Zameen.pk-Scan-Report

Generated with ZAP on Mon 19 Dec 2022, at 18:48:43

Contents

- About this report
  - Report parameters
- Summaries
  - Alert counts by risk and confidence
  - Alert counts by site and risk
  - Alert counts by alert type
- Alerts
  - Risk=High, Confidence=High (1)
  - Risk=Medium, Confidence=High (4)
  - Risk=Medium, Confidence=Medium (4)
  - Risk=Medium, Confidence=Low (1)
  - Risk=Low, Confidence=High (2)
  - Risk=Low, Confidence=Medium (10)
  - Risk=Low, Confidence=Low (1)

- Risk=Informational, Confidence=Medium (3)
- Risk=Informational, Confidence=Low (4)

- Appendix
  - Alert types

About this report

Report parameters

Contexts

No contexts were selected, so all contexts were included by default.

Sites

The following sites were included:

- https://www.zameen.com
- https://googleads.g.doubleclick.net

(If no sites were selected, all sites were included by default.)

An included site must also be within one of the included contexts for its data to be included in the report.

Risk levels

Included: High, Medium, Low, Informational

Excluded: None

Confidence levels

Included: User Confirmed, High, Medium, Low

Excluded: User Confirmed, High, Medium, Low, False Positive

Summaries

Alert counts by risk and confidence

This table shows the number of alerts for each level of risk and confidence included in the report.

(The percentages in brackets represent the count as a percentage of the total number of alerts included in the report, rounded to one decimal place.)

		Confidence				
		User Confirmed	High	Medium	Low	Total
Risk	High	0 (0.0%)	1 (3.3%)	0 (0.0%)	0 (0.0%)	1 (3.3%)
	Medium	0 (0.0%)	4 (13.3%)	4 (13.3%)	1 (3.3%)	9 (30.0%)
	Low	0 (0.0%)	2 (6.7%)	10 (33.3%)	1 (3.3%)	13 (43.3%)
	Informational	0 (0.0%)	0 (0.0%)	3 (10.0%)	4 (13.3%)	7 (23.3%)
	Total	0 (0.0%)	7 (23.3%)	17 (56.7%)	6 (20.0%)	30 (100%)

Alert counts by site and risk

This table shows, for each site for which one or more alerts were raised, the number of alerts raised at each risk level.

Alerts with a confidence level of "False Positive" have been excluded from these counts.

(The numbers in brackets are the number of alerts raised for the site at or above that risk level.)

Site	Risk: High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
https://www.zameen.com	1 (1)	7 (8)	11 (19)	6 (25)
https://googleads.g.doubleclick.net	0 (0)	2 (2)	2 (4)	1 (5)

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
PII Disclosure	High	4 (13.3%)
Absence of Anti-CSRF Tokens	Medium	5465 (18,216.7%)
Application Error Disclosure	Medium	105 (350.0%)
Total		30

Alert type	Risk	Count
CSP: Wildcard Directive	Medium	287 (956.7%)
CSP: script-src unsafe-inline	Medium	287 (956.7%)
CSP: style-src unsafe-inline	Medium	287 (956.7%)
Content Security Policy (CSP) Header Not Set	Medium	1047 (3,490.0%)
Cross-Domain Misconfiguration	Medium	3 (10.0%)
Missing Anti-clickjacking Header	Medium	563 (1,876.7%)
Vulnerable JS Library	Medium	6 (20.0%)
Application Error Disclosure	Low	6 (20.0%)
Big Redirect Detected (Potential Sensitive Information Leak)	Low	2 (6.7%)
Cookie No HttpOnly Flag	Low	1155 (3,850.0%)
Cookie Without Secure Flag	Low	1135 (3,783.3%)
Cookie with SameSite Attribute None	Low	393 (1,310.0%)
Total		30

Alert type	Risk	Count
Cookie without SameSite Attribute	Low	1137 (3,790.0%)
Cross-Domain JavaScript Source File Inclusion	Low	8519 (28,396.7%)
Information Disclosure - Debug Error Messages	Low	17 (56.7%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	142 (473.3%)
Strict-Transport-Security Header Not Set	Low	1104 (3,680.0%)
Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)	Low	1 (3.3%)
Timestamp Disclosure - Unix	Low	9050 (30,166.7%)
X-Content-Type-Options Header Missing	Low	901 (3,003.3%)
Content-Type Header Missing	Informational	6 (20.0%)
Information Disclosure - Suspicious Comments	Informational	1616 (5,386.7%)
Loosely Scoped Cookie	Informational	376 (1,253.3%)
Modern Web Application	Informational	1326 (4,420.0%)
Total		30

Alert type	Risk	Count
Re-examine Cache-control Directives	Informational	342 (1,140.0%)
Retrieved from Cache	Informational	88 (293.3%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	16 (53.3%)
Total		30

Alerts

Risk=High, Confidence=High (1)

https://www.zameen.com (1)

PII Disclosure (1)

▶ GET https://www.zameen.com/Plots/Karachi_Naya_Nazimabad-10079-1.html

Risk=Medium, Confidence=High (4)

https://www.zameen.com (3)

CSP: Wildcard Directive (1)

▶ GET https://www.zameen.com/

CSP: script-src unsafe-inline (1)

▶ GET https://www.zameen.com/

CSP: style-src unsafe-inline (1)

▶ GET https://www.zameen.com/

https://googleads.g.doubleclick.net (1)

Content Security Policy (CSP) Header Not Set (1)

▶ GET https://googleads.g.doubleclick.net/pagead/interaction/?ai=C_hYAZDmfY8CnH4a6kgOdxLhwkf7_6m2Z0o_kmBHAjbcBEAEg3fbvMGDL_LQFoAGG2uyOKcgBCakCvz5GhmdhtD6oAwHIA8sEqgTkAU_Qd49bnY1B0OvFPlMlZjZlOhQfoM35MzOFHnXScLP81Cn_7yK7Lm3H_LLBpv3slubEI1Lrp8CIolpOc4rxXGe4qOUuyZCghjx-VoyxvQcWJojwePxerLZdwo-FPSx6GFJHZ0GUb6e75r8d4Earj7A3qoL0frDIYgLbC9uRmu8Sja4wpwGoNlovY_4TEIHsA4xvPiu220da-e8yIGtoZxMFdbOs4815nJmNH87NpA7ARdUyYb2vvWYPyyOPTaM9nm21YTv2DL2uKpqH3npzf7EFc9J7Nt8zAJOcvXIajScpAgHKGcAEgp6ziocEoAYugAeGkr3uA6gHjs4bqAeT2BuoB-6WsQKoB_6esQKoB6SjsQKoB9XJG6gHpr4bqAeaBqgH89EbqAeW2BuoB6qbsQKoB_-esQKoB9-fsQLYBwDSCBAIiGEQARgfMgOKggE6AoBAsQlKYRnELp4VB4AKAYoKG2h0dHA6Ly9zaG9wcG9ydGFjdXBwZXIuY29tL5gLAcgLAeALAYAMAbgMAdgTCtAVAfgWAYAXAQ&sigh=jmDKfG0u80E&cid=CAQSPgDq26N9KPJAMdDIeL4UtwtmxlQyQ9p3kaH19BWIyaoEhir9faVwRkf2IFoRktWC4KUvsJy44yUIFiua2MJZIBM&label=window_focus&gqid=ZDmfY6KaGouE9fgPvPmr2A4&qqid=CMDp94vFg_wCFQadZAodHSIODg&fg=1

Risk=Medium, Confidence=Medium (4)

https://www.zameen.com (3)

Application Error Disclosure (1)

▶ GET https://www.zameen.com/nfpage/

Missing Anti-clickjacking Header (1)

▶ GET https://www.zameen.com/nfpage/

Vulnerable JS Library (1)

▶ GET https://www.zameen.com/v3/js/jquery-ui_1_12_1.js

https://googleads.g.doubleclick.net (1)

Cross-Domain Misconfiguration (1)

▶ GET https://googleads.g.doubleclick.net/pagead/interaction/?ai=C_hYAZDmfY8CnH4a6kgOdxLhwkf7_6m2Z0o_kmBHAjbcBEAEg3fbvMGDL_LQFoAGG2uyOKcgBCakCvz5GhmdhtD6oAwHIA8sEqgTkAU_Qd49bnY1B0OvFPlMlZjZlOhQfoM35MzOFHnXScLP81Cn_7yK7Lm3H_LLBpv3slubEI1Lrp8CIolpOc4rxXGe4qOUuyZCghjx-VoyxvQcWJojwePxerLZdwo-FPSx6GFJHZ0GUb6e75r8d4Earj7A3qoL0frDIYgLbC9uRmu8Sja4wpwGoNlovY_4TEIHsA4xvPiu220da-e8yIGtoZxMFdbOs4815nJmNH87NpA7ARdUyYb2vvWYPyyOPTaM9nm21YTv2DL2uKpqH3npzf7EFc9J7Nt8zAJOcvXIajScpAgHKGcAEgp6ziocEoAYugAeGkr3uA6gHjs4bqAeT2BuoB-6WsQKoB_6esQKoB6SjsQKoB9XJG6gHpr4bqAeaBqgH89EbqAeW2BuoB6qbsQKoB_-esQKoB9-fsQLYBwDSCBAIiGEQARgfMgOKggE6AoBAsQlKYRnELp4VB4AKAYoKG2h0dHA6Ly9zaG9wcG9ydGFjdXBwZXIuY29tL5gLAcgLAeALAYAMAbgMAdgTCtAVAfgWAYAXAQ&sigh=jmDKfG0u80E&cid=CAQSPgDq26N9KPJAMdDIeL4UtwtmxlQyQ9p3kaH19BWIyaoEhir9faVwRkf2IFoRktWC4KUvsJy44yUIFiua2MJZIBM&label=window_focus&gqid=ZDmfY6KaGouE9fgPvPmr2A4&qqid=CMDp94vFg_wCFQadZAodHSIODg&fg=1

Risk=Medium, Confidence=Low (1)

https://www.zameen.com (1)

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.zameen.com/sitemap.xml

Risk=Low, Confidence=High (2)

https://www.zameen.com (1)

Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec) (1)

▶ GET https://www.zameen.com/ur/search/

https://googleads.g.doubleclick.net (1)

Strict-Transport-Security Header Not Set (1)

▶ GET https://googleads.g.doubleclick.net/pagead/interaction/?ai=C_hYAZDmfY8CnH4a6kgOdxLhwkf7_6m2Z0o_kmBHAjbcBEAEg3fbvMGDL_LQFoAGG2uyOKcgBCakCvz5GhmdhtD6oAwHIA8sEqgTkAU_Qd49bnY1B0OvFPlMlZjZlOhQfoM35MzOFHnXScLP81Cn_7yK7Lm3H_LLBpv3slubEI1Lrp8CIolpOc4rxXGe4qOUuyZCghjx-VoyxvQcWJojwePxerLZdwo-FPSx6GFJHZ0GUb6e75r8d4Earj7A3qoL0frDIYgLbC9uRmu8Sja4wpwGoNlovY_4TEIHsA4xvPiu220da-e8yIGtoZxMFdbOs4815nJmNH87NpA7ARdUyYb2vvWYPyyOPTaM9nm21YTv2DL2uKpqH3npzf7EFc9J7Nt8zAJOcvXIajScpAgHKGcAEgp6ziocEoAYugAeGkr3uA6gHjs4bqAeT2BuoB-6WsQKoB_6esQKoB6SjsQKoB9XJG6gHpr4bqAeaBqgH89EbqAeW2BuoB6qbsQKoB_-esQKoB9-fsQLYBwDSCBAIiGEQARgfMgOKggE6AoBAsQlKYRnELp4VB4AKAYoKG2h0dHA6Ly9zaG9wcG9ydGFjdXBwZXIuY29tL5gLAcgLAeALAYAMAbgMAdgTCtAVAfgWAYAXAQ&sigh=jmDKfG0u80E&cid=CAQSPgDq26N9KPJAMdDIeL4UtwtmxlQyQ9p3kaH19BWIyaoEhir9faVwRkf2IFoRktWC4KUvsJy44yUIFiua2MJZIBM&label=window_focus&gqid=ZDmfY6KaGouE9fgPvPmr2A4&qqid=CMDp94vFg_wCFQadZAodHSIODg&fg=1

Risk=Low, Confidence=Medium (10)

https://www.zameen.com (9)

Application Error Disclosure (1)

▶ GET https://www.zameen.com/ur/new-projects/

Big Redirect Detected (Potential Sensitive Information Leak) (1)

▶ GET https://www.zameen.com/search/results.html?property_type=9%2C8%2C21%2C22%2C20%2C24%2C25&sb_price_from=No+Min&sb_price_to=No+Max&sb_sel_area=-1&tab=1&tab_beds=-1&tab_city=3&tab_price&tab_purpose=0&tab_search=1&tab_sqft&tab_sqft_conv_unit=-1&tab_sqft_custom=1&tab_sqft_input1=No+Min&tab_sqft_input2=No+Max&tab_type=9%2C8%2C21%2C22%2C20%2C24%2C25

Cookie No HttpOnly Flag (1)

▶ GET https://www.zameen.com/sitemap.xml

Cookie Without Secure Flag (1)

▶ GET https://www.zameen.com/sitemap.xml

Cookie without SameSite Attribute (1)

▶ GET https://www.zameen.com/sitemap.xml

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.zameen.com/sitemap.xml

Information Disclosure - Debug Error Messages (1)

▶ GET https://www.zameen.com/Flats_Apartments/Karachi_Gulshan_e_Iqbal_Town-6858-1.html

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (1)

▶ GET https://www.zameen.com/area-guides/

X-Content-Type-Options Header Missing (1)

▶ GET https://www.zameen.com/robots.txt

https://googleads.g.doubleclick.net (1)

Cookie with SameSite Attribute None (1)

▶ GET https://googleads.g.doubleclick.net/pagead/interaction/?ai=C_hYAZDmfY8CnH4a6kgOdxLhwkf7_6m2Z0o_kmBHAjbcBEAEg3fbvMGDL_LQFoAGG2uyOKcgBCakCvz5GhmdhtD6oAwHIA8sEqgTkAU_Qd49bnY1B0OvFPlMlZjZlOhQfoM35MzOFHnXScLP81Cn_7yK7Lm3H_LLBpv3slubEI1Lrp8CIolpOc4rxXGe4qOUuyZCghjx-VoyxvQcWJojwePxerLZdwo-FPSx6GFJHZ0GUb6e75r8d4Earj7A3qoL0frDIYgLbC9uRmu8Sja4wpwGoNlovY_4TEIHsA4xvPiu220da-e8yIGtoZxMFdbOs4815nJmNH87NpA7ARdUyYb2vvWYPyyOPTaM9nm21YTv2DL2uKpqH3npzf7EFc9J7Nt8zAJOcvXIajScpAgHKGcAEgp6ziocEoAYugAeGkr3uA6gHjs4bqAeT2BuoB-6WsQKoB_6esQKoB6SjsQKoB9XJG6gHpr4bqAeaBqgH89EbqAeW2BuoB6qbsQKoB_-esQKoB9-fsQLYBwDSCBAIiGEQARgfMgOKggE6AoBAsQlKYRnELp4VB4AKAYoKG2h0dHA6Ly9zaG9wcG9ydGFjdXBwZXIuY29tL5gLAcgLAeALAYAMAbgMAdgTCtAVAfgWAYAXAQ&sigh=jmDKfG0u80E&cid=CAQSPgDq26N9KPJAMdDIeL4UtwtmxlQyQ9p3kaH19BWIyaoEhir9faVwRkf2IFoRktWC4KUvsJy44yUIFiua2MJZIBM&label=window_focus&gqid=ZDmfY6KaGouE9fgPvPmr2A4&qqid=CMDp94vFg_wCFQadZAodHSIODg&fg=1

Risk=Low, Confidence=Low (1)

https://www.zameen.com (1)

Timestamp Disclosure - Unix (1)

▶ GET https://www.zameen.com/society_maps/

Risk=Informational, Confidence=Medium (3)

https://www.zameen.com (3)

Content-Type Header Missing (1)

▶ GET https://www.zameen.com/tools/area-guides

Modern Web Application (1)

▶ GET https://www.zameen.com/sitemap.xml

Retrieved from Cache (1)

▶ GET https://www.zameen.com/assets/apple-touch-icon.1dbbcc9e3f454ad14d4fd0f5a25d37a3.png

Risk=Informational, Confidence=Low (4)

https://www.zameen.com (3)

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.zameen.com/sitemap.xml

Re-examine Cache-control Directives (1)

▶ GET https://www.zameen.com/robots.txt

User Controllable HTML Element Attribute (Potential XSS) (1)

▶ GET https://www.zameen.com/blog/?post_type=post&s=ZAP

https://googleads.g.doubleclick.net (1)

Loosely Scoped Cookie (1)

▶ GET https://googleads.g.doubleclick.net/pagead/interaction/?ai=C_hYAZDmfY8CnH4a6kgOdxLhwkf7_6m2Z0o_kmBHAjbcBEAEg3fbvMGDL_LQFoAGG2uyOKcgBCakCvz5GhmdhtD6oAwHIA8sEqgTkAU_Qd49bnY1B0OvFPlMlZjZlOhQfoM35MzOFHnXScLP81Cn_7yK7Lm3H_LLBpv3slubEI1Lrp8CIolpOc4rxXGe4qOUuyZCghjx-VoyxvQcWJojwePxerLZdwo-FPSx6GFJHZ0GUb6e75r8d4Earj7A3qoL0frDIYgLbC9uRmu8Sja4wpwGoNlovY_4TEIHsA4xvPiu220da-e8yIGtoZxMFdbOs4815nJmNH87NpA7ARdUyYb2vvWYPyyOPTaM9nm21YTv2DL2uKpqH3npzf7EFc9J7Nt8zAJOcvXIajScpAgHKGcAEgp6ziocEoAYugAeGkr3uA6gHjs4bqAeT2BuoB-6WsQKoB_6esQKoB6SjsQKoB9XJG6gHpr4bqAeaBqgH89EbqAeW2BuoB6qbsQKoB_-esQKoB9-fsQLYBwDSCBAIiGEQARgfMgOKggE6AoBAsQlKYRnELp4VB4AKAYoKG2h0dHA6Ly9zaG9wcG9ydGFjdXBwZXIuY29tL5gLAcgLAeALAYAMAbgMAdgTCtAVAfgWAYAXAQ&sigh=jmDKfG0u80E&cid=CAQSPgDq26N9KPJAMdDIeL4UtwtmxlQyQ9p3kaH19BWIyaoEhir9faVwRkf2IFoRktWC4KUvsJy44yUIFiua2MJZIBM&label=window_focus&gqid=ZDmfY6KaGouE9fgPvPmr2A4&qqid=CMDp94vFg_wCFQadZAodHSIODg&fg=1

Appendix

Alert types

This section contains additional information on the types of alerts in the report.

PII Disclosure

Source	raised by a passive scanner (PII Disclosure)

CWE ID	359
WASC ID	13

Absence of Anti-CSRF Tokens

Source	raised by a passive scanner (Absence of Anti-CSRF Tokens)
CWE ID	352
WASC ID	9
Reference	▪ http://projects.webappsec.org/Cross-Site-Request-Forgery ▪ http://cwe.mitre.org/data/definitions/352.html

Application Error Disclosure

Source	raised by a passive scanner (Application Error Disclosure)
CWE ID	200
WASC ID	13

CSP: Wildcard Directive

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ http://www.w3.org/TR/CSP2/

- http://www.w3.org/TR/CSP/
- http://caniuse.com/#search=content+security+policy
- http://content-security-policy.com/
- https://github.com/shapesecurity/salvation
- https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

CSP: script-src unsafe-inline

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://caniuse.com/#search=content+security+policy http://content-security-policy.com/ https://github.com/shapesecurity/salvation https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

CSP: style-src unsafe-inline

Source	raised by a passive scanner (CSP)
CWE ID	693
WASC ID	15
Reference	▪ http://www.w3.org/TR/CSP2/ ▪ http://www.w3.org/TR/CSP/ ▪ http://caniuse.com/#search=content+security+policy ▪ http://content-security-policy.com/ ▪ https://github.com/shapesecurity/salvation ▪ https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

Content Security Policy (CSP) Header Not Set

Source	raised by a passive scanner (Content Security Policy (CSP) Header Not Set)
CWE ID	693
WASC ID	15
Reference	▪ https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy

- https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
- http://www.w3.org/TR/CSP/
- http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html
- http://www.html5rocks.com/en/tutorials/security/content-security-policy/
- http://caniuse.com/#feat=contentsecuritypolicy
- http://content-security-policy.com/

Cross-Domain Misconfiguration

Source	raised by a passive scanner (Cross-Domain Misconfiguration)
CWE ID	264
WASC ID	14
Reference	• https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy

Missing Anti-clickjacking Header

Source	raised by a passive scanner (Anti-clickjacking Header)
CWE ID	1021

WASC ID 15

Reference
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Vulnerable JS Library

Source raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))

CWE ID 829

Reference
- https://bugs.jqueryui.com/ticket/15284
- https://nvd.nist.gov/vuln/detail/CVE-2022-31160
- https://github.com/jquery/jquery-ui/security/advisories/GHSA-h6gj-6jjq-h8g9
- https://github.com/jquery/jquery-ui/security/advisories/GHSA-gpqq-952q-5327
- https://nvd.nist.gov/vuln/detail/CVE-2021-41184
- https://nvd.nist.gov/vuln/detail/CVE-2021-41183
- https://github.com/jquery/jquery-ui/security/advisories/GHSA-9gj3-hwp5-pmwc
- https://nvd.nist.gov/vuln/detail/CVE-2021-41182

Application Error Disclosure

Source	raised by a passive scanner (Application Error Disclosure)
CWE ID	200
WASC ID	13

Big Redirect Detected (Potential Sensitive Information Leak)

Source	raised by a passive scanner (Big Redirect Detected (Potential Sensitive Information Leak))
CWE ID	201
WASC ID	13

Cookie No HttpOnly Flag

Source	raised by a passive scanner (Cookie No HttpOnly Flag)
CWE ID	1004
WASC ID	13
Reference	▪ https://owasp.org/www-community/HttpOnly

Cookie Without Secure Flag

Source	raised by a passive scanner (Cookie Without Secure Flag)
CWE ID	614
WASC ID	13

Reference	▪ https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

Cookie with SameSite Attribute None

Source	raised by a passive scanner (Cookie without SameSite Attribute)
CWE ID	1275
WASC ID	13
Reference	▪ https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

Cookie without SameSite Attribute

Source	raised by a passive scanner (Cookie without SameSite Attribute)
CWE ID	1275
WASC ID	13
Reference	▪ https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site

Cross-Domain JavaScript Source File Inclusion

Source	raised by a passive scanner (Cross-Domain JavaScript Source File Inclusion)
CWE ID	829

WASC ID 15

Information Disclosure - Debug Error Messages

Source raised by a passive scanner (Information Disclosure - Debug Error Messages)

CWE ID 200

WASC ID 13

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Source raised by a passive scanner (Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))

CWE ID 200

WASC ID 13

Reference

- http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx
- http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

Strict-Transport-Security Header Not Set

Source raised by a passive scanner (Strict-Transport-Security Header)

CWE ID 319

WASC ID 15

Reference

- https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
- https://owasp.org/www-community/Security_Headers
- http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security
- http://caniuse.com/stricttransportsecurity
- http://tools.ietf.org/html/rfc6797

Strict-Transport-Security Multiple Header Entries (Non-compliant with Spec)

Source raised by a passive scanner (Strict-Transport-Security Header)

CWE ID 319

WASC ID 15

Reference

- http://tools.ietf.org/html/rfc6797#section-8.1

Timestamp Disclosure - Unix

Source raised by a passive scanner (Timestamp Disclosure)

CWE ID 200

WASC ID 13

Reference	▪ http://projects.webappsec.org/w/page/13246936/Information%20Leakage

X-Content-Type-Options Header Missing

Source	raised by a passive scanner (X-Content-Type-Options Header Missing)
CWE ID	693
WASC ID	15
Reference	▪ http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx ▪ https://owasp.org/www-community/Security_Headers

Content-Type Header Missing

Source	raised by a passive scanner (Content-Type Header Missing)
CWE ID	345
WASC ID	12
Reference	▪ http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx

Information Disclosure - Suspicious Comments

Source	raised by a passive scanner (Information Disclosure - Suspicious Comments)
CWE ID	200

WASC ID 13

Loosely Scoped Cookie

Source raised by a passive scanner (Loosely Scoped Cookie)

CWE ID 565

WASC ID 15

Reference

- https://tools.ietf.org/html/rfc6265#section-4.1
- https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html
- http://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies

Modern Web Application

Source raised by a passive scanner (Modern Web Application)

Re-examine Cache-control Directives

Source raised by a passive scanner (Re-examine Cache-control Directives)

CWE ID 525

WASC ID 13

Reference

- https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
- https://grayduck.mn/2021/09/13/cache-control-recommendations/

Retrieved from Cache

Source raised by a passive scanner (Retrieved from Cache)

Reference

- https://tools.ietf.org/html/rfc7234
- https://tools.ietf.org/html/rfc7231
- http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)

User Controllable HTML Element Attribute (Potential XSS)

Source raised by a passive scanner (User Controllable HTML Element Attribute (Potential XSS))

CWE ID 20

WASC ID 20

Reference

- http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute