Cheetay-Scan-Report

Generated with ZAP on Mon 19 Dec 2022, at 17:13:10

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://googleads.g.doubleclick.net
- http://www.cheetay.pk
- https://www.cheetay.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%)	1 (5.3%)	2 (10.5%)	1 (5.3%)	4 (21.1%)
	Low	0 (0.0%)	2 (10.5%)	6 (31.6%)	1 (5.3%)	9 (47.4%)
	Informational	0 (0.0%)	0 (0.0%)	2 (10.5%)	4 (21.1%)	6 (31.6%)
	Total	0 (0.0%)	3 (15.8%)	10 (52.6%)	6 (31.6%)	19 (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)	1 (1)	1 (2)	1 (3)
	http://www.cheetay.pk	0 (0)	0 (0)	1 (1)	0 (1)
	https://www.cheetay.pk	0 (0)	3 (3)	7 (10)	5 (15)

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	232 (1,221.1%)
Content Security Policy (CSP) Header Not Set	Medium	116 (610.5%)
Total		19

Alert type	Risk	Count
Cross-Domain Misconfiguration	Medium	3 (15.8%)
Vulnerable JS Library	Medium	9 (47.4%)
Cookie No HttpOnly Flag	Low	783 (4,121.1%)
Cookie Without Secure Flag	Low	832 (4,378.9%)
Cookie with SameSite Attribute None	Low	3 (15.8%)
Cookie without SameSite Attribute	Low	832 (4,378.9%)
Cross-Domain JavaScript Source File Inclusion	Low	170 (894.7%)
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	1 (5.3%)
Strict-Transport-Security Header Not Set	Low	306 (1,610.5%)
Timestamp Disclosure - Unix	Low	68 (357.9%)
X-Content-Type-Options Header Missing	Low	240 (1,263.2%)
Information Disclosure - Sensitive Information in URL	Informational	2 (10.5%)
Total		19

Alert type	Risk	Count
Information Disclosure - Suspicious Comments	Informational	51 (268.4%)
Loosely Scoped Cookie	Informational	3 (15.8%)
Modern Web Application	Informational	88 (463.2%)
Re-examine Cache-control Directives	Informational	85 (447.4%)
User Controllable HTML Element Attribute (Potential XSS)	Informational	29 (152.6%)
Total		19

Alerts

Risk=Medium, Confidence=High (1)

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

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

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

Risk=Medium, Confidence=Medium (2)

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

Cross-Domain Misconfiguration (1)

▶ GET https://googleads.g.doubleclick.net/pagead/interaction/?ai=ClKU4KzmfY9zwEKiG9fgPnoWGMIrfq6lrq4vTx5QQ6K6OwYsOEAEg3fbvMGDL_LQFoAGu44mlAsgBAagDAcgDwwSqBMsBT9DIl0TgTluZMiFx-xT59lkUrt6uV5D5lEGns7kqt1u8hCg9Za-uD1z9C-Nt6FDH3bVFtrWXNh1amxWDMq_qwZZWzq4OwxaYfDwm54UJ814yJA3UJSwkkGTp-dzjiU2Z2BtBlyxhHLCqz9xc8Ls40FumxpWsxai0sI_PRMLykgVDv0gQroDlVYl58y7Nnk_f3uHHa2ZSBFnsaxUAkXOrjQoy8AnBwoCWrSpqBMReG1lCZJ0reZlOW8QiFQhRtTSse3UGO4Ki9yfWCpbABIqO7dSKBKAGZoAHupz22gGoB47OG6gHk9gbqAfulrECqAf-nrECqAeko7ECqAfVyRuoB6a-G6gHmgaoB_PRG6gHltgbqAeqm7ECqAf_nrECqAffn7EC2AcB0ggQCIhhEAEYHzIDioIBOgKAQLEJpx-UWEHbT62ACgGYCwHICwG4DAHYEw3QFQGYFgH4FgGAFwE&sigh=PJc7ElTvsIA&cid=CAQSPgDq26N9D28AWalrmCDKetU5XgkxotpNHiHoWfAAg4J3yMWS6cG1ZNAXJGT45T7OljoCqCTi-2asFOfzUQIkIBM&label=window_focus&gqid=KzmfY9eeELmM9fgPoLeI-A0&qqid=CJyy0vDEg_wCFShDHQkdnoIBBg&fg=1

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

Vulnerable JS Library (1)

▶ GET https://www.cheetay.pk/static/js/newLandingPage/jquery-3.4.1.min.js

Risk=Medium, Confidence=Low (1)

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

Absence of Anti-CSRF Tokens (1)

▶ GET https://www.cheetay.pk/xoom/

Risk=Low, Confidence=High (2)

http://www.cheetay.pk (1)

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

▶ GET http://www.cheetay.pk/

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

Strict-Transport-Security Header Not Set (1)

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

Risk=Low, Confidence=Medium (6)

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

Cookie with SameSite Attribute None (1)

▶ GET https://googleads.g.doubleclick.net/pagead/interaction/?ai=Cjr8oYDmfY-m6KbiJ5LcPpcWXkA-9kujabYO_6b6XELX3w5qRDhABIN327zBgy_y0BaAB4ojH9QLIAQmoAwHIA8sEqgTUAU_Qeq2De9-7K8DDeZTaTgmfIamHvk7416agbxFPWj9mHRRCyj1FDJHkKaPQD5JzHApXrzfGX_KxVtM64Lqeq4ioJgPdYKTIyYga38UdzIQQ_m9UItFkUkiv0JL_bHdDimq7OxtHk0M0QoWoJAODNRAkeAQ62evf_i5PkdcVzQS27NjJtIGpKCdAW1JmXCQS3tt5wyJd-ixDv65Y2rxFtEb7eIOXER_Ik60Wn4wysOUK6eGg1dHFKSI0hRj-MimKdLkk9WxckTh95bH4zgRBECDdlKVpwASsppqwgQSgBi6AB4b3uIoBqAeOzhuoB5PYG6gH7paxAqgH_p6xAqgHpKOxAqgH1ckbqAemvhuoB5oGqAfz0RuoB5bYG6gHqpuxAqgH_56xAqgH35-xAtgHANIIEAiIYRABGB8yA4qCAToCgECxCQhFmPzmigFAgAoBmAsByAsBgAwBuAwB2BMNiBQB0BUBmBYB-BYBgBcB&sigh=FK-Dwf1JY1E&cid=CAQSPgDq26N9-xT33Xjm7sWlnE1oizh8pWvbkZu9PPOAjfgZSRwp-

Qch08OTjeNiZ6Ju2lu0qY64lVA8NYNM9Gp1IBM&label=window_focus&gqid=YDmfY-ygJNWF9fgP_MqVmAY&qqid=COnqjYrFg_wCFbgE-QAdpeIF8g&fg=1

https://www.cheetay.pk (5)

Cookie No HttpOnly Flag (1)

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

Cookie Without Secure Flag (1)

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

Cookie without SameSite Attribute (1)

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

Cross-Domain JavaScript Source File Inclusion (1)

▶ GET https://www.cheetay.pk/

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

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

Risk=Low, Confidence=Low (1)

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

Timestamp Disclosure - Unix (1)

▶ GET https://www.cheetay.pk/cheetay-tiffin/

Risk=Informational, Confidence=Medium (2)

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

Information Disclosure - Sensitive Information in URL (1)

▶ GET https://www.cheetay.pk/newsletter/subscribe?email=foo-bar%40example.com

Modern Web Application (1)

▶ GET https://www.cheetay.pk/

Risk=Informational, Confidence=Low (4)

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

Loosely Scoped Cookie (1)

▶ GET https://googleads.g.doubleclick.net/pagead/interaction/?ai=Cjr8oYDmfY-m6KbiJ5LcPpcWXkA-9kujabYO_6b6XELX3w5qRDhABIN327zBgy_y0BaAB4ojH9QLIAQmoAwHIA8sEqgTUAU_Qeq2De9-7K8DDeZTaTgmfIamHvk7416agbxFPWj9mHRRCyj1FDJHkKaPQD5JzHApXrzfGX_KxVtM64Lqeq4ioJgPdYKTIyYga38UdzIQQ_m9UItFkUkiv0JL_bHdDimq7OxtHk0M0QoWoJAODNRAkeAQ62evf_i5PkdcVzQS27NjJtIGpKCdAW1JmXCQS3tt5wyJd-ixDv65Y2rxFtEb7eIOXER_Ik60Wn4wysOUK6eGg1dHFKSI0hRj-MimKdLkk9WxckTh95bH4zgRBECDdlKVpwASsppqwgQSgBi6AB4b3uIoBqAeOzhuoB5PYG6gH7paxAqgH_p6xAqgHpKOxAqgH1ckbqAemvhuoB5oGqAfz0RuoB5bYG6gHqpuxAqgH_56xAqgH35-xAtgHANIIEAiIYRABGB8yA4qCAToCgECxCQhFmPzmigFAgAoBmAsByAsBgAwBuAwB2BMNiBQB0BUBmBYB-BYBgBcB&sigh=FK-Dwf1JY1E&cid=CAQSPgDq26N9-xT33Xjm7sWlnE1oizh8pWvbkZu9PPOAjfgZSRwp-Qch08OTjeNiZ6Ju2lu0qY64lVA8NYNM9Gp1IBM&label=window_focus&gqid=YDmfY-ygJNWF9fgP_MqVmAY&qqid=COnqjYrFg_wCFbgE-QAdpeIF8g&fg=1

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

Information Disclosure - Suspicious Comments (1)

▶ GET https://www.cheetay.pk/static/js/newLandingPage/jquery-3.4.1.min.js

Re-examine Cache-control Directives (1)

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

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

▶ POST https://www.cheetay.pk/accounts/login/?next

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

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

Vulnerable JS Library

Source	raised by a passive scanner (Vulnerable JS Library (Powered by Retire.js))
CWE ID	829
Reference	▪ https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/

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

Information Disclosure - Sensitive Information in URL

Source	raised by a passive scanner (Information Disclosure - Sensitive Information in URL)
CWE ID	200
WASC ID	13

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/

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