to stick to one well-trusted and effective tool like ImmuniWeb “Website Security Scanner”, which already provides a thorough overview of key security elements, supplemented with ImmuniWeb SSL Security Test, which focuses more on SSL/TLS analysis. This simple, yet strategic approach allows for a well-structured analysis without overwhelming the study with repetitive data from multiple sources.

5.2.1 ImmuniWeb Website Security Test and SSL Security Test

As already mentioned, Website Security Test is one of the free tests provided by the ImmuniWeb community edition platform. This test is capable of detecting key website vulnerabilities related to SSL/TLS, PCI DSS, HTTP Headers, DNSSEC, Web software security test and more. However, the information provided related to SSL/TLS security analysis is limited therefore, the analysis is supplemented with ImmuniWeb SSL Security test.

The steps on how to use such tools have been already covered in the previous sections, therefore there is no need to show the procedure again step by step. Nevertheless, it is important to get a short overview of how the generated reports look. Some snapshots containing examples of both ImmuniWeb tests are displayed on the images below.

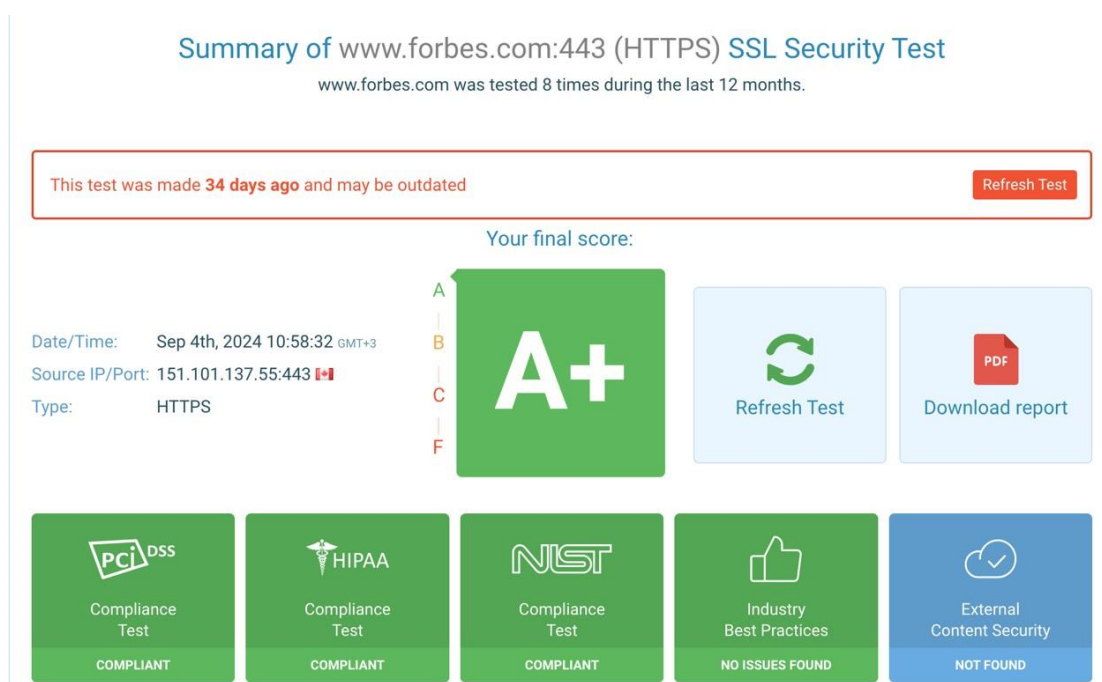


Figure 26: ImmuniWeb Security Scan Report Example (1/5)

SSL Certificate Analysis	
RSA CERTIFICATE INFORMATION	
Issuer	GlobalSign Atlas R3 DV TLS CA 2024 Q1
Trusted	Yes
Common Name	*.forbes.com
Key Type/Size	RSA 2048 bits
Serial Number	1407814948136838003765942695804520785
Signature Algorithm	sha256WithRSAEncryption
Subject Alternative Names	DNS:*.forbes.com
Transparency	Yes
Validation Level	DV
CRL	http://crl.globalsign.com/ca/gsatlasr3dvtlsca2024q1.crl
OCSP	http://ocsp.globalsign.com/ca/gsatlasr3dvtlsca2024q1
OCSP Must-Staple	No
Supports OCSP Stapling	Yes
Valid From	March 15, 2024 15:33 CET
Valid To	April 16, 2025 15:33 CET
CERTIFICATE CHAIN	

Figure 27: ImmuniWeb Security Scan Report Example (2/5)

PCI DSS Compliance Test of www.forbes.com	
Reference: PCI DSS 4.0 , Requirement 4.2	
CERTIFICATES ARE TRUSTED ⓘ	
All the certificates provided by the server are trusted.	Good configuration
SUPPORTED CIPHERS	
List of all cipher suites supported by the server:	
TLSV1.3	
TLS_CHACHA20_POLY1305_SHA256	Good configuration
TLS_AES_128_GCM_SHA256	Good configuration
TLS_AES_256_GCM_SHA384	Good configuration
TLSV1.2	
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
SUPPORTED PROTOCOLS	
List of all SSL/TLS protocols supported by the server:	
TLSv1.2	Good configuration

Figure 28: ImmuniWeb Security Scan Report Example (3/5)

CERTIFICATE CHAIN	
Root CA GlobalSign Type/Size RSA 2048 bits Serial Number 4835703278459759426209954 Signature sha256WithRSAEncryption SHA256 cbb522d7b7f127ad6a...5a7cf4720dc963c53b PIN cGuxAXyFXFKWm61cF4...rS9j0aSqN0k4AP+4A= Expires in 1,622 days Comment Self-signed Download	Intermediate CA GlobalSign Atlas R3 DV TLS CA 2024 Q1 Type/Size RSA 2048 bits Serial Number 16976021724444371372959058656761257820 Signature sha256WithRSAEncryption SHA256 0152f86354fca9525b...723226ae67238db190 PIN slyusJrUkgaV+NuUk4...HYRzOm0Ugic011Dok= Expires in 374 days Comment - Download
Server certificate *.forbes.com Type/Size RSA 2048 bits Serial Number 1407814948136838003765942695804520785 Signature sha256WithRSAEncryption SHA256 6b7b02e2279d7d6f9e...612baa0c0f3ce362f9 PIN a7i1xrKckrmQITy94+...RjzQITmn18lwP42ws= Expires in 190 days Comment - Download	

Figure 29: ImmuniWeb Security Scan Report Example (4/5)

Industry Best Practices Test of www.forbes.com	
DNSCAA ⓘ This domain has a Certification Authority Authorization (CAA) record. issue: geotrust.com issue: globalsign.com issue: letsencrypt.org issue: pki.goog issue: amazon.com issue: sectigo.com issue: digicert.com Good configuration	
CERTIFICATES HAVE A VALIDITY PERIOD OF 398 DAYS OR LESS ⓘ All the server certificates provided have been validated for less than 398 days (13 months). Good configuration	
CERTIFICATES DO NOT PROVIDE EV The RSA certificate provided is NOT an Extended Validation (EV) certificate. Information	
TLS 1.3 SUPPORTED The server supports TLS 1.3 which is the only version of TLS that currently has no known flaws or exploitable weaknesses. Good configuration	
TLS 1.3 EARLY DATA (0-RTT) ⓘ Server's TLS 1.3 Early Data (RFC 8446, page 17) is not enabled. Information	

Figure 30: ImmuniWeb Security Scan Report Example (5/5)

These are just some parts of the reports. In the next chapter we will cover each aspect of these reports in great detail.

5.3 Honourable Mentions

Despite using the aforementioned tools, there is a large variety of tools that perform similar operations. This subsection briefly describes some of the tools that have been into consideration during the early stages of this thesis.

5.3.1 Qualys SSL Labs

Qualys SSL Labs was evaluated as a potential candidate for its comprehensive analysis of SSL/TLS configurations, helping to assess the encryption strength and identify vulnerabilities in certificate setups. It is a very respected and easy to use tool. It works exactly like the previously discussed tools; the user only needs to provide a valid website URL and after a few minutes a detailed report is generated.

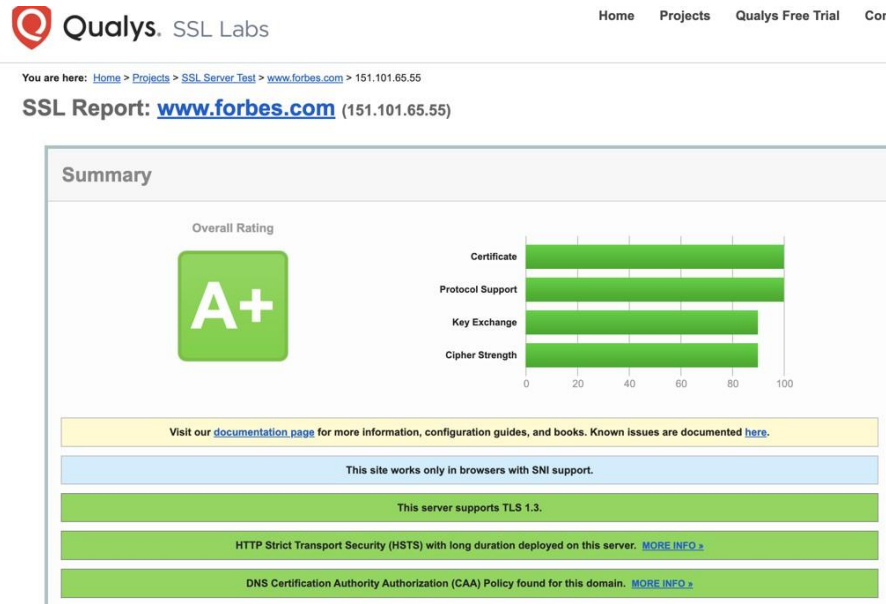


Figure 31: Qualys SSL Labs Scan Output Example

However, this tool was only used when the ImmuniWeb scan failed to execute.

This selection was done, mainly because using ImmuniWeb for both privacy and security testing provided a more streamlined approach, ensuring consistency in the study since both tests came from the same provider. This made the overall analysis process smoother and more cohesive.

5.3.2 Webbkoll by dataskydd.net

Webbkoll is another great tool for evaluating both website security and privacy. Though doing both at the same time leads to not offering the breadth of features needed to meet the comprehensive objectives of this study. Furthermore, it does not work in all websites. Despite that, it is a very useful tool, easy and quick to use.

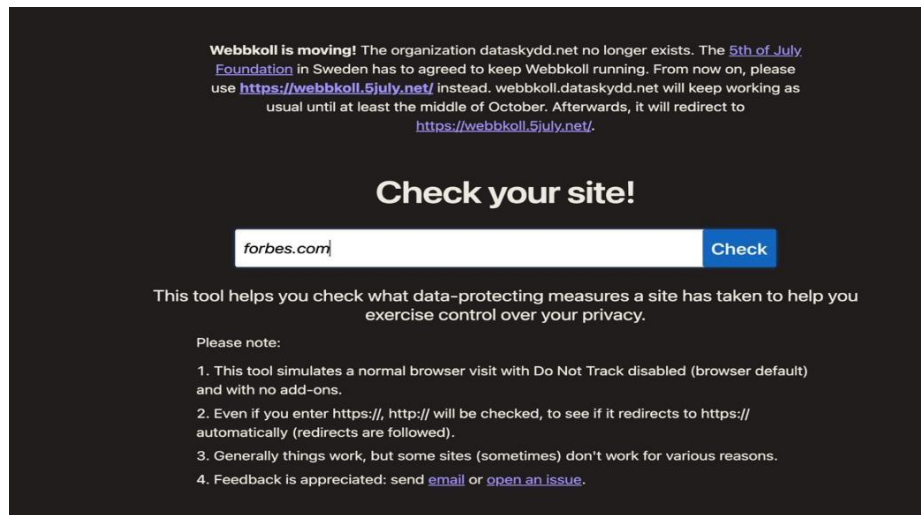


Figure 32: Webbkoll Scanner UI

We strongly believe that it could be a top consideration for another thesis project, especially a more code related one, since Webbkoll code is open source.

6. Examining Websites in Practice

The primary objective of this thesis was to assess ten websites for their security features and other ten websites for their compliance with the ePrivacy Directive, which serves as the foundational regulation, followed by GDPR cookie compliance. As already discussed, each task was performed separately using different methods. In both cases, every action related to the analysis is performed using free commercial tools, which are easy to use and can be accessed through almost any web browser without needing any software installation, significant computing power or specific operating system configurations. This makes the methodology reproducible and scalable, allowing others to perform similar evaluations without facing technical barriers.

What is more, relying on these established tools ensures that the analysis is conducted with reliable, tested solutions and methods, which enhances the credibility of the results. Using pre-built tools is perfectly valid in this context, as the objective of the thesis is to evaluate website security and cookie compliance, not to develop new software solutions. By leveraging existing tools, the focus remains on practical assessment and compliance, which is both time-efficient and effective.

This chapter is dedicated to presenting the methodology and providing practical examples of the analysis conducted throughout this thesis. Furthermore, the analysis is based on real-world examples to illustrate how these methods were applied to specific websites, offering a clear understanding of the evaluation process. Lastly, due to the extensive nature of the website analysis, this chapter will only present key examples that highlight the most important findings.

6.1 Evaluation Framework and Approach

In this section the methodology and the standards regarding the evaluation of the websites in terms of security and privacy are outlined. More emphasis is placed around the analysis involving cookie compliance, since it is significantly more complex and dynamic.

6.1.1 Standards for Assessing Cookie Non-Compliance and deviation from best practises

Leveraging the knowledge discussed in the previous sections, regarding the ePrivacy Directive, GDPR policies, best practises and other standards set based on specific articles; the following checklist was set in order to assess potential non-compliance in terms of website cookies.

1. **Undeclared Cookies:** Cookies that are found when scanning or visiting the website but are not disclosed nor listed in a website's cookie policy or consent banner.
2. **Unclassified Cookies:** Cookies that have been declared, but have not been classified into cookie categories, based on their type or intent.
3. **Incorrectly Assigned Labels for Cookies with a Well-Defined Purpose:** This refers to cases where a cookie, such as a Google Analytics cookie, is labelled in a way that doesn't align with its widely recognized purpose. For example, a cookie meant for analytics and tracking might be inaccurately categorized as "essential" or "functional" instead of "analytics."
4. **Missing or Misconfigured Cookie Consent Banner:** The presence of a cookie banner on websites is considered as a best practice for ensuring cookie compliance, helping to inform users and obtain their consent for cookie installation.

However, in many cases, these banners are misconfigured, either unintentionally or maliciously, to trick users into giving consent.

These four standards are strict and straight forward, however in this study a few more are set, mainly focusing on the interaction between the user and the website:

- A. The level of clarity regarding the information provided to users about the cookie installation.
- B. User must always be informed properly before giving consent for cookie installation.
- C. Users must be allowed to easily reject some or all cookies, without being "nudged" into consenting through design choices that make refusal difficult.
- D. User must be able allowed to withdraw consent.

At this point it should be made clear that the regulations are strict, but at the same time it seems that ensuring full compliance seems tough and overwhelming. Before even starting the analysis, it should be expected that a lot of websites are not a hundred percent compliant with the regulations by the ePrivacy Directive and the GDPR. This is mainly because of the following reasons:

- Hosts are not fully aware of the cookies that are present on their websites, since there is almost no tool, which is able to automatically achieve full coverage and compliance.
- They simply do not give enough emphasis, since getting fined for small misconfigurations is very unlikely.

Either way, we presume that many of these incompliances originate not necessary from malicious intent, but also from neglect. However, it is worth noting that nowadays almost every website has at least a cookie banner and follows most standards, something that was by no means the norm a few years ago. More details regarding how websites were checked for compliance with these standards, are presented later in the methodology subsection of this chapter.

6.1.2 Standards for Assessing Website Security

As previously discussed, assessing security on websites is a very broad topic. Combined with the fact that in this study, we are only performing passive scans, it leads to limitations in the number of vulnerabilities that can be detected and therefore keeps the whole analysis within certain bounds.

Although limiting, this makes the whole analysis significantly simpler and straightforward, since the objectives are not so chaotic and dynamic. In the assessment of website security, several key standards were considered to ensure that each site follows best practices for securing data and protecting user information. These standards focus on areas such as:

- PCI DSS compliance
- DNSSEC
- HTTPS implementation (including TLS Encryption)
- Web Software and Content Security

While these are just the tip of the iceberg, they are often considered sufficient to assess or grade the security of the users visiting the website, rather than just the security of the

website itself. The emphasis leans more on how well the website's first line of defence protects its users' data and online interactions from potential threats. Lastly, it should be mentioned that they set standards for website security, just like GDPR sets for privacy. For example, the NIS 2 Directive and ISO/IEC 27001. However, these are incredibly broad, and we cannot ensure full compliance by only using free tools and it is also far too complicated for a thesis project.

6.2 Methodology

This subsection provides a step-by-step analysis in an attempt to provide complete transparency behind the assessments that were conducted. The rationale behind each step is covered, along with the specific techniques and procedures that were carried out to ensure accuracy and reliability of the findings.

6.2.1 Website Selection Criteria

To perform the analysis, 20 different websites were selected. Since, the evaluation is split in two different categories, namely security and privacy, half of these websites were primarily tested in terms of security and the other half in terms of privacy. While the number of selected websites for each category is the same, the selection criteria are significantly different.

The selected websites for examination for GDPR cookie compliance are e-shops, news and media websites. E-shops were selected, because they tend to collect excessive amount of personal data, like payment details, names, addresses and create purchase histories. Moreover, both e-shops and news-media websites often use cookies to track user behaviour and create analytics in order to present personalized ads to the customer. While these practises are by no means always malicious or illegal, often website administrators tend to trick users into accepting cookies or even hiding them, so that they can collect more information without them noticing or giving consent. Apart from that, targeting such websites provides a more detailed analysis, due to the diverse cookie usage that these websites tend to implement. E-shops generally use many different cookies for shopping cart functionality, user authentication, and session tracking, while media websites often use cookies for personalized content delivery and extensive tracking for targeted advertising. Thus, this selection provides a wide range of different cookie types and purposes to evaluate.

At first, the selected websites for examination in terms of security were based on a single criterion, specifically websites that fall under the guidelines and requirements outlined in the NIS 2 Directive. This would ensure that the evaluation aligns with the security standards expected of public bodies and critical sectors identified within the directive. This decision was made in order to make the study more specific and at the same time provide more value and meaningful insights. However as it was expected, these websites implement very strict policies in terms of scanning, blocking almost every attempt that was initiated. This led to the selection being a bit broader, which is not a major setback for this analysis.

In conclusion, this strategic selection of websites was carefully crafted to not only enhance the specificity of the project, but to also provide valuable insights into the current state of website security and privacy compliance.

6.2.2 Websites Under Examination

Based on the previously referenced criteria, the following websites were selected.

For Privacy – Cookie Compliance Testing

Table 2: Website Selection for Privacy Evaluation

	Website URL	Category
1	www.atticadps.gr	Online Shopping
2	www.cnn.gr	News - Content
3	www.e-shop.gr	Online Shopping
4	www.kathimerini.gr	News - Content
5	www.lifo.gr	News - Content
6	www.notos.gr	Online Shopping
7	www.plaisio.gr	Online Shopping
8	www.protothema.gr	News - Content
9	www.public.gr	Online Shopping
10	www.tovima.gr	News - Content

For Security Compliance Testing

Table 3: Website Selection for Security Evaluation

	Website URL	Category
1	www.gov.gr	Government
2	www.dei.gr	Energy
3	www.nbg.gr	Banking / Finance
4	www.oasa.gr	Public Transportation
5	www.nis.gr	Public Safety
6	www.eydap.gr	Water Utility
7	www.alphabank.gr	Banking / Finance
8	www.aegeanair.com	Airlines
9	www.helpe.gr	Energy
10	www.ert.gr	Public Media

6.2.3 The Procedure

This section contains a step-by-step breakdown of the actions performed in to carry out both the privacy and security compliance testing.

The Security Testing Procedure

Firstly, the procedure regarding the website security evaluation is presented, since it is simpler and straightforward. As previously discussed, to test websites for their security, the free Website Security Test and SSL Security Test tools by ImmuniWeb are used. The

only thing required to conduct the analysis is to give as input a valid URL in the browser UI. After a few minutes (typically five to ten), a report presented, and it can be downloaded as long as the user has created a free account. Therefore, after downloading the report, the appropriate information and conclusions can be drawn.

However, when the test refers to a NIS 2 directive related website (government, bank, public sector, etc.) the scanning is sometimes blocked. In that case, we can only test the website using the Qualys SSL Server Test tool which we mentioned previously, which in most cases is not totally blocked. In those cases, we can only extract results regarding the TLS configuration of the website.

The aforementioned process is shown on the flowchart below:

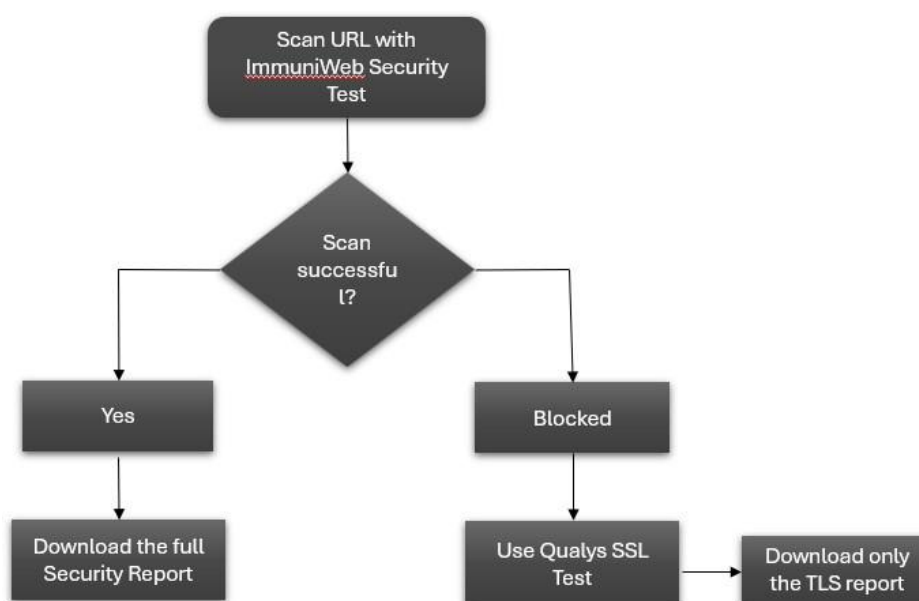


Figure 33: Security Testing Procedure Flowchart

The Privacy Testing Procedure

On the other hand, the procedure regarding the GDPR compliance test involves more steps, compared to the previously covered one.

At first, two scans are initiated using the ImmuniWeb Privacy test and CookieYes free test that were mentioned in the previous chapter. After gathering the reports, in case there are cookies that are unknown to the CookieYes free database, these can be further examined using the following domain: <https://cookiepedia.co.uk/>. This website is the largest database of pre-categorized cookies and often contains more information regarding cookies that are absent from the CookieYes database. After these two steps, the last step is to manually visit the website using any web browser with the Cookie-Editor extension installed. Specifically, two visits are required. During the first one in case there is a cookie banner, all cookies are rejected during the first visit and in contrast accepted in the second one. These actions are performed, so that the legitimacy of the reject and accept statements can be verified. In summary, by visiting the website, we can perform a dynamic analysis of cookies, which allows us to see the cookies being set, as well as gain insights into the cookie banner's behaviour. Additionally, we can observe which cookies are accepted or rejected based on user interaction, providing further information on GDPR compliance.

The aforementioned process is shown on the flowchart below:

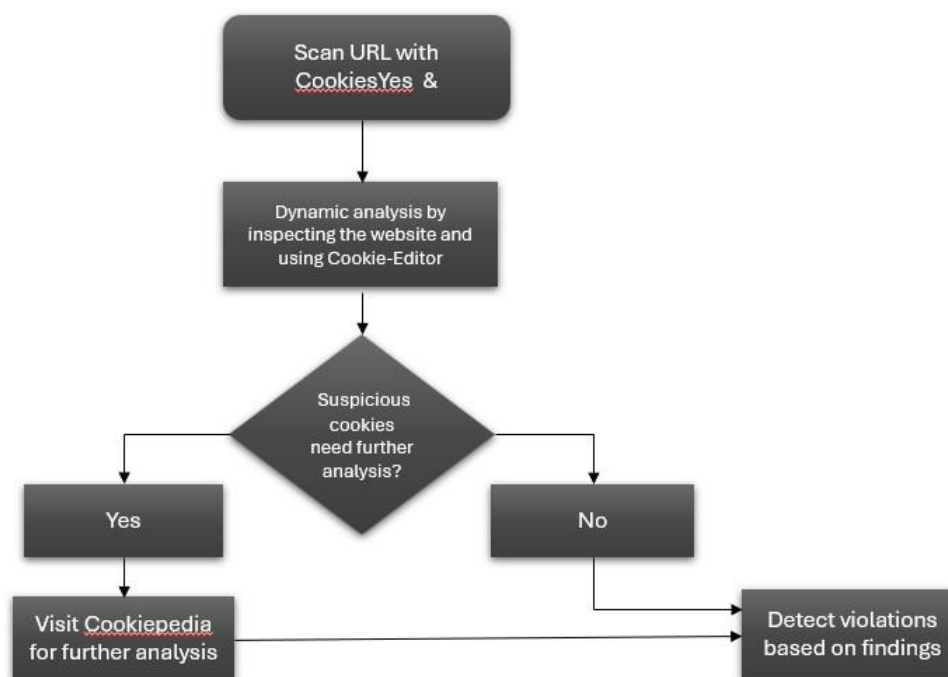


Figure 34: Privacy Testing Procedure Flowchart

6.2.4 Practical Evaluation and Analysis on Cookie Compliance

This section covers the actual testing and evaluation process of the selected websites, which took place toward the end of 2024 using the previously mentioned scanning tools. This analysis has two main pillars: Firstly, to test the selected websites for their privacy – cookie compliance and secondly to assess the selected tools regarding their accuracy and reliability by analysing potential faults, limitations, or inconsistencies that may arise during the actual testing process. While on paper, these tools are flawless, unfortunately that is not always the case since they often face some problems or limitations. This analysis will provide deeper insights into whether these tools can be reliably used for academic and professional use for evaluating website privacy compliance, or if further measures and methods are required to meet today’s high and complex standards.

6.2.5 Case Study 1: www.plaisio.gr (Extended)

Plaisio Computers is a major Greek retailer specializing in technology related products. Its website plaisio.gr mainly operates as an online store. In this subsection the testing and analysis regarding this site’s compliance with the cookie regulations takes place. Therefore, let’s break down the analysis step by step.

By now it should be made clear that the first step involves scanning the website using the selected free tools. To begin with, the ImmuniWeb Website Privacy Test scan is initiated (ImmuniWeb and CookieYes scans can be initiated at the same time and their results can be analysed in any order. This presentation is for clarity purposes.). After a few minutes the scan is completed successfully, and a full report is generated. It is clearly stated that this report is an intellectual property of ImmuniWeb and must not be used for commercial purposes. Since this thesis clearly has an academic purpose and is not for commercial use, only some snapshots containing the most relatable information to our study will be presented. Keep in mind, that this applies to all the case studies covered in this thesis.

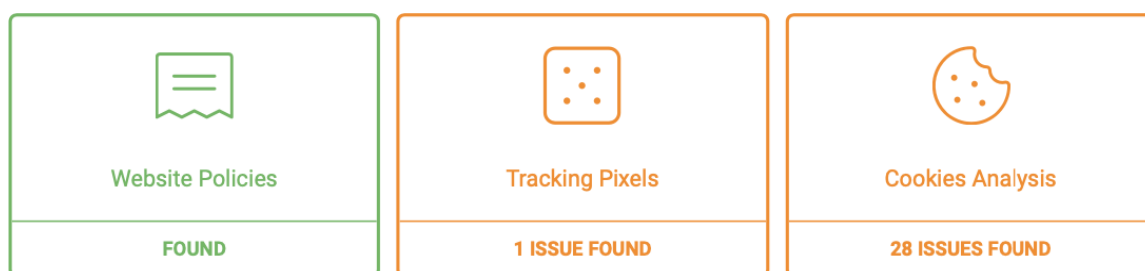


Figure 35: ImmuniWeb Scan plaisio.gr (1/4)

As illustrated in the image above, these are the key fields most pertinent to our study, namely: 1) Website Policies, 2) Tracking Pixels and 3) Cookie Analysis. Let's examine its one in more depth.

Starting with Website Policies, by digging a bit deeper into the report the following information can be found:

Privacy Policy was found on the website	Good configuration
Cookie Consent Banner was found on the website	Good configuration
The copyright notice is up-to-date: © 2024 Plaisio Computers	Good configuration

Figure 36: ImmuniWeb Scan plaisio.gr (2/4)

The first box, namely Website Privacy Policy is a formal legal document which governs how the visitor's personal data is stored and used by the website operator. This is crucial for both overall privacy and cookie compliance. As shown, this document seems to be present and correctly structured, since it is listed as: good configuration. Apparently, this scanning tool does not provide more details regarding what exactly lead to that conclusion, however since our main focus cookie compliance, this is beyond of the scope of this study. The same applies for the third box, which is a check for a valid and up to date copyright notice. The second - middle box however is the most crucial regarding the assessment of cookie compliance, which is the Cookie Consent Banner or simply Cookie Banner. It has already been made clear that the absence of a cookie Banner constitutes a substantial deviation from best practices for cookie compliance, creating a significant gap in alignment with privacy regulations and user consent requirement. Based on the image, a banner is present on the website, which as the report claims equals to good configuration. Considering the evaluation criteria set in this chapter, the limitations of such scanning tools are already noticeable. While the presence of a cookie banner is crucial for compliance in terms of cookies, it is just the bare minimum and by no means equals or even indicates good configuration. A common practise when creating cookie banners is to intentionally design them with "dark patterns" to mislead or pressure users into giving consent without fully understanding what they are agreeing to. For example, some banners might come with pre-selected consent options, hide rejection options in hard-to-find menus, or make the process of rejecting non-essential cookies more complicated and frustrating than simply accepting all. Therefore, while scanning tools like this one may detect the existence of a banner, they cannot always determine if it is designed to manipulate consent.

Moving on from the Website Policies section, there are two more displayed on the report, the first one being Pixel Tracking. This is a technique that usually inserts an invisible human eye tracker into a webpage code. Although, this technique is not directly related

to cookies it is worth mentioning since it serves a similar purpose and are they are often combined to achieve user tracking. Also, they are often subject to similar regulations under the GDPR.

Lastly, there is the Cookie Analysis section. A portion of the information regarding this section is displayed on the images below.

First-Party Cookies

There are 16 first-party cookies without a Secure flag						Misconfiguration or weakness	
There are 19 first-party cookies without an HttpOnly flag						Misconfiguration or weakness	
Name	Value	Domain	Path	Expires	Samesite	Secure	HttpOnly
Constru ... ient_id	253efdd3- 2713 ... - a7e79db2382	.plaisio.gr	/	Oct 7th, 2025		No	No

Figure 37: ImmuniWeb Scan plaisio.gr (3/4)

Third-Party Cookies

3 Cookies c.clarity.ms [United States] 							
All third-party cookies have a Secure flag						Good configuration	
There are 3 third-party cookies without an HttpOnly flag						Misconfiguration or weakness	
There are no third-party cookies with an expiration time exceeding 3 months						Good configuration	
Name	Value	Domain	Path	Expires	Samesite	Secure	HttpOnly
SM	C	.c.clarity.ms	/	Immediately	None	Yes	No

Figure 38: ImmuniWeb Scan plaisio.gr (4/4)

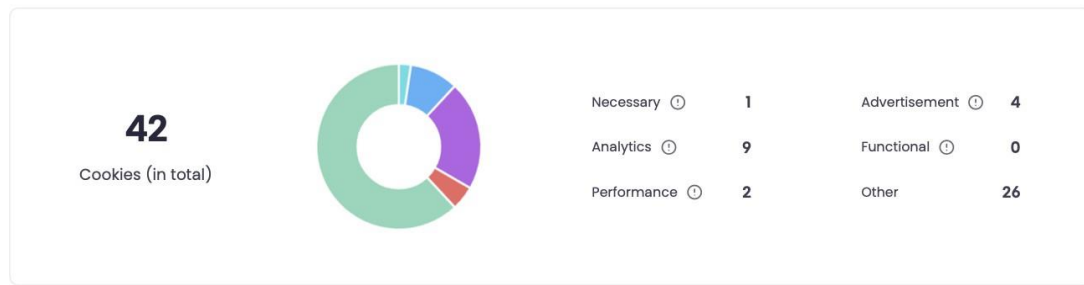
This final part of the report contains information about the cookies detected on the website. However, it only focuses around the Samesite, Secure and HTTPOnly flag presence providing very limited information, which is not enough for the purposes of this study. In contrast, dedicated cookie scanner tools provide far better and more detailed results.

The second part of the analysis is structured around the CookieYes free scanning tool. Unlike the ImmuniWeb scan, this scan is quite faster, and the report is generated in just a couple of seconds. This time there are no copyright claims or limitations regarding the report.

SCAN REPORT

<http://WWW.PLAISIO.GR>

GENERATED ON 2024-10-07 10:45:51 GMT

[Copy scan report](#)**Figure 39: CookieYes Scan Results for Plaisio.gr**

This is the top part of the report, listing the total number of cookies detected on the website, along with the category they belong to. After that, the report continues with listing each one of the 42 total cookies, along with their description (when that is available in the CookieYes database), duration and type. A portion of these results is displayed on the table below.

Table 4: Cookies Detected on plaisio.gr

<u>Cookie</u>	<u>Description</u>	<u>Duration</u>	<u>Type</u>
ai_user	"Microsoft Azure sets this cookie as a unique user identifier cookie	1 year	Advertisement
ConstructorID_client_id	No description available.	1 year	Other
ConstructorID_session_id	No description available.	1 year	Other
pls_uid	No description available.	1 year	Other
azuappgwplsgr	No description available.	session	Other
azuappgwplsgrCORS	No description available.	session	Other
ai_session	This is a unique anonymous session identifier cookie set by Microsoft Application Insights software to gather statistical	1 hour	Analytics

	usage and telemetry data for apps built on the Azure cloud platform.		
SC_ANALYTICS_GLOBAL_COOKIE	Sitecore sets this cookie to track the number of visits a visitor makes to the website.	1 year 1 month 4 days	Analytics
PlaisioB2C_Carts	No description available.	3 months 8 days	Other
rr_rcs	No description available.	1 year 1 month 4 days	Other
CLID	Microsoft Clarity set this cookie to store information about how visitors interact with the website.	1 year	Analytics
_ALGOLIA	Algolia sets this cookie for the website to function and cannot be switched off in our systems.	6 months	Necessary
cp_total_cart_items	No description available.	1 year	Other
cp_total_cart_value	No description available.	1 year	Other
cpab	No description available.	1 year	Other
bi	No description available.	1 year	Other
_clk	Microsoft Clarity sets this cookie to retain the browser's Clarity User ID and settings	1 year	Analytics

	exclusive to that website.		
cp_sessionTime	No description available.	1 hour	Other
RT	"Akamai Boomerang set this cookie which gauges visitor experience with page load times."	session	Other
SM	Microsoft Clarity set this cookie for synchronizing MUID	session	Analytics

Now that both scans are complete it is time to inspect the results, based on the standards were set in this chapter. This is done by visiting the website and performing manual, real-time testing.

The first thing that must be examined is the cookie banner. Inspecting a website's cookie banner is simple and can be done from any browser, as long as the preferences regarding that specific website's cookie banner have not been accepted or rejected. Thus, it is best to perform such activities with a clear web browser. A snapshot of the visited site's cookie banner is shown on the image below.

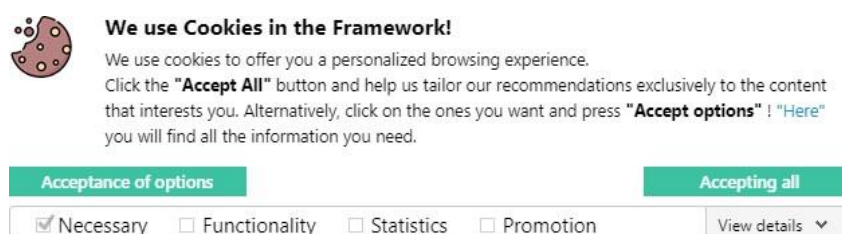


Figure 40: Overview of plaisio.gr Cookie Banner

Firstly, it is verified that the website has a cookie banner, just like the ImmuniWeb scan indicated. Also, the cookie banner offers a clear categorization of all the cookies, along with clear choice options and offers granular consent. As stated, pre checked boxed boxes on cookie banners are dark practices, however in this case only the necessary cookies category is preselected, which is fine since they are exempt from needing consent under the current regulations. Moreover both “accepting all” and “acceptance options” are balanced in terms of design. Thus, the cookie banner is correctly configured.

Although, the analysis of the cookie banner is over we will continue to interact with it to carry out the rest of the analysis. By clicking “View details” in the bottom right corner and then clicking “Relatively” the following box is displayed.

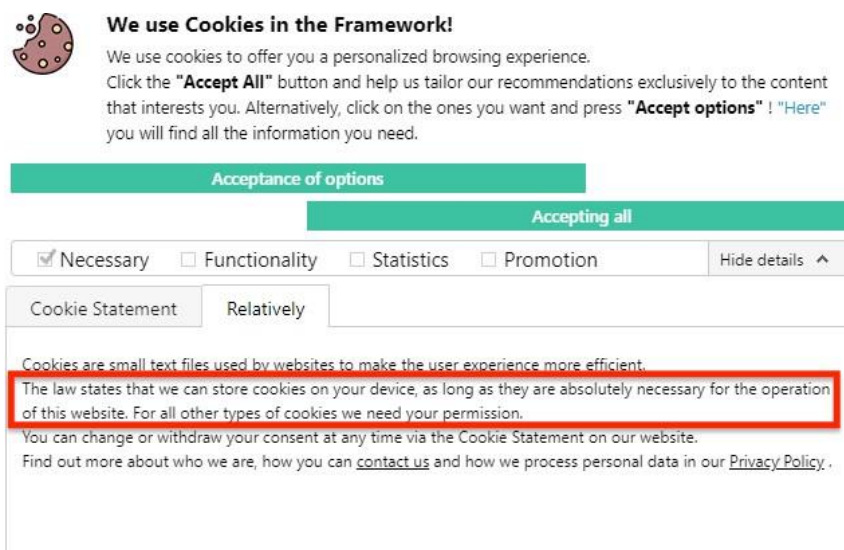


Figure 41: Expanded Cookie Banner - plaisio.gr (1/2)

The highlighted statement has already been referenced multiple times throughout this thesis. Therefore, considering that the cookie banner is compliant and that only the necessary cookies category is preselected it looks like the website is fully compliant, unfortunately though this cannot be verified before completing the full cookie analysis. By clicking the “Cookie Statement” the following information is displayed on the banner.

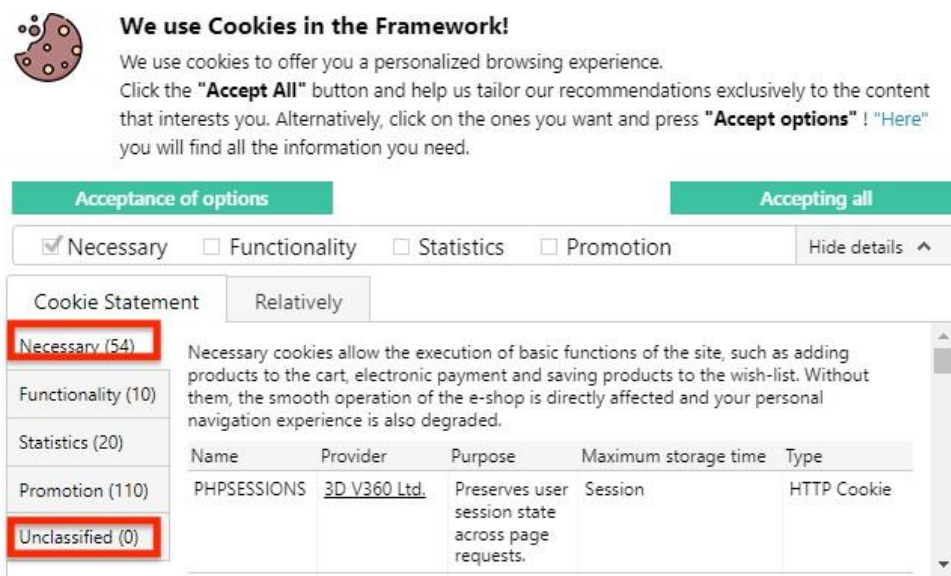


Figure 42: Expanded Cookie Banner - plaisio.gr (2/2)

The thing that stands out the most is the number of cookies displayed, specifically 194 total cookies, 54 of which are necessary. The CookieYes scanning tool on the other hand only detected 42 cookies. That is expected several reasons, mainly because:

- The scanning tool does not scan the whole website, but only the given URL (front page).
- Some cookies only tend to install after specific user interactions with the website
- Some cookies are set by subdomains or external services (e.g., content delivery networks, embedded third-party content).

The large number of cookies present makes the analysis a bit complex, however the standards set in the previous section will help to quickly check for cookie compliance. Looking at the bottom left corner of the image we can see that there are zero Unclassified cookies, meaning that another criterion regarding cookie compliance is met.

The next thing to check for are cookies with incorrectly assigned labels. These types of cookies are mainly cookies that are falsely listed as necessary. In our case, the website has 54 necessary cookies a large number, which acts as a high indicator for incorrectly assigned labels. By clicking on the “Necessary” tab, a full list containing all the necessary cookies is displayed. Reviewing the list, many suspicious cookies are detected, along with the corresponding descriptions:

- **cpab (ContactPigeon):** This cookie collects information on products viewed and the content of the shopping cart to increase the website’s conversion rate via targeted advertisement.
- **rr_rcs:** Used by a Product Recommendation engine, which typically serves to enhance the user experience, but it might not be essential for the website's core functionality.

Skrouz cookies (including **_b_in_session** and more): Tracking user activity after switching from Skrouz.gr to record purchases and support billing models or analytics functions.

By reviewing the description of those cookies, it looks like their purpose is more centred towards advertisement, functionality and marketing. As a result, their categorization as “Necessary” does not seem justified. To dig a bit deeper, these cookies are thrown into the cookiepedia database to verify the findings. The cpab and Skrouz cookies purposes could not be found in the database. However, the rr_rcs gave the following results.

Cookies Search Results: rr_rcs

About this cookie:

This cookie name is associated with Rich Relevance which is used to provide an ID for personalized product recommendations on the site.

The main purpose of this cookie is: **Functionality**

Key numbers for rr_rcs:

Cookies with this name have been found on **298** websites, set by **205** host domains.

It has been found as a **First Party** cookie on **515** websites and a **Third Party** cookie on **22** websites.

It has been found as a **Persistent** cookie on **312** websites, with an average life span of **696** days.

It has been found as a **Session** cookie on **225** websites.

Figure 43: rr_rcs Searched on Cookiepedia

Considering the above findings, there is a very high indication for incorrectly assigned labels for cookies with a well-known purpose, resulting in a breach of the set regulations.

The last thing to check for, are undeclared cookies, meaning cookies that the scanning tool detected, but are not listed on the website. Since it is a time-consuming procedure and at the same time it does not provide extra value to this study, we won’t emphasize on the number of undeclared cookies, but rather on their presence. In case there is even one undeclared cookie, the analysis is stopped, and this is marked as a violation, since transparency on cookies is prerequisite for their lawful usage. In this case for example, a cookie named CLID made from Microsoft to store information about how visitors interact with the website is not listed, making it undeclared. This cookie was detected using CookieYes and is listed on the previous table. Keep in mind that in case no undeclared cookies have been detected by this time this does not mean that they don’t exist, since

there is a chance that the CookieYes scan missed them. To be completely certain a new visit is required on the website, using the cookie-editor extension.

In conclusion, while meeting most of the standards set in this study for ensuring cookie compliance, this website failed two critical checks regarding:

1. **Incorrectly Assigned Labels for Cookies with a Well-Defined Purpose**
2. **Undeclared Cookies**

6.2.6 Case study 2: www.tovima.gr

ToVima.gr is Greek news website that is part of the "To Vima" newspaper, which is one of the oldest and most well-known newspapers in Greece. Since, the step-by-step coverage of the analysis process is presented on the previous subsection - Case study 1, let's proceed directly into the findings.

The core part of the ImmuniWeb report is shown on the image below.

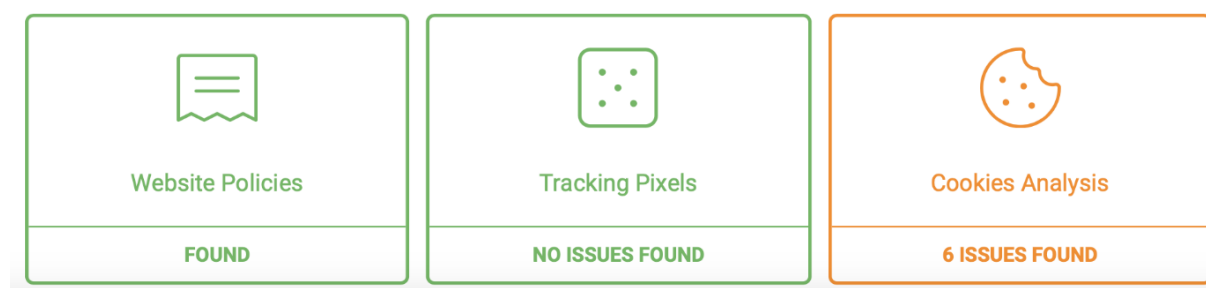


Figure 44: ImmuniWeb Scan tovima.gr (1/4)

Starting with Website Policies, by digging a bit deeper into the report the following information can be found:

Privacy Policy was found on the website	Good configuration
Cookie Consent Banner was found on the website	Good configuration
No copyright information found on the website	Misconfiguration or weakness

Figure 45: ImmuniWeb Scan tovima.gr (2/4)

Just like the previous case study, both Privacy Policy and Cookie Consent Banner are marked as: good configuration. On the other hand, no copyright information was found on the website. What matters most though, is the cookie banner which will be further examined later by visiting the website in the same manner as we did in the previous case study.

Moving on the report, there are no issues related to tracking pixels, therefore there is nothing to display there. The last section of the report is the Cookies Analysis as shown on the images below.

First-Party Cookies

There are 3 first-party cookies without a Secure flag						Misconfiguration or weakness	
There are 6 first-party cookies without an HttpOnly flag						Misconfiguration or weakness	
Name	Value	Domain	Path	Expires	Samesite	Secure	HttpOnly
_ga_TZN1DMYFRS	GS1.1.1728295 ... 295036.60.0.0	.tovima.gr	/	Nov 11th, 2025		No	No
_ga	GA1.1.1427526488.1728295037	.tovima.gr	/	Nov 11th, 2025		No	No
FCNEC	%5B%5B%22AKsR ... D%3D%22%5D%5D	.tovima.gr	/	Oct 7th, 2025		No	No

Figure 46: ImmuniWeb Scan tovima.gr (3/4)

1 Cookie doubleclick.net [United States] 🇺🇸

All third-party cookies have a Secure flag	Good configuration
All third-party cookies have an HttpOnly flag	Good configuration
There are no third-party cookies with an expiration time exceeding 3 months	Good configuration

Name	Value	Domain	Path	Expires	Samesite	Secure	HttpOnly
test_cookie	CheckForPermission	.doubleclick.net	/	Oct 7th, 2024	None	Yes	Yes

1 Cookie onesignal.com

All third-party cookies have a Secure flag	Good configuration
All third-party cookies have an HttpOnly flag	Good configuration
There are no third-party cookies with an expiration time exceeding 3 months	Good configuration

Name	Value	Domain	Path	Expires	Samesite	Secure	HttpOnly
__cf_bm	PQnQNGQ5i4ZzW ... vLV_4QaJ6Y3ww	.onesignal.com	/	Oct 7th, 2024	None	Yes	Yes

Figure 47: ImmuniWeb Scan tovima.gr (4/4)

Following the ImmuniWeb scan results, the CookieYes findings are presented below.

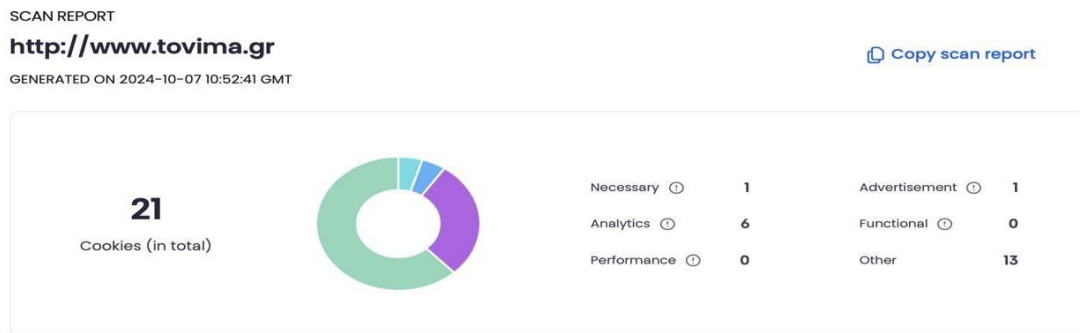


Figure 48: CookieYes Scan tolima.gr

In this case, there are a lot less cookies detected something that is generally expected from a news-media website, since they tend to offer limited features and simple functionality, compared to an online store and making their dependence on cookies way less significant. The detected cookies along with their details are listed on the following table:

Table 5: Cookies Detected - tolima.gr

<u>Cookie</u>	<u>Description</u>	<u>Duration</u>	<u>Type</u>
__cf_bm	This cookie, set by Cloudflare, is used to support Cloudflare Bot Management.	1 hour	Necessary
_cbt	No description available.	session	Other
_ga_*	Google Analytics sets this cookie to store and count page views.	1 year 1 month 4 days	Analytics
_ga	installed by Google Analytics, calculates visitor, session and campaign data.	1 year 1 month 4 days	Analytics

_cb	collect data such as visitors ' IP addresses, geographical locations and website navigation. This information is used for internal optimization and statistics.	1 year 1 month	Analytics
_chartbeat2	Chartbeat sets this cookie to be used by the web analytics company to register whether the user has visited the website before.	1 year 1 month	Advertisement
_cb_svref	Chartbeat sets this cookie to store the original referrer for this site visitor.	1 hour	Analytics
FCNEC	for analytics to help collect data that allows services to understand how users interact with a	1 year	Analytics

	particular service.		
Cb_svref_expires	ChartBeat sets this cookie for webshop statistics.	never	Analytics
__3perf_googleFonts_2c850	No description available.	never	Other
_cb_expires	No description available.	never	Other
Os_pageviews	No description available.	never	Other
Gbc_consent	No description available.	never	Other
_chartbeat2_expires	No description available.	never	Other
isOptedOut	No description available.	never	Other
isPushNotificationsEnabled	No description available.	never	Other
CMPList	No description available.	never	Other
___nrbi	No description available.	session	Other
Onesignal_pageview_count	No description available.	session	Other
___nrbic	No description available.	session	Other
ONESIGNAL_HTTP_PROMPT_SHOWN	No description available.	session	Other

After successfully completing the two scans, the next step is to perform dynamic analysis by visiting the website.

Starting the analysis, the first thing that is under examination is the cookie banner, which is displayed on the image below.

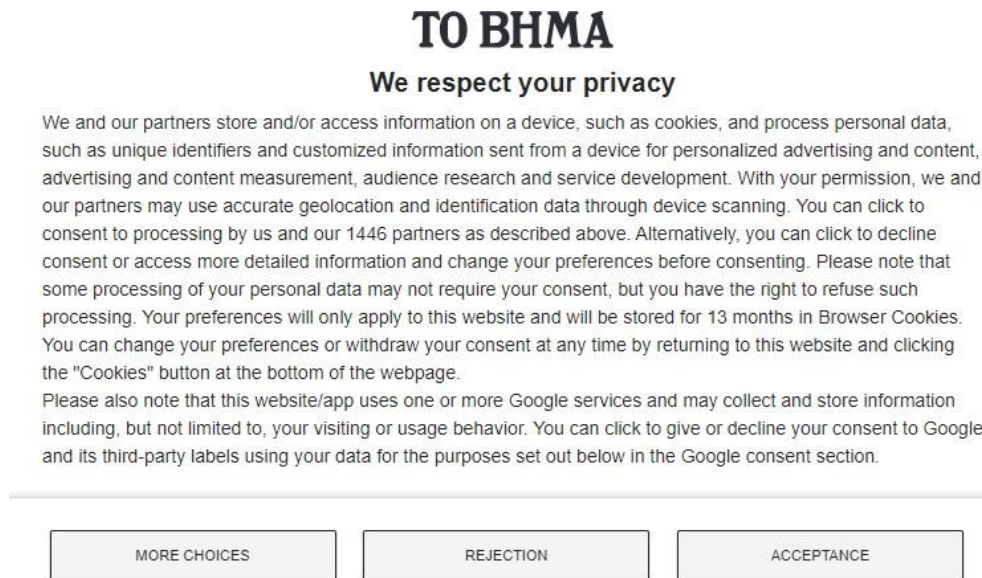


Figure 49: Overview of vima.gr Cookie Banner

This banner is clearly different from the previous one and this is expected especially when the genre of the websites is different. Firstly, it must be pointed out that the claim of the ImmuniWeb scanning, for the presence of a cookie banner is indeed true. The next thing to analyse is if this banner implements any malicious practices in order to trick the users into accepting cookies. So far, everything looks normal, and both the acceptance and rejection buttons seem equally pointed out and placed. By clicking the “More Choices”, this is what appears on the banner.

TO BHMA

We respect your privacy

We and our partners store and/or access information on a device, such as cookies, and process personal data, such as unique identifiers and customized information sent from a device for personalized advertising and content, advertising and content measurement, audience research and service development. With your permission, we and our partners may use accurate geolocation and identification data through device scanning. You can click to consent to processing by us and our **1446** partners as described above. Alternatively, you can click to decline consent or access more detailed information and change your preferences before consenting. Please note that some processing of your personal data may not require your consent, but you have the right to refuse such processing. Your preferences will only apply to this website and will be stored for 13 months in Browser Cookies. You can change your preferences or withdraw

[I REJECT EVERYTHING](#)
[I ACCEPT EVERYTHING](#)

Accurate geolocation data and identification through device scanning	ENABLED	✓
Personalized advertising and content, advertising and content measurement, audience research and service development	DISABLED	>
Storage and/or access to a device's data (691 partners)	DISABLED	>
Special Purposes (598 partners)		>
Features (598 partners)		>
Google consents		>

Figure 50: Expanded Cookie Banner - tovima.gr (1/2)

By accepting everything the user also agrees to give consent for data processing to 1446 partners. Notice that this number is extremely large, and this indicates a red flag. In case the user tries to load the list, it is almost impossible to navigate, since it loads in bunches and very slowly, meaning that it would a very large amount of time.

[ΑΠΟΡΡΙΨΗ ΟΛΩΝ](#)
[ΑΠΟΔΕΧΟΜΑΙ ΤΑ ΠΑΝΤΑ](#)

AdInMo LTD	>
Aitude, Inc.	>
Adkernel LLC	>
Adloox SA	>
ADMAN - Phaistos Networks, S.A.	>
Admixer EU GmbH	>
Adnami Aps	>

Figure 51: Expanded Cookie Banner - tovima.gr (2/2)

Therefore, while there is a list with all the partners in practice it is not transparent. The same applies to the amount of text displayed on the image. Chaotic banners like this might overwhelm users, leading them to just accept to save time. Lastly, there is no

detailed list containing all the cookies that are present on the websites, unlike the previous case. Thus, while all these do not directly count as a violation, there is substantial indication of using “dark” practices into tricking users to give consent for cookie installation.

Moving towards the cookies analysis, in this case there is no way to be totally certain about the presence of a policy violation, since the full list of cookies on the website is unavailable. First, it cannot be totally verified if there are cookies with incorrectly assigned labels, since there is no available information regarding the labels assigned. Secondly, there is no way to check for undeclared or unclassified cookies.

Despite this limitation, the dynamic analysis is not over yet. We continue by proceeding to the next step, which is selecting the button “REJECTION” on the cookie banner, meaning that we deny the installation of any cookies that are not necessary for the operation of the website. Then, by using the cookie-editor extension we can see the following cookies present in our browser.

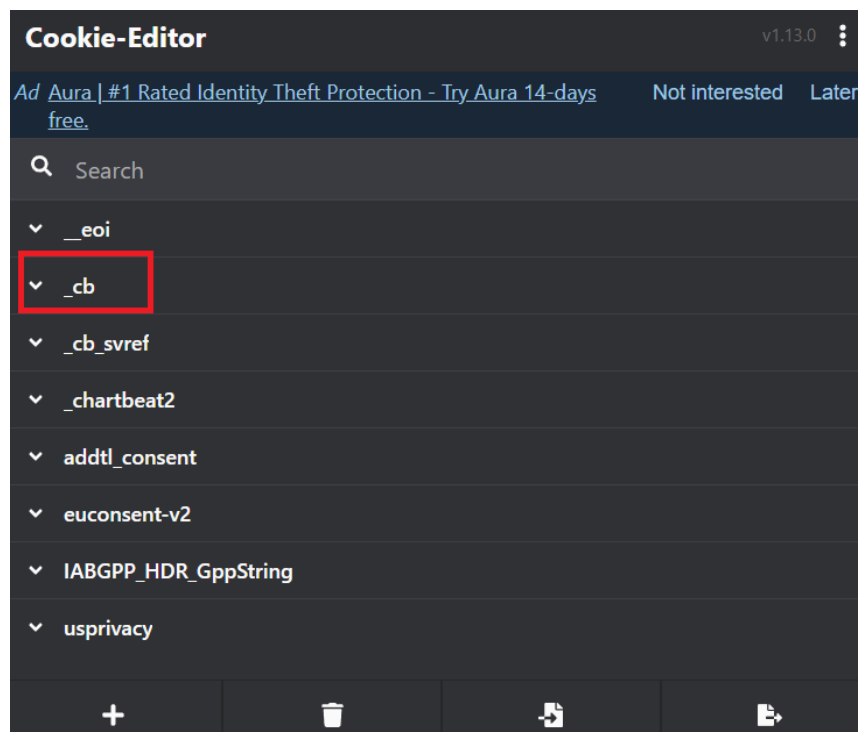


Figure 52: Cookie-Editor Output - tovima.gr with Reject All option

As highlighted, a cookie named `_cb` is installed. This is a well-known cookie and according to Cookiepedia it serves targeting advertising purposes. Therefore, it indicates a possible violation.

Cookies Search Results: `_cb`

About this cookie:

This is a Microsoft MSN 1st party cookie used to measure the use of the website for internal analytics.

The main purpose of this cookie is: **Targeting/Advertising**

Key numbers for `_cb`:

Cookies with this name have been found on **3,528** websites, set by **3,443** host domains.

It has been found as a **First Party** cookie on **3,582** websites and a **Third Party** cookie on **2,641** websites.

It has been found as a **Persistent** cookie on **6,223** websites, with an average life span of **41,107** days.

It has been found as a **Session** cookie on **0** websites.

Figure 53: `_cb` Searched on Cookiepedia

The last action left to do is to re-visit the site and select the “Acceptance” option, which will accept every cookie that the website wants to install. Using cookie-editor once again, let’s see a snapshot containing a portion of the cookies installed.

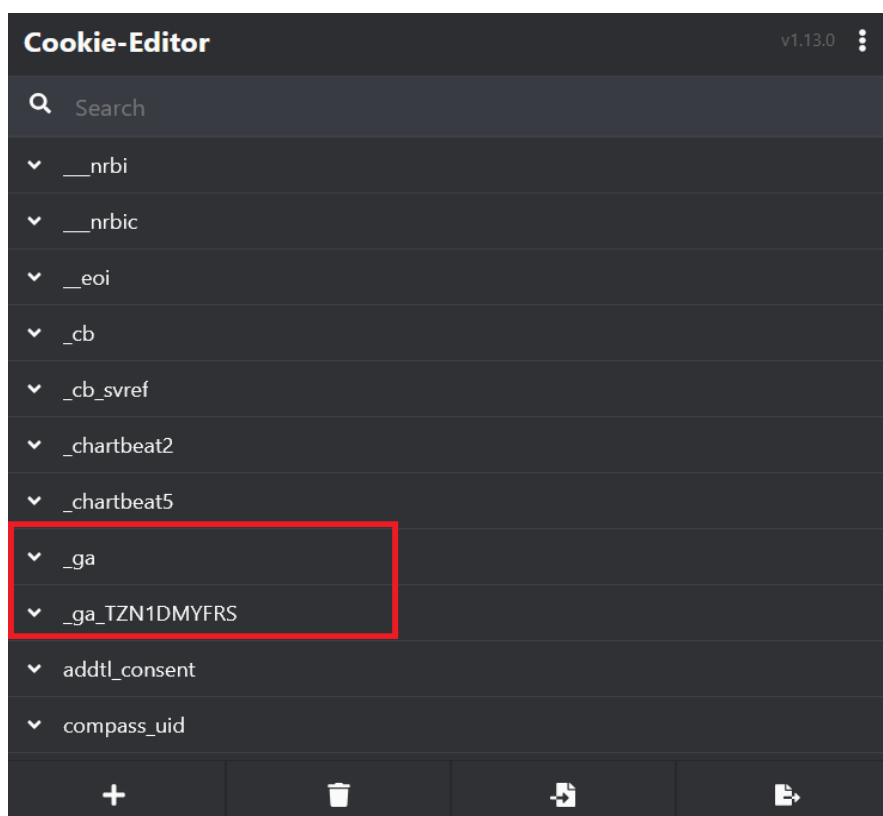


Figure 54: Cookie-Editor Output - tovima.gr with Accept All option

Clearly, the list is different. The highlighted cookies are well-known cookies called `_ga`, which stands for “Google Analytics”, these are by no means necessary cookies, and they are used for advertising and tracking purposes. Now this is completely expected and does not indicate a violation, since consent has been given. However, even if we now select to revoke consent, these cookies still remain on the browser. This indicates another possible violation.

In conclusion, although this analysis was limited, there were clear indications suggesting potential violations and digress from best practices, like:

1. **Incorrectly assigned labels**
2. **Non-necessary cookies remain after revoking consent.**

6.2.7 Case Study 3: www.public.gr

Public.gr is an online e-shop based in Greece that offers a wide range of products, just like plaisio.gr and is considered one of the leading online retailers in the country. Starting the analysis, the ImmuniWeb scan is triggered and after a couple of minutes the report is generated. The main findings are shown below.

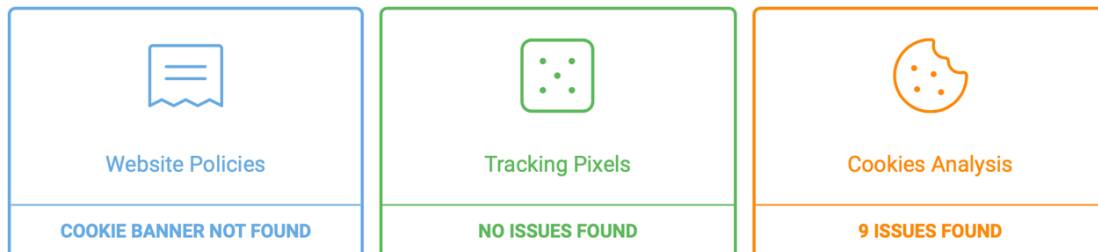


Figure 55: ImmuniWeb Scan - public.gr (1/4)

Taking a closer look into the Website Policies section of the report, these are the findings:

Privacy Policy was found on the website	Good configuration
Cookie Consent Banner was not found on the website	Information
The copyright notice is up-to-date: © 2023 Public Retail S	Good configuration

Figure 56: ImmuniWeb Scan - public.gr (2/4)

As shown, while there is a privacy policy and an up-to-date copyright notice, there is no cookie consent banner detected on the website. The absence of a cookie banner is not in alignment with best practices, indicating a failure to adhere to established guidelines. Also, there are no tracking pixels detected; therefore, we directly jump to the Cookie Analysis section of the report.

First-Party Cookies

There are 9 first-party cookies without a Secure flag					Misconfiguration or weakness		
There are 6 first-party cookies without an HttpOnly flag					Misconfiguration or weakness		
Name	Value	Domain	Path	Expires	Samesite	Secure	HttpOnly
language	el-GR	www.public.gr	/public/v1/	Nov 11th, 2025		No	No
language	el-GR	www.public.gr	/rest/	Nov 11th, 2025		No	No

Figure 57: ImmuniWeb Scan - public.gr (3/4)

Third-Party Cookies



Figure 58: ImmuniWeb Scan - public.gr (4/4)

While the main emphasis regarding cookies is given on the CookieYes report, the image above shows that there are no third-party cookies, which is a sign of good configuration regarding user privacy.

The part of the analysis is the CookieYes scan. All the findings generated are presented below.

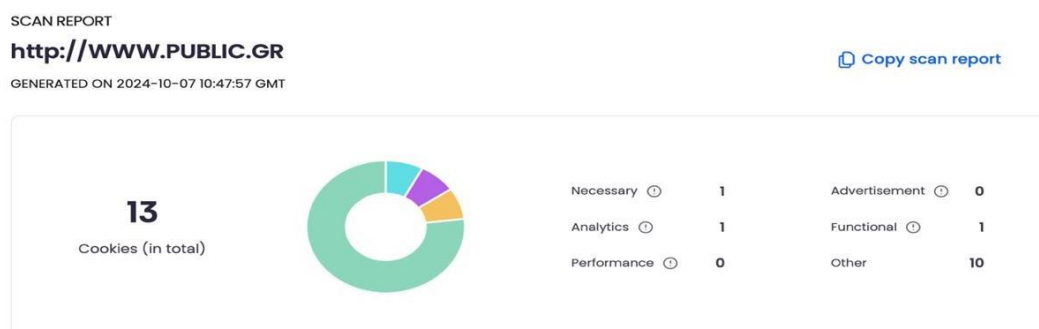


Figure 59: CookieYes Scan public.gr

There are 13 cookies detected, including one necessary cookie. The cookies along with their details and description are listed on the table below.

Table 6: Cookies Detected - public.gr

<u>Cookie</u>	<u>Description</u>	<u>Duration</u>	<u>Type</u>
language	This cookie is used to store the language preference of the user.	1 year 1 month 4 days	Functional
RT	"Akamai Boomerang set this cookie which gauges visitor experience with page load times	7 days	Analytics
DYN_USER_ID	No description available.	6 months	Other
DYN_USER_CONFIRM	No description available.	6 months	Other

JSESSIONID	The JSESSIONID cookie is used by New Relic to store a session identifier so that New Relic can monitor session counts for an application.	7 days	Necessary
J2ROUTE	No description available.	session	Other
8348568911_oc	No description available.	1 year	Other
CITRUS_AD_ID	No description available.	session	Other
klarna_sdk_version	never	never	Other
cart_id	No description available.	never	Other
ATG_profile_id	No description available.	never	Other
klarna_sdk_default_config	No description available.	session	Other
klarna_sdk_identity_api	No description.	session	Other

Now that all the results from the scanning tools are collected, the next step is to visit the website and perform dynamic analysis to verify the results and to dive deeper into the analysis.

By visiting the website, the first thing that is encountered is a cookie banner, as shown on the image below.

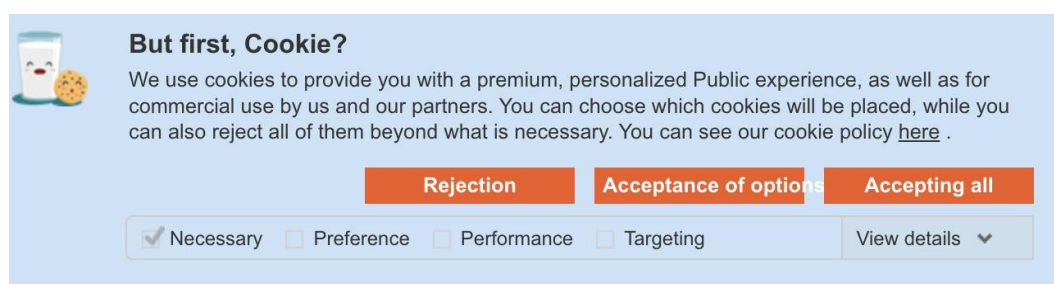


Figure 60: Overview of public.gr Cookie Banner

However, the ImmuniWeb scanning tool claimed that there was no cookie banner on the website, therefore providing a false result. This could be happening for a few reasons. For example, some websites only display cookie banners after specific interactions like clicking and scrolling or they are JavaScript dependent, which the scanning tool may not trigger. Thus, scanning tools have many limitations and flaws, that is why in this study they are combined with manual verification to ensure a higher level of accuracy.

Now let's examine the cookie banner itself. This cookie banner is almost identical to the one shown on the case study 1, meaning it is well and clearly structured and no "dark" practices are implemented.

The next step involves the cookie examination, to ensure that there are no policy violations, based on the evaluation framework that was set. By clicking the "View Details" option the following information is displayed on the banner.

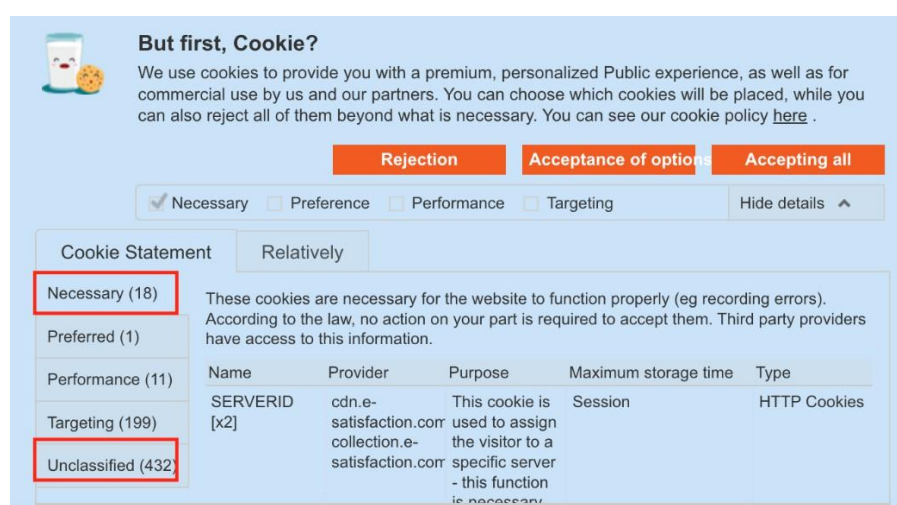


Figure 61: Expanded Cookie Banner - public.gr

The results are significantly different from those from case study 1. Firstly, there is a smaller number of necessary cookies, specifically 18, meaning that there is a lower risk for the presence of cookies with incorrectly assigned labels. Navigating through the "Necessary" list the only cookie that is debatable regarding its purpose is **RT (s.gom-pulse.net)**, which is used for identifying visitors through applications like LinkedIn for login purposes. This cookie could be listed as a functionality cookie, however this by no means indicates a clear violation. On the contrary, on the bottom left corner of the cookie banner, it is clearly stated that there are 432 unclassified cookies, which indicates a policy violation.

The last thing to check for are undeclared cookies, meaning cookies that the scanning tool detected, but are not listed on the website. Based on the CookieYes scan the **8348568911_oc** was found during the website scan, however it is not listed inside in any of the categories of the cookie banner. There is no description for this cookie in any

database, therefore it cannot be verified if this is just a misconfiguration or if it is done with malicious intent. However, it still indicates a possible violation.

In summary, while meeting most of the standards set in this study for ensuring compliance, the following flaws were detected:

1. **Unclassified Cookies**
2. **Undeclared Cookies**

6.2.8 Case study 4: www.notos.gr

In this case, the study targets the official website of Notos, a Greek department store chain that offers a wide variety of products, including fashion items, beauty products. Once again, following the standard operating procedure the, the ImmuniWeb privacy scan is initiated, generating the following result.

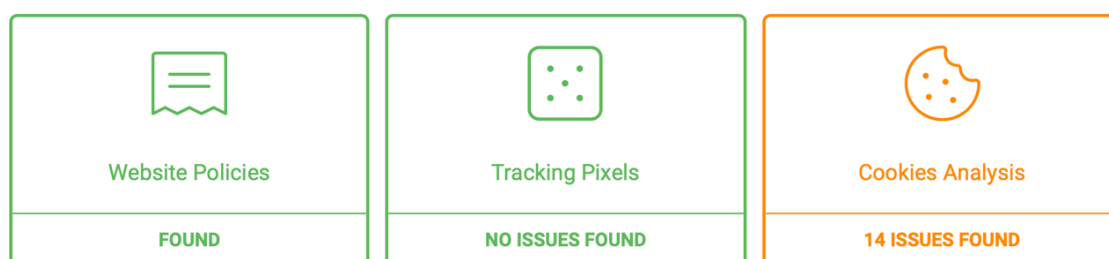


Figure 62: ImmuniWeb Scan - notos.gr (1/4)

By expanding the “Website Policies” category, the following results are displayed.

Privacy Policy was found on the website	Good configuration
Cookie Consent Banner was found on the website	Good configuration
No copyright information found on the website	Misconfiguration or weakness

Figure 63: ImmuniWeb Scan - notos.gr (2/4)

The scanning tool detected both the presence of a privacy policy and a cookie consent banner on the website, along with no tracking pixels, however there was absence of copyright information.

In terms of cookies a portion of the collected information is presented below.

First-Party Cookies

There are 5 first-party cookies without a Secure flag						Misconfiguration or weakness	
There are 6 first-party cookies without an HttpOnly flag						Misconfiguration or weakness	
Name	Value	Domain	Path	Expires	SameSite	Secure	HttpOnly
Netvolu ... ore_SID	69779264- dd34 ... - f7d4c35550c 8	www.notos.gr	/	Oct 7th, 2025		No	No
_clk	14zf10f%7C2 %7 ... pt%7C0%7C1 741	.notos.gr	/	Oct 7th, 2025		No	No

Figure 64: ImmuniWeb Scan - notos.gr (3/4)

Third-Party Cookies

3 Cookies c.clarity.ms [United States] 							
All third-party cookies have a Secure flag						Good configuration	
There are 3 third-party cookies without an HttpOnly flag						Misconfiguration or weakness	
There are no third-party cookies with an expiration time exceeding 3 months						Good configuration	
Name	Value	Domain	Path	Expires	SameSite	Secure	HttpOnly
SM	C	.c.clarity.ms	/	Immediately	None	Yes	No
MR	0	.c.clarity.ms	/	Oct 14th, 2024	None	Yes	No

Figure 65: ImmuniWeb Scan - notos.gr (4/4)

There were many third-party cookies detected, which indicates poor privacy configuration, however as already mentioned, most browsers block third-party cookies by default. Therefore, no extra analysis in towards that direction is required.

Continuing the analysis, the results of the CookieYes scan are shown below.

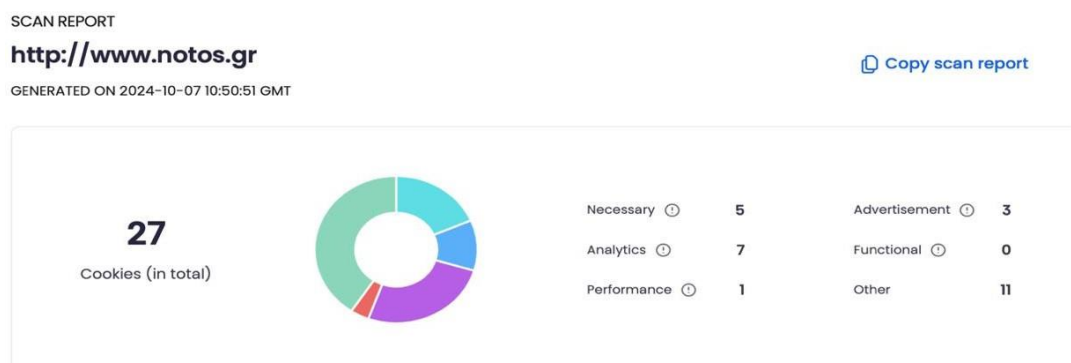


Figure 66: CookieYes Scan - notos.gr

Table 7: Cookies Detected - notos.gr

<u>Cookie</u>	<u>Description</u>	<u>Duration</u>	<u>Type</u>
Netvolution_eStore_SID	No description available.	1 year	Other
Visid_incap_*	Incapsula sets this cookie to provide cloud-based website security services.	1 year	Necessary
nibi_*	The Hotels Network sets this cookie to improve security and provide load-balancing to ensure that a client's requests are sent to the same origin server	session	Necessary
incap_ses*	This is an Incapsula DDoS Protection and Web Application Firewall cookie that is used to relate HTTP requests to a certain session.	session	Necessary
Visid_incap_*	Incapsula sets this cookie to provide cloud-based	1 year	Necessary

	website security services.		
__utmv	s installed by Google Analytics to gather data on the user's site usage.	1 year	Analytics
CLID	Microsoft Clarity set this cookie to store information about how visitors interact with the website	1 year	Analytics
_clk	Microsoft Clarity sets this cookie to retain the browser's Clarity User ID and settings exclusive to that website.	1 year	Analytics
Ds.sessionID	No description available.	session	Other
Ds.anonymousUserid	No description available.	1 year	Other
_clsk	Microsoft Clarity sets this cookie to store and consolidate a user's pageviews into a single session recording.	1 day	Analytics
MUID	Microsoft Bing sets this	1 year 24 days	Advertisement

	cookie to identify unique web browsers visiting Microsoft sites.		
MR	This cookie, set by Bing, is used to collect user information for analytics purposes.	7 days	Analytics
ANOICLK	set by Bing, is used to store a user's session ID and verify the clicks from ads on the Bing search engine.	10 minutes	Advertisement
User	No description available.	Never	Other
Wishlist	No description available.	Never	Other
Cart	No description available.	Never	Other
listStorage	No description available.	Never	Other
User.timestamp	No description available.	Never	Other
Cart.Timestamp	No description available.	Never	Other
Wishlist.timestamp	No description available.	Never	Other

__ctlk	No description available	session	Other
--------	--------------------------	---------	-------

After collecting all the data, the dynamic analysis of the website takes place. By visiting the website, the first thing that is encountered, is the following cookie banner.

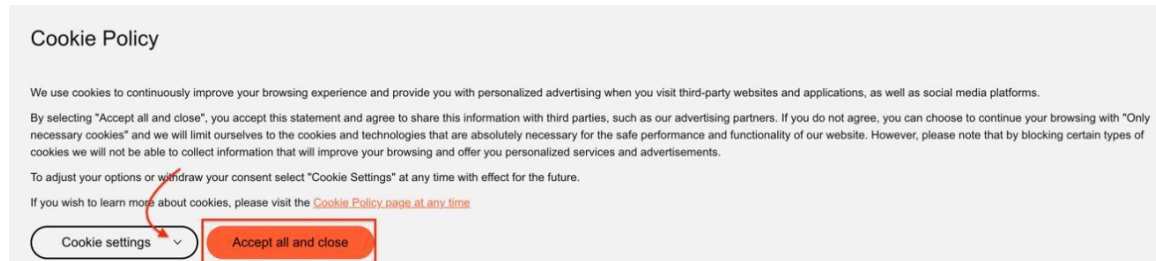


Figure 67: Cookie Banner Overview - notos.gr

Since there is a cookie banner, the ImmuniWeb claim is verified. However, there are some serious flaws with this banner. Firstly, the highlighted box, saying “Accept all and Close” is painted orange to stand out from the left option, which is “Cookie settings”. Also, there is no direct choice to reject all the cookies. By interacting with the banner and click the arrow option in the picture the following information is displayed on the screen.

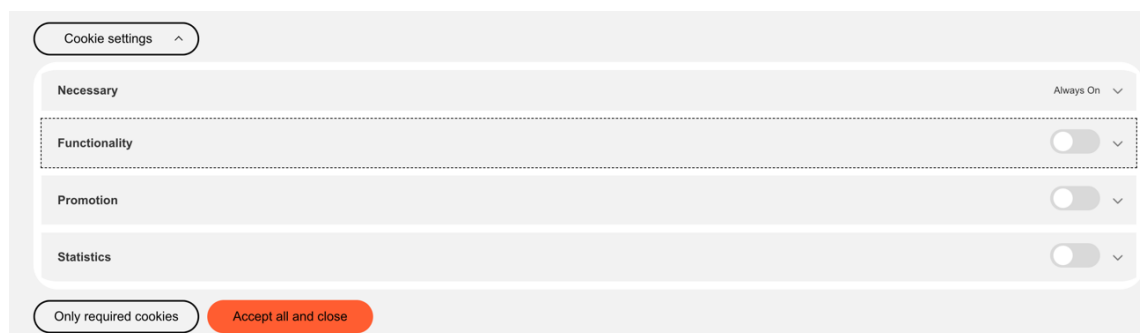


Figure 68: Extended Cookie Banner - notos.gr (1/2)

This time there is an option to accept select “Only required cookies”. These deceptive techniques can push users to inadvertently accept more cookies than necessary, compromising their privacy and are a strong indication of a possible violation.

What is next, is the cookie direct cookie examination. Based on the previous image, there are no unclassified cookies. The next parameter to check for are cookies with incorrect labels. By clicking expanding the “Necessary “category the following list is displayed.

Cookie name	Cookie Description	Provider	Cookie Expiration
visid_incap_*	Preserves user's states across page requests to improve performance of the website.	atcom.gr	Session
incap_ses_*	Preserves user's states across page requests to improve performance of the website.	atcom.gr	Session
Netvolution_eStore_SID	Netvolution based cookies. It is used in order to save user's actions, such as "add to basket" selection	www.notos.gr	Session
FrontendManagedAccount_Id	FrontEndManagedAccount_Id	www.notos.gr	Session
RegistrationForm_Id	RegistrationForm_Id	www.notos.gr	Session
GiftCardSessionID	Netvolution based cookies	www.notos.gr	Session
sessionId	A session ID is a unique number assigned to a specific user for the duration of that user's visit (session)	www.notos.gr	Session
Netvolution_AnonymousId	An anonymous ID is a unique and anonymous value assigned to a visitor on each visit	www.notos.gr	Session
lkws_12471	A sessionStorage item to mark an affiliation source	www.notos.gr	Session
cpab		notos.gr	1 Year
SplitTest_navment	A Cookie for split test navment sets	www.notos.gr	1 Days

Figure 69: Figure 68: Extended Cookie Banner - notos.gr (2/2)

What stands out from the list is the **cpab** named cookie, which is the only one without a description.

Cookies Search Results: cpab

About this cookie:

There is not yet any general information about this cookie based on its name only. If you have any information about this cookie, [please get in touch](#).

The main purpose of this cookie is: **Unknown**

Key numbers for cpab:

Cookies with this name have been found on **41** websites, set by **45** host domains.

It has been found as a **First Party** cookie on **43** websites and a **Third Party** cookie on **11** websites.

It has been found as a **Persistent** cookie on **54** websites, with an average life span of **364** days.

It has been found as a **Session** cookie on **0** websites.

Figure 70: cpab Searched on cookiepedia

Searching the Cookiepedia database no clear description was found; however, it seems that is mainly used for advertising and user tracking. Thus, there is a high chance that this cookie is assigned with an incorrect label.

Moving forward, a check is performed to determine if there are any undeclared cookies. By comparing the CookieYes scan results with the list provided by the website, several undeclared cookies are detected for example **MUID**, which is used for targeted advertising based on both CookieYes and Cookiepedia.

This analysis detected the following possible violations:

1. **Undeclared cookies**
2. **Incorrectly assigned labels**
3. **Cookie banner “dark” practices**

6.2.9 Case Study 5: www.atticadps.gr

Attica is another popular retail store in Greece, mainly selling fashion related items. Starting with the ImmuniWeb scans, the results are presented below.

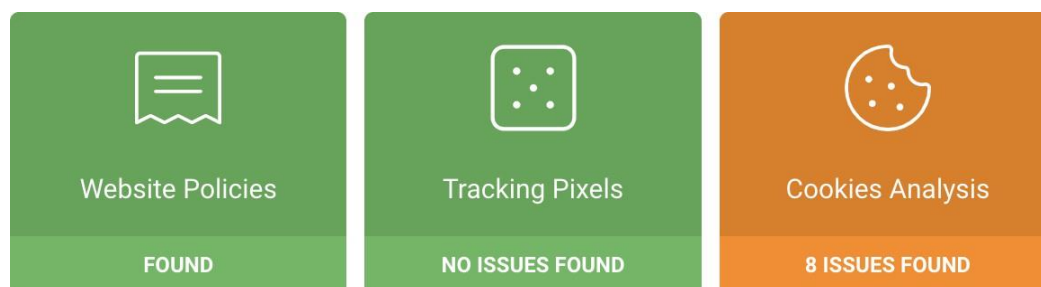


Figure 71: ImmuniWeb Scan - atticadps.gr (1/4)

Navigating through the “Website Policies” category, the following information is found in the report.

Privacy Policy was found on the website	Good configuration
Cookie Consent Banner was found on the website	Good configuration
The copyright notice is up-to-date: © 2024 attica	Good configuration

Figure 72: ImmuniWeb Scan - atticadps.gr (2/4)

Based on this information there are no flaws in terms of website policies or tracking pixels and most importantly a cookie banner is detected.

Regarding cookies, the scanning tool generated the following.

First-Party Cookies							
There are 7 first-party cookies without a Secure flag						Misconfiguration or weakness	
There are 7 first-party cookies without an HttpOnly flag						Misconfiguration or weakness	
Name	Value	Domain	Path	Expires	Samesite	Secure	HttpOnly
_gcl_au	1.1.299547748.1728809745	.atticadps.gr	/	Jan 11th, 2025		No	No
_ga	GA1.2.133868968.1728809745	.atticadps.gr	/	Nov 17th, 2025		No	No

Figure 73: ImmuniWeb Scan - atticadps.gr (3/4)

Third-Party Cookies	
+ 2 Cookies	atcom.gr [Greece] 🇬🇷
+ 1 Cookie	cookiemon-analytics.azurewebsites.net [The Netherlands] 🇳🇱

Figure 74: ImmuniWeb Scan - atticadps.gr (4/4)

Moving on, the CookieYes scanning tool results are displayed below.

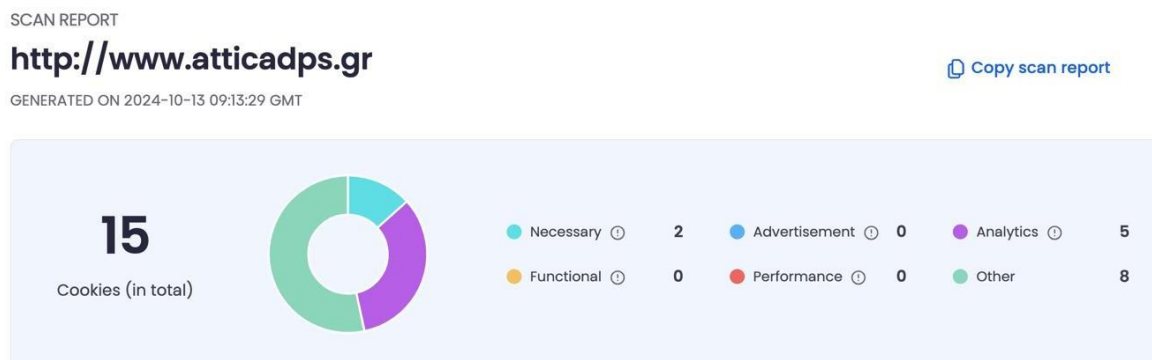


Figure 75: CookieYes Scan - atticadps.gr

Table 8: Cookies Detected on atticadps.gr

Cookie	Description	Duration	Type
Visid_incap_*	Incapsula sets this cookie to provide cloud-based website security services.	1 year	Neccesary
Incap_ses_*	DDoS Protection and Web Application Firewall cookie that is used to relate HTTP requests to a certain session.	session	Necessary
_glc_au	Google Tag Manager sets this cookie to experiment advertisement efficiency of websites using their services.	3 months	Analytics
_ga	Google Analytics, calculates visitor, session and campaign data and keeps track of site usage for the site's analytics report. T	1 year 1 month and 4 days	Analytics
_gid	Google Analytics, _gid cookie stores information on how visitors use a website, while also creating an analytics report of the website's performance. provide cloud-based website security services.	1 day	Analytics
_gat_UA	Google analytics user behaviour tracking	1 minute	Analytics
Netvolution_estore_SID	No description available	1 year	Other
_uid	This is a Google UserID cookie that tracks users across various website segments.	1 year 1 month 4 days	Analytics
sessioniid	No description available.	1 day	Other

Cart	No description available.	Never	Other
User.timestamp	No description available.	Never	Other
User	No description available.	Never	Other
Cart.timestamp	No description available.	Never	Other
Wishlist	No description available.	Never	other
Wishlist.timestamp	No description available.	Never	Other

As always, the last step involves the dynamic analysis of the website. Let's first examine the cookie banner.

COOKIE POLICY

We use cookies to make our site work properly, personalize content and ads, provide social media features and analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners. Read the Cookies Policy



Figure 76: Cookie Banner Overview - atticadps.gr

In contrast to the previous case, the cookie banner is correctly configured and there is nothing indicating the use of “dark” practices. Specifically, both options “Reject all” and “Accept and close” are clearly listed and highlighted in the same manner.

After those steps, the cookie analysis takes place. By clicking the “Cookie settings” button the cookie banner is expanded, displaying the following information.

COOKIE POLICY

We use cookies to make our site work properly, personalize content and ads, provide social media features and analyze our traffic. We also share information about your use of our site with our social media, advertising and analytics partners. Read the Cookies Policy



Figure 77: Expanded Cookie Banner - atticadps.gr (1/2)

First, there are no unclassified cookies. Secondly, to check for cookies with incorrectly assigned labels, the “Strictly necessary cookies” section is expanded.

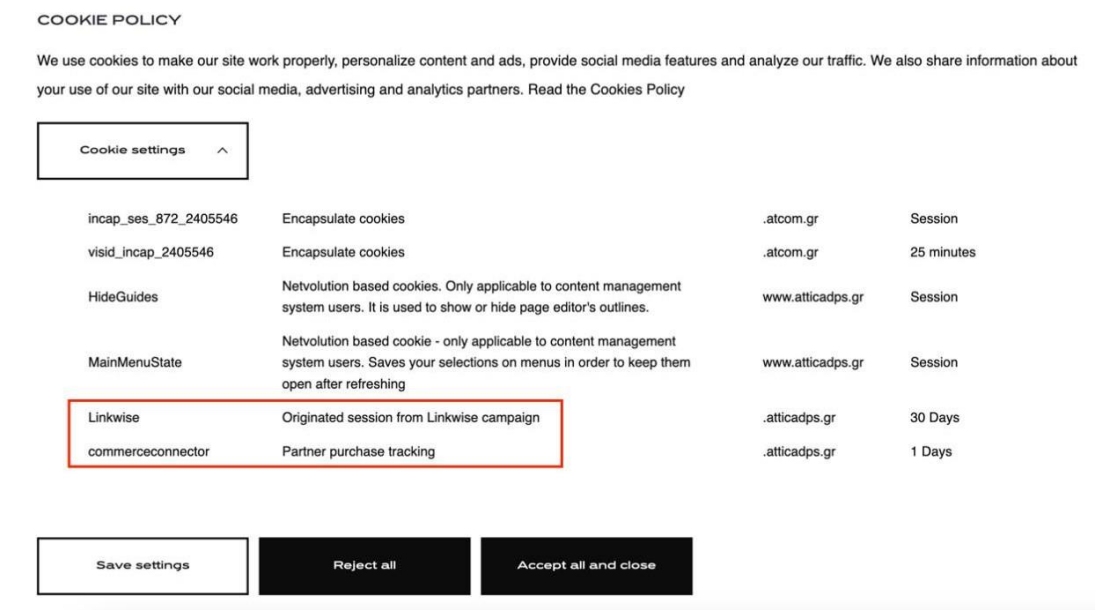


Figure 78: Expanded Cookie Banner - atticadps.gr (1/2)

The two highlighted cookies raise suspicions, especially **Linkwise**, which is used for tracking sessions from a Linkwise campaign, which seems related to affiliate marketing or advertising. Such cookies are typically categorized under marketing or tracking, not necessary. Therefore, there is a strong indication for cookies with a well-known purpose that have incorrectly assigned labels.

At last, before finishing the analysis of this website at final check is performed regarding undeclared cookies. The only cookies that were undeclared are the cookies **wishlist** and **wishlist.timestamp**. They were detected by the CookieYes scanner, however not listed on the website. They are mainly considered functionality cookies, however this still indicates a possible violation.

Finally, the user can revoke consent at any time, using the “cookie options” button, which as highlighted in the snapshot below.



Figure 79: Revoke Consent Option - atticadps.gr

In this case study, the following violations were detected:

- 1. Undeclared Cookies**
- 2. Incorrectly assigned Labels**

6.2.10 Case Study 6: www.kathimerini.gr

Kathimerini.gr is the online edition of the Greek newspaper *Kathimerini*. It is one of Greece's most widely read newspapers, mainly known for its political and business news coverage.

A few minutes after initiating the ImmuniWeb privacy scan, the report is generated containing the following results.

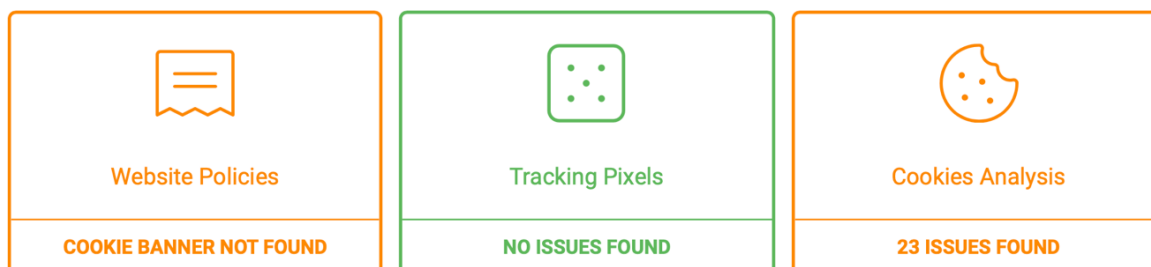


Figure 80: ImmuniWeb Scan - kathimerini.gr (1/4)

By inspecting the “Website Policies” category the following information is displayed.

Privacy Policy was found on the website	Good configuration
The website has third-party cookies and the cookie consent banner was not found	Misconfiguration or weakness
No copyright information found on the website	Misconfiguration or weakness

Figure 81: ImmuniWeb Scan - kathimerini.gr (2/4)

The scan did not detect a cookie consent banner nor copyright information. Moreover, no tracking pixels were found.

Regarding the cookies analysis, a portion of the results is displayed below.

First-Party Cookies

There are 13 first-party cookies without a Secure flag					Misconfiguration or weakness		
There are 21 first-party cookies without an HttpOnly flag					Misconfiguration or weakness		
Name	Value	Domain	Path	Expires	SameSite	Secure	HttpOnly
__tbc	%7Bkpex%7Dg1Z ...LNeAcPnSBh4kp	.kathimerini.gr /		Nov 11th, 2025	Lax	No	No
__pat	10800000	.kathimerini.gr /		Nov 6th, 2024	Lax	No	No

Figure 82: ImmuniWeb Scan - kathimerini.gr (3/4)

Third-Party Cookies



Figure 83: ImmuniWeb Scan - kathimerini.gr (4/4)

As shown, there are third-party cookies present on the website and 1 of them has an expiration period longer than 3 months, which indicates poor privacy configuration. In continuation of this analysis, the CookieYes scan is executed, generating the following results.

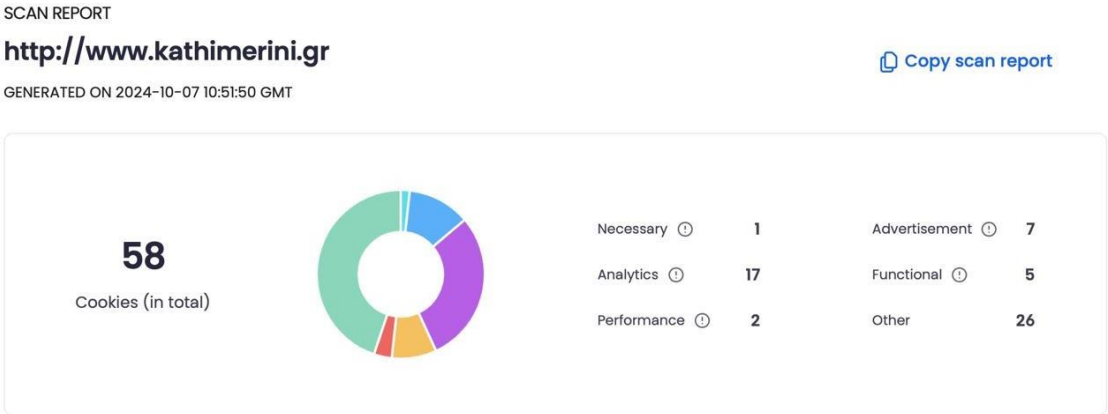


Figure 84: CookieYes Scan - kathimerini.gr

Table 9: Cookies Detected on kathimerini.gr

Cookie	Description	Duration	Type
__cf_bm	Used by Cloudflare for bot management	1 hour	Necessary
_pctx	No description available	1 year 1 month	Other

Evaluation of Websites with Respect to Security and Privacy Services

_pcid	No description available	1 year 1 month	Other
__tbc	Used for measuring the efficiency of advertisements by registering data on visitors from multiple sites	1 year 1 month 4 days	Advertisement
__pat	No description available	1 month	Other
__pvi	Used for implementing news content from other sites	1 day	Functional
xbc	Optimizes advertisements on the website by analyzing user behavior and interaction	1 year 1 month 4 days	Advertisement
g *	Google Analytics cookie for storing and counting page views	1 year 1 month 4 days	Analytics
_ga	Tracks visitor, session, and campaign data for site usage and analytics	1 year 1 month 4 days	Analytics
_cb	Set by Chartbeat, collects visitor IP address, geographical location, and navigation data	1 year 1 month	Analytics
_chartbeat2	Registers whether the user has visited the website before	1 year 1 month	Advertisement
_cb_svref	Stores the original referrer of the site visitor	1 hour	Analytics
pnespsdk_ssn	No description available	Session	Other

pnespsdk_visitor	No description available	1 year	Other
_cookie_test	No description available	1 minute	Other
cX_P	Used by Cxense for site-specific user sessions	1 year 1 month	Analytics
Gckp	Set by Cxense to build user profile information across sites in the Cxense network	1 year	Other
LANG	Set by LinkedIn for storing the user's preferred language	1 year 1 month 4 days	Functional
LANG_CHANGED	No description available	1 day	Other
_gid	Set by Google Analytics to store information on how visitors use the site	1 day	Analytics
_gat	Set by Google Universal Analytics to throttle request rate on high traffic sites	1 minute	Performance
gat_gtag_UA*	Set by Google Analytics to store unique user ID	1 minute	Analytics
_gat_pianoTracker	No description available	1 minute	Other
cX_G	Set by Cxense for storing a global ID, mapping different IDs into one	1 year 1 month	Functional
CLID	Set by Microsoft Clarity to store information about visitor interactions on the site	1 year	Analytics
_gcl_au	Set by Google Tag Manager to	3 months	Analytics

	test the efficiency of advertisements		
SM	Set by Microsoft Clarity to synchronize the MUID across Microsoft domains	Session	Analytics
MUID	Set by Microsoft Bing to identify unique web browsers across Microsoft sites	1 year 4 days	Advertisement
Lidc	Set by LinkedIn to facilitate data center selection	1 day	Functional
Bcookie	Set by LinkedIn to track the use of embedded services	1 year	Advertisement
li_gc	Set by LinkedIn to store visitor's consent regarding cookie usage for non-essential purposes	6 months	Functional
MR	Set by Bing to collect user information for analytics purposes	7 days	Analytics
SRM_B	Used by Microsoft Advertising as a unique ID for visitors	1 year 4 days	Performance
ANONCHK	Set by Bing for storing the user's session ID and verifying clicks from ads	10 minutes	Advertisement
_clk	Set by Microsoft Clarity to retain the browser's Clarity User ID and settings	1 year	Analytics

_fbp	Set by Facebook to store and track interactions	3 months	Analytics
_clk	Set by Microsoft Clarity to store and consolidate user's pageviews into a single session recording	1 day	Analytics
_gat_UA-*	Set by Google Analytics for user behavior tracking	1 minute	Analytics
_cb_svref_expires	Set by Chartbeat for webshop statistics	Never	Analytics
_cb_expires	No description available	Never	Other
_cX_atfr	No description available	Never	Other
__tp_gaAccount	No description available	Never	Other
gbc_consent	No description available	Never	Other
_chartbeat_expires	No description available	Never	Other
lastExternalReferrer	No description available	Never	Other
lastExternalReferrerTime	No description available	Never	Other
lucidsdkver	No description available	Never	Other
_ls_ttl	No description available	Never	Other
_cX_1stP1Time	No description available	Never	Other
CMPList	No description available	Never	Other
_ls_ttl	No description available	Never	Other
_cX_1st	No description available	Never	Other
_cX_S	No description available	Session	Other

_cltk	No description available	Session	Other
-------	--------------------------	---------	-------

After the successful scanning, the next step involves the dynamic analysis of the website. A snapshot of the website's front page is listed below.

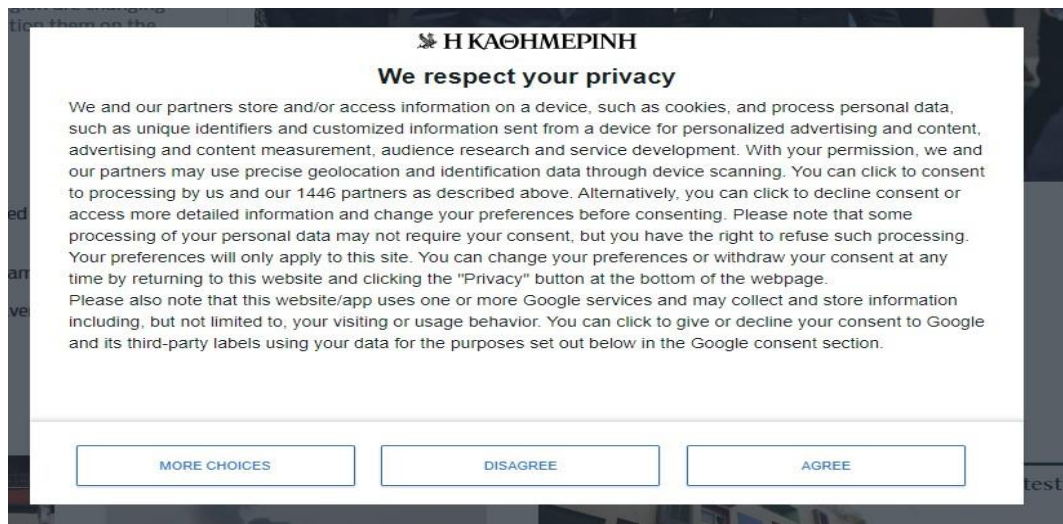


Figure 85: Cookie Banner Overview - kathimerini.gr

As shown, there is a cookie banner present on the website, therefore the ImmuniWeb scan result was false. The reasons why scanning tools, like ImmuniWeb may provide false results regarding cookie banners have already been explained in case study 3. So far, there is indication of “dark” practices used in this website, since every option is clearly and equally displayed. By clicking on the “More Choices” button, the cookie banner expands and provides the following information.

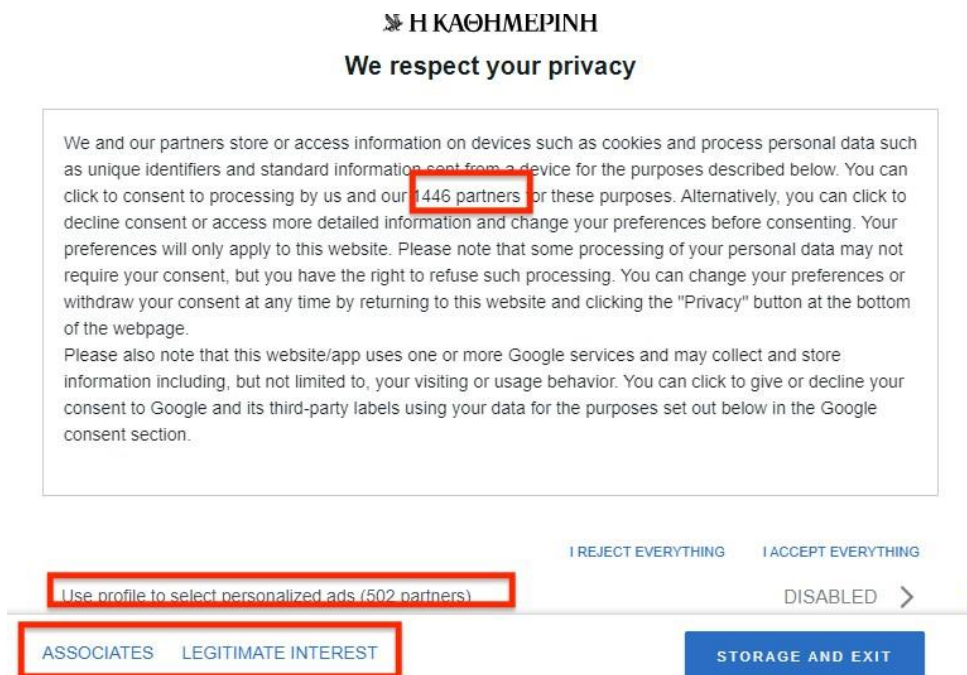


Figure 86: Expanded Cookie Banner - kathimerini.gr

This cookie banner is almost identical to the one examined in case study 2. As highlighted, there is large number of partners listed on cookie banner. However, if the

user tries to navigate through the banner and check for who they actually are it is almost impossible to do. This is an indirect indication of using “dark” practices to mislead and trick users into giving consent. Lastly, this cookie banner does not provide a detailed list of the cookies present on the website, just like in case study 2.

Since, there is no detailed list provided on the cookie banner, there is no way to check for undeclared or unclassified cookies and the analysis regarding cookies with incorrectly assigned labels is limited.

Proceeding with the final steps of this analyst, the website is revisited and the “Disagree” option is selected. Using the cookie-editor extension the following cookies are detected.

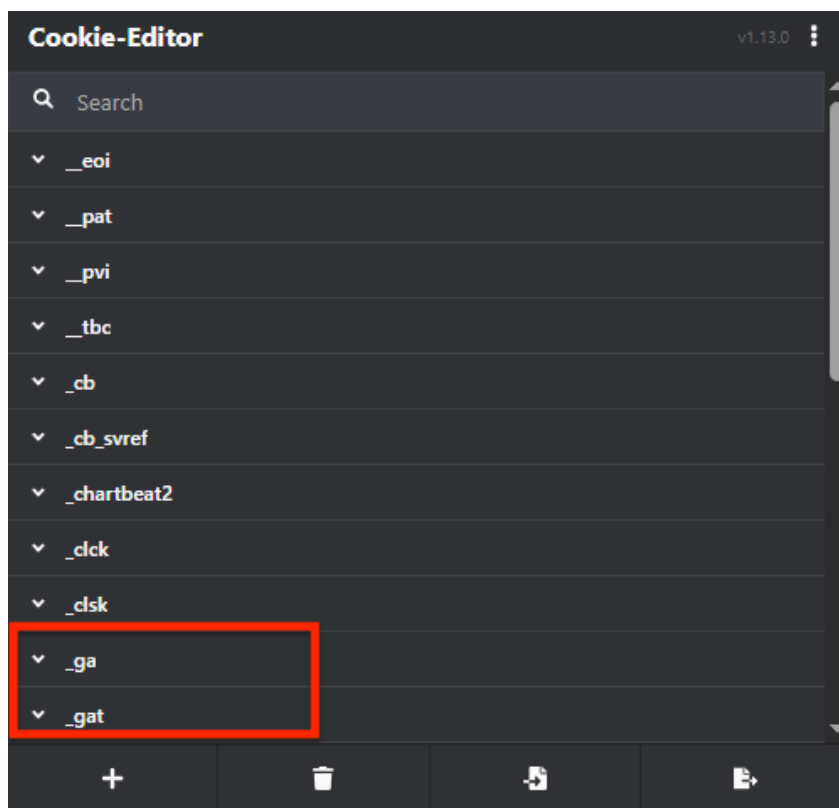


Figure 87: Cookie-editor Output - kathimerini.gr

This is just a fraction of cookies installed on the browser, after rejecting all non-necessary cookies. However, as highlighted on the pictures two cookies, namely **_ga** and **_gat** are detected by the cookie-editor extension. As already discussed, these are cookies with a well-known purpose, specifically google analytics cookies. This can also be verified by visiting the Cookiepedia database or by checking the previously listed table from the CookieYes scan. Such cookies are by no means strictly necessary and therefore should not be installed in the browser.

Summarizing, throughout this investigation the following violations have been detected.

1. Incorrectly assigned labels

6.2.11 Case Study 7: www.lifo.gr

LIFO is yet another news website in Greece. Once again, the website is scanned with the ImmuniWeb tool, which gives the following results.

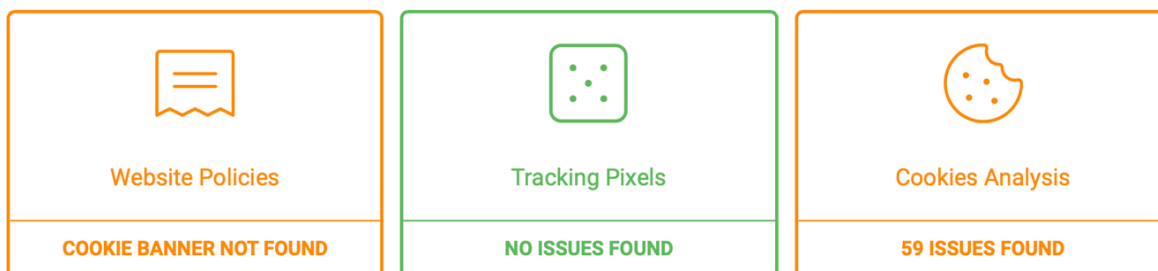


Figure 88: ImmuniWeb Scan - lifo.gr (1/4)

Expanding the “Website Policies” category, more details are presented.

Privacy Policy was found on the website	Good configuration
The website has third-party cookies and the cookie consent banner was not found	Misconfiguration or weakness
No copyright information found on the website	Misconfiguration or weakness

Figure 89: ImmuniWeb Scan - lifo.gr (2/4)

While privacy policy was found on the website and there were no issues with tracking pixels, the scan indicated two errors regarding the absence of the cookie banner and copy right information.

Furthermore, the cookies analysis found many third-party cookies, indicated poor privacy configuration. A portion of that report section is attached below.

First-Party Cookies

There are 16 first-party cookies without a Secure flag

Misconfiguration or weakness

There are 20 first-party cookies without an HttpOnly flag

Misconfiguration or weakness

Name	Value	Domain	Path	Expires	Samesite	Secure	HttpOnly
_gid	GA1.2.89560700.1728295457	.lifo.gr	/	Oct 8th, 2024		No	No
_gat	1	.lifo.gr	/	Oct 7th, 2024		No	No

Figure 90: ImmuniWeb Scan - lifo.gr (3/4)

Third-Party Cookies



Figure 91: ImmuniWeb Scan - lifo.gr (4/4)

Moving on with the analysis, the CookieYes report findings are listed below.

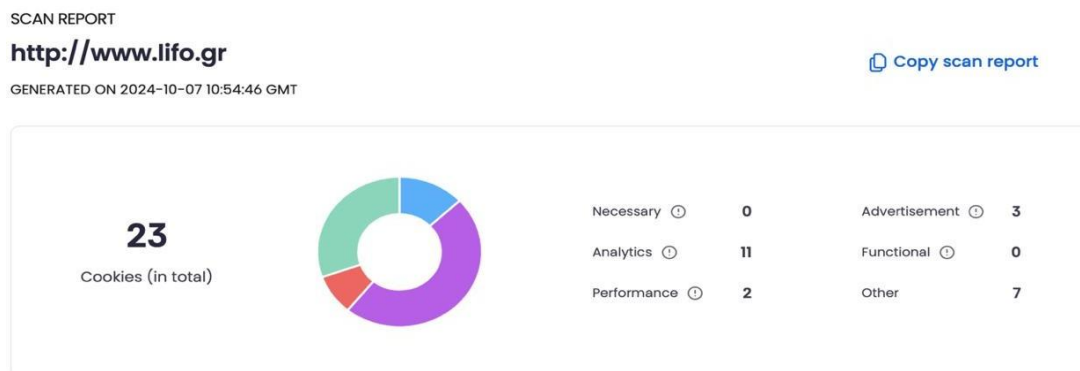


Figure 92: CookieYes Scan - lifo.gr

Table 10: Cookies Detected - lifo.gr

<u>Cookie</u>	<u>Description</u>	<u>Duration</u>	<u>Type</u>
_ga	Google Analytics cookie that calculates visitor, session, and campaign data for analytics purposes	1 year 1 month 4 days	Analytics
_gid	Google Analytics cookie that stores information on how visitors use the website	1 day	Analytics
_gat	Google Universal Analytics cookie to restrain request rate and limit data collection	1 minute	Performance
homevisible	No description available	3 months	Other
CLID	Set by Microsoft Clarity to store information about visitor interactions on the website	1 year	Analytics
_ga_*	Google Analytics cookie to store and count page views	1 year 1 month 4 days	Analytics
_clck	Set by Microsoft Clarity to retain browser's Clarity User ID and settings for future visits	1 year	Analytics
SM	Set by Microsoft Clarity for synchronizing MUID across Microsoft domains	Session	Analytics
MUID	Set by Microsoft Bing to identify unique web browsers visiting Microsoft sites	1 year 4 days	Advertisement

MR	Set by Bing to collect user information for analytics purposes	7 days	Analytics
SRM_B	Used by Microsoft Advertising as a unique ID for visitors	1 year 4 days	Performance
uid	Google UserID cookie that tracks users across various website segments	1 year 1 month 4 days	Analytics
sessionid	No description available	1 day	Other
exitIntentFlag	Used to record the user's intention to leave the page and tracks page views	Session	Analytics
ANONCHK	Set by Bing to store session ID and verify clicks from ads on the Bing search engine	10 minutes	Advertisement
_clsk	Set by Microsoft Clarity to store and consolidate user's pageviews into a single session recording	1 day	Analytics
msf_shown	No description available	7 days	Other
gbc_consent	No description available	Never	Other
CMPList	No description available	Never	Other
lp_visited	No description available	Never	Other
_cltk	No description available	Session	Other

After collecting the scan results, the next step is to perform the dynamic analysis of the website. The first thing that is encountered visiting the website is the cookie banner, as shown on the image below.

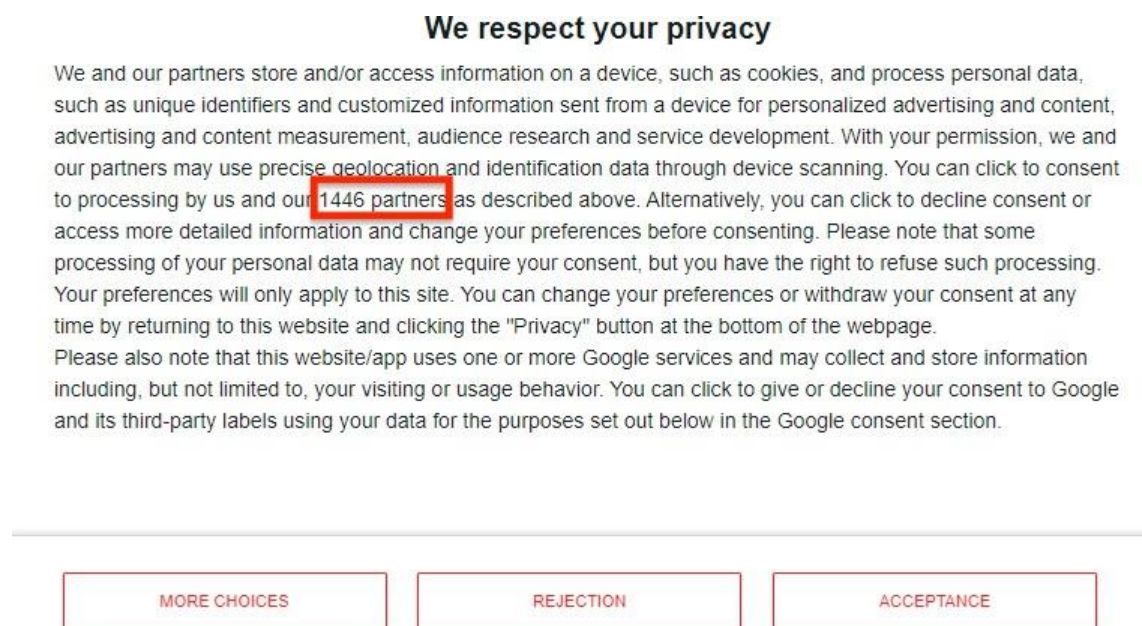


Figure 93: Cookie Banner Overview - lifo.gr

The first thing that needs to be mentioned is that the ImmuniWeb scan result is incorrect, since the website offers a cookie banner. The banner is identical to case studies 1 and 6, meaning that there is no use of direct “dark” practices, apart from the large number and listing of the 1446 partners that access user data, in case the user gives consent. By clicking the “More Choices”, the cookie banner expands providing more information as shown on the image below.

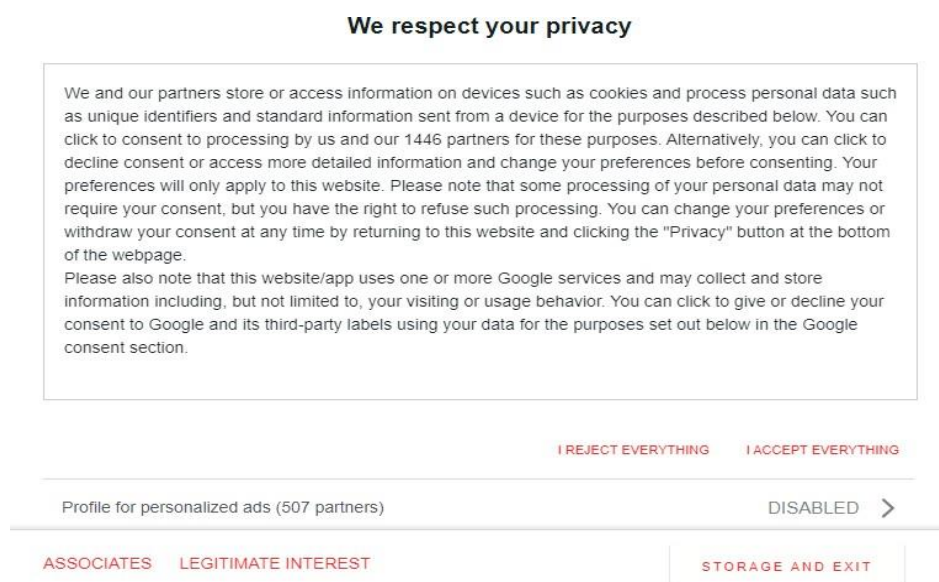


Figure 94: Expanded Cookie Banner - lifo.gr

Furthermore, the website does not provide a list, containing specific cookie information. This means, that there is no way to check for undeclared or unclassified cookies and the analysis regarding cookies with incorrectly assigned labels is limited.

Thus, to finish the investigation the “Rejection” option is selected, and the cookie-editor extension displays the following findings.

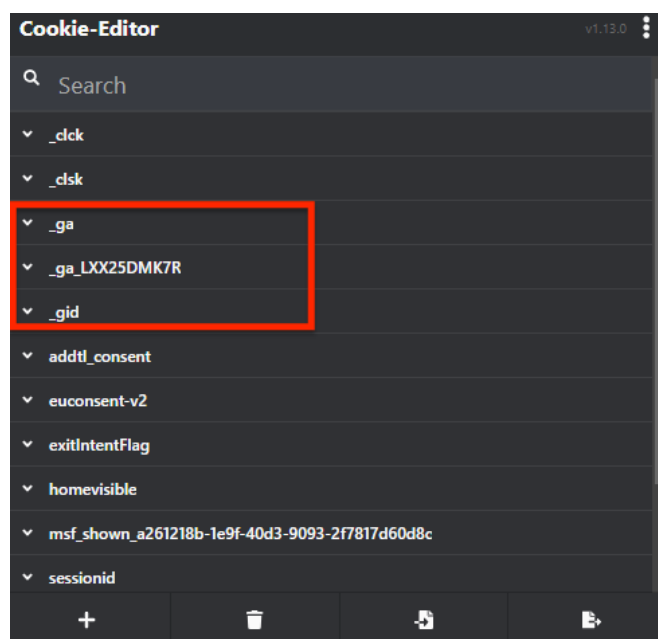


Figure 95: Cookie-editor Output - lifo.gr

The highlighted cookies are google analytics cookies, mainly used for advertising purposes and user tracking. This can be verified from both Cookipedia and the previously listed CookieYes findings. Since, the rejection option has been selected, only strictly necessary cookies should be installed. This is a violation, specifically a violation regarding cookies with incorrectly assigned labels. Finally, this website enables users to revoke consent by clicking the “Privacy” button that is shown on the bottom left side of the website, which when clicked reloads the cookie banner. For clarity a snapshot is presented below.

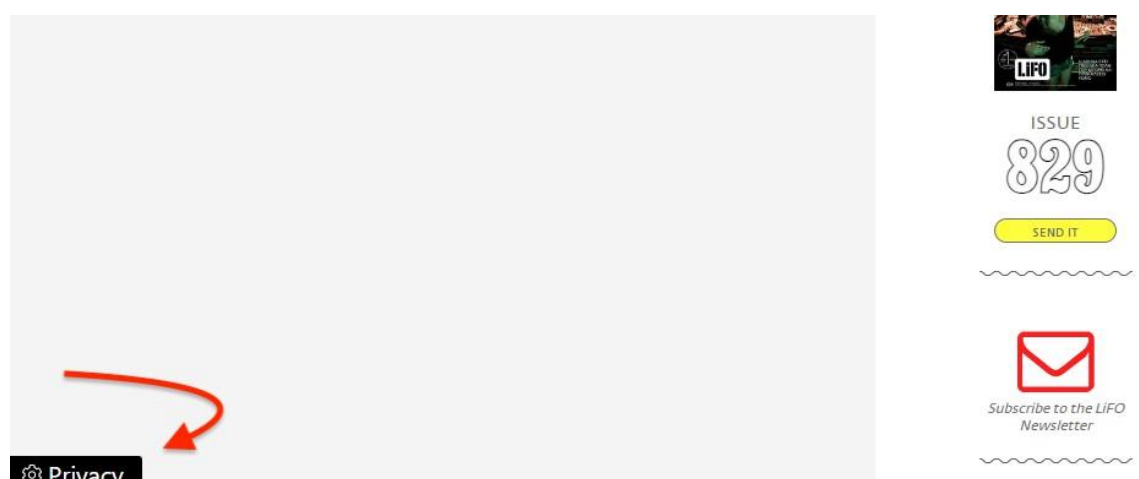


Figure 96: Revoke Consent Option - lifo.gr

In conclusion, the only policy violation detected in this website is the detection of cookies with **incorrectly assigned labels**.

6.2.12 Case study 8: www.cnn.gr

CNN.gr is the Greek edition of the international news network CNN (Cable News Network). It operates as a localized version of CNN, providing news and content tailored

specifically for Greek-speaking audiences. At first, the ImmuniWeb privacy scan is used, and its findings are listed below.

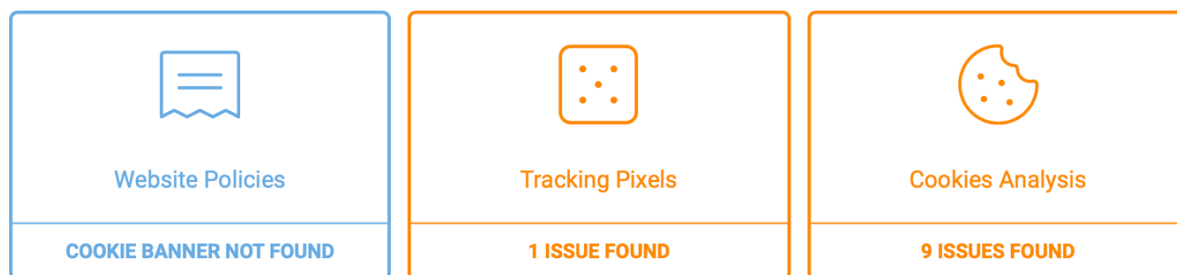


Figure 97: ImmuniWeb Scan - cnn.gr (1/4)

By digging deeper into the “Website Policies” section of the report, additional information is found.

Privacy Policy was found on the website	Good configuration
Cookie Consent Banner was not found on the website	Information
No copyright information found on the website	Misconfiguration or weakness

Figure 98: ImmuniWeb Scan - cnn.gr (2/4)

Based on the information provided, the website does not have a cookie banner, nor copy right information and also contains tracking pixels.

Next, the cookie analysis part of the report, is presented below.

First-Party Cookies

There are 6 first-party cookies without a Secure flag

Misconfiguration or weakness

There are 9 first-party cookies without an HttpOnly flag

Misconfiguration or weakness

Name	Value	Domain	Path	Expires	Samesite	Secure	HttpOnly
_ga_2XXPVV300L	GS1.1.1728295 ... 295978.60.0.0	.cnn.gr	/	Nov 11th, 2025		No	No
_ga_HRJMP4ZXT	GS1.1.1728295 ... 8295978.0.0.0	.cnn.gr	/	Nov 11th, 2025		No	No

Figure 99: ImmuniWeb Scan - cnn.gr (3/4)

Third-Party Cookies

There are no third-party cookies	Good configuration
----------------------------------	--------------------

Figure 100: ImmuniWeb Scan - cnn.gr (4/4)

There are no third-party cookies detected on the website, indicating good privacy configuration.

Continuing the analysis, the CookieYes scan collected the following additional information.

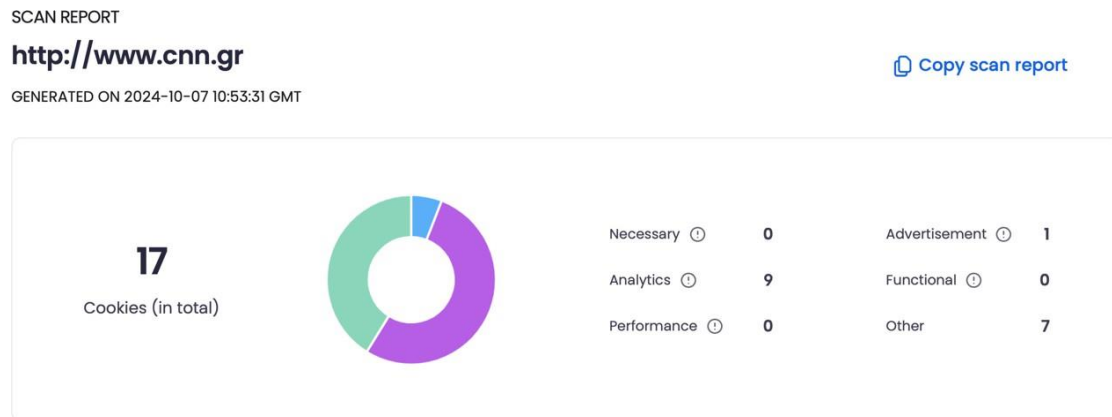


Figure 101: CookieYes Scan - cnn.gr

Table 11: Cookies Detected on cnn.gr

<u>Cookie</u>	<u>Description</u>	<u>Duration</u>	<u>Type</u>
_cb	Chartbeat sets this cookie to collect data like visitors' IP addresses, geographical locations, and website navigation	1 year 1 month	Analytics
_chartbeat2	Chartbeat sets this cookie to register whether the user has visited the website before	1 year 1 month	Advertisement
_cb_svref	Chartbeat sets this cookie to store the original referrer for this site visitor	1 hour	Analytics
_ga_*	Google Analytics sets this cookie to store and count page views	1 year 1 month 4 days	Analytics
_ga	Google Analytics cookie that calculates visitor,	1 year 1 month 4 days	Analytics

	session, and campaign data and keeps track of site usage		
_gid	Google Analytics cookie that stores information on how visitors use the website and creates a performance report	1 day	Analytics
_gat_gtag_UA_*	Google Analytics cookie to store a unique user ID	1 minute	Analytics
_fbp	Facebook sets this cookie to store and track interactions	3 months	Analytics
_cb_svref_expires	Chartbeat sets this cookie for webshop statistics	Never	Analytics
_cb_expires	No description available	Never	Other
_chartbeat_expires	No description available	Never	Other
lastExternalReferrer	No description available	Never	Other
lastExternalReferrerTime	No description available	Never	Other
CMPList	No description available	Never	Other
cleverpush-alert-shown	No description available	Session	Other
cleverpush-confirm-alert-reported	No description available	Session	Other

After the scanning, the dynamic analysis takes places by visiting the website. The website's frontpage is captured on the image below.

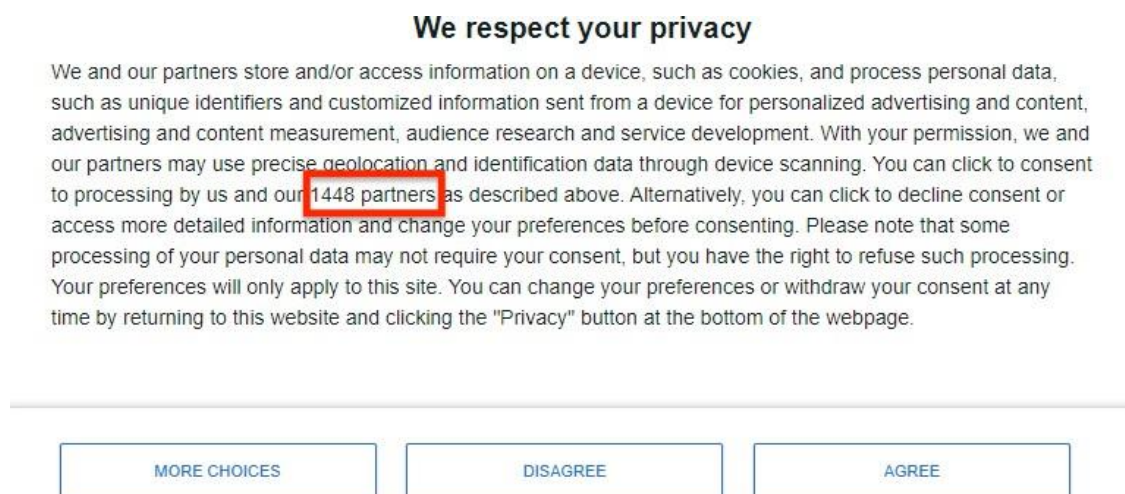


Figure 102: Cookie Banner Overview - cnn.gr

First, there is a cookie banner on the website, meaning that the ImmuniWeb scan failed to detect it. The reasoning behind the scan providing false result has been explained in case 3. Moreover, the banner is identical to use cases 2,6 and 7. The options are clearly listed and there is no strong indication of “dark” practices used to trick users into giving consent. By clicking the “More Choices” option, the cookie banner expands and provides additional information.

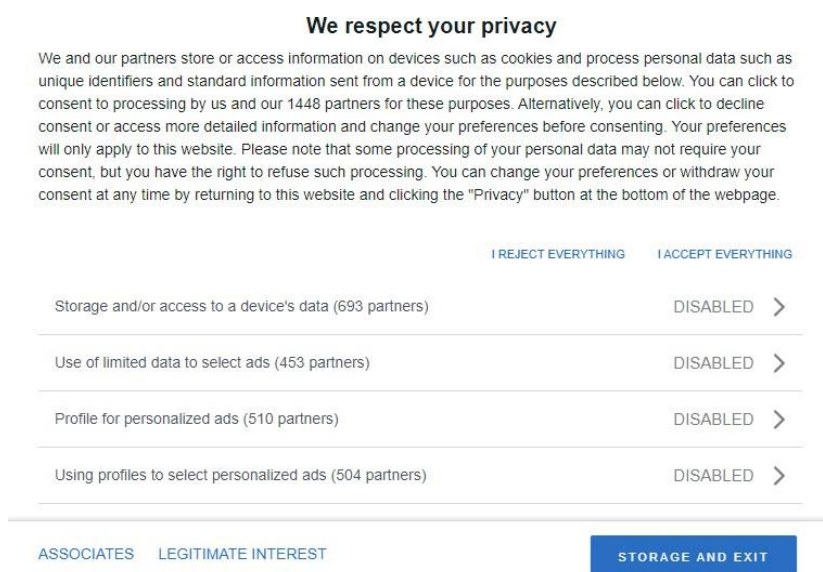


Figure 103: Expanded Cookie Banner - cnn.gr

Navigating through the options of the cookie banner, there is no cookie list to be found. Thus, there is no way to check for undeclared or unclassified cookies and the analysis regarding cookies with incorrectly assigned labels is limited.

To finish the analysis, the “Disagree” option is selected, and the cookie-editor captures the cookies that are displayed on the image below.

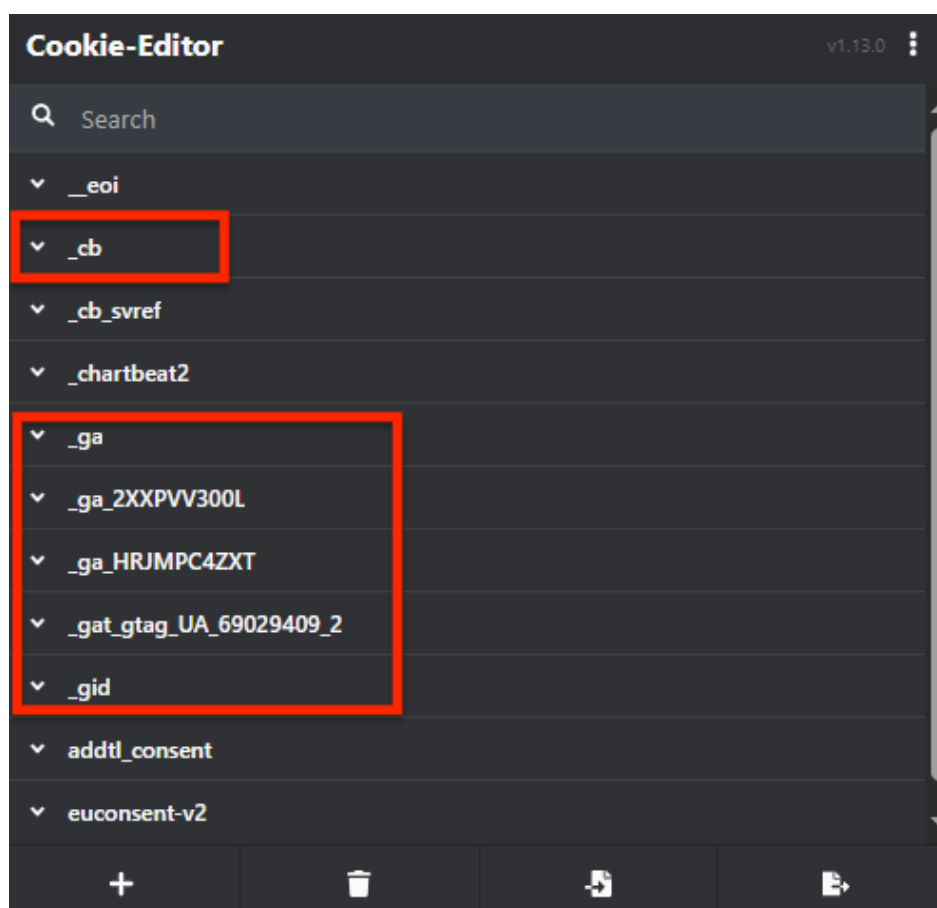


Figure 104: Cookie-editor Output - cnn.gr

As we can see, despite not giving consent for installing non-necessary cookies, the cookie-editor extension detected several cookies that are used for analytics and advertising. This can be verified from the CookieYes findings that were listed previously or the cookiepedia database. Thus, the website has cookies with incorrectly assigned labels.

Summarizing this analysis pointed out the following violations:

1. **Incorrectly assigned labels**

6.2.13 Case Study 9: www.protothema.gr

Protothema is the online version of the popular similarly named Greek newspaper. The ImmuniWeb scan results are listed below.

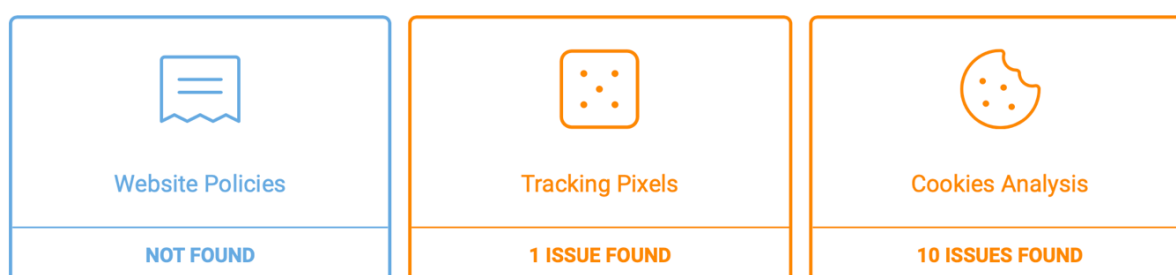


Figure 105: ImmuniWeb Scan - protothema.gr (1/4)

There are several issues listed inside the “Websites Policies” section.

Privacy Policy was not found on the website	Information
Cookie Consent Banner was not found on the website	Information
The copyright notice is up-to-date: © 2024	Good configuration

Figure 106: ImmuniWeb Scan - protothema.gr (2/4)

While the copyright notice is present and up to date, there is no privacy policy and cookie consent banner detected on the website. Also, there are issues related to tracking pixels on the website.

Moving on, the cookie analysis results are listed below.

First-Party Cookies

There are 7 first-party cookies without a Secure flag					Misconfiguration or weakness		
There are 10 first-party cookies without an HttpOnly flag					Misconfiguration or weakness		
Name	Value	Domain	Path	Expires	SameSite	Secure	HttpOnly
_gid	GA1.2.1829721134.1728295259	.protothema.gr	/	Oct 8th, 2024		No	No
_gat	1	.protothema.gr	/	Oct 7th, 2024		No	No

Figure 107: ImmuniWeb Scan - protothema.gr (3/4)

Third-Party Cookies

There are no third-party cookies	Good configuration
----------------------------------	--------------------

Figure 108: ImmuniWeb Scan - protothema.gr (4/4)

In this case, no third-party cookies were found, indicating good privacy configuration. Then, the CookieYes scanning tool is used, providing the following data.

SCAN REPORT

<http://www.protothema.gr>

GENERATED ON 2024-10-07 10:55:35 GMT

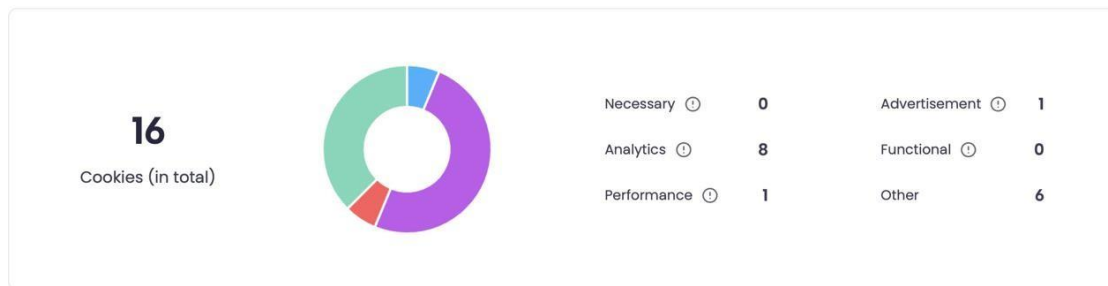
[Copy scan report](#)

Figure 109: CookieYes Scan - protothema.gr

Table 12: Cookies Detected on protothema.gr

<u>Cookie</u>	<u>Description</u>	<u>Duration</u>	<u>Type</u>
_ga	Google Analytics cookie that calculates visitor, session, and campaign data for analytics purposes	1 year 1 month 4 days	Analytics
_gid	Google Analytics cookie that stores information on how visitors use the website	1 day	Analytics
_gat	Google Universal Analytics cookie to restrain request rate and limit data collection	1 minute	Performance
_cb	Chartbeat sets this cookie to collect data like visitors' IP addresses, geographical locations, and website navigation	1 year 1 month	Analytics
_chartbeat2	Chartbeat sets this cookie to register whether the user has	1 year 1 month	Advertisement

	visited the website before		
_cb_svref	Chartbeat sets this cookie to store the original referrer for this site visitor	1 hour	Analytics
_ga_*	Google Analytics sets this cookie to store and count page views	1 year 1 month 4 days	Analytics
_gcl_au	Google Tag Manager sets this cookie to experiment with advertisement efficiency	3 months	Analytics
_fbp	Facebook sets this cookie to store and track interactions	3 months	Analytics
lastExternalReferrerTime	No description available	Never	Other
gbc_consent	No description available	Never	Other
CMPList	No description available	Never	Other
reconsent	No description available	Never	Other
lastExternalReferrer	No description available	Never	Other
ebx_webtag_	No description available	Session	Other

After collecting the result from the scanning operations, the last step is the dynamic analysis of the website. By visiting it the first thing that is displayed is the cookie banner, meaning that once again the ImmuniWeb privacy scan failed to detect it.

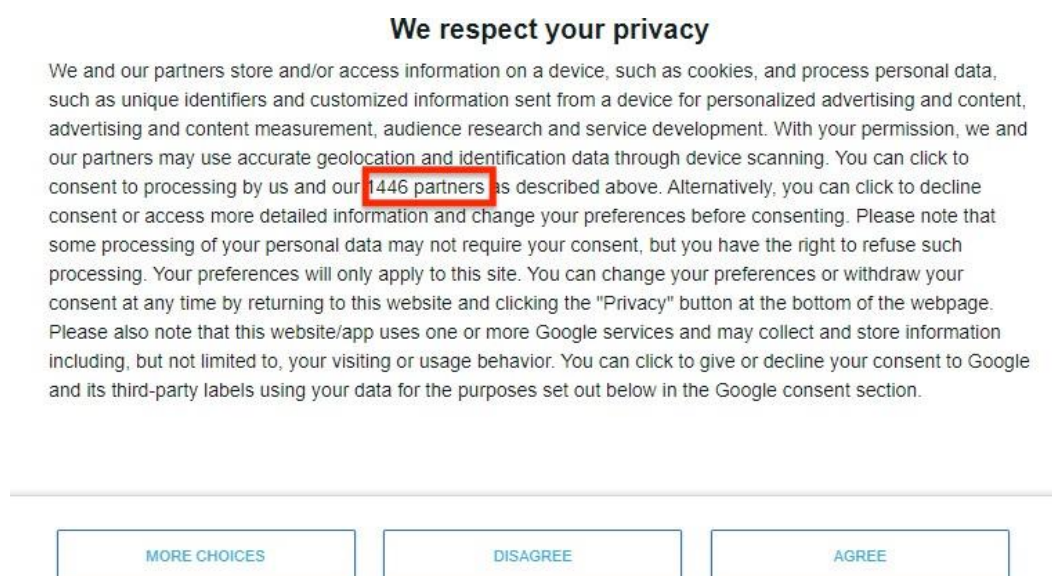


Figure 110: Cookie Banner Overview - protothema.gr

The cookie banner looks similar the all previously covered media-news websites. As a result, there is no significant use of “dark” practices in this case. By selecting “More Choices” the cookie banner is expanded as shown on the image below.

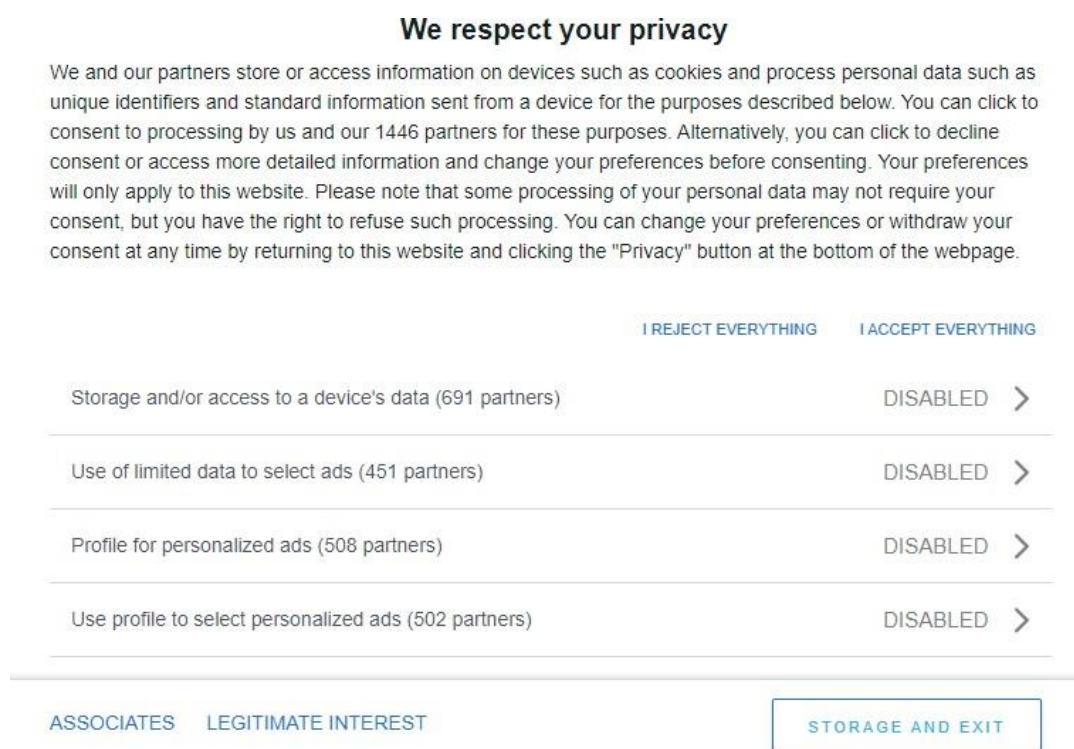


Figure 111: Expanded Cookie Banner – protothema.gr

Again there is no cookie list provided, resulting in no way to check for undeclared or unclassified cookies and making the analysis regarding cookies with incorrectly assigned labels limited.

Proceeding with the final part of the analysis, the “Disagree” option is selected. The following results are then extracted using the cookie-editor extension.

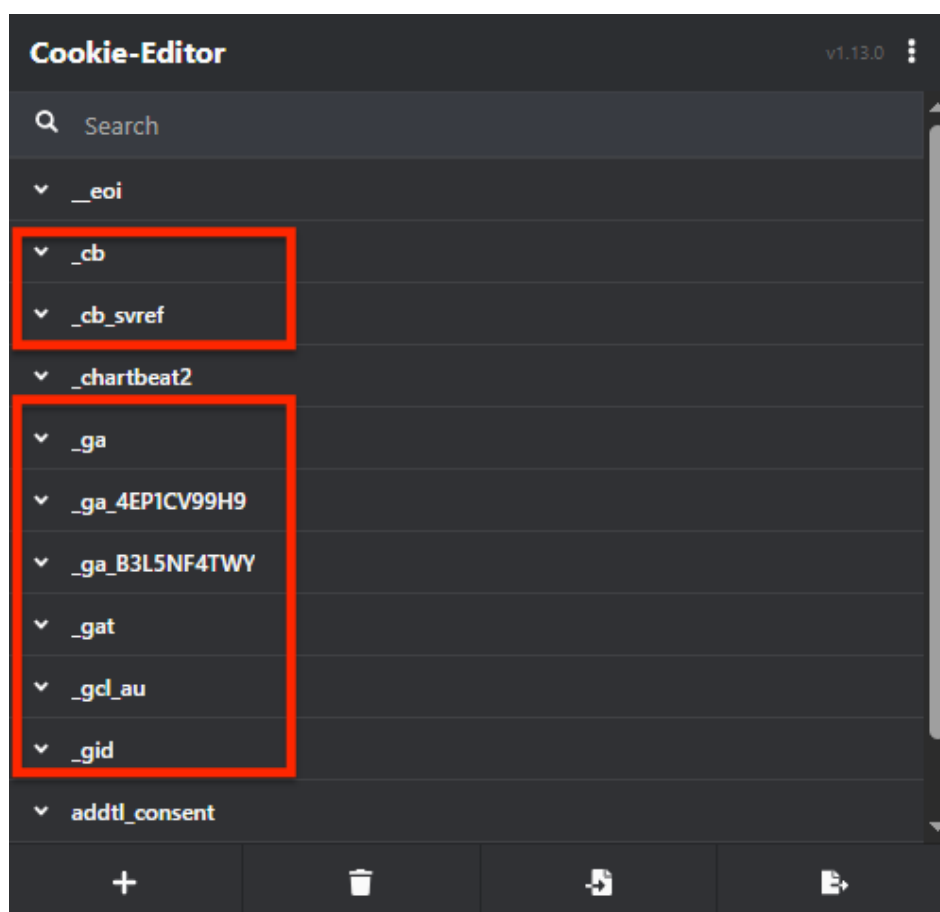


Figure 112: Cookie-editor Output - protothema.gr

The highlighted cookies, namely `_cb`, `_cb_svref` and the well-known google analytics cookies are by no means strictly necessary, since they serve tracking and advertising purposes, and this can be verified by both the CookieYes scan and Cookipedia database. Thus, there is a clear indication for cookies with incorrectly assigned labels.

Lastly, the website offers the options to revert the cookie banner and revoke consent by clicking the “Privacy” option on the bottom right corner of the website.

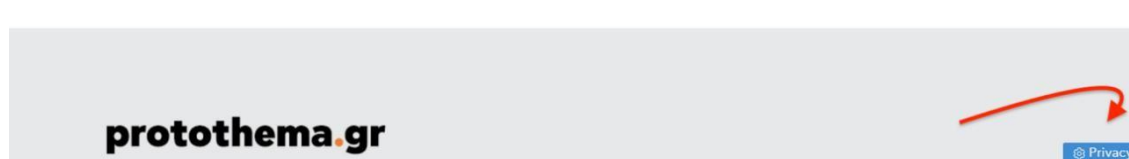


Figure 113: Revoke Consent Option - protothema.gr

In conclusion, the only violation identified on the website pertains to cookies with **incorrectly assigned labels**

6.2.14 Case Study 10: www.factoryoutlet.gr

The factory outlet website is the online format of a very popular outlet store located in Greece, and it mainly features clothing, footwear and accessories products. Starting with analysis breakdown, the ImmuniWeb scanning tool generated the following results.

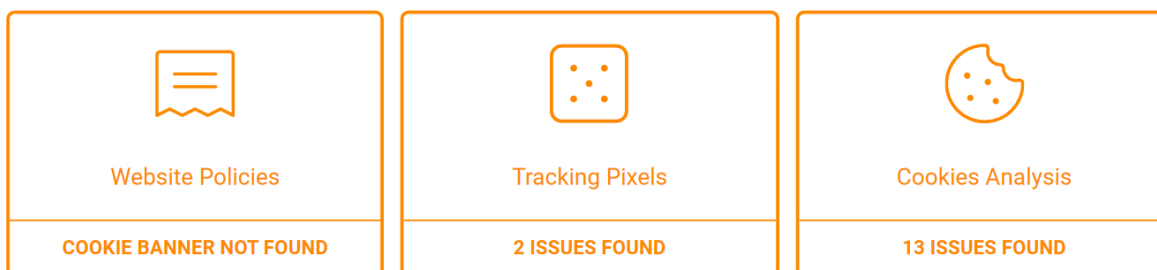


Figure 114: ImmuniWeb Scan - factoryoutlet.gr (1/4)

By expanding the “Website Policies” category of the report, the below additional information is displayed.

Privacy Policy was found on the website	Good configuration
The website has third-party cookies and the cookie consent banner was not found	Misconfiguration or weakness
The copyright notice is up-to-date: © 2024 Factory Outlet	Good configuration

Figure 115: ImmuniWeb Scan - factoryoutlet.gr (2/4)

The first issues detected, is the absence of a cookie consent banner and the use of tracking pixels on the website.

Next, two snapshots of the cookies analysis are attached below.

First-Party Cookies

There are 11 first-party cookies without a Secure flag	Misconfiguration or weakness
There are 12 first-party cookies without an HttpOnly flag	Misconfiguration or weakness

Name	Value	Domain	Path	Expires	Samesite	Secure	HttpOnly
ASPSESS ... SSTQTQQ	NAPOGLLBID FNJPACAJLK BCKL	www.factoryo utlet.gr	/	Immediately		No	No

Figure 116: ImmuniWeb Scan - factoryoutlet.gr (3/4)

Third-Party Cookies



Figure 117: ImmuniWeb Scan - factoryoutlet.gr (4/4)

The main concerning issue is the presence of one third-party cookie with an unusual expiration time.

Additionally, the results of the CookieYes scan are listed below.

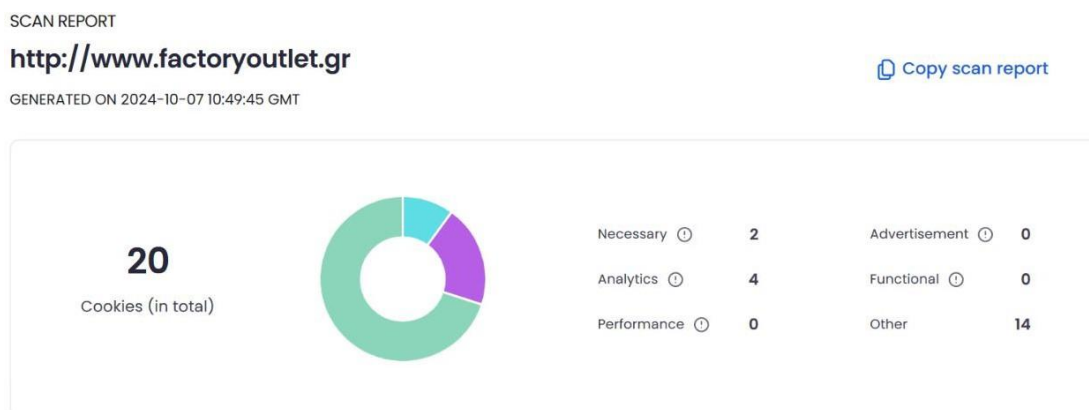


Figure 118: CookieYes Scan - factoryoutlet.gr

Table 13: Cookies Detected on factoryoutlet.gr

Cookie	Description	Duration	Type
ASPSESSIONIDCSSTQTQQ	No description available	Session	Other
cookiesession1	Set by Fortinet firewall to protect the website from abuse	1 year	Necessary
__cf_bm	Set by Cloudflare to support Cloudflare Bot Management	1 hour	Necessary
cp_total_cart_items	No description available	1 year	Other

Evaluation of Websites with Respect to Security and Privacy Services

cp_total_cart_value	No description available	1 year	Other
cpab	No description available	1 year	Other
Filters	No description available	Session	Other
ASPSESSIONIDAQBSSTQR	No description available	Session	Other
_fbp	Set by Facebook to store and track interactions	3 months	Analytics
_gcl_au	Set by Google Tag Manager to experiment with advertisement efficiency	3 months	Analytics
cp_sessionTime	No description available	1 hour	Other
_ga_*	Set by Google Analytics to store and count page views	1 year 1 month 4 days	Analytics
_ga	Set by Google Analytics to calculate visitor, session, and campaign data	1 year 1 month 4 days	Analytics
cf_clearance	No description available	1 year	Other
lastExternalReferrerTime	No description available	Never	Other
wantsnots	No description available	Never	Other
cp_localStorageTrigger	No description available	Never	Other
lastExternalReferrer	No description available	Never	Other
cp_shSess	No description available	Never	Other
bi	No description available	1 year	Other

After gathering all the scanning data, the last step involves the dynamic analysis, which is done by visiting the website. A snapshot of the website's front page is presented on the image below.

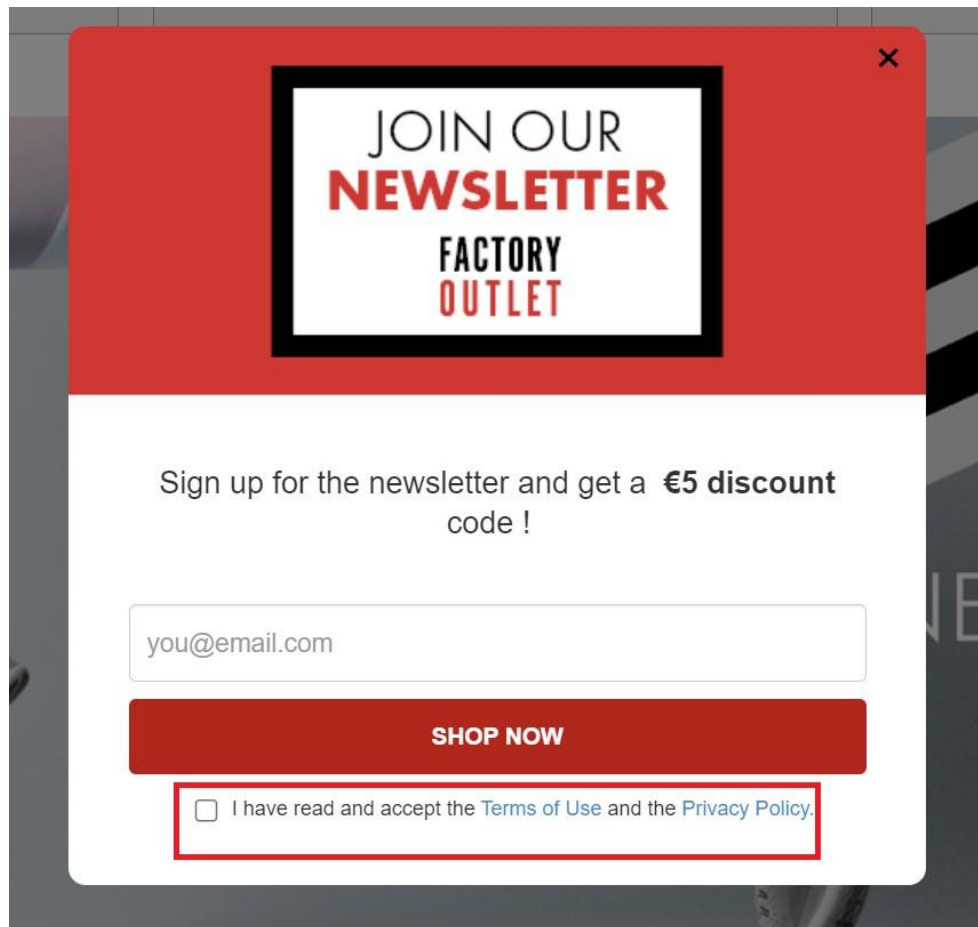


Figure 119: Cookie Banner Overview - factoryoutlet.gr

By inspecting the image, we can see that there is no clear and direct cookie consent banner detected. Therefore, the ImmuniWeb scan result regarding the cookie banner is correct. However, by clicking the “Privacy Policy” option on the bottom highlighted portion of this pop-up, a new tab opens and displays the following information.

PERSONAL DATA

▼ What personal information about you do we collect and how?

▼ What do we use your information for?

▼ What is the legal basis for data processing?

▼ Your email contact list

▼ How do we store and protect your personal data?

▼ Who will we share your personal data with?

▼ Why do we keep your information and how can you access it?

▼ What are your rights?

▼ FF OPSCO Cookies Policy

▼ What are cookies? Why do we use them?

▼ How can we change this policy?

▼ Communication

▼ Privacy Policy regarding the use of the Website

Figure 120: Extended Cookie Banner - factoryoutlet.gr (1/3)

By expanding the first highlighted option, we get the following additional information.

1. Types of cookies and why we use them:

There are two types of cookies that may be used when you browse the Factory Outlet website:

- Strictly necessary cookies: they are necessary for the proper functioning of the website and for the browsing by the user - without them the user may not be able to see the pages correctly or use certain features.

- Advertising cookies: they are used to create user accounts and send electronic messages with advertising content according to the preferences of each user during their browsing.

Cookies, in addition to being necessary and advertising, can also be categorized as follows:

- Functionality cookies: they are used to recognize users during browsing and are necessary for it, such as e.g. they remember some of your settings. Without them, some of the services provided (such as the use of the shopping cart) on the website will not be able to be provided.

- Performance cookies: they are used to collect information and analyze how visitors use the website (for example movements to and from it, total sales through the website, pages that have the most frequent traffic and those that show errors) so that to continuously improve the shopping experience on our website; All information collected by cookies is anonymous and is not used to identify you.

- Preference cookies: remember preferences and help us customize your purchases.

- Targeting and advertising cookies: used to send you customized advertisements based on your preferences so that they are more relevant to you. They limit the number of times you will see one of our ads and help us measure the effectiveness of each advertising campaign.

- Third-party cookies: used by third-party partner companies of Factory Outlet for promotional and advertising actions. These cookies allow us to make more correct and informed decisions about the needs and preferences of our customers. Third parties may use more than one type of cookie. All information collected is anonymous.

Figure 121: Extended Cookie Banner - factoryoutlet.gr (2/3)

2. [Can I check or delete cookies ?](#)

You can, if you wish, set your browser not to accept cookies. You also have the option to use our website without cookies enabled. However, it should be noted that with cookies disabled, your browsing on the website may be affected and/or the effectiveness of the functions and services provided will be reduced.

Figure 122: Extended Cookie Banner - factoryoutlet.gr (3/3)

As we can see, there is no detailed list containing all the cookies present on the website and there is also no option to reject all cookies or select specific categories. Furthermore, in the second image while the document claims that the user has the option to use the website without cookies enabled, there is no clear option or guidance on how to do that. Maybe this is done by not checking the “I have read and accept the Terms of use and Privacy Policy” box, which was shown on the previously listed image. Thus, this pop up cannot be considered as legit cookie banner and even if that was the case there are clear indications of using “dark” practices into tricking user consent.

As already stated, there is no detailed cookie list displayed on the website. Therefore, there is no way to check for undeclared or unclassified cookies and this also makes the analysis regarding cookies with incorrectly assigned labels limited. Using the cookie-editor extension, while not checking or checking the “I have read and accept the Terms of use and Privacy Policy”, the following cookies are detected.

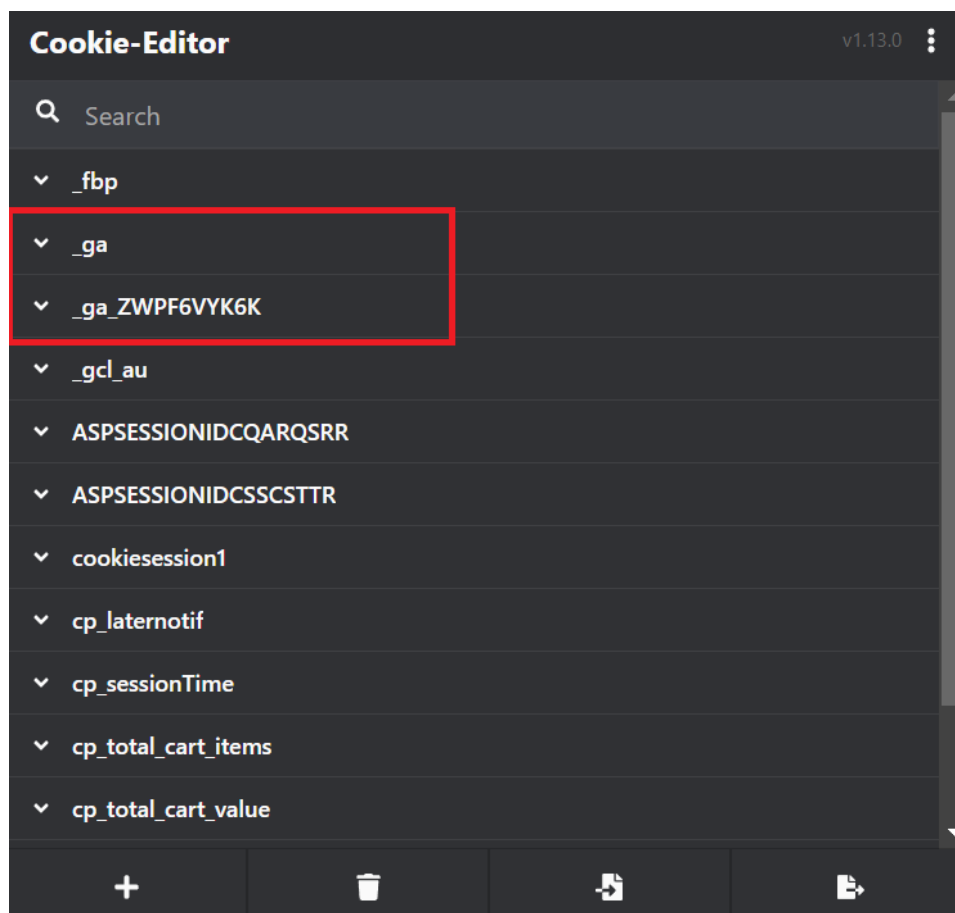


Figure 123: Cookie-editor Output - factoryoutlet.gr

As highlighted, there are cookies google analytics cookies detected on the browser, even though no consent was given for non-strictly necessary cookies. Thus, there is clear violation for cookies with incorrectly assigned labels.

In summary, the following privacy violations have been detected:

1. Absence of clear-dedicated cookie consent banner
2. Dark practices
3. Incorrectly assigned labels

6.3 Practical Evaluation and Analysis on Website Security

This section covers the actual testing and evaluation process of the selected websites, using the previously mentioned scanning tools. However, this analysis is fairly limited compared to the privacy focused evaluation, because of two main reasons.

First, the analysis relies solely on passive scanning techniques, which restrict the depth of insights. Second, in this case no dynamic analysis is performed, therefore the research is solely dependent on the output provided by the scanning tools.

Despite these limitations, by carefully analysing and interpreting these results we can draw valuable, although generic conclusions.

6.3.1 Case Study 1: www.gov.gr

Gov.gr is the official online portal of the Greek government, which is mainly designed for simplifying interactions between the government and citizens, by offering various services online.

As already mentioned, the security related analysis is very straightforward. First, the ImmuniWeb Website Security scan is triggered by simply entering the website URL. While the scan is supposed to last a couple of minutes, the following result is displayed on the screen after just a few seconds.



Figure 124: ImmuniWebSec Scan - gov.gr

As we can see, the website scan is not completed, since the server denied the request. This is probably due to the website's security measures, that block automated scanning tools (even passive ones) from analysing and testing for vulnerabilities. Furthermore, it is possible the website security configuration implements geo-restrictions and therefore preventing access from specific locations or IPs. To confirm that a variety of different scanning tools and proxies were used, but the website consistently blocked both the scans and the attempted visits.

Although, the ImmuniWeb security test failed and the overall security of the website cannot be investigated, it can still be assessed for its SSL/TLS configuration and overall security posture. This is done by using the Qualys SSL Labs tool, which unlike ImmuniWeb, was not blocked during the assessment. The most important findings, related to the scope of this invitation are listed below.

Configuration		
 Protocols		
TLS 1.3		Yes
TLS 1.2		Yes*
TLS 1.1		No
TLS 1.0		No*
SSL 3		No
SSL 2		No

Figure 125: Qualys SSL Labs Test - gov.gr (1/4)

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO »](#)

Figure 126: Qualys SSL Labs Test - gov.gr (2/4)

First, the website only supports the latest and most secure versions of the TLS protocol namely 1.2 and 1.3, ensuring a secure communication channel. On the contrary, the older versions of TLS are disabled, meaning that with the support from the enabled HSTS protocol the risk of protocol downgrade attacks is significantly reduced. Additionally, the website mostly uses modern and strong cipher suites boosting its overall security. A more detailed view of the findings is shown on the following image.

Cipher Suites		
# TLS 1.3 (suites in server-preferred order)		
TLS_AES_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH x25519 (eq. 3072 bits RSA) FS	256P
TLS_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_128_CCM_8_SHA256 (0x1305)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_128_CCM_SHA256 (0x1304)	ECDH x25519 (eq. 3072 bits RSA) FS	128
# TLS 1.2 (suites in server-preferred order)		
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0a8)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256P
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	128

Figure 127: Qualys SSL Labs Test - gov.gr (3/4)

Moreover, the website uses advanced certificates, for example the RSA 2048-bit certificates issued by “R10”. All the certificates are up-to-date and have a complete chain of trust.

Certificate #1: RSA 2048 bits (SHA256withRSA)	
Server Key and Certificate #1	
Subject	www.gov.gr Fingerprint SHA256: be860e3b9b1686c80a3b1cdec38d960f2615bab5dc0fac215086274d58039 Pin SHA256: Oorg:moWzTrX3hRvnu2JAR6VHpxnRcTZgY4VWwbsPD=
Common names	www.gov.gr
Alternative names	aade.gr aesop.iep.edu.gr astinomia.gr astynomia.gr covid19stats.gov.gr culture.gov.gr dialaneia.hellenicparliament.gr e-egrafes.minedu.gov.gr ekato.gr elearning.iep.edu.gr eody.gov.gr epistoliki.yes.gov.gr epistolikiorg.yes.gov.gr files.asep.gr form.gov.gr forma.gov.gr g-testing.hdb.gr government.gov.gr gsis.gr hcq.gr hellenicpolice.gr info.asep.gr kep.gov.gr kyc-test.hdb.gr kyc.hdb.gr kycapp- test.hdb.gr kycapp.hdb.gr mfa.gr minagric.gov.gr minagric.gr mindigital.gr minedu.gov.gr minedu.gr ministryofjustice.gr minocp.gov.gr mocp.gr moj.gov.gr mopo.gr mopocp.gov.gr mpp.yes.gov.gr police.gr primeminister.gr prostasiapoliti.gr self-testing.gov.gr sustainability.visitgreece.gr trapeza.iep.edu.gr visitgreece.gr www.aade.gr www.astinomia.gr www.astynomia.gr www.culture.gov.gr www.ekato.gr www.eody.gov.gr www.gov.gr www.government.gov.gr www.gsis.gr www.hcq.gr www.hellenicparliament.gr www.hellenicpolice.gr www.howto.gov.gr www.kep.gov.gr www.mfa.gr www.minagric.gov.gr www.minagric.gr www.mindigital.gr www.minedu.gov.gr www.minedu.gr www.ministryofjustice.gr www.minocp.gov.gr www.mocp.gr www.moj.gov.gr www.mopo.gr www.mopocp.gov.gr www.parliament.gr www.police.gr www.primeminister.gr www.prostasiapoliti.gr www.visitgreece.gr www.ydt.gr www.ynanp.gr www.ypeph.gr www.ypes-dt.gr www.ypes.gov.gr www.ypes.gr www.yptp.gr ydt.gr ynanp.gr ypeph.gr ypes-dt.gr ypes.gov.gr ypes.gr yptp.gr
Serial Number	04fc5b042961c8fab39d5c164856e3ad83
Valid from	Tue, 13 Aug 2024 09:34:19 UTC
Valid until	Mon, 11 Nov 2024 09:34:18 UTC (expires in 24 days, 20 hours)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	R10 AAA: http://r10.i.lelencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r10.o.lelencr.org
Revocation status	Good (not revoked)

Figure 128: Qualys SSL Labs Test - gov.gr (4/4)

Lastly, no known TLS related vulnerabilities were detected during the scanning process.

Summarizing, the overall TLS configuration of the gov.gr website is solid, and no issues were found, although some of the previously highlighted TLS 1.2 weaker suites may be considered as a very marginal vulnerability.

However, while this scan provides valuable insights into the site's SSL/TLS encryption practices, it alone is not sufficient to fully evaluate the security posture expected from a government website.

6.3.2 Case study 2: www.dei.gr

The website dei.gr belongs to the Public Power Corporation (PPC) which is the largest electric power company in Greece. PPC provides electricity generation, transmission, and distribution services throughout the country.

First, the ImmuniWeb Website Security scan is triggered. This time, the scan is partially blocked, due to the security configuration of the website.

It appears that system is not responding or blocking software fingerprinting attempts, performed from the following IP ranges: 192.175.111.224/27, 64.15.129.96/27, 70.38.27.240/28, 72.55.136.144/28. Please whitelist them for successful continuation of the test.

Misconfiguration or weakness

Figure 129: Partial Scan Blockage - dei.gr

Despite that, some web software related vulnerabilities were detected, mainly due to the presence of an outdated version of the jQuery UI library, specifically version 1.12.1. These are listed on the table below.

Table 14: Software Related Vulnerabilities - dei.gr

<u>CVSSv3.1 Score</u>	<u>Vulnerability CVE-ID</u> <u>CVE</u>	<u>Vulnerability Type</u>
5.5 Medium	CVE-2021-41184	CWE-79 - Cross-site scripting
5.3 Medium	CVE-2021-41182	CWE-79 - Cross-site scripting
5.3 Medium	CVE-2021-41183	CWE-79 - Cross-site scripting
4.1 Medium	CVE-2022-31160	CWE-79 - Cross-site scripting

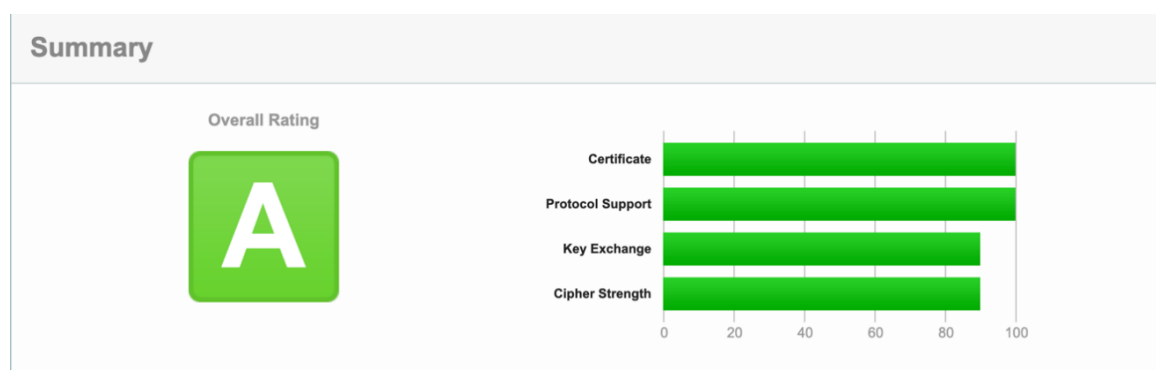
Also, the following components were also listed as outdated, but in that case, there were no known security vulnerabilities found.

- **Vue 3.2.36:** The component is outdated. Update to the most recent version 3.5.11.
- **Core-js 3.0.0:** The component is outdated. Update to the most recent version 3.38.1.
- **Jquery-validation 1.19.5:** The component is outdated. Update to the most recent version 1.21.0.

However, it is important to clarify that the name of CMS and the components were fingerprinted using passive and non-intrusive techniques and therefore the accuracy and validity of these results is not guaranteed.

Regarding PCI DSS Compliance, the only finding was there was no Web Application Firewall (WAF) present on the website. No additional findings were extracted due to the scan's partial blockage.

Lastly, the ImmuniWeb scanning tool detected good TLS configuration. This can also be verified by running the SSL Qualys Labs test. The main results of that test are listed below, and they are almost identical to case study 1.

**Figure 130: Qualys SSL Labs Test - dei.gr (1/3)**

Protocols	
TLS 1.3	Yes
TLS 1.2	Yes*
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

Figure 131: Figure 130: Qualys SSL Labs Test - dei.gr (2/3)

Cipher Suites	
# TLS 1.3 (suites in server-preferred order)	
TLS_AES_128_GCM_SHA256 (0x1301) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_CHACHA20_POLY1305_SHA256 (0x1303) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_AES_256_GCM_SHA384 (0x1302) ECDH x25519 (eq. 3072 bits RSA) FS	256
# TLS 1.2 (suites in server-preferred order)	
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH x25519 (eq. 3072 bits RSA) FS WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) WEAK	256

Figure 132: Figure 130: Qualys SSL Labs Test - dei.gr (3/3)

In conclusion, the only vulnerability detected on the website is the outdated jQuery UI (v1.12.1), which results to several Cross-Site Scripting (XSS) vulnerabilities. Some of the previously highlighted TLS 1.2 weaker suites may also be considered as a very marginal vulnerability.

6.3.3 Case study 3: www.nbg.gr

The website www.nbg.gr belongs to the National Bank of Greece (NBG), one of the largest and oldest financial institutions in Greece.

Starting the analysis, ImmuniWeb Security Scan is triggered. The scan was completely successful, and its main findings are listed below.

First, regarding DNSSEC, one unassigned DNS record was detected, specifically the CNAME (Canonical Name) record pointing to www.nbg.gr.cdn.cloudflare.net. This may leave the website exposed to DNS spoofing related threats.

Additionally, there were no serious web software security issues, nor any CMS vulnerabilities detected. The following components were also listed as outdated, but in that case, there were no known security vulnerabilities found.

- **jQuery 3.6.0:** The component is outdated. Update to the most recent version 3.7.1.

- **Angular 10.0.14:** The component is outdated. Update to the most recent version 18.2.8.
- **Core-js3.2.1:** The component is outdated. Update to the most recent version 3.38.1.

However, it is important to clarify that the name of CMS and the components were fingerprinted using passive and non-intrusive techniques and therefore the accuracy and validity of these results is not guaranteed.

In terms of PCI DSS compliance, the scan indicated that the following requirements were met:

- No publicly known vulnerabilities seem to be present in the fingerprinted versions of the website CMS and its components.
- The website seems to be protected by a WAF.

Lastly, the scan detected good TLS configuration. This can be furtherly evaluated by using the ImmuniWeb dedicated SSL scan (since there is no scan blockage in this case). The main findings are listed below.

CERTIFICATES ARE TRUSTED ⓘ

All the certificates provided by the server are trusted. Good configuration

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLSV1.3

TLS_CHACHA20_POLY1305_SHA256	Good configuration
TLS_AES_256_GCM_SHA384	Good configuration
TLS_AES_128_GCM_SHA256	Good configuration

TLSV1.2

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_GCM_SHA384	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration

Figure 133: ImmuniWeb TLS Test - nbgr.gr (1/2)

SUPPORTED PROTOCOLS

List of all SSL/TLS protocols supported by the server:

TLSv1.2	Good configuration
TLSv1.3	Good configuration

Figure 134: ImmuniWeb TLS Test - nbgr.gr (2/2)

As shown, the website has an exceptional TLS configuration, and this is why no known vulnerabilities were detected.

In summary, no critical weaknesses or known vulnerabilities were found during the analysis of this website

6.3.4 Case study 4: www.oasa.gr

OASA.gr is the official website of the Athens Urban Transport Organization. It manages the public transportation services in the greater Athens area, including buses, trolleys, trams, and the metro trains.

First, the ImmuniWeb Website Security scan is triggered. This time, the scan is partially blocked, due to the security configuration of the website.

It appears that system is not responding or blocking software fingerprinting attempts, performed from the following IP ranges: 192.175.111.224/27, 64.15.129.96/27, 70.38.27.240/28, 72.55.136.144/28. Please whitelist them for successful continuation of the test.

Misconfiguration or weakness

Figure 135: Partial Scan Blockage - oasa.gr

Regardless of the limitations, some web software related vulnerabilities were detected, mainly due to the presence of an outdated version of the Bootstrap framework, specifically version 3.3.4. These are listed on the table below.

Table 15: Software Related Vulnerabilities - oasa.gr

<u>CVSSv3.1 Score</u>	<u>Vulnerability CVE-ID CVE</u>	<u>Vulnerability Type</u>
5.5 Medium	CVE-2016-10735	CWE-79 - Cross-site scripting
5.5 Medium	CVE-2018-14040	CWE-79 - Cross-site scripting
5.5 Medium	CVE-2018-14042	CWE-79 - Cross-site scripting
5.5 Medium	CVE-2018-14041	CWE-79 - Cross-site scripting
5.3 Medium	CVE-2024-6485	CWE-79 - Cross-site scripting
5.3 Medium	CVE-2024-6484	CWE-79 - Cross-site scripting
5.3 Medium	CVE-2019-8331	CWE-79 - Cross-site scripting
5.3 Medium	CVE-2018-20677	CWE-79 - Cross-site scripting
5.3 Medium	CVE-2018-20676	CWE-79 - Cross-site scripting

Also, the following components were also listed as outdated, but in that case, there were no known security vulnerabilities found.

- **Breeze – WordPress cache plugin 2.1.14:** The component is outdated. Update to the most recent version 2.1.15.
- **jQuery Migrate 3.4.1:** The component is outdated. Update to the most recent version 3.5.2.
- **Isotope 2.2.2:** The component is outdated. Update to the most recent version 3.0.6.

- **jQuery1.11.1—3.7.1** The component is outdated. Update to most recent version is 3.7.1.

However, it is important to clarify that the name of CMS and the components were fingerprinted using passive and non-intrusive techniques and therefore the accuracy and validity of these results is not guaranteed.

In terms of PCI DSS compliance, the scan indicated the following issues

- Fingerprinted website CMS or its components contain the publicly known vulnerabilities that were listed above.
- Absence of WAF

Lastly, the ImmuniWeb scanning tool detected good TLS configuration. This can also be verified by running the SSL Qualys Labs test. The main results of that test are listed below, and they are almost identical to case study 1.

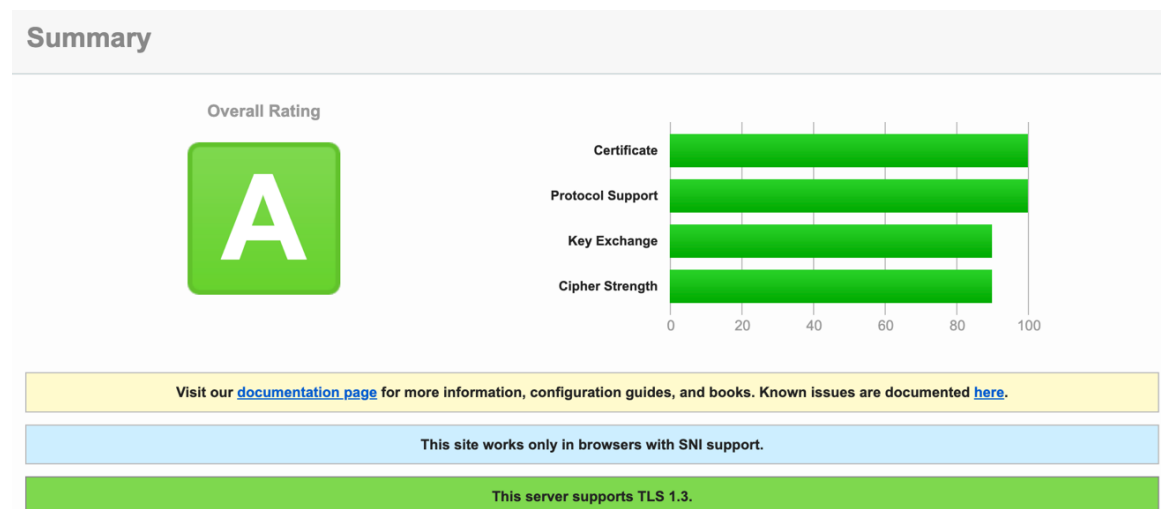


Figure 136: Qualys SSL Labs Test - oasa.gr (1/3)

Protocols	
TLS 1.3	Yes
TLS 1.2	Yes*
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

Figure 137: Qualys SSL Labs Test - oasa.gr (2/3)

Cipher Suites

# TLS 1.3 (suites in server-preferred order)			[-]
TLS_AES_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA) FS		256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH x25519 (eq. 3072 bits RSA) FS		256
TLS_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA) FS		128
# TLS 1.2 (suites in server-preferred order)			[-]
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH x25519 (eq. 3072 bits RSA) FS		256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH x25519 (eq. 3072 bits RSA) FS		128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH x25519 (eq. 3072 bits RSA) FS	WEAK	256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0xc077)	ECDH x25519 (eq. 3072 bits RSA) FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH x25519 (eq. 3072 bits RSA) FS	WEAK	128
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (0xc076)	ECDH x25519 (eq. 3072 bits RSA) FS	WEAK	128
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)	ECDH x25519 (eq. 3072 bits RSA) FS		256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc061)	ECDH x25519 (eq. 3072 bits RSA) FS		256
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc060)	ECDH x25519 (eq. 3072 bits RSA) FS		128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH x25519 (eq. 3072 bits RSA) FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH x25519 (eq. 3072 bits RSA) FS	WEAK	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits FS		256
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0aa)	DH 2048 bits FS		256
TLS_DHE_RSA_WITH_AES_256_CCM_8 (0xc0a3)	DH 2048 bits FS		256
TLS_DHE_RSA_WITH_AES_256_CCM (0xc09f)	DH 2048 bits FS		256
TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc053)	DH 2048 bits FS		256

Figure 138: Qualys SSL Labs Test - oasa.gr (3/3)

Thus, the main vulnerability detected on the website is the outdated Bootstrap framework (v3.3.4), which results to several Cross-Site Scripting (XSS) vulnerabilities. Some of the previously highlighted TLS 1.2 weaker suites may also be considered as a very marginal vulnerability.

6.3.5 Case study 5: www.nis.gr

The website www.nis.gr is associated with EYP Greece. This agency is responsible for intelligence gathering, national security, and counterintelligence operations in Greece.

Beginning the investigation, the ImmuniWeb Security scan is triggered. As expected due to the nature of the selected website, the scanning is almost fully blocked.

It appears that system is not responding or blocking software fingerprinting attempts, performed from the following IP ranges: 192.175.111.224/27, 64.15.129.96/27, 70.38.27.240/28, 72.55.136.144/28. Please whitelist them for successful continuation of the test.

Misconfiguration or weakness

First, regarding DNSSEC, one unassigned DNS record was detected, specifically the CNAME (Canonical Name) record pointing to xzuf74h.impervadns.net.. This may leave the website exposed to DNS spoofing related threats.

Next, in terms of web software security, the scanning detected two out-of-date components, namely Vue 2.6.14 and Core-js 3.18.0. The first one is vulnerable to public known vulnerabilities.

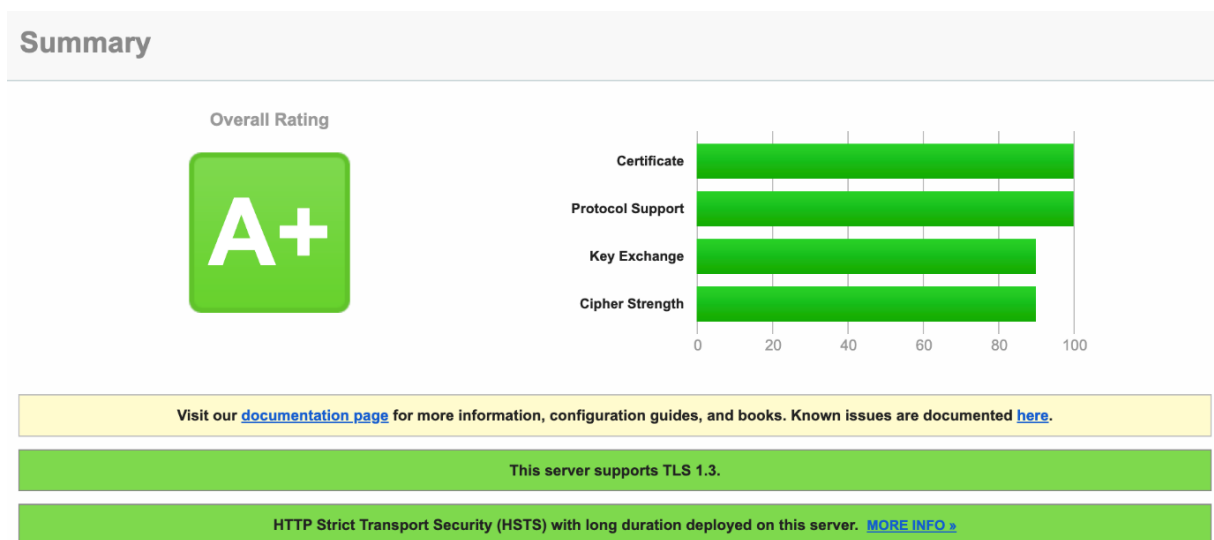
Table 16: Software Related Vulnerabilities - nis.gr

<u>CVSSv3.1 Score</u>	<u>Vulnerability CVE-ID</u> <u>CVE</u>	<u>Vulnerability Type</u>
5.5 Medium	CVE-2024-6783	CWE-79 - Cross-site scripting

However, it is important to clarify that the name of CMS and the components were fingerprinted using passive and non-intrusive techniques and therefore the accuracy and validity of these results is not guaranteed.

On the other hand, the PCI DSS test is not applicable in this case, however the scanning detected the presence of WAF, which is an indication of good overall security configuration.

Lastly, the ImmuniWeb scanning tool, suggested that the website has a perfect TLS configuration, which is also verified from the Qualys SSL Labs test. The main findings of that scan are listed below.

**Figure 139: Qualys SSL Labs Test - nis.gr (1/2)**

Protocols		
TLS 1.3		Yes
TLS 1.2		Yes
TLS 1.1		No
TLS 1.0		No
SSL 3		No
SSL 2		No
Cipher Suites		
# TLS 1.3 (suites in server-preferred order)		
TLS_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_AES_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA) FS	256
# TLS 1.2 (suites in server-preferred order)		
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH x25519 (eq. 3072 bits RSA) FS	128

Figure 140: Qualys SSL Labs Test - nis.gr (2/2)

Therefore, no significant vulnerabilities were detected on this website, apart from the Cross-Site Scripting (XSS) vulnerability, originating from the outdated Vue 2.6.14 component.

6.3.6 Case Study 6: www.eydap.gr

EYDAP is the largest water supply and sewerage company in Greece and its website is www.eydap.gr.

The ImmuniWeb Website Security scan is triggered and after a couple of minutes it is successfully completed. The main findings are listed below.

Starting with DNSSEC, one unassigned DNS record was detected, specifically the A type record pointing to IP address 159.60.131.71. This may leave the website exposed to DNS spoofing related threats.

Next, several issues arise regarding the web software security and CMS. Firstly, an outdated component, namely **jQuery UI 1.8.12** was detected. This version is vulnerable to the subject to the following vulnerabilities.

Table 17: Software Related Vulnerabilities - eydap.gr

<u>CVSSv3.1 Score</u>	<u>Vulnerability CVE-ID</u> <u>CVE</u>	<u>Vulnerability Type</u>
5.5 Medium	CVE-2021-41184	CWE-79 - Cross-site scripting
5.3 Medium	CVE-2021-41182	CWE-79 - Cross-site scripting
5.3 Medium	CVE-2021-41183	CWE-79 - Cross-site scripting
5.3 Medium	CVE-2010-5312	CWE-79 - Cross-site scripting

5.3 Medium	CVE-2012-6662	CWE-79 - Cross-site scripting
5.3 Medium	CVE-2016-7103	CWE-79 - Cross-site scripting
4.1 Medium	CVE-2022-31160	CWE-79 - Cross-site scripting

Additionally, the following components are also outdated, but in that case no associated known vulnerabilities were found.

- **Bootstrap 5.0.2:** The component is outdated. Update to the most recent version 5.3.3.
- **Core-js 3.0.0:** The component is outdated. Update to the most recent version 3.38.1.
- **Prettyphoto 3.1.3:** The component is outdated. Update to the most recent version 3.1.6.

However, it is important to clarify that the name of CMS and the components were fingerprinted using passive and non-intrusive techniques and therefore the accuracy and validity of these results is not guaranteed.

Next, in terms of PCI DSS compliance, while the website seems to be protected by a WAF, the previously mentioned vulnerabilities lead are listed as serious misconfigurations.

Lastly, the scan detected good TLS configuration. This can be furtherly evaluated by using the ImmuniWeb dedicated SSL scan (since there is no scan blockage in this case). The main findings are listed below.

 Root CA DigiCert Global Root G2 Type/Size: RSA 2048 bits Serial Number: 4293743540046975378534879503202253541 Signature: sha256WithRSAEncryption SHA256: cb3ccbb76031e5e013...4cea27d46a5ab1cb5f PIN: i7WTqTvh0Oiolrulf...rS2rdiVPI/s2uC/CY= Expires in: 4,837 days Comment: Self-signed Download: 	 Intermediate CA DigiCert Global G2 TLS RSA SHA256 2020 CA1 Type/Size: RSA 2048 bits Serial Number: 17226682543955925492517929723242541158 Signature: sha256WithRSAEncryption SHA256: c8025f9fc65fd95b...17463fc813d0b625a9 PIN: Wec45nQIFwKvHtuHxS...+uPSw9JIEkxhvYPHk= Expires in: 2,354 days Comment: Extended Validation Download: 
 Server certificate *.eydap.gr Type/Size: RSA 2048 bits Serial Number: 4576420808807664587280664219208875273 Signature: sha256WithRSAEncryption SHA256: e93b2868c99d69c51b...6355256de4c1cf6804 PIN: eewU5bs0vB2NZX/L5w...Af1mtQwnAdKpp4DyA= Expires in: 359 days Comment: - Download: 	

Figure 141: ImmuniWeb TLS Test (1/2) - eydap.gr

CERTIFICATES ARE TRUSTED ⓘ

All the certificates provided by the server are trusted. Good configuration

SUPPORTED CIPHERS

List of all cipher suites supported by the server:

TLSV1.3

TLS_CHACHA20_POLY1305_SHA256	Good configuration
TLS_AES_256_GCM_SHA384	Good configuration
TLS_AES_128_GCM_SHA256	Good configuration

TLSV1.2

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Good configuration

SUPPORTED PROTOCOLS

List of all SSL/TLS protocols supported by the server:

TLSv1.2	Good configuration
TLSv1.3	Good configuration

Figure 142: ImmuniWeb TLS Test (2/2) - eydap.gr

As shown, the TLS configuration on this website is very good.

In conclusion, no significant vulnerabilities were detected on this website, apart from the Cross-Site Scripting (XSS) vulnerability, originating from the outdated jQuery UI 1.8.12 component.

6.3.7 Case Study 7: www.alphabank.gr

Alpha Bank is yet another one of the largest financial institutions in Greece, offering a range of banking products and services, including retail, corporate, and investment banking.

In this case, the ImmuniWeb Security scan was completely blocked as we can see on the picture below.

Summary of www.alpha.gr [Desktop version] Website Security Test

www.alpha.gr was tested 3 times during the last 12 months.

Your final score:

Tested on: Oct 18th, 2024 12:27:38 GMT+3 Server IP: 23.53.4.24 Reverse DNS: a23-53-4-24.deploy.static.akamaitechnologies.com Location: Montreal 🇨🇦 Client: Desktop version	A B C F			
---	-------------------------------------	--	--	--

The remote server responded with a status code "403". Web server security can't be tested. Information

Figure 143: ImmuniWeb Security Scan - alphabank.gr

As a result, the analysis is strictly limited to just checking the SSL/TLS configuration, using the SSL Qualys scanning tool. The main findings of the new scan are listed below.

Certificate #1: RSA 2048 bits (SHA256withRSA)	
 Server Key and Certificate #1 Download	
Subject	www.alpha.gr Fingerprint SHA256: 3a7c6ffdcffbc699f19df12b90e149a07e1f8254f04f3da6c925c989cb7ec15 Pin SHA256: HfWfQM6rj0UyEz/OA/5fhwP3HpRRGZ/tKLnR8/41zE=
Common names	www.alpha.gr
Alternative names	www.alpha.gr www.alphaholdings.gr secure.alpha.gr alpha.gr
Serial Number	0d0c8734557bf44bb8e413bf79f5b5c9
Valid from	Tue, 18 Jun 2024 00:00:00 UTC
Valid until	Tue, 17 Jun 2025 23:59:59 UTC (expires in 7 months and 30 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	DigiCert SHA2 Extended Validation Server CA AIA: http://cacerts.digicert.com/DigiCertSHA2ExtendedValidationServerCA.crt
Signature algorithm	SHA256withRSA
Extended Validation	Yes
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl3.digicert.com/sha2-ev-server-g3.crl OCSP: http://ocsp.digicert.com
Revocation status	Good (not revoked)

Figure 144: Qualys SSL Labs Test - alphabank.gr (1/3)

Configuration	
 Protocols	
TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

Figure 145: Qualys SSL Labs Test - alphabank.gr (2/3)

Cipher Suites		
# TLS 1.3 (suites in server-preferred order)		
TLS_AES_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH x25519 (eq. 3072 bits RSA) FS	256 ^P
TLS_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_128_CCM_8_SHA256 (0x1305)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_128_CCM_SHA256 (0x1304)	ECDH x25519 (eq. 3072 bits RSA) FS	128
# TLS 1.2 (suites in server-preferred order)		
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256 ^P
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256 ^P
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	WEAK	128

Figure 146: Qualys SSL Labs Test - alphabank.gr (3/3)

First, the website only supports the latest and most secure versions of the TLS protocol namely 1.2 and 1.3, ensuring a secure communication channel. Additionally, the website mostly uses modern and strong cipher suits boosting its overall security. Moreover, the website uses advanced certificates, for example the RSA 2048-bit certificate. All the certificates are up-to-date and have a complete chain of trust.

Summarizing, the overall TSL configuration of this website is solid, and no issues were found, although some of the previously highlighted TLS 1.2 weaker suites may be considered as a very marginal vulnerability.

However, while this scan provides valuable insights into the site's SSL/TLS encryption practices, it alone is not sufficient to fully evaluate the security posture expected from a banking website.

6.3.8 Case Study 8: www.aegeanair.com

Aegean Air is the largest Greek airline offering a variety of travel related services, like booking tickets or checking-in.

First, the ImmuniWeb Website Security scan is triggered, but unsuccessfully. As shown on the image below the scan is completely blocked by the website's server.

Evaluation of Websites with Respect to Security and Privacy Services

www.aegeanair.com was tested 7 times during the last 12 months.

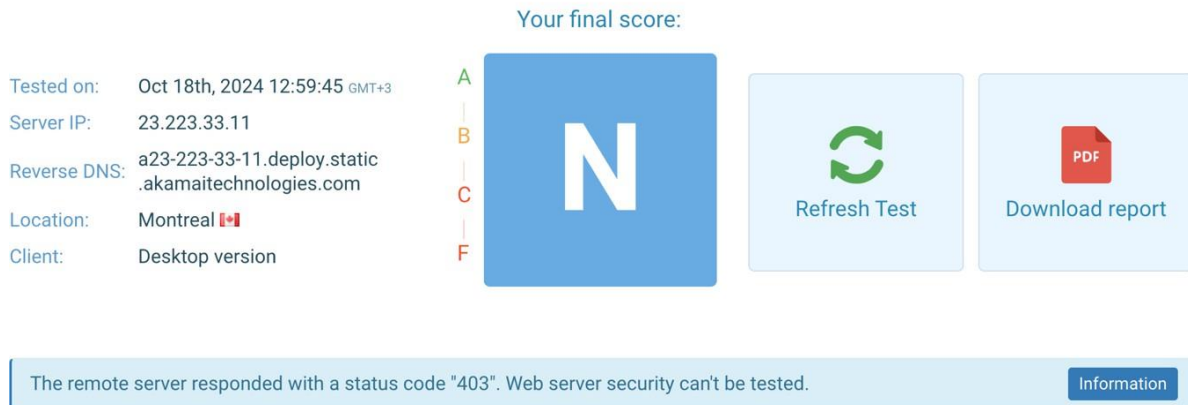


Figure 147: ImmuniWeb Security Test – aegeanair.com

As a result, the analysis is strictly limited to just checking the SSL/TLS configuration, using the SSL Qualys scanning tool. The main findings are listed below.

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1	
Subject	www.aegeanair.com Fingerprint SHA256: c76386b255849079009d0791ce72ac5a26f5842fbc7bac359046ce8cabf29d5 Pin SHA256: r0K0d15snISP91LdNJOpBi2pAmhyYjp/w3LnDrb+yyPw=
Common names	www.aegeanair.com
Alternative names	www.aegeanair.com book.aegeanair.com de.about.aegeanair.com de.aegeanair.com el.about.aegeanair.com el.aegeanair.com en.about.aegeanair.com en.aegeanair.com es.about.aegeanair.com es.aegeanair.com fr.about.aegeanair.com fr.aegeanair.com it.about.aegeanair.com it.aegeanair.com mobile.aegeanair.com notifications.aegeanair.com rentacar.aegeanair.com ro.about.aegeanair.com ro.aegeanair.com ru.about.aegeanair.com ru.aegeanair.com shopintheclouds.aegeanair.com
Serial Number	022cfbc00b91eca4979e440b84e53e59
Valid from	Fri, 12 Jul 2024 00:00:00 UTC
Valid until	Tue, 12 Aug 2025 23:59:59 UTC (expires in 9 months and 25 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	GeoTrust EV RSA CA G2 AIA: http://cacerts.digicert.com/GeoTrustEVRSAAG2.crt
Signature algorithm	SHA256withRSA
Extended Validation	Yes
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl3.digicert.com/GeoTrustEVRSAAG2.crl OCSP: http://ocsp.digicert.com
Revocation status	Good (not revoked)

Figure 148: Qualys SSL Labs Test - aegeanair.com (1/3)

Protocols	
TLS 1.3	Yes
TLS 1.2	Yes*
TLS 1.1	No
TLS 1.0	No*
SSL 3	No
SSL 2	No

Figure 149: Qualys SSL Labs Test - aegeanair.com (2/3)

Cipher Suites			
# TLS 1.3 (suites in server-preferred order)			
TLS_AES_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA)	FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH x25519 (eq. 3072 bits RSA)	FS	256 ^P
TLS_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA)	FS	128
# TLS 1.2 (suites in server-preferred order)			
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	256 ^P
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA)	FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA)	FS WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA)	FS WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA)	FS WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)		WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)		WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)		WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)		WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		WEAK	128

Figure 150: Qualys SSL Labs Test - aegeanair.com (3/3)

First, the website only supports the latest and most secure versions of the TLS protocol namely 1.2 and 1.3, ensuring a secure communication channel. Additionally, the website mostly uses modern and strong cipher suits boosting its overall security. Moreover, the website uses advanced certificates, for example the RSA 2048-bit certificates issued by GeoTrust EV. All the certificates are up-to-date and have a complete chain of trust.

Thus, the overall TSL configuration of this website is solid, and no issues were found, although some of the previously highlighted TLS 1.2 weaker suites may be considered as a very marginal vulnerability. However, while this scan provides valuable insights into the site's SSL/TLS encryption practices, it alone is not sufficient to fully evaluate the security posture expected from this website.

6.3.9 Case Study 9: www.helpe.gr

The website www.helpe.gr is the official website of Hellenic Petroleum S.A one of the largest energy groups in Greece and Southeast Europe.

First, the ImmuniWeb Website Security scan is triggered and this time it is completed successfully.

First, regarding DNSSEC, one unassigned DNS record was detected, specifically the CNAME (Canonical Name) record pointing tohelpe.gr. This may leave the website exposed to DNS spoofing related threats.

Moving on, only one outdated component, namely **jQuery UI 1.10.1** was detected. This version is vulnerable to the subject to the following vulnerabilities.

Table 18: Software Related Vulnerabilities - helpe.gr

<u>CVSSv3.1 Score</u>	<u>Vulnerability CVE-ID</u> <u>CVE</u>	<u>Vulnerability Type</u>
5.5 Medium	CVE-2020-11022	CWE-79 - Cross-site scripting
5.3 Medium	CVE-2015-9251	CWE-79 - Cross-site scripting
4.8 Medium	CVE-2019-11358	CWE-1321 - Prototype pollution
4.1 Medium	CVE-2020-11023	CWE-79 - Cross-site scripting

Regarding PCI DSS compliance, although the website is not applicable to this analysis, it is marked as incompliant, due to the existence of the previously listed vulnerabilities and the absence of a WAF.

Lastly, the scan detected good TLS configuration. This can be furtherly evaluated by using the ImmuniWeb dedicated SSL scan (since there is no scan blockage in this case). The main findings are listed below.

CERTIFICATE CHAIN

Root CA	DigiCert Global Root G2	Intermediate CA	GeoTrust TLS RSA CA G1
Type/Size	RSA 2048 bits	Type/Size	RSA 2048 bits
Serial Number	4293743540046975378534879503202253541	Serial Number	17318747245906231087668175401711030649
Signature	sha256WithRSAEncryption	Signature	sha256WithRSAEncryption
SHA256	cb3ccbb76031e5e013...4cea27d46a5ab1cb5f	SHA256	c06e307f7cfc1d32fa...64978a2eca6c8a230e
PIN	i7WTqTvh00iolrulfF...rS2rdiVPI/s2uC/CY=	PIN	SDG5orEv8iX6MNenIA...ROB/6+llsZdXHZNqs=
Expires in	4,837 days	Expires in	1,110 days
Comment	Self-signed	Comment	-
Download		Download	

Server certificate	www.helpe.gr
Type/Size	RSA 2048 bits
Serial Number	1986967632071572449823152884008013719
Signature	sha256WithRSAEncryption
SHA256	3e199b83ad4c682487...7aa0a4093e3de7f6d1
PIN	xued7R6aW7ChgzWeyv...lcfdeZO9E0TQ9M8s=
Expires in	275 days
Comment	-
Download	

Figure 151: ImmuniWeb TLS Test - helpe.gr (1/4)

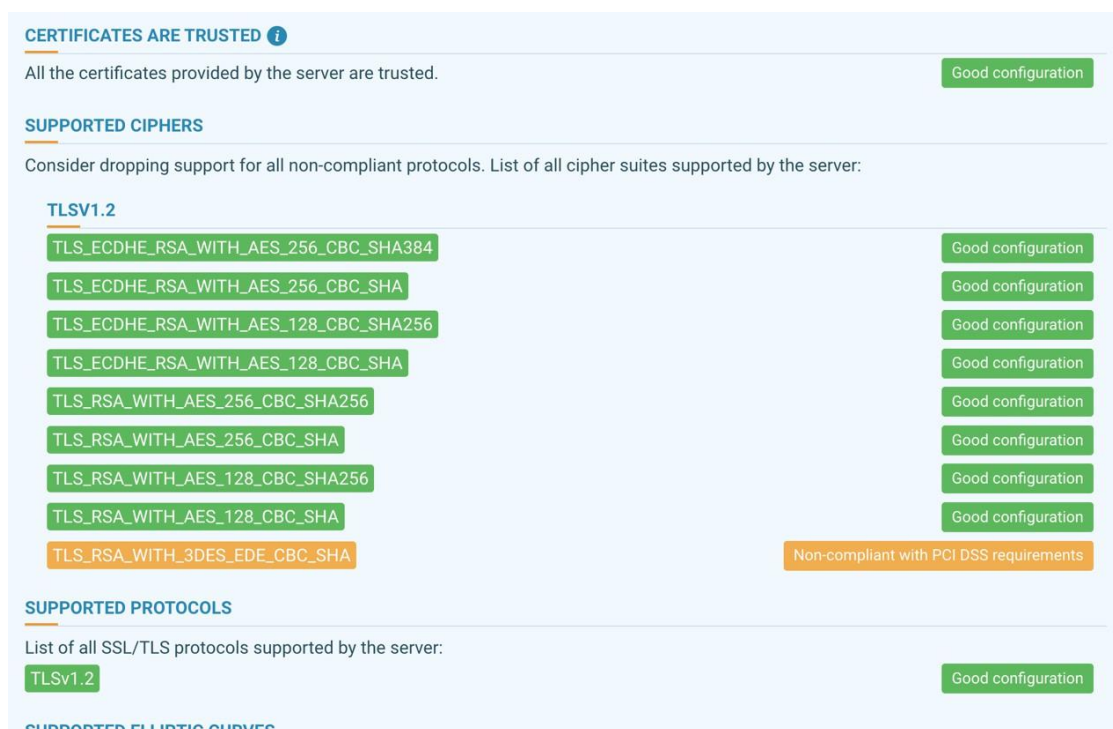


Figure 152: ImmuniWeb TLS Test - helpe.gr (2/4)

As we can see from the second image, in this case the website supports only TLS 1.2 and does not support Authenticated encryption (AEAD) cipher suites. Thus, by further expanding the report we can see the following warnings.

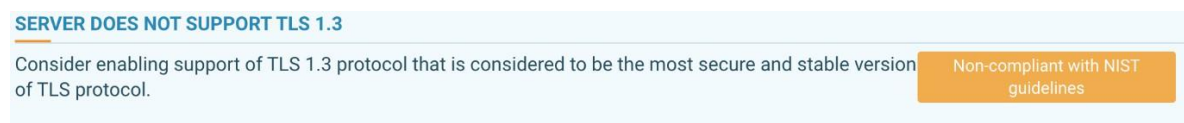


Figure 153: ImmuniWeb TLS Test - helpe.gr (3/4)

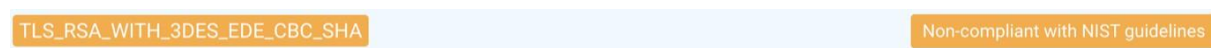


Figure 154: ImmuniWeb TLS Test - helpe.gr (4/4)

In summary, this website has the following main security flaws:

- Weak TLS configuration, specifically TLS version 1.3 is not enabled and in addition there is usage of weak cipher suites
- Cross-Site Scripting (XSS) vulnerability, originating from the outdated jQuery UI 1.10.1

6.3.10 Case Study 10: www.ert.gr

Ert.gr is the official website of the Hellenic Broadcasting Corporation (ERT), which is the public radio and television broadcaster of Greece.

Once again, the ImmuniWeb scan is triggered, however it is partially blocked. The main findings are listed below.



Figure 155: Partial Scan Blockage - ert.gr

Starting with DNSSEC, one unassigned DNS record was detected, specifically the CNAME (Canonical Name) record pointing ertcdn.siliconweb.com. This may leave the website exposed to DNS spoofing related threats.

Next, some marginal issues arise regarding the web software security and CMS. Specifically, the following outdated components have been detected.

- **Menu image, icons made easy 3.10:** The component is outdated. Update to the most recent version 3.11.
- **Dflip – 3d flipbook 2.0.86:** The component is outdated. Update to the most recent version 2.3.32.
- **Timed content 2.77:** The component is outdated. Update to the most recent version 2.90.
- **Onesignal – web push notifications 2.4.0:** The component is outdated. Update to the most recent version 2.4.4.
- **Smart slider 3.5.1.19:** The component is outdated. Update to the most recent version 3.5.1.24.
- **jQuery 3.5.1:** The component is outdated. Update to the most recent version 3.7.1.
- **Underscore.js 1.8.3:** The component is outdated. Update to the most recent version 1.13.7.
- **Core-js3.0.0—3.26.1:** The component is outdated. Current most recent version is 3.38.1.
- **jQuery Migrate 3.3.2:** The component is outdated. Update to the most recent version 3.5.2.

Despite these components being outdated, no related known vulnerabilities were found.

Regarding PCI DSS compliance, although the website is indirectly applicable to this analysis, it is marked as partially incompliant, due to the existence of the previously listed vulnerabilities and the absence of a WAF.

Lastly, the ImmuniWeb scanning tool, suggested that the website has a perfect TLS configuration, which is also verified from the Qualys SSL Labs test. The main findings of that scan are listed below.

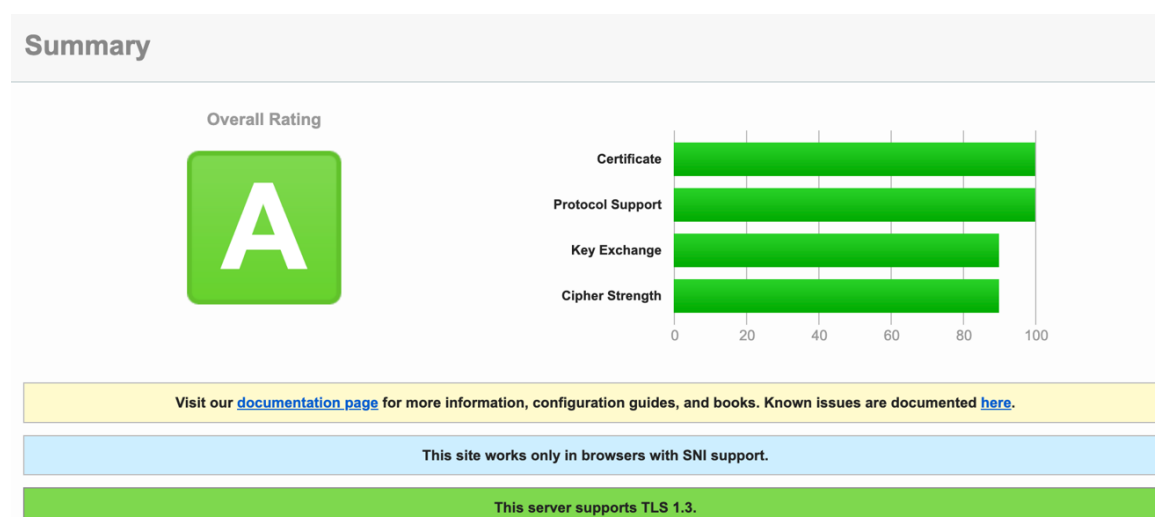


Figure 156: Qualys SSL Labs Test - ert.gr (1/3)

Protocols	
TLS 1.3	Yes
TLS 1.2	Yes*
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

Figure 157: Qualys SSL Labs Test - ert.gr (2/3)

Cipher Suites	
# TLS 1.3 (server has no preference)	
TLS_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA) FS 128
TLS_AES_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA) FS 256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH x25519 (eq. 3072 bits RSA) FS 256
# TLS 1.2 (server has no preference)	
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp521r1 (eq. 15360 bits RSA) FS 128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp521r1 (eq. 15360 bits RSA) FS WEAK 256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp521r1 (eq. 15360 bits RSA) FS WEAK 256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp521r1 (eq. 15360 bits RSA) FS 256

Figure 158: Qualys SSL Labs Test - ert.gr (3/3)

As shown, the TLS configuration is perfect, apart from the two highlighted weak TLS 1.2 cipher suites.

In conclusion, no critical vulnerabilities were detected on this case.

7. Additional Analysis

The appendix is focused on covering aspects that were not covered in the main analysis. As already covered, the website evaluation selection was split into do distinct categories, namely: privacy and security. While the division between privacy and security checks was made for organisational and research purposes, it may not reflect the inherent accuracy of such separation.

Websites in the privacy category, particularly online shops, still have substantial security requirements, especially concerning user transactions. This distinction is evident in cases like *Plaisio.gr* or *e-shop.gr*, which, despite their security needs, were not assessed for security.

On the other hand, the websites that fall under the NIS2 directive, included in the security category must also comply with the cookie regulations set on the ePrivacy Directive and GDPR. Although, a variety of advertising cookies are not expected in public sector websites, other types of cookies like analytic cookies are likely to be present.

Thus, this section contains supplementary security checks for e-commerce websites and cookie checks for all public sector websites. However, it is expected that the findings will be limited in comparison to the main research.

7.1 Supplementary Website Cookie Evaluations

To carry out the cookie evaluation for the rest of the websites, the same methodology was consistently applied throughout. This time however, the results from the ImmuniWeb Privacy scanning tool are not included in this instance, as the websites fully blocked the tool's access.

7.1.1 Gov.gr

First, the CookieYes scanning tool is used, generating the following results.

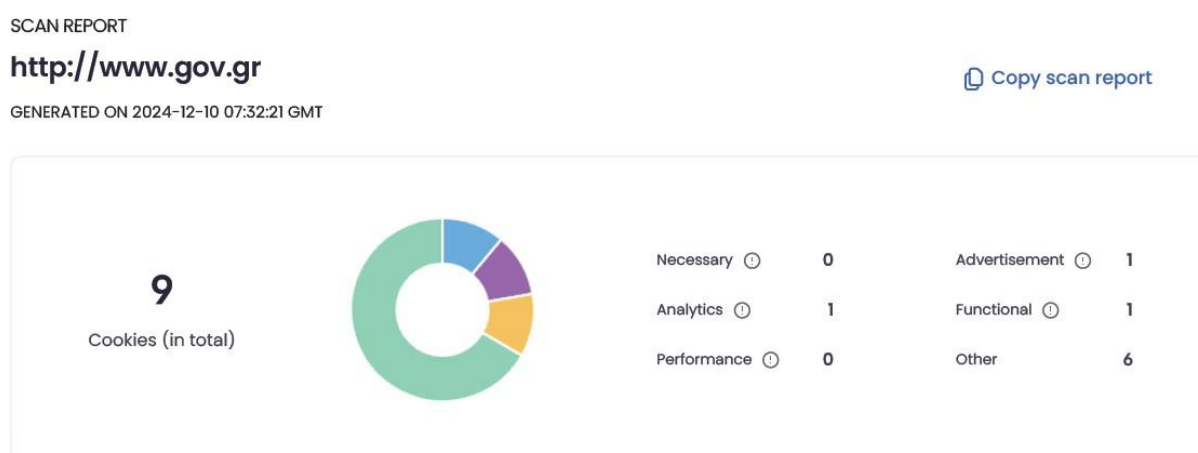


Figure 159: CookieYes Scan Gov.gr

Table 19: CookieYes Cookies gov.gr

<u>Cookie</u>	<u>Description</u>	<u>Duration</u>	<u>Type</u>
topalert	No description available	1 day	Other
Ai_user	Microsoft Azure sets this cookie as a unique useridentifier cookie, enabling counting of the number of users accessing the application over time.	1 year	Advertisement
ai_session	Microsoft insights software to gather statistical and telemetry data	1 hour	Analytics
uw-uid	No description available	never	Other
pubkey.broadcastChannel-account-bannedUntil	No description available	never	Other
locale	No description available	never	Functional
AI_sentBuffer	No description available	Session	Other
AI_buffer	No description available	Session	Other

As expected, only a small number of cookies is detected on the website and only one for analytics purposes, namely Ai_user. According to Cookiepedia, this cookie is often referred to as strictly necessary.

Cookies Search Results: ai_user

This search has identified a match with a recognised pattern type cookie: **userXXXXXXXXXXXXXXXXXX**. The results below are based on data aggregated from all known incidences of this pattern.

About this cookie:

Used to track usage of the embedded video player.

The main purpose of this cookie is: **Strictly Necessary**

Figure 160: ai_user searched on cookiepedia

So far, there are no flaws detected, regarding the cookie configuration. The final step of the evaluation is the dynamic testing, which is carried out once again by visiting the website. The first thing that we can see, is that there is a cookie banner present on the website.



Figure 161: Cookie Banner gov.gr

The cookie banner looks correctly configured and there is no clear indication of dark practises usage, apart from the “Acceptance” box been more transparent. Moreover, by using the cookie-editor extension and clicking the “Rejection” button, no cookies are detected on the websites, apart from a cookie called “Topalert”.



Figure 162: Cookie-Editor gov.gr

As a result, no violations were detected on this website when assessed against the established standards, apart from lack of a “**Revoking Consent**” option, indicating almost full compliance with the required guidelines.

7.1.2 Dei.gr

First, the CookieYes scanning tool is used, generating the following results.

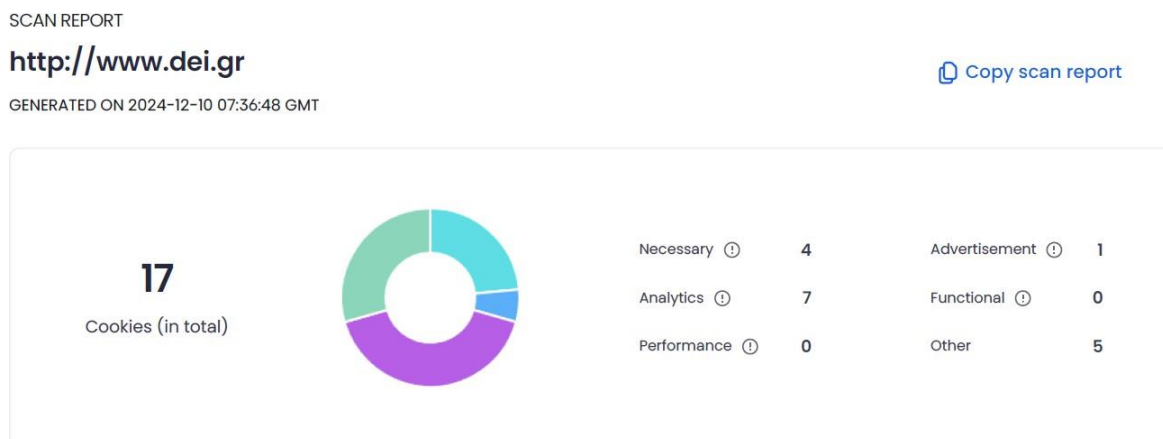


Figure 163: CookieYes scan gov.gr

Table 20: CookieYes Cookies dei.gr

<u>Cookie</u>	<u>Description</u>	<u>Duration</u>	<u>Type</u>
Visid_incap_*	Incapsula sets this cookie to provide cloud-based security services.	1 year	Necessary
Incap_ses_*	Incapsula sets this cookie for DDoS protection	Session	Necessary
.AspNetCore.Antiforgery	Set by Microsoft for Anti-forgery protection	Session	Necessary
Ai_user	Microsoft Azure sets this cookie enabling counting of the number of users accessing the application over time.	1 year	Advertisement
_gcl_a	Aadvertisement efficiency by Google	3 months	Analytics
---utmvc	installed by Google to gather data on the user's site usage	Less than a minute	Analytics
Ai_session	Set my Microsoft to gather statistical and telemetry data	1 hour	Analytics
_ga	Google Analytics, calculates visitor, session and campaign data and also keeps track of site usage for the site's	More than a year	Analytics
_gid	Google Analytics stores information on how visitors use the website.	1 day	Analytics

_gat_gtag_UA_*	Google Analytics sets this cookie to store a unique user ID	1 Minute	Analytics
OptanonConsent	OneTrust sets this cookie to store details about the site's cookie category and check whether visitors have given or withdrawn consent from the use of each category.	1 year	Necessary
_fbp	Facebook cookie to store and track interactions.	3 months	Analytics
lastExternalReferrerTime	No description available	Never	Other
lastExternalReferrer	No description available	Never	Other
Ai_sentBuffer	No description available	Session	Other
AI_buffer	No description available	Session	Other
.AspNetCore.Mvc	No description available	Past	Other

As expected, only a small number of cookies is detected on the website and once again only one for advertising purposes, namely Ai_user. According to Cookiepedia, this cookie is often referred to as strictly necessary.

Next, by visiting the website we initiate the dynamic analysis, by first inspecting the cookie banner.

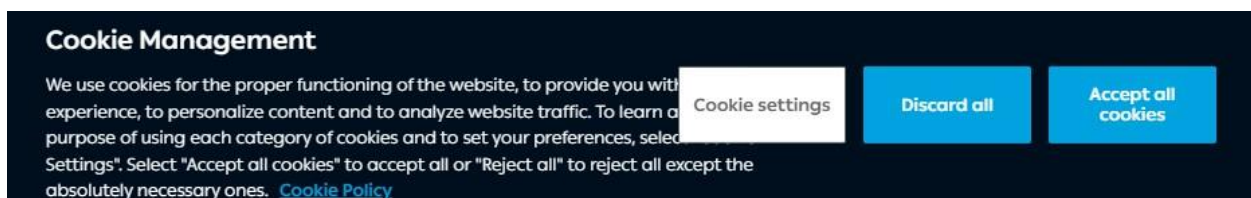


Figure 164: Cookie banner dei.gr

By clicking the “Cookie settings”, the cookie banner is expanded, as shown on the image below.

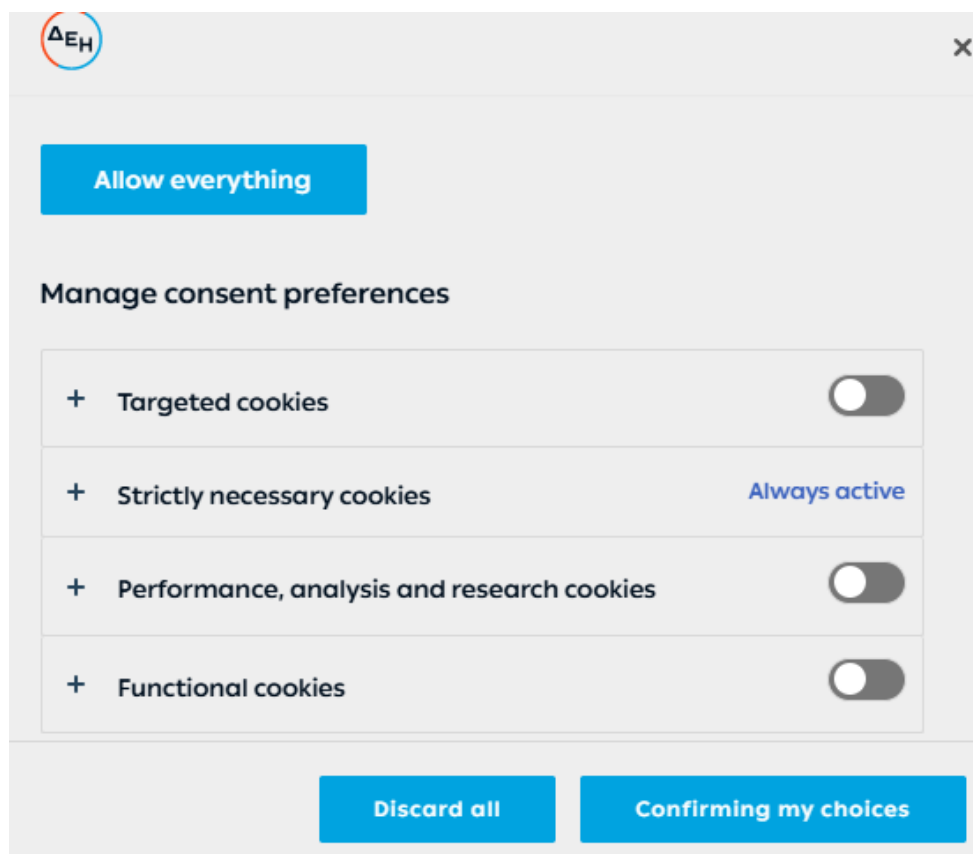


Figure 165: Expanded cookie banner dei.gr

Therefore, the cookie banner is properly configured, and there is no evidence of dark patterns or misleading practices, ensuring a transparent and user-friendly experience.

Finally, by clicking the “Discard all” options, we accept only Strictly necessary cookies. Contrary to this, the output from the Cookie-Editor extension, as shown in the image below, indicates otherwise.

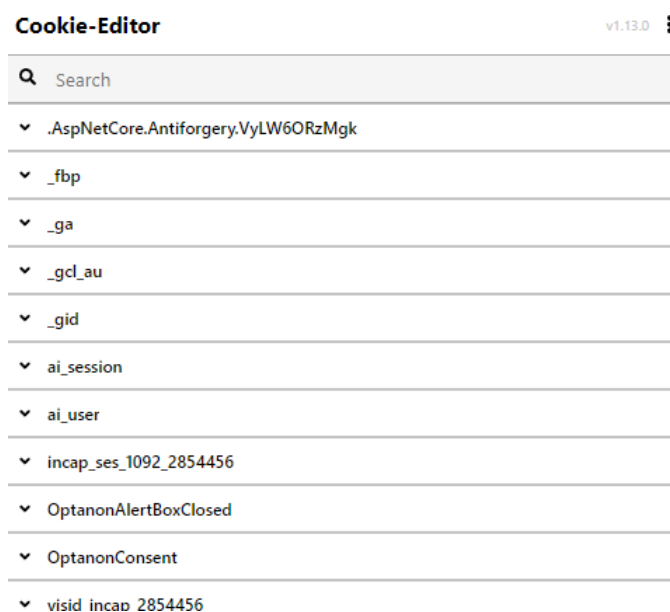


Figure 166: Cookie-Editor dei.gr

The cookie-Editor, detected cookies like, _ga, _gcl_au, _gid, which are google analytics cookies and by no means strictly necessary. Therefore, in this case there is a clear

violation, specifically cookies with incorrectly assigned labels. Additionally, there is no option to revoke consent.

In summary, one violation was detected:

- **Incorrectly Assigned Labels for Cookies with a Well-Defined Purpose**

7.1.3 Nbg.gr

Initiating the analysis, the CookieYes scan is executed, generating the following results.

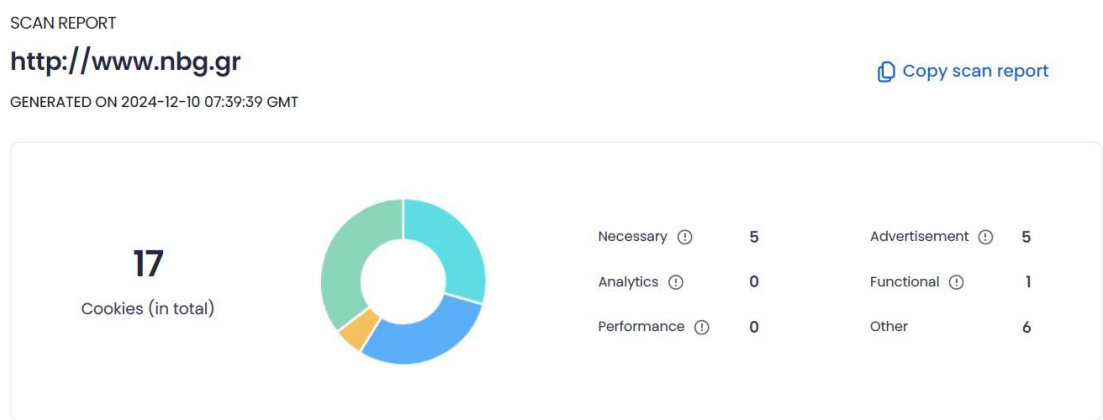


Figure 167: CookieYes scan nbg.gr

Table 21: CookieYes cookies nbg.gr

Cookie	Description	Duration	Type
YSC	Set by Youtube to track views of embedded videos.	Session	Advertisement
--Secure-Roullout_TOKEN	No description available	6 months	Other
VISITOR_INFO1_LIVE	Set by Youtube to measure bandwidth	6 months	Advertisement
VISITOR_PRIVACY_METADATA	Youtube sets this to store the user's cookie consent state for the current domain	6 months	Advertisement
OptanonConsent	OneTrust sets this cookie to store details about the site's cookie	1 year	Necessary

	category and check whether visitors have given or withdrawn consent from the use of each category.		
ApplicationGatewayAffinityCORS	No description available	Session	Other
ApplicationGatewayAffinity	This cookie is set by the Laravel Framework. This cookie is used for managing browsing sessions.	Session	Necessary
Ak_bmsc	Used by Akamai to optimize security and bot protection	2 hours	Necessary
ARRAffinity	Azure	Session	Necessary
ARRAffinitySameSite	This cookie is set by Windows Azure cloud, and is used for load balancing to make sure the visitor page requests are routed to the same server in any browsing session.	Session	Necessary
Plyr	No description available	Never	Other
Cache-sprite-plyr	No description available	Never	Other
yt.innertube::nextId	by YouTube, registers a unique ID to store data on what videos	Never	Advertisement

	from YouTube the user has seen.		
ytidb::LAST_RESULT_ENTRY_KEY	is used by YouTube to store the last search result entry that was clicked by the user.	Never	Functional

In this case, five advertisement cookies were detected, which is to be expected given that the website belongs to a bank. Financial institutions often use such cookies for targeted advertising and promotions.

Next, the dynamic analysis takes place, by first inspecting the cookie banner as shown on the image below.

To ensure a top browsing experience, to analyze traffic and to use personalized ads, the website uses cookies. For more information, click [here](#).

[Cookie settings](#)

Discard all

Accept all

Figure 168: Cookie banner nbgr.gr

By clicking the “Cookie Settings” option, the banner is expanded, displaying the following information.

The image shows an expanded cookie banner for the website ΕΘΝΙΚΗ ΤΡΑΠΕΖΑ. At the top, there is a close button (X) and an "Allow everything" button. Below this, the section "Manage consent preferences" is displayed. It contains a list of cookie categories with expandable plus signs and toggle switches:

- Strictly necessary cookies: Always active
- Functional cookies: Toggle switch (off)
- Targeted cookies: Toggle switch (off)
- Performance cookies: Toggle switch (off)
- Profiling: Toggle switch (off)

At the bottom of the banner, there are two buttons: "Discard all" and "Confirming my choices".

Figure 169: Expanded cookie banner nbgr.gr

Thus, the cookie banner is properly configured. The final step involves scanning the website with the Cookie-editor extension, after first clicking the “Discard all” option. Cookie-editor detected the following cookies on the website.

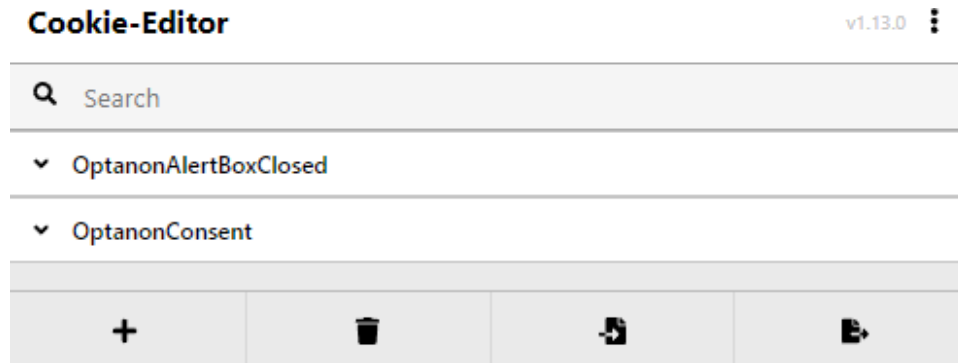


Figure 170: Cookie-editor nbg.gr

In conclusion, the website demonstrated full compliance, with no violations identified in its cookie practices or overall configuration.

7.1.4 Oasa.gr

First, the CookieYes scan was triggered, detecting zero cookies on the website.

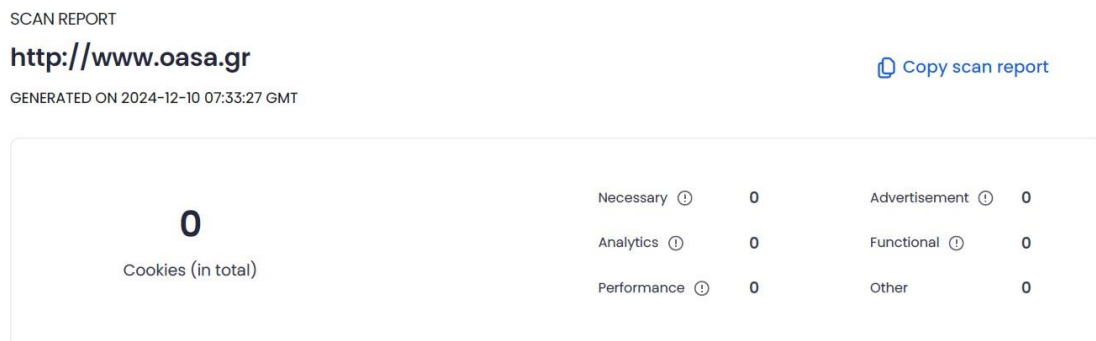


Figure 171: CookieYes scan oasa.gr

Then by visiting the website, the following cookie banner is displayed.

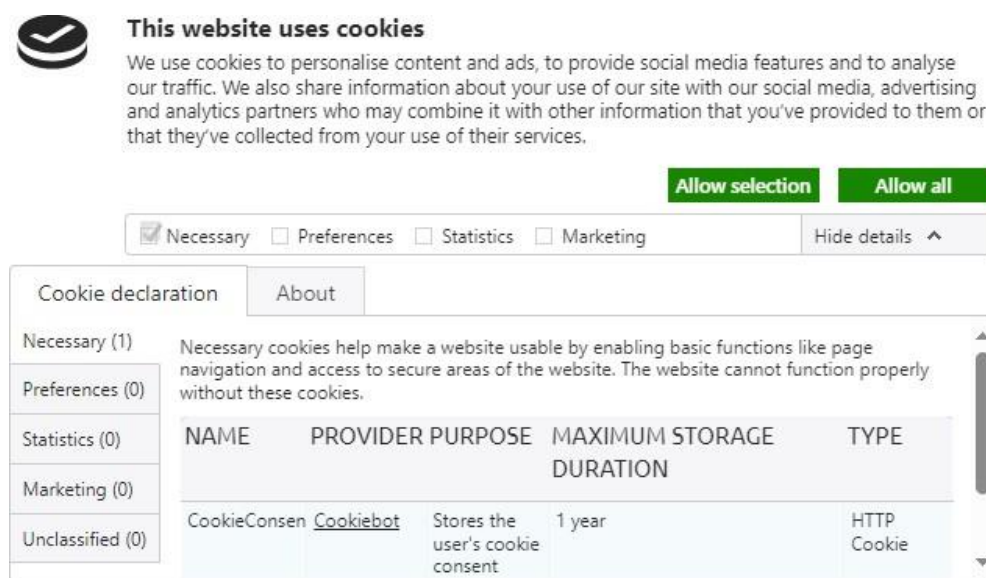


Figure 172: Cookie banner oasa.gr

The cookie banner is correctly configured, and it also states that the only cookie present on the website, is one necessary cookie, namely CookieConsent cookie. By clicking the “Allow Selection” option and using the cookie-editor extension the following cookies are detected.

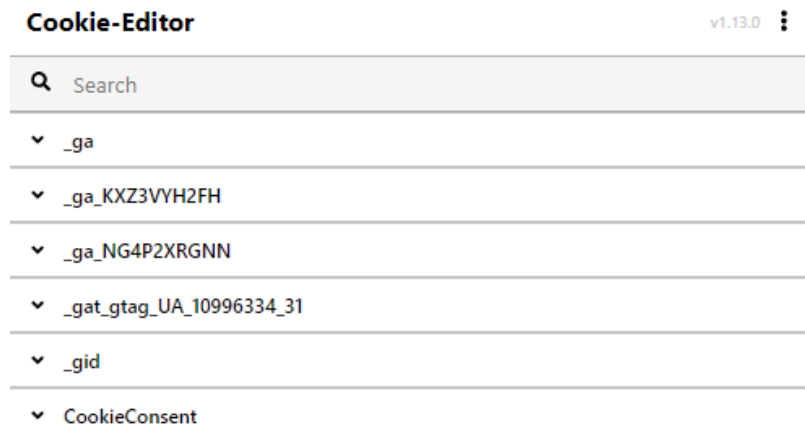


Figure 173: Cookie-editor oasa.gr

As shown, apart from the CookieConsent cookie there are also Google Analytics cookies present on the website, indicating a clear violation. Lastly, in this case there is an option to withdraw consent.

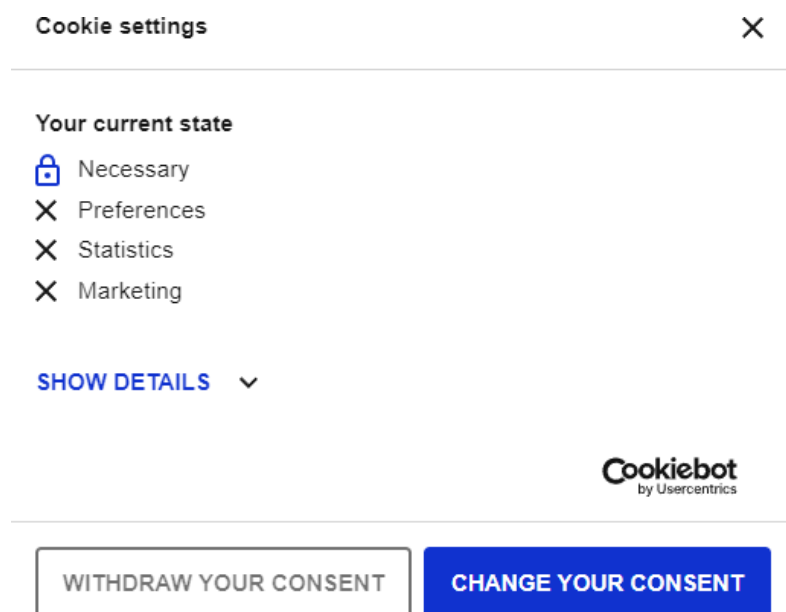


Figure 174: Revoking consent option oasa.gr

Thus, the findings in this case are:

- **Incorrectly Assigned Labels for Cookies with a Well-Defined Purpose**
- **Undeclared Cookies**

7.1.5 Nis.gr

Once again, initiating the CookieYes scan; the results are listed below.

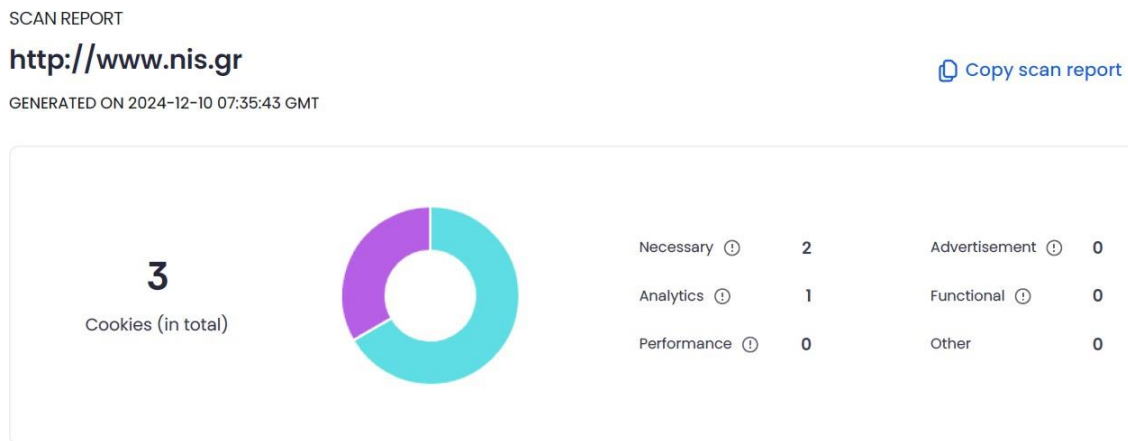


Figure 175: CookieYes scan nis.gr

Table 22: CookieYes cookies nis.gr

Cookie	Description	Duration	Type
Visid_incap_*	Incapsula sets this cookie to provide cloud-based security services.	1 year	Necessary
Incap_ses_*	Incapsula sets this cookie for DDoS protection	Session	Necessary
---utmvc	installed by Google to gather data on the user's site usage	Session	Analytics

According to the scan results, no advertising cookies are detected.

Furthermore, after visiting the website, there is no cookie banner present on the website. Lastly, the cookie-editor extension detected the exact same cookies with CookieYes, as shown on the image below.

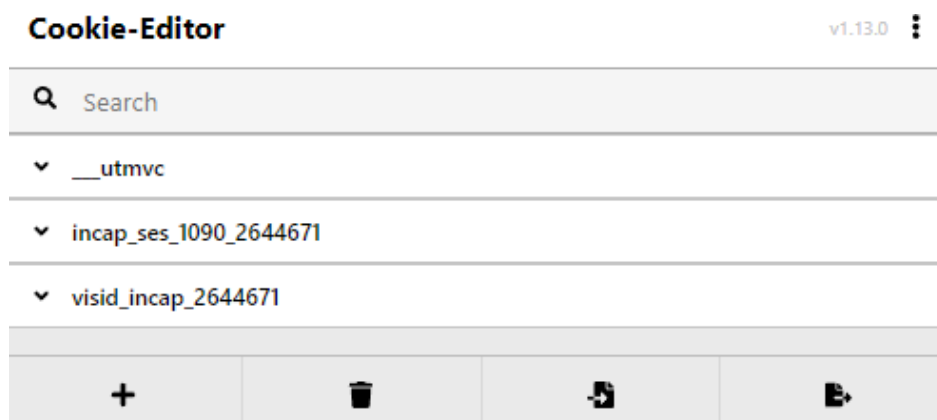


Figure 176: Cookie-editor nis.gr

Therefore, the only violation detected is the **absence of a cookie banner**.

7.1.6 Eydap.gr

Initiating the analysis, the CookieYes scan is executed, generating the following results.

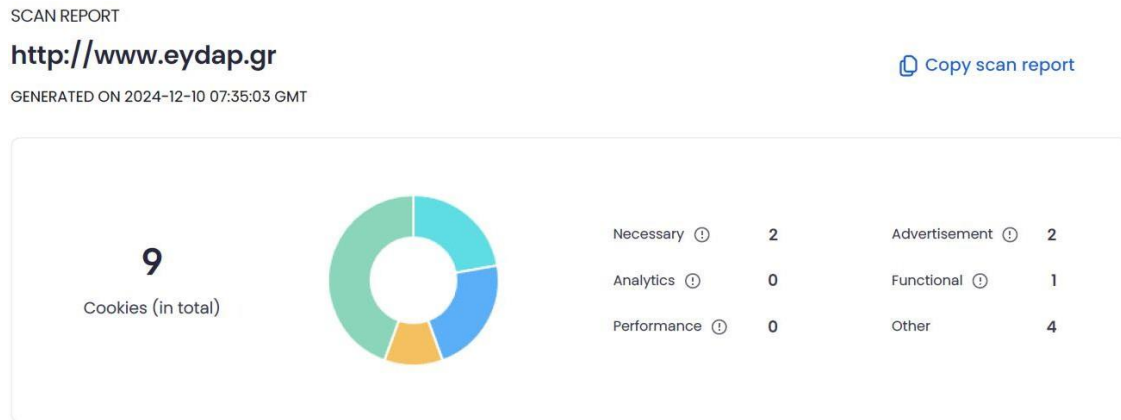


Figure 177: CookieYes scan eydap.gr

Table 23: CookieYes cookies eydap.gr

<u>Cookie</u>	<u>Description</u>	<u>Duration</u>	<u>Type</u>
ASP.NET_SessionId	Issued by Microsoft's ASP.NET Application, this cookie stores session data during a user's website visit.	Session	Necessary
TS01	Wix sets this cookie for security and anti-fraud purposes	Session	Necessary
Uw-icon-locales	No description available	Never	Other
Uw-uid	No description available	Never	Other
Yt.innertube::nextId	Set by youtube to store data on what videos the user has seen	Never	Advertisement
ytidb::LAST_RESULT_ENTRY_KEY	By YouTube to store the last search result entry that was	Never	Functional

	clicked by the user.		
yt.innertube::requests	by YouTube, registers a unique ID to store data on what videos from Youtube the user has seen	Never	Advertisement
-7d035e0f-71cc6de5	No description available	Session	Other
lu5q-!O9@\$	No description available	Session	Other

This time, there are Youtube advertisement cookies present.

Moving on with the dynamic analysis, which is conducted by visiting the website we can verify that there is a cookie banner present on the website.

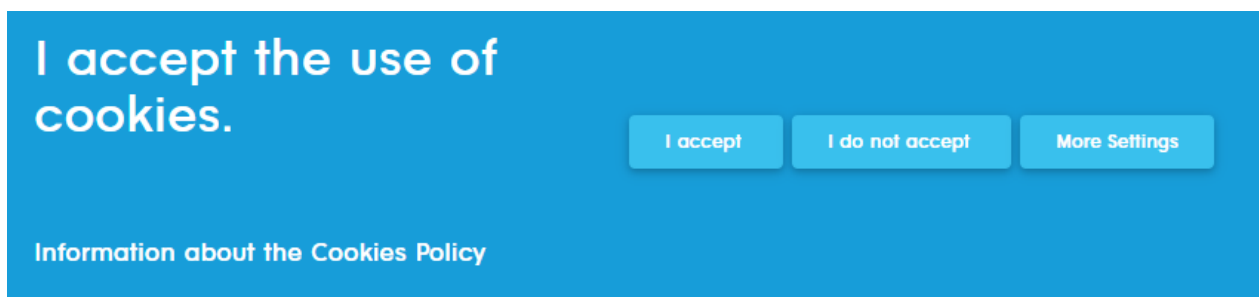


Figure 178: Cookie banner eydap.gr

By clicking “More Settings”, the cookie banner is expanded as shown on the image below.

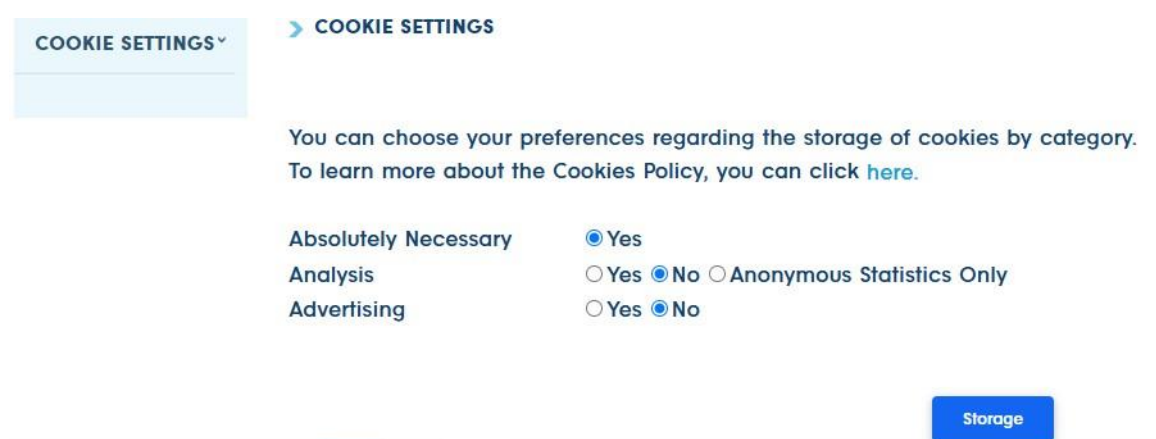


Figure 179: Expanded cookie banner eydap.gr

Therefore, the cookie banner is properly configured. Then, by selecting “I do not accept», only strictly necessary cookies should be installed on the browser. This is verified by the cookie-editor output, as shown on the image below.

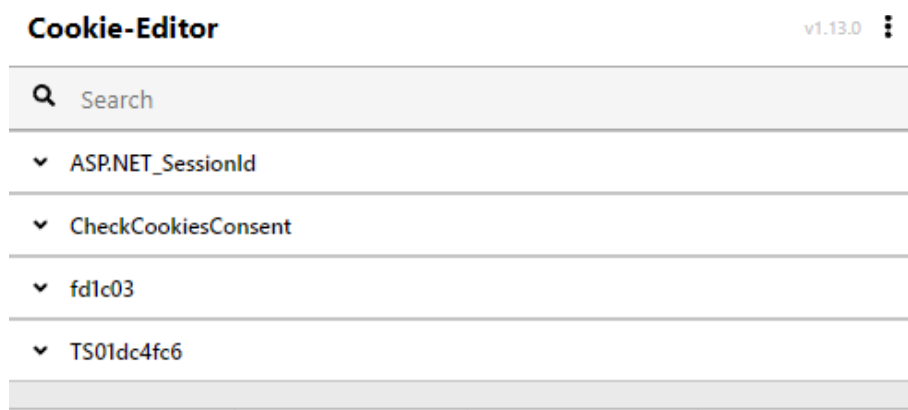


Figure 180: Cookie-editor eydap.gr

This website has exemplary cookie settings and is fully compliant with the set privacy regulations.

7.1.7 Alpha.gr

First, the CookieYes scan is triggered, detecting zero cookies on the website.

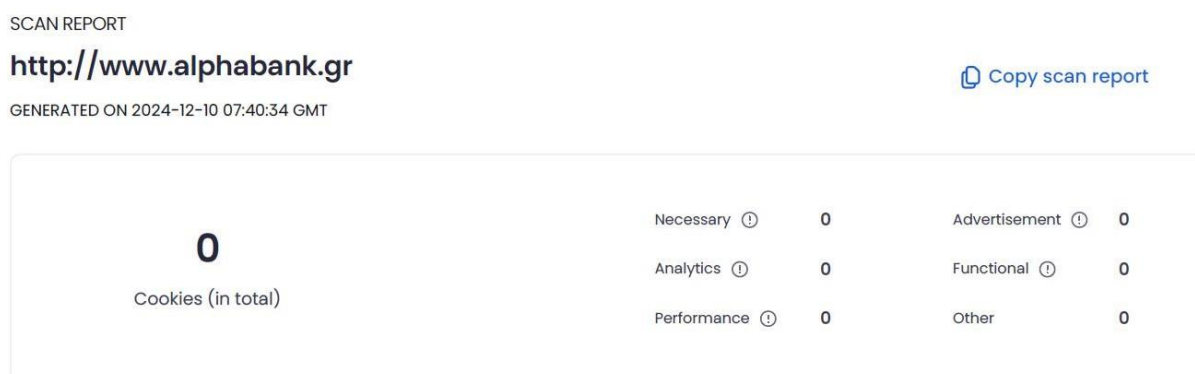


Figure 181: CookieYes scan alpha.gr

Then, by visiting the website to perform the dynamic analysis, the first thing that is detected is the presence of a cookie banner.

We use cookies for the proper and secure operation of our site. To provide you with a personalized online experience, we use additional cookies with your consent. If you agree to all additional cookies, select "I accept". If you do not agree, select "I do not accept". Please read our Cookie Policy and select "Cookie Settings" to manage your preferences. [Cookie Policy](#)



Figure 182: Cookie banner alpha.gr

By clicking on the "Cookie Settings" button, the cookie banner expands, providing additional information.

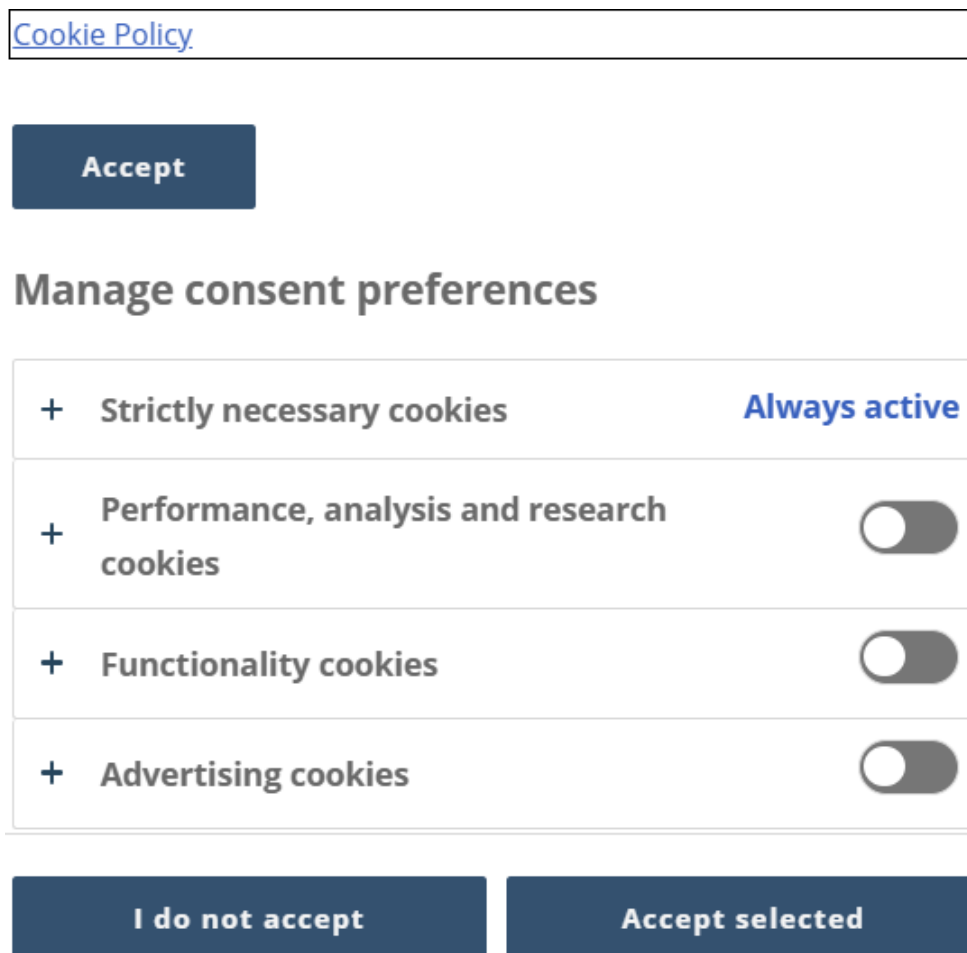


Figure 183: Expanded cookie banner alpha.gr

As shown, the cookie banner is correctly configured. Then, by selecting the “I do not accept” option, only strictly necessary cookies should be installed on the browser. This is confirmed by the findings of the cookie-editor extension, which are displayed on the image below.

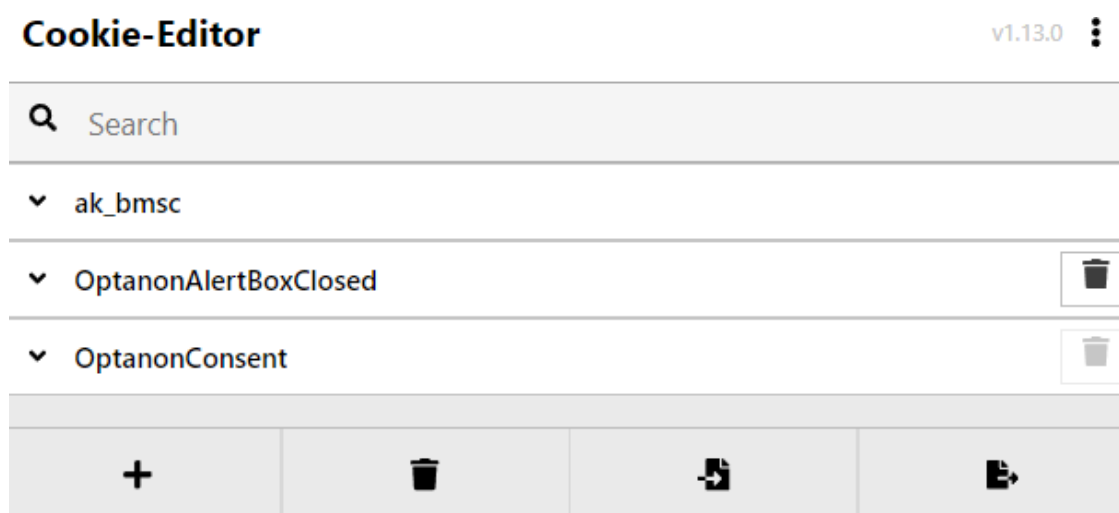


Figure 184: Cookie-editor alpha.gr

Thus, the website has perfect configuration in terms of cookies.

7.1.8 Aegeanair.com

First, the CookieYes scan is triggered and generates the following findings.

SCAN REPORT

<http://www.aegeanair.com>

[Copy scan report](#)

GENERATED ON 2024-12-10 07:37:40 GMT

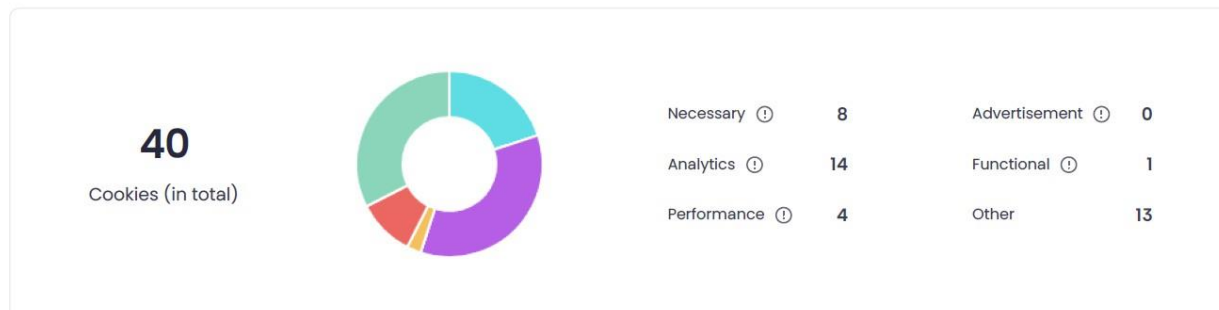


Figure 185: CookieYes scan aegeanair.com

The scan detected zero advertisement cookies. In this case the full cookie list is not attached, due to its excessive size.

Moving forward with the dynamic analysis, by visiting the website the first thing that is verified is that the website has a cookie banner.



Figure 186: Cookie banner aegeanair.com

By clicking “Settings”, the cookie banner expands displaying the following information.

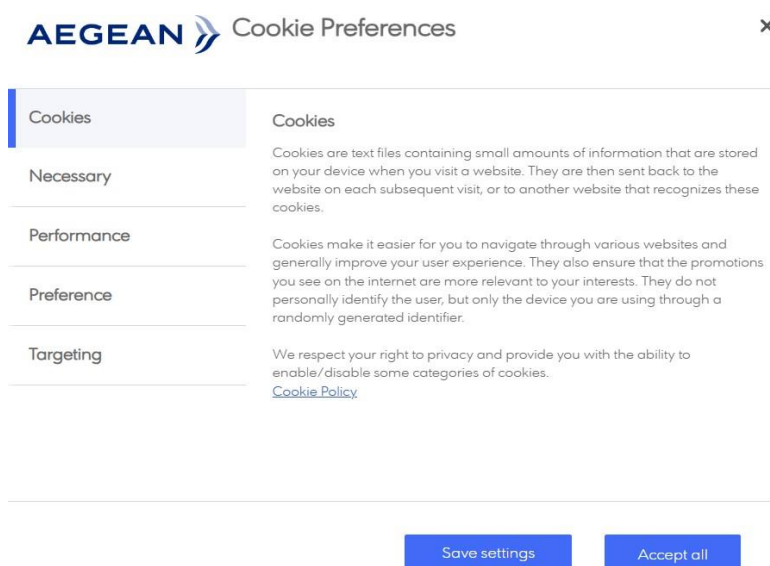


Figure 187: Expanded cookie banner aegeanair.com

As shown, the cookie banner is properly configured. Then by clicking the “Rejection” option only strictly necessary cookies should be installed on the browser. However, this is not the case based on the cookie-editor findings.

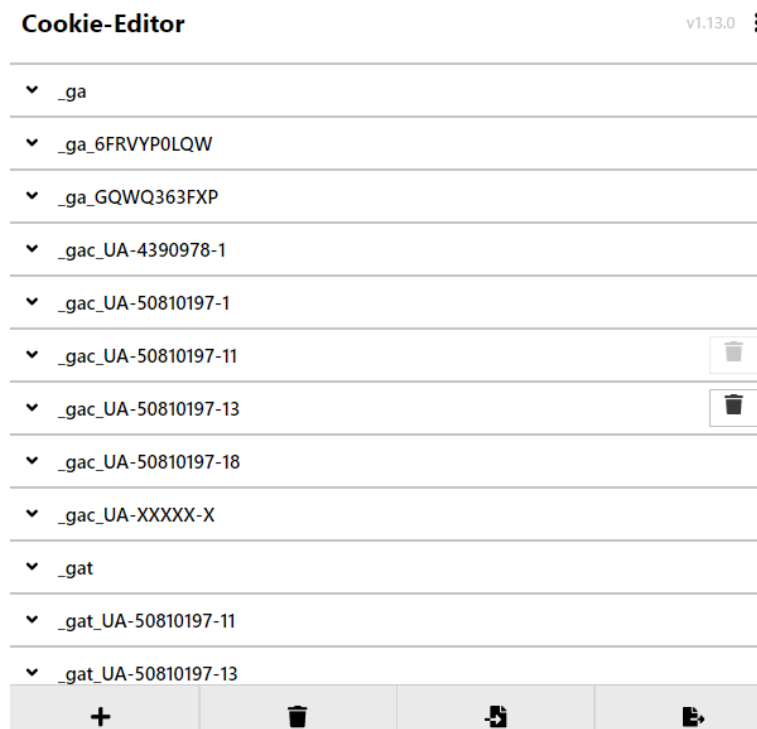


Figure 188: Cookie-editor aegeanair.com

As we can see, there is a large number of Google Analytics cookies detected. Furthermore, there is no option for revoking consent

In summary, through the examination the following violations were detected:

- **Incorrectly Assigned Labels for Cookies with a Well-Defined Purpose**
- **No clear option for revoking consent**

7.1.9 Helpe.gr

As always, the CookieYes scan is triggered, generating the following results.

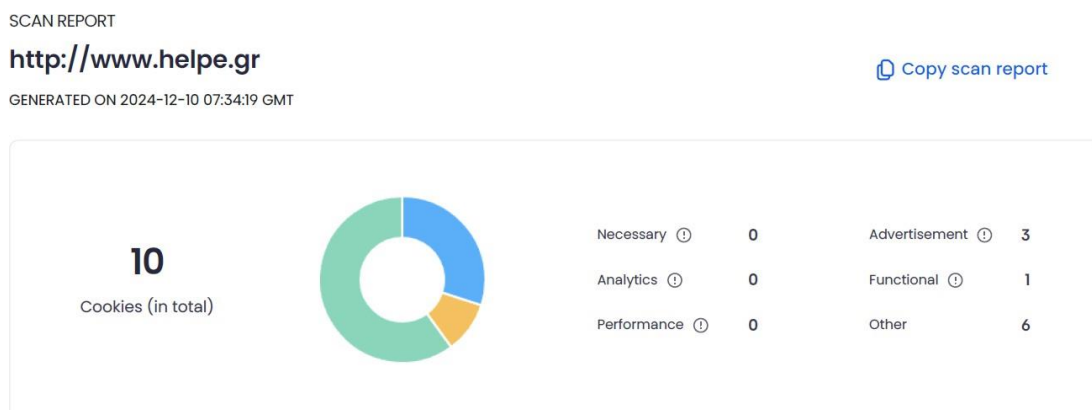


Figure 189: CookieYes scan helpe.gr

Table 24: CookieYes Cookies helpe.gr

<u>Cookie</u>	<u>Description</u>	<u>Duration</u>	<u>Type</u>
VISITOR_INFO1_LIVE	By youtube to measure bandwidth	6 Months	Advertisement
VISITOR_PRIVACY_METADATA	By youtube to store user's cookie consent	6 Months	Advertisement
Simple-FONtresize	No description available	Session	Other
ytidb::LAST_RESULT_ENTRY_KEY	By YouTube to store the last search result entry that was clicked by the user.	Never	Functional
History.store	No description available	Session	Other
-7d035e0f-71cc6de5	No description available	Session	Other
lu5q-!O9@\$	No description available	Session	Other
7c5f2124731215	By youtube / no description	Session	Other

Specifically, two well-known advertisement cookies from YouTube have been detected. In continuation of the examination, the dynamic analysis takes place. Starting, there is a cookie banner present on the website.

Consent

Details

About

This website uses cookies.

We use cookies to personalize content and ads, provide social media features, and analyze our traffic. In addition, we share information about how you use our website with social media, advertising, and analytics partners, who may combine it with other information you have provided to them or that they have collected in connection with your use of their services.

Absolutely Necessary 	Preference 	Statistics 	Advertising
---------------------------------	-----------------------	-----------------------	------------------------

Refusal

Choice allowed

Allow everything

Figure 190: Cookie banner helpe.gr

By clicking the “Details” option, the cookie banner expands and displays the following information.

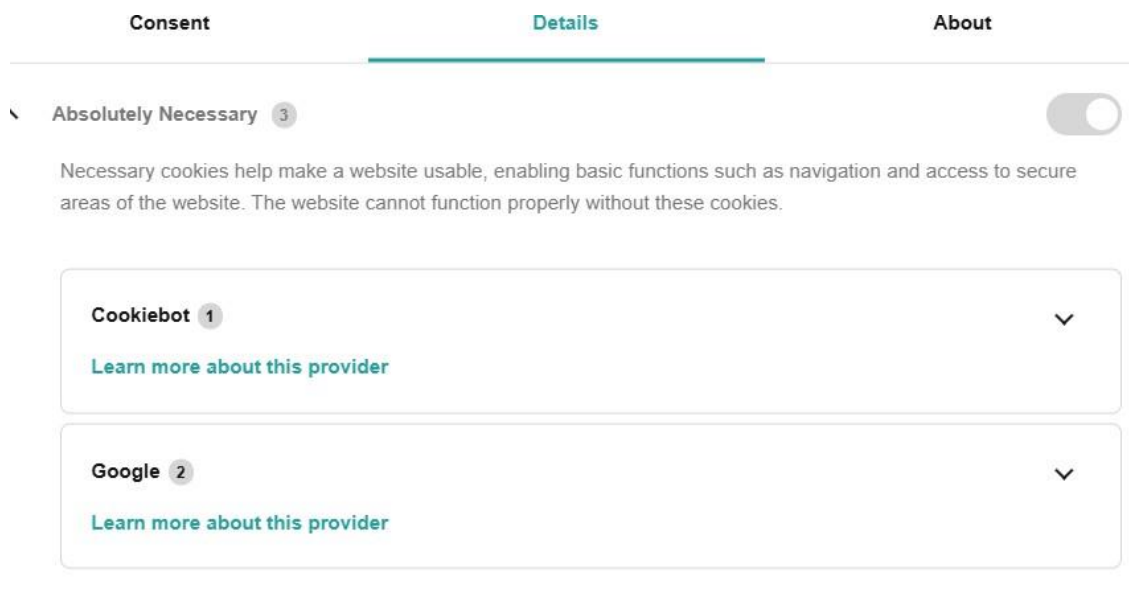


Figure 191: Expanded Cookie banner helpe.gr

As shown, there are Google cookies listed as strictly necessary. Therefore, there is a high indication that Google Analytics cookies may have been falsely labelled. To verify this assumption, we click the “Refusal” option and then use the cookie-editor extension.



Figure 192: Cookie-editor helpe.gr

As shown there no Google cookies detected. Therefore, the statement in the cookie banner was false. Also, there is an option for revoking consent.

Despite google cookies not being installed, this is still a **marginal violation for cookies with incorrectly assigned labels.**

7.1.10 Ert.gr

By scanning the website with CookieYes the following data is extracted.

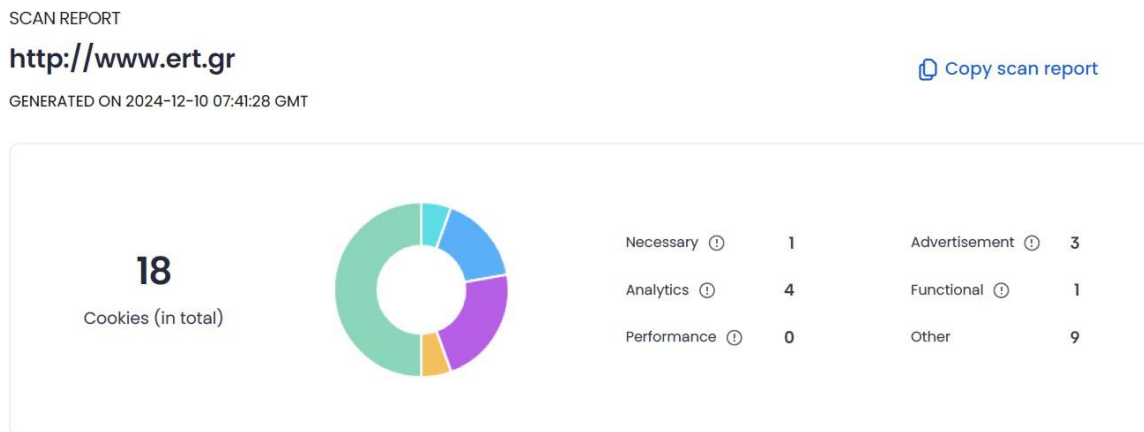


Figure 193: CookieYes scan ert.gr

Table 25: CookieYes cookies ert.gr

<u>Cookie</u>	<u>Description</u>	<u>Duration</u>	<u>Type</u>
__cf_bm	Set by Cloudflare for bot management	1 hour	Necessary
_ga_*	Google Analytics for storing and counting page views	More than a year	Analytics
_ga	Google Analytics for tracking	More than a year	Analytics
_fbp	Facebook cookie for interaction tracking	3 months	Analytics
C	No description available	1 Month	Other
Khaos	Rubicon Project sets this for analytics	1 year	Advertisement
Audit	By Rubicon for recording cookie consent	1 year	Functional
Uid	Google UserID that	2 months	Analytics

	tracks users in website segments		
I	By OpenX to record anonymized user data	1 year	Advertisement
Pd	By OpenX to provide users with personalised marketing content	15 days	Advertisement
Ar_debug	No description available	Past	Other
lastExternalReferrerTime	No description available	Never	Other
Os_pageviews	No description available	Never	Other
isOptedOut	No description available	Never	Other
lastExternalReferrer	No description available	Never	Other
isPushNotificationsEnabled	No description available	Never	Other
Onesignal-pageview-count	No description available	Session	Other
ONESIGNAL_HTTP_PROMPT_SHOWN	No description available	Session	Other

In this case, three advertisement cookies have been detected.

Moving forward, the website is visited in order to conduct the dynamic analysis. Firstly, there is a cookie banner present on the website.

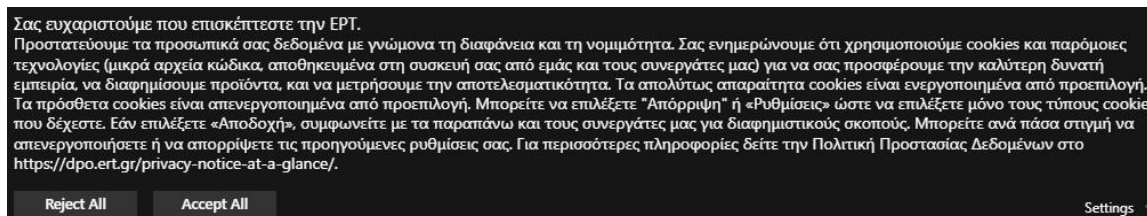


Figure 194: Cookie banner ert.gr

By clicking the “Settings” option, the cookie banner is expanded providing additional information regarding the cookies present on the website.

Cookie Statement

Ads Settings

About

Necessary (12)

Preferences (9)

Statistics (11)

Commercial promotion (30)

Uncategorized (100)

Necessary cookies help make a website usable, enabling basic functions such as navigation and access to secure areas of the website. The website cannot function properly without these cookies.

Name	Provider	Purpose	Maximum storage duration	Type
Cookie Consent [x4]	archive.ert.gr helpdesk.ert.gr program.ert.gr Cookiebot	Stores the user's cookie consent state for the	1 year	HTTP Cookies

Figure 195: Expanded cookie banner ert.gr

As we can see there are 100 uncategorized cookies listed on the banner, which according to our framework counts as a violation. Next, by selecting the “Reject all” option and using the cookie-editor extension, the following cookies are detected on the browser.



Figure 196: Cookie-editor ert.gr

A google analytics cookie has been detected, which was not listed in the Necessary cookie list, therefore this counts as another violation. Moreover, there is no option for revoking cookie consent.

Thus, in this case the following violations have been detected.

- **Unclassified Cookies**
- **Incorrectly Assigned Labels for Cookies with a Well-Defined Purpose**
- **No clear option for revoking consent**

7.2 Supplementary Website Security Evaluations

As already discussed, while examining sites within the scope of NIS2, it's important to note that security assessment and scanning are equally applicable to e-commerce websites, e-shops, and similar platforms. These sites, regardless of industry or regulatory requirements, remain vulnerable to cyber threats and require ongoing monitoring and strong security practices to protect user data and business operations.

Unfortunately, in this case all the scanning attempts were blocked by the website security safeguards. As a result, the evaluation is limited just to the SSL/TLS configuration.

7.2.1 Plaisio.gr

Likewise with previous examples, the Qualys SSL labs scan is initiated, generating the following results.

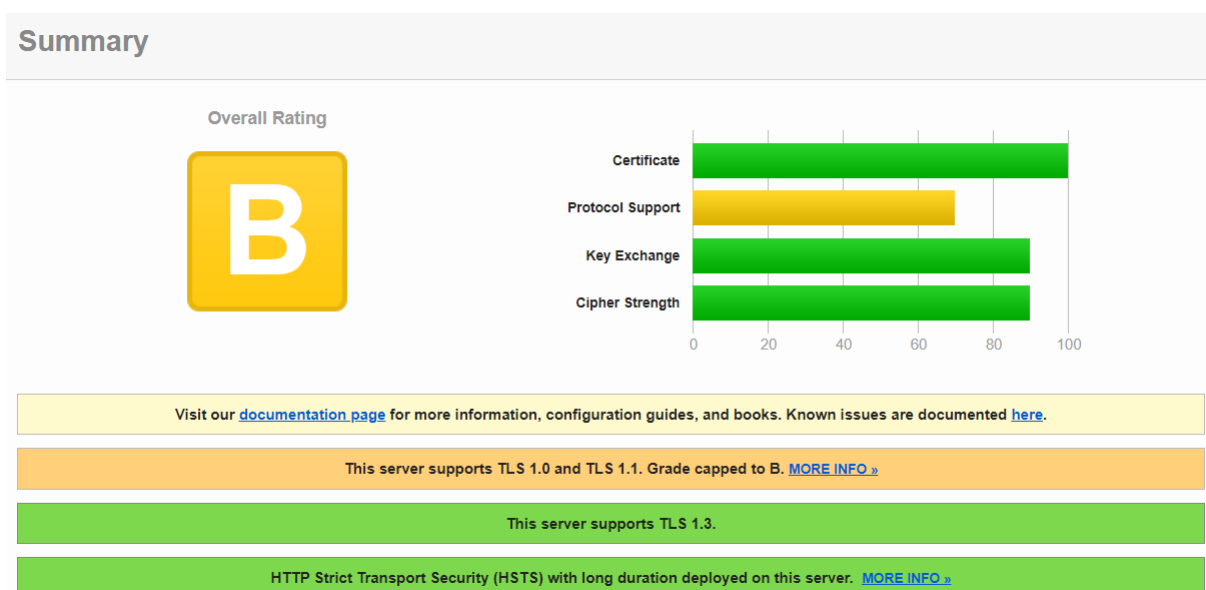


Figure 197: SSL Scan rating plaisio.gr

Configuration

Protocols	
TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

Figure 198: SSL configuration plaisio.gr

# TLS 1.2 (suites in server-preferred order)			
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS		256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS		128
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)	ECDH secp256r1 (eq. 3072 bits RSA) FS		256 ^P
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	WEAK	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)		WEAK	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)		WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)		WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)		WEAK	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		WEAK	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		WEAK	128

Figure 199: TLS cipher suites plaisio.gr

Based on the scanning results, the website has several issues with its SSL/TLS configuration. Specifically, it supports TLS 1.0 and TLS 1.1, along with weak cypher suites. As a result, the website is vulnerable to downgrading attacks, which combined with the weak cipher suites can lead to data breaches, eavesdropping and other malicious activities.

To mitigate the risk, it is best to disable the older version of the TLS protocol.

7.2.2 Public.gr

The Qualys SSL labs scan is triggered, generating the following results.

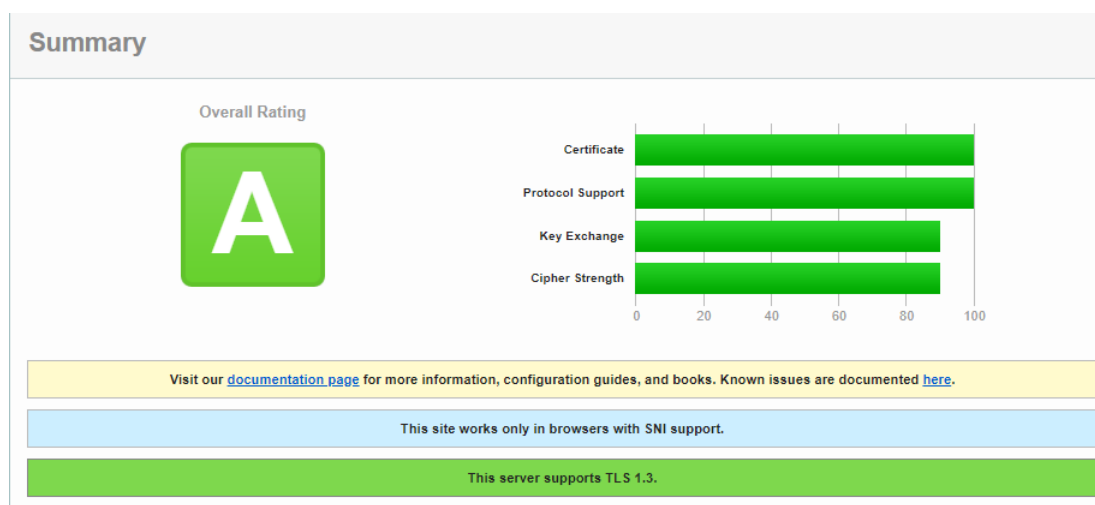


Figure 200: SSL scan rating public.gr

Configuration		
	Protocols	
	TLS 1.3	Yes
	TLS 1.2	Yes
	TLS 1.1	No
	TLS 1.0	No
	SSL 3	No
	SSL 2	No

Figure 201: SLL configuration public.gr

Based on the findings, the website has a strong TLS configuration, as older versions like TLS 1.0 and TLS 1.1 are disabled. While TLS 1.2 does have some known vulnerabilities, it is nearly impossible to disable it entirely, as it remains essential for compatibility with many clients and systems.

7.2.3 E-shop.gr

The Qualys SSL Labs scan is triggered, generating the following results.

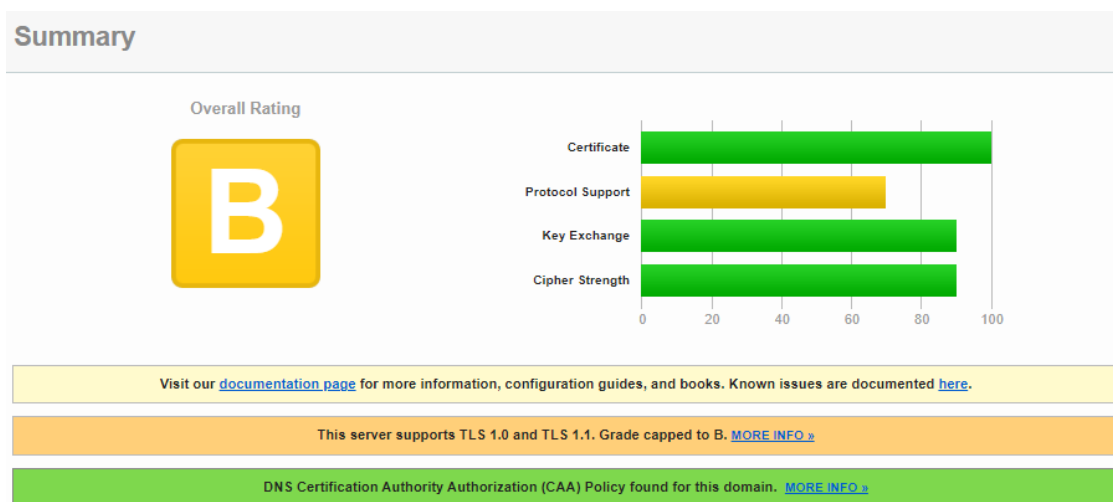


Figure 202: SSL scan rating e-shop.gr

Configuration		
	Protocols	
	TLS 1.3	No
	TLS 1.2	Yes
	TLS 1.1	Yes
	TLS 1.0	Yes
	SSL 3	No
	SSL 2	No

Figure 203: SSL configuration e-shop.gr

Evaluation of Websites with Respect to Security and Privacy Services

 Cipher Suites		
# TLS 1.2 (suites in server-preferred order)		
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128 WEAK
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128 WEAK
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256 WEAK
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256 WEAK
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 2048 bits FS	128 WEAK
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 2048 bits FS	256 WEAK
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)		128 WEAK
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)		256 WEAK
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)		128 WEAK
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)		256 WEAK
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		128 WEAK
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		256 WEAK
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)		112 WEAK
# TLS 1.1 (suites in server-preferred order)		
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128 WEAK
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256 WEAK
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		128 WEAK
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		256 WEAK
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)		112 WEAK
# TLS 1.0 (suites in server-preferred order)		
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128 WEAK
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256 WEAK
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)		128 WEAK
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)		256 WEAK
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)		112 WEAK

Figure 204: TLS cipher suites e-shop.gr

Based on the scanning results, the website has several issues with its SSL/TLS configuration. Specifically, it supports TLS 1.0 and TLS 1.1, along with weak cypher suites. As a result, the website is subject to vulnerabilities like, downgrading attacks, which combined with the weak cipher suites can lead to data breaches, eavesdropping and other malicious activities.

7.2.4 Factoryoutlet.gr

Once again, after the SSL scanning completion, the following results are generated.

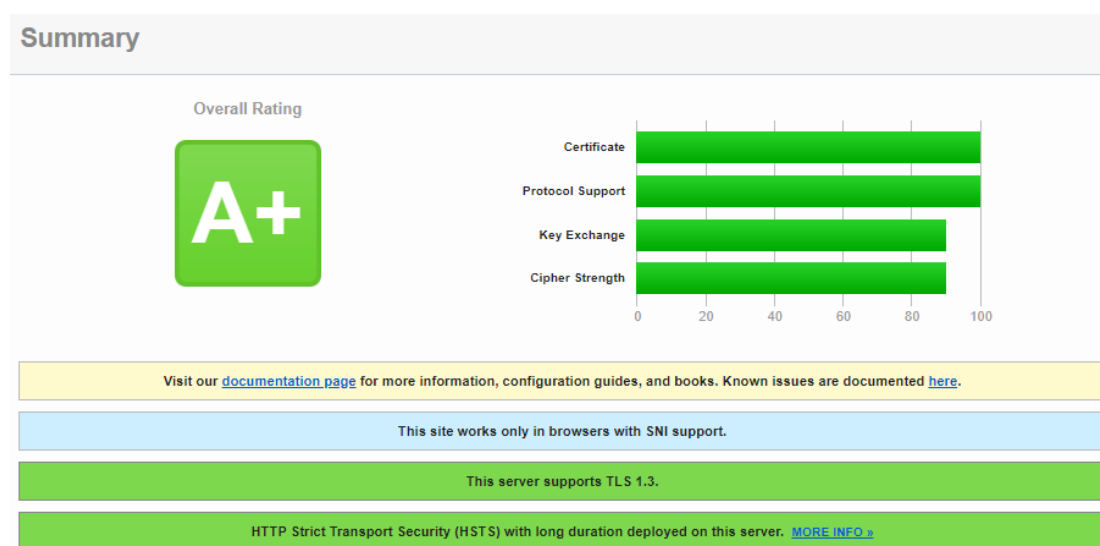


Figure 205: SSL scan rating factoryoutlet.gr

Configuration

Protocols	Status
TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No

Figure 206: TLS configuration factoryoutlet.gr

This time, the scan revealed a flawless SSL/TLS configuration. The only issue detected is the inclusion of weak ciphers within the enabled TLS 1.2. However, it is important to note that TLS 1.2 remains crucial for the functionality and compatibility of most websites.

7.2.5 Notos.gr

This time, the Qualys SSL Labs scan gave the following results.

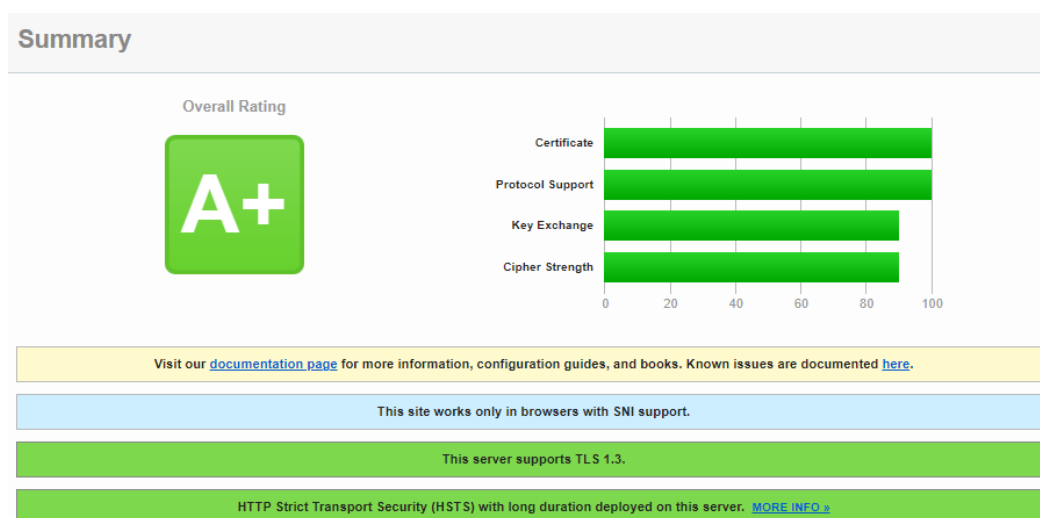


Figure 207: SSL scan notos.gr

Configuration		
	Protocols	
	TLS 1.3	Yes
	TLS 1.2	Yes*
	TLS 1.1	No
	TLS 1.0	No
	SSL 3	No
	SSL 2	No

Figure 208: TLS configuration notos.gr

This time, the scan revealed a flawless SSL/TLS configuration. The only issue detected is the inclusion of weak ciphers within the enabled TLS 1.2. However, as already discussed, TLS 1.2 remains crucial for the functionality and compatibility of most websites.

8. Findings summary

In this chapter, the findings from the evaluation of the selected websites are presented. The analysis is once again divided into two parts: privacy and security. The first part centres on GDPR cookie compliance, while the second part delves into the security configurations of the websites, with particular emphasis on those adhering to the NIS 2 Directive's focus on critical infrastructure sectors. The gathering and comparative analysis of the previously extracted results, allows for the extraction of valuable insights, highlighting common trends, issues, and areas of non-compliance or vulnerabilities.

8.1 Privacy Evaluation Results

This table contains all the findings that were extracted during the investigation of the previously covered 10 case studies. In case a listed violation is not applicable to a case study, the cell is marked as “-”.

Table 26: Cookie Violations Summary

<u>Website URL</u>	<u>Cookie Banner Violation</u>	<u>Dark Practices Violation</u>	<u>Undeclared Cookies Violation</u>	<u>Unclassified Cookies Violation</u>	<u>Incorrectly assigned Labels Violation</u>	<u>Consent Revoke Option Violation</u>
www.atticadps.gr	NO	NO	YES	NO	YES	NO
www.factoryoutlet.gr	YES	YES	-	-	YES	NO
www.cnn.gr	NO	NO	-	-	YES	NO
www.kathimerini.gr	NO	NO	-	-	YES	NO
www.lifo.gr	NO	NO	-	-	YES	NO
www.notos.gr	NO	YES	YES	NO	YES	NO
www.plaisio.gr	NO	NO	YES	NO	YES	NO
www.protothema.gr	NO	NO	-	-	YES	NO
www.public.gr	NO	NO	YES	YES	NO	NO
www.tovima.gr	NO	NO	-	-	YES	NO

The following charts provide a clear representation of the frequency of each type of violation. Please note that the “-” option has been considered as no violation.

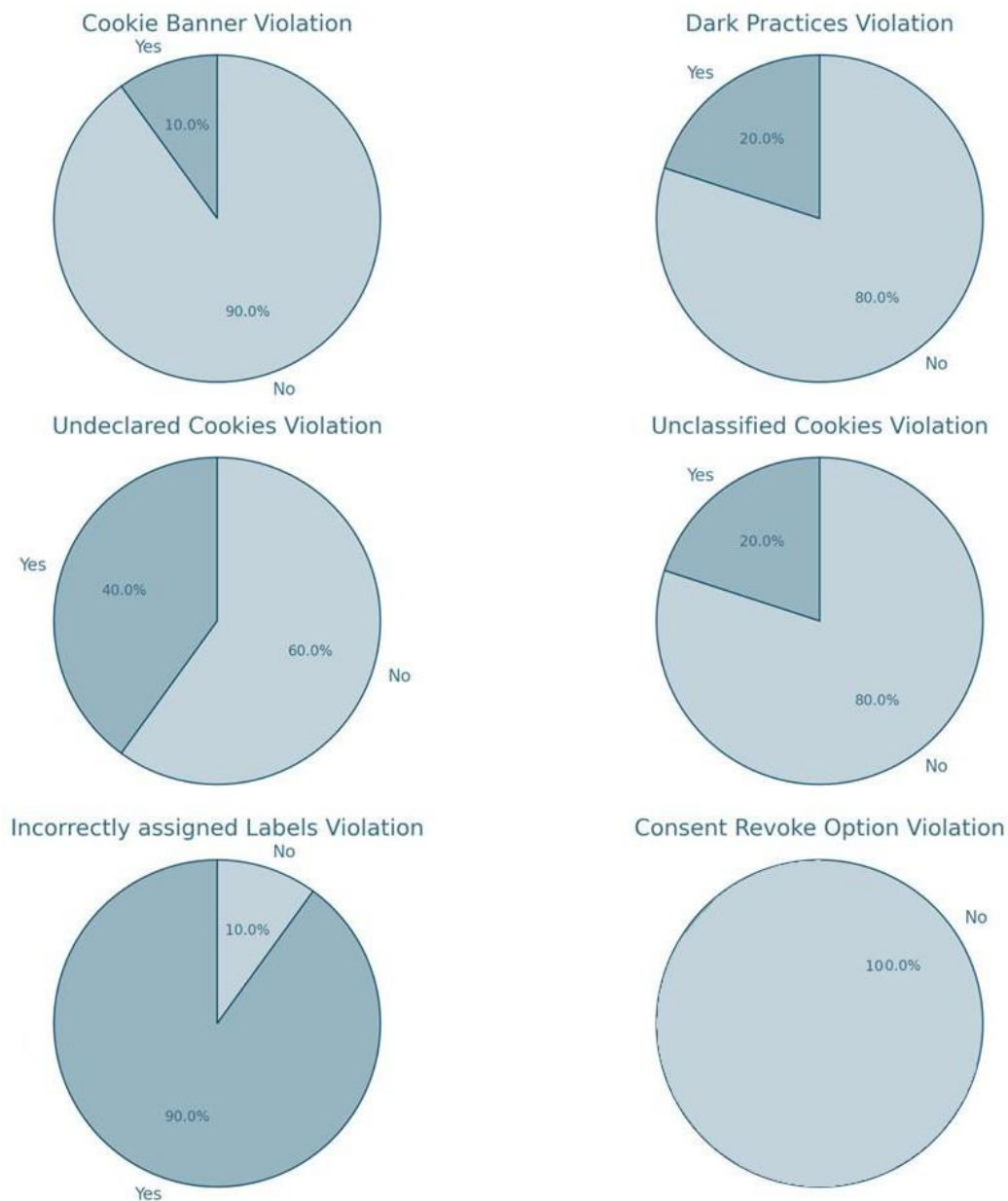


Figure 209: Cookie Violations by Percentage

Based on the findings presented above, the following main conclusions can be drawn.

- At least one violation was detected in each website.
- All websites had a revoke consent option.
- Cookies with a well-known purpose that have incorrectly assigned labels is the most common violation, detected in 90% of the tested websites.
- Lastly, most websites display a cookie banner and do not exhibit dark practices, likely because these are easily visible to users. However, these measures only address surface-level compliance. With further investigation, like the dynamic analysis that was performed in this study, it is verified that cookie violations persist beneath this initial layer.

8.2 Security Evaluation Results

This table contains all the findings that were extracted during the investigation of the previously covered 10 case studies. In case a listed factor is not applicable to a case study, the cell is marked as “-”.

Table 27: Security Evaluation Results

<u>Website URL</u>	<u>Scan Blockage</u>	<u>TLS Issues</u>	<u>DNSSEC Issues</u>	<u>PCI DSS Compliance</u>	<u>Known vulnerabilities*</u>
www.gov.gr	FULL	NO	-	-	-
www.dei.gr	PARTIAL	NO	NO	-	YES
www.nbg.gr	NO	NO	YES	YES	NO
www.oasa.gr	PARTIAL	NO	NO	NO	YES
www.nis.gr	PARTIAL	NO	NO	-	YES
www.eydap.gr	NO	NO	YES	NO	YES
www.alphabank.gr	FULL	NO	-	-	-
www.aegeanair.com	FULL	NO	-	-	-
www.helpe.gr	FULL	YES	YES	-	YES
www.ert.gr	PARTIAL	NO	NO	NO	NO

Based on the findings presented above, the following main conclusions can be drawn.

- The analysis was fairly limited, due to almost all websites fully or partially blocking the scanning process
- NIS2-related websites, emphasize on TLS configuration, to ensure secure data protection.

Disclaimer: The known vulnerabilities that were detected during the scanning process are strictly linked to outdated web software components. However, there is a significant chance that these results may include false positives, especially in those cases that the scan was partially blocked.

8.3 Observations on the Additional Analysis

Although supplementary, the additional analysis provided significant insights into both website security and privacy evaluation.

First, regarding cookies, it was observed that even websites in critical sectors, which typically have little concern for advertising or personal data collection, often exhibit cookie violations. This once again confirms that cookies are highly diverse and complex, making full compliance difficult, particularly when evaluated against the strict framework established in this thesis. Combined with the main findings, there are questions raised about the effectiveness of current cookie consent mechanisms and whether they provide meaningful transparency to users.

On the other hand, the website security evaluation for online stores was limited to a TLS configuration check, as the ImmuniWeb scans were blocked. This limitation, however, indicates the use of strict security measures by these websites to defend against potential attacks from competitors, malicious actors, or other threats. Regarding the TLS configuration, no significant findings were extracted.

9. Conclusions and Future Work

This master thesis presents a comprehensive evaluation that leads to several valuable and well-founded conclusions. These insights not only foreground critical areas for improvement, but also establish a robust framework for further research.

Starting with the privacy portion of the analysis, it becomes evident that almost all selected websites fail to fully comply with the established evaluation framework. These findings, combined with the fact that the analysed websites fall under prominent categories, which often possess greater resources and visibility, suggest that smaller- scale websites are likely to exhibit more pronounced violations and therefore higher levels of non-compliance. Thus, there is a clear indication for the need of stronger and stricter privacy protection measures, followed by more rigorous enforcement by the authorities in charge.

On the contrary the security evaluation yielded different results. Most websites appeared to be sufficiently secure, at least based on the high-level analysis that the free scanning tools could perform. Considering the findings of the high-level analysis, it seems that more emphasis is placed on the security of websites by companies and organizations, often prioritizing it over user privacy.

While this study has provided a valuable and detailed examination of website security and privacy – GDPR cookie compliance, there were some fundamental limitations that must be addressed.

Firstly, the sample size. Although the target selection of 10 websites for each scope provided valuable insights, it is not sufficient to fully capture the broader picture.

Secondly, apart from the dynamic analysis that took place during the cookie-related investigation, only passive scanning techniques have been utilized. In addition, the implementation of active penetration testing techniques could enhance the investigation for potential vulnerabilities that are non-discoverable with passive scanning.

Lastly, these passive techniques were solely relied on free scanning tools which have limited depth of findings. Also, as observed during the examination, some results were false positives further highlighting the limitations of these tools.

To build upon the current study, a great starting point would be to analyse a larger sample of websites across different sectors, for example by using automated crawling techniques and scripts for advanced data collection. This could provide a more comprehensive view of compliance in both privacy and security. On the other hand, performing penetration testing in such websites is unrealistic due to legal implications. Still, the use of paid and/or more advance tools could yield better results. At last, another important direction for further research involves observing compliance and security measures over time, which would examine how these websites adapt to evolving standards and threats.

10. BIBLIOGRAPHY

- [1] “European Parliament, Council of the European Union. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Direct,” 2008. [Online]. Available: <https://eur-lex.europa.eu/eli/dir/2002/58/oj>. [Accessed 2024].
- [2] “Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (E,” 2022. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022L2555>. [Accessed 2024].
- [3] “OWASP SQL Injection,” [Online]. Available: https://owasp.org/www-community/attacks/SQL_Injection. [Accessed 2024].
- [4] “Cross Site Scripting (XSS),” [Online]. Available: <https://owasp.org/www-community/attacks/xss/>. [Accessed 2024].
- [5] EY, “Are you ready for NIS2?,” 2024. [Online]. Available: https://www.ey.com/en_ie/are-you-ready-for-nis2-how-will-it-impact-your-organisation-are-you-prepared?utm_source=chatgpt.com. [Accessed 2024].
- [6] CISA, “Website Security,” 2021.
- [7] “AWS - What is an SSL/TLS Certificate,” [Online]. Available: <https://aws.amazon.com/what-is/ssl-certificate/>. [Accessed 2024].
- [8] S. Roi, “Baeuldung CS, Popular Authentication Methods for Web Apps,” 2024. [Online]. Available: <https://www.baeldung.com/cs/authentication-web-apps>. [Accessed 2024].
- [9] E. Iosifidis, “Security Attacks and Performance Evaluation of SSL/TLS Protocols,” Open University of Cyprus, 2016.
- [10] CISA, “SSL 3.0 Protocol Vulnerability and POODLE Attack,” 2016. [Online]. Available: <https://www.cisa.gov/news-events/alerts/2014/10/17/ssl-30-protocol-vulnerability-and-poodle-attack>. [Accessed 2024].
- [11] “CVE-MITRE,” 2011,2013. [Online]. Available: <https://www.cve.org/>. [Accessed 2024].
- [12] T. Diekrs and C. Allen, “The TLS Protocol Version 1.0,” The Internet Society, 1999.
- [13] T. Dierks and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2,” The IETF Trust, 2008.
- [14] B. Dowling, M. Fischlin, F. Günther and D. Stebila, “A Cryptographic Analysis of the TLS 1.3 Handshake Protocol,” Association for Computing Machinery, 2015.
- [15] K. Bhargavan, C. Fournet, M. Kohlweiss, A. Pironti, P.-Y. Strub and S. Zanella-Beguelin, “Proving the TLS Handshake Secure (As It Is),” Journal of Cryptology, 2014.
- [16] “Cloudflare,” [Online]. Available: www.cloudflare.com.
- [17] J. Ćurguz, “VULNERABILITIES OF THE SSL/TLS PROTOCOL,” The Sixth International Conference on Computer Science, Engineering and Information Technology, 2016.
- [18] H. Zahid and U. Khan, “Comparative Study of Authentication Techniques,” Institute of Information Technology University of Science C Technology, Bannu Khyber Pakhtoon Khwa, Pakistan, 2012.

- [19] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen and Y. Koucheryavy, "Multi-Factor Authentication: A Survey," MDPI - Journal of Cryptography, 2018.
- [20] D. Fett, R. Küsters and G. Schmitz, "The Web SSO Standard OpenID Connect: In-depth Formal Security Analysis and Security Guidelines," IEEE 30th Computer Security Foundations Symposium (CSF), Santa Barbara, CA, USA, 2017.
- [21] B. s. Saini, "A Review of Bot Protection using CAPTCHA for Web Security," Article in IOSR Journal of Computer Engineering, 2013.
- [22] S. Ariyapperuma and C. J. Mitchell, "Security vulnerabilities in DNS and DNSSEC," The Second International Conference on Availability, Reliability and Security (ARES'07), Vienna, Austria, 2007.
- [23] J. Seaman, "PCI DSS Compliance Guide," 2020.
- [24] P. Kashyap and V. Selvarajah, "Analysis of Different Methods of Reconnaissance," Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC), 2021.
- [25] "PortSwigger," [Online]. Available: www.portswigger.net.
- [26] S. Alazmi and D. Conte De Leon, "A Systematic Literature Review on the Characteristics and Effectiveness of Web Application Vulnerability Scanners," Asia Pacific University of Technology & Innovation, Malaysia, 2022.
- [27] C. Aaron, A. Scott, B. Paul and S. Muthukrishnan, "An Empirical Study of Web Cookies," WWW '16: Proceedings of the 25th International Conference on World Wide Web, 2016.
- [28] E. Hatzikosti, "Assessment of the degree of conformity of the web pages in relation to the legal and technological requirements for the use of cookies," Open University of Cyprus, 2023.
- [29] X. Hu and N. Sastry, "Characterising Third Party Cookie Usage in the EU after GDPR," WebSci '19: Proceedings of the 10th ACM Conference on Web Science, 2019.
- [30] "GDPR EU," [Online]. Available: <https://gdpr.eu/cookies/>.
- [31] X. Hu, N. Sastry and M. Mondal, "CCCC: Corraling Cookies into Categories with CookieMonster," WebSci '21: Proceedings of the 13th ACM Web Science Conference, 2021.
- [32] K. LaCroix, Y. L. Loo and Y. B. Choi, "Cookies and Sessions: A Study of What They Are, How They Work and How They Can Be Stolen," International Conference on Software Security and Assurance (ICSSA), Altoona, PA, USA, 2017.
- [33] S. Khodayari and G. Pellegrino, "The State of the SameSite: Studying the Usage, Effectiveness, and Adequacy of SameSite Cookies," IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2022.
- [34] R. Sandhu, "Secure cookies on the Web," IEEE Internet Computing, 2000.
- [35] T. Bujlow, V. Carela-Español and J. Solé-Paret, "A Survey on Web Tracking: Mechanisms, Implications, and Defenses," Proceedings of the IEEE, 2017.
- [36] J. Jokinen, "Personal Internet Privacy and Surveillance," JAMK University of Applied Sciences, 2018.
- [37] "Web Browser History Detection as a Real-World Privacy Threat," Conference: Computer Security - ESORICS 2010, 15th European Symposium on Research in Computer Security, Athens, Greece, 2010.

- [38] Ł. Olejnik, C. Castelluccia and . A. Janc3, “Why Johnny Can’t Browse in Peace: On the Uniqueness of Web Browsing History Patterns,” 2022.
- [39] O. Olukoya, “Assessing frameworks for eliciting privacy C security requirements from laws and regulations,” *Computers C Security Volume 117*, 2022.
- [40] GDPR, “Art. 94 GDPRRepeal of Directive 95/46/EC,” 2018.
- [41] HDPa, “ Issue NO 137 LAW NO. 4624,” *Government Gazette Of the Hellenic Republic, Athens,Greece*, 2019.
- [42] I. Papantoni, “On the way to the survey of eprivacy. the material to be regulated and the stakes of the new regulatory framework,” *University of Piraeus, Athens,Greece*, 2022.
- [43] H. Pauliina, “A Review of GDPR Impacts on Information Security,” *Proceedings of the 26th Pacific Asia Conference on Information Systems. AI-IS-ASIA : Artificial Intelligence, Information Systems, in Pacific Asia (Article 83). Association for Information Systems*, 2022.
- [44] “Art. 4 GDPR Definitions,” 2015. [Online]. Available: <https://gdpr-info.eu/art-4-gdpr/>. [Accessed 2024].
- [45] “Art. 25 GDPRData protection by design and by default,” 2018. [Online]. Available: <https://gdpr-info.eu/art-25-gdpr/>. [Accessed 2024].
- [46] “Art. 32 GDPR Security of processing,” 2018. [Online]. Available: <https://gdpr-info.eu/art-32-gdpr/>. [Accessed 2024].
- [47] “Art. 34 GDPR Communication of a personal data breach to the data subject,” 2018. [Online]. Available: <https://gdpr-info.eu/art-34-gdpr/>. [Accessed 2024].
- [48] L. Bufalieri, M. La Morgia, A. Mei and J. Stefa, “GDPR: When the Right to Access Personal Data Becomes a Threat Publisher: IEEE Cite This,” *IEEE International Conference on Web Services (ICWS), Beijing, China*, 2020.
- [49] “Art. 15 GDPRRight of access by the data subject,” 2018. [Online]. Available: <https://gdpr-info.eu/art-15-gdpr/>. [Accessed 2024].
- [50] B. Dino, “Analyzing Cookies Compliance with the GDPR,” *ETH Zurich*, 2021.
- [51] “Art. 6 GDPRLawfulness of processing,” 2018. [Online]. Available: <https://gdpr-info.eu/art-6-gdpr/>. [Accessed 2024].
- [52] “Art. 7 GDPRConditions for consent,” 2018. [Online]. Available: <https://gdpr-info.eu/art-7-gdpr/>. [Accessed 2024].
- [53] “Recital 32 Conditions for Consent,” 2018. [Online]. Available: <https://gdpr-info.eu/recitals/no-32/>. [Accessed 2024].
- [54] “Art. 83 GDPRGeneral conditions for imposing administrative fines,” 2018. [Online]. Available: <https://gdpr-info.eu/art-83-gdpr/>. [Accessed 2024].
- [55] “Recital 30 Online Identifiers for Profiling and Identification,” 2018. [Online]. Available: <https://gdpr-info.eu/recitals/no-30/>. [Accessed 2024].
- [56] “CookieYes,” [Online]. Available: <https://www.cookieyes.com>.
- [57] “ImmuniWeb,” [Online]. Available: <https://www.immuniweb.com/>.
- [58] D. Shravani, “Web Services Security Architectures Composition and Contract Design using RBAC,” (*IJCSE*) *International Journal on Computer Science and Engineering*, 2010.
- [59] “European Parliament, Council of the European Union. Regulation (EU) 2016/679 Of the European Parliament and of the Council of 27 April 2016 on the protection of

natural persons with regard to the processing of personal data and on the free movement of suc,” 2016. [Online]. Available: <https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04>. [Accessed 2024].