Naheed.pk-ZAP Scanning Report

Generated with ZAP on Tue 13 Dec 2022, at 19:30:41

Contents

About this report

Report parameters

Contexts

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

Sites

The following sites were included:

- https://contile.services.mozilla.com
- https://fonts.gstatic.com
- https://www.gstatic.com
- https://www.facebook.com
- https://connect.facebook.net
- https://googleads.g.doubleclick.net
- https://analytics.google.com
- https://stats.g.doubleclick.net
- https://www.google.com.pk
- https://media.naheed.pk
- https://safebrowsing.googleapis.com
- https://static.naheed.pk
- https://location.services.mozilla.com
- http://naheed.pk
- https://www.google.com
- https://incoming.telemetry.mozilla.org
- https://www.google-analytics.com

- http://r3.o.lencr.org
- https://aus5.mozilla.org
- https://content-signature-2.cdn.mozilla.net
- https://www.googletagmanager.com
- https://push.services.mozilla.com
- https://firefox.settings.services.mozilla.com
- https://classify-client.services.mozilla.com
- https://www.mozilla.org
- https://www.naheed.pk

(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%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
	Medium	0 (0.0%)	4 (15.4%)	3 (11.5%)	1 (3.8%)	8 (30.8%)
	Low	0 (0.0%)	3 (11.5%)	7 (26.9%)	1 (3.8%)	11 (42.3%)
	Informational	0 (0.0%)	0 (0.0%)	2 (7.7%)	5 (19.2%)	7 (26.9%)
	Total	0 (0.0%)	7 (26.9%)	12 (46.2%)	7 (26.9%)	26 (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.)

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://googleads.g.doubleclick.net	0 (0)	0 (0)	1 (1)	1 (2)

	Risk			
	High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
https://static.naheed.pk	0 (0)	2 (2)	1 (3)	0 (3)
https://www.google.com	0 (0)	2 (2)	1 (3)	0 (3)
https://www.google-analytics.com	0 (0)	1 (1)	0 (1)	0 (1)
https://aus5.mozilla.org	0 (0)	0 (0)	0 (0)	1 (1)
https://firefox.settings.services.mozilla.com	0 (0)	1 (1)	0 (1)	1 (2)
https://www.naheed.pk	0 (0)	2 (2)	8 (10)	4 (14)

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
Absence of Anti-CSRF Tokens	Medium	21388 (82,261.5%)
Total		26

Alert type	Risk	Count
CSP: Wildcard Directive	Medium	2 (7.7%)
CSP: style-src unsafe-inline	Medium	2 (7.7%)
Content Security Policy (CSP) Header Not Set	Medium	2400 (9,230.8%)
Cross-Domain Misconfiguration	Medium	193 (742.3%)
Missing Anti-clickjacking Header	Medium	9 (34.6%)
Session ID in URL Rewrite	Medium	19 (73.1%)
Vulnerable JS Library	Medium	4 (15.4%)
Application Error Disclosure	Low	2 (7.7%)
CSP: Notices	Low	2 (7.7%)
Cookie No HttpOnly Flag	Low	213 (819.2%)
Cookie Without Secure Flag	Low	127 (488.5%)
Cookie with SameSite Attribute None	Low	8 (30.8%)
Total		26

Alert type	Risk	Count
Cookie without SameSite Attribute	Low	4162 (16,007.7%)
Cross-Domain JavaScript Source File Inclusion	Low	4451 (17,119.2%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	2841 (10,926.9%)
Strict-Transport-Security Header Not Set	Low	233 (896.2%)
Timestamp Disclosure - Unix	Low	37 (142.3%)
X-Content-Type-Options Header Missing	Low	189 (726.9%)
Charset Mismatch	Informational	1 (3.8%)
Information Disclosure - Suspicious Comments	Informational	2304 (8,861.5%)
Loosely Scoped Cookie	Informational	8 (30.8%)
Modern Web Application	Informational	1891 (7,273.1%)
Re-examine Cache-control Directives	Informational	12 (46.2%)
Retrieved from Cache	Informational	30 (115.4%)
Total		26

Alert type	Risk	Count
User Controllable HTML Element Attribute (Potential XSS)	Informational	62 (238.5%)
Total		26

Alerts

Risk=Medium, Confidence=High (4)

https://www.google.com (2)

CSP: Wildcard Directive (1)

▶ GET https://www.google.com/recaptcha/api2/anchor?ar=1&k=6LcH_9oUAAAAADTPSH9lcJKINdI7L9eztMoPkovS&co=aHR0cHM6Ly93d3cubmFoZWVkLnBrOjQ0Mw..&hl=en&v=pn3ro1xnhf4yB8qmnrhh9iD2&theme=light&size=normal&cb=4xp22v9vxgkt

CSP: style-src unsafe-inline (1)

▶ GET https://www.google.com/recaptcha/api2/anchor?ar=1&k=6LcH_9oUAAAAADTPSH9lcJKINdI7L9eztMoPkovS&co=aHR0cHM6Ly93d3cubmFoZWVkLnBrOjQ0Mw..&hl=en&v=pn3ro1xnhf4yB8qmnrhh9iD2&theme=light&size=normal&cb=4xp22v9vxgkt

https://www.google-analytics.com (1)

Session ID in URL Rewrite (1)

▶ POST https://www.google-analytics.com/g/collect?v=2&tid=G-MQ7767QQQW&gtm=2oebu0&_p=449680073&cid=960893931.1667379708&ul=en-

us&sr=1366x768&_s=1&sid=1670941301&sct=1&seg=0&dl=https%3A%2F%2Fwww.mozilla.org%2Fen-US%2Ffirefox%2F107.0.1%2Fwhatsnew%2F%3Foldversion%3D106.0.5&dt=What%E2%80%99s%20new%20with%20Firefox%20-%20More%20privacy%2C%20more%20protections.&en=page_view&_fv=1&_ss=1

https://www.naheed.pk (1)

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

▶ GET https://www.naheed.pk/

Risk=Medium, Confidence=Medium (3)

https://static.naheed.pk (2)

Missing Anti-clickjacking Header (1)

▶ GET https://static.naheed.pk/version1670925824/frontend/Naheed/NaheedTheme/en_US/Magento_Ui/templates/modal/modal-popup.html

Vulnerable JS Library (1)

▶ GET https://static.naheed.pk/version1670925824/frontend/Naheed/NaheedTheme/en_US/jquery.min.js

https://firefox.settings.services.mozilla.com (1)

Cross-Domain Misconfiguration (1)

▶ GET https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/ms-language-packs/records/cfr-v1-en-US

Risk=Medium, Confidence=Low (1)

https://www.naheed.pk (1)

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.naheed.pk/

Risk=Low, Confidence=High (3)

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

CSP: Notices (1)

▶ GET https://www.google.com/recaptcha/api2/anchor?ar=1&k=6LcH_9oUAAAAADTPSH9lcJKINdI7L9eztMoPkovS&co=aHR0cHM6Ly93d3cubmFoZWVkLnBrOjQ0Mw..&hl=en&v=pn3ro1xnhf4yB8qmnrhh9iD2&theme=light&size=normal&cb=4xp22v9vxgkt

https://www.naheed.pk (2)

Server Leaks Version Information via "Server" HTTP Response Header Field (1)

▶ GET https://www.naheed.pk/robots.txt

Strict-Transport-Security Header Not Set (1)

▶ GET https://www.naheed.pk/groceries-pets?manufacturer=1143

Risk=Low, Confidence=Medium (7)

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

Cookie with SameSite Attribute None (1)

▶ GET https://googleads.g.doubleclick.net/pagead/viewthroughconversion/766060466/?random=1670941330515&cv=11&fst=1670941330515&bg=ffffff&guid=ON&async=1&gtm=2oabu0&u_w=1366&u_h=768&hn=www.googleadservices.com&frm=0&url=https%3A%2F%2Fwww.naheed.pk%2F&tiba=Naheed.pk%20-%20Online%20Shopping%20in%20Pakistan%3A%20Cosmetics%2C%20Groceries%2C%20Mobiles%2C%20Fashion%2C%20Electronics%20%26%20More%20%7C%20Online%20Shopping%20in%20Karachi%2C%20Lahore%20and%20Pakistan&auid=1075537231.1670941331&data=event%3Dgtag.config&rfmt=3&fmt=4

https://www.naheed.pk (6)

Application Error Disclosure (1)

▶ GET https://www.naheed.pk/setup/

Cookie No HttpOnly Flag (1)

▶ POST https://www.naheed.pk/newsletter/subscriber/new/

Cookie Without Secure Flag (1)

▶ GET https://www.naheed.pk/app/

Cookie without SameSite Attribute (1)

▶ GET https://www.naheed.pk/robots.txt

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.naheed.pk/

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

▶ GET https://www.naheed.pk/sitemap.xml

Risk=Low, Confidence=Low (1)

https://static.naheed.pk (1)

Timestamp Disclosure - Unix (1)

▶ GET
https://static.naheed.pk/version1670925824/_cache/merged/2fa35f08438ff04a3c656e7dcb78386f.min.css

Risk=Informational, Confidence=Medium (2)

https://firefox.settings.services.mozilla.com (1)

Retrieved from Cache (1)

▶ GET
https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/ms-language-packs/records/cfr-v1-en-US

https://www.naheed.pk (1)

Modern Web Application (1)

▶ GET https://www.naheed.pk/

Risk=Informational, Confidence=Low (5)

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

Loosely Scoped Cookie (1)

▶ GET https://googleads.g.doubleclick.net/pagead/viewthroughconversion/766060466/?random=1670941330515&cv=11&fst=1670941330515&bg=ffffff&guid=ON&async=1&gtm=2oabu0&u_w=1366&u_h=768&hn=www.googleadservices.com&frm=0&url=https%3A%2F%2Fwww.naheed.pk%2F&tiba=Naheed.pk%20-%20Online%20Shopping%20in%20Pakistan%3A%20Cosmetics%2C%20Groceries%2C%20Mobiles%2C%20Fashion%2C%20Electronics%20%26%20More%20%7C%20Online%20Shopping%20in%20Karachi%2C%20Lahore%20and%20Pakistan&auid=1075537231.1670941331&data=event%3Dgtag.config&rfmt=3&fmt=4

https://aus5.mozilla.org (1)

Charset Mismatch (1)

▶ GET https://aus5.mozilla.org/update/3/GMP/107.0.1/20221128144904/WINNT_x86_64-msvc-x64/en-US/release/Windows_NT%2010.0.0.0.19044.2251%20(x64)/default/default/update.xml

https://www.naheed.pk (3)

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.naheed.pk/

Re-examine Cache-control Directives (1)

▶ GET https://www.naheed.pk/sitemap.xml

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

▶ GET https://www.naheed.pk/groceries-pets?cat=53

Appendix

Alert types

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

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

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: 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

Session ID in URL Rewrite

Source	raised by a passive scanner (Session ID in URL Rewrite)
CWE ID	200
WASC ID	13
Reference	• http://seclists.org/lists/webappsec/2002/Oct-Dec/0111.html

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	829
Reference	▪ https://github.com/jquery/jquery/issues/2432 ▪ http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ ▪ http://research.insecurelabs.org/jquery/test/ ▪ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ ▪ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 ▪ https://nvd.nist.gov/vuln/detail/CVE-2015-9251 ▪ https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b ▪ https://bugs.jquery.com/ticket/11974 ▪ https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

Application Error Disclosure

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

CSP: Notices

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

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

Server Leaks Version Information via "Server" HTTP Response Header Field

Source	raised by a passive scanner (HTTP Server Response Header)
CWE ID	200
WASC ID	13
Reference	▪ http://httpd.apache.org/docs/current/mod/core.html#servertokens ▪ http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 ▪ 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

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

Charset Mismatch

Source	raised by a passive scanner (Charset Mismatch)
CWE ID	436
WASC ID	15
Reference	▪ http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection

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