PhishGuard ZAP Report

Sites: https://chromewebstore.googleapis.com https://cdnjs.cloudflare. com https://static.canva.com https://challenges.cloudflare.com https://static.cloudflareinsights.com https://www.canva.com https://canva.com https://content-autofill.googleapis.com https://ssl. gstatic.com https://fonts.googleapis.com https://fonts.gstatic.com https://lh3.googleusercontent.com http://localhost:5001 https://chromewebstore.google.com https://chrome.google.com https://update.googleapis.com https://play.google.com https://apis. google.com https://ogads-pa.clients6.google.com https://www.gstatic. com https://www.google.com https://optimizationguide-pa.googleapis. com https://accounts.google.com http://clients2.google.com

Generated on Fri, 9 May 2025 02:23:36

ZAP Version: 2.16.1

ZAP by [Checkmarx](#)

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	9
Low	6
Informational	11

Alerts

Name	Risk Level	Number of Instances
[Absence of Anti-CSRF Tokens](#)	Medium	1
[CSP: Failure to Define Directive with No Fallback](#)	Medium	10
[CSP: Wildcard Directive](#)	Medium	5
[CSP: script-src unsafe-eval](#)	Medium	13
[CSP: script-src unsafe-inline](#)	Medium	2
[CSP: style-src unsafe-inline](#)	Medium	15
[Content Security Policy (CSP) Header Not Set](#)	Medium	20
[Cross-Domain Misconfiguration](#)	Medium	10
[Missing Anti-clickjacking Header](#)	Medium	22
[CSP: Notices](#)	Low	5
[Cookie with SameSite Attribute None](#)	Low	4
[Cross-Domain JavaScript Source File Inclusion](#)	Low	1

Strict-Transport-Security Header Not Set	Low	59	
Timestamp Disclosure - Unix	Low	241	
X-Content-Type-Options Header Missing	Low	29	
CSP: Header & Meta	Informational	5	
Content Security Policy (CSP) Report-Only Header Found	Informational	1	
Information Disclosure - Information in Browser sessionStorage	Informational	2	
Information Disclosure - Sensitive Information in URL	Informational	1	
Information Disclosure - Suspicious Comments	Informational	16	
Loosely Scoped Cookie	Informational	5	
Modern Web Application	Informational	14	
Re-examine Cache-control Directives	Informational	15	
Retrieved from Cache	Informational	16	
Session Management Response Identified	Informational	6	
User Controllable Charset	Informational	1	

Alert Detail

Medium	Absence of Anti-CSRF Tokens
Description	No Anti-CSRF tokens were found in a HTML submission form.
	A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL /form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.
	CSRF attacks are effective in a number of situations, including:
	* The victim has an active session on the target site.
	* The victim is authenticated via HTTP auth on the target site.
	* The victim is on the same local network as the target site.
	CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	https://www.google.com/sorry/index?continue=https://www.google.com/search%3Fq%3Dcanva.com%26oq%3Dcanva.com%26gs_lcrp%3DEgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE%26sourceid%3Dchrome%26ie%3DUTF-8%26sei%3DxB8daOXfHK-R4-EPzemMwAE&q=EgS2sN70GMi_9MAGIjAaBowNa3-eeVgj-e2FOxtvdzFSUA-SHTcJ5-a3xXNnKk6SJFPWzEcBx8ukuf03gHkyAnJSWgFD
Method	GET
Attack	
Evidence	<form id="captcha-form" action="index" method="post">

Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "continue" "q"].
Instances	1
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Medium	CSP: Failure to Define Directive with No Fallback
Description	The Content Security Policy fails to define one of the directives that has no fallback. Missing/exc same as allowing anything.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/7sbwg /0x4AAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	default-src 'none'; script-src 'nonce-KqXPejJer189nz9s' 'unsafe-eval'; script-src-attr 'none'; work 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; form-ac 'self'; sandbox allow-same-origin allow-scripts allow-popups allow-forms
Other Info	The directive(s): frame-ancestors is/are among the directives that do not fallback to default-src.

URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/iu289/0x4AAAAAAADnPlDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	default-src 'none'; script-src 'nonce-UWDhdRC48bH6c094' 'unsafe-eval'; script-src-attr 'none'; w src 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; form uri 'self'; sandbox allow-same-origin allow-scripts allow-popups allow-forms
Other Info	The directive(s): frame-ancestors is/are among the directives that do not fallback to default-src.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/ixl4x/0x4AAAAAAADnPlDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	default-src 'none'; script-src 'nonce-xtUXrNYr2ZQmNM0g' 'unsafe-eval'; script-src-attr 'none'; wo src 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; form uri 'self'; sandbox allow-same-origin allow-scripts allow-popups allow-forms
Other Info	The directive(s): frame-ancestors is/are among the directives that do not fallback to default-src.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/o8ic5/0x4AAAAAAADnPlDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	default-src 'none'; script-src 'nonce-U7QbVnQRiLJw0j9C' 'unsafe-eval'; script-src-attr 'none'; wo 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; form-ac 'self'; sandbox allow-same-origin allow-scripts allow-popups allow-forms
Other Info	The directive(s): frame-ancestors is/are among the directives that do not fallback to default-src.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/u2hhw/0x4AAAAAAADnPlDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	default-src 'none'; script-src 'nonce-ESUe9ETIU75F8KmH' 'unsafe-eval'; script-src-attr 'none'; w src 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; form uri 'self'; sandbox allow-same-origin allow-scripts allow-popups allow-forms
Other Info	The directive(s): frame-ancestors is/are among the directives that do not fallback to default-src.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	require-trusted-types-for 'script';report-uri /_/ChromeWebStoreConsumerFeUi/cspreport
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	script-src 'report-sample' 'nonce-dbVRdrpgV3yImHOgsq7drQ' 'unsafe-inline';object-src 'none';ba /ChromeWebStoreConsumerFeUi/cspreport;worker-src 'self'
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to

URL	https://chromewebstore.google.com/	
	Method	GET
	Attack	
	Evidence	script-src 'unsafe-inline' 'unsafe-eval' blob: data: 'self' https://apis.google.com https://ssl.gstatic.c com https://www.googletagmanager.com https://www.gstatic.com https://www.google-analytics. google.com/inapp/ https://www.google.com/tools/feedback/ https://www.gstatic.com/inproduct_h gstatic.com/support/content/ https://www.googleapis.com/appsmarket/v2/installedApps/;report-u /ChromeWebStoreConsumerFeUi/cspreport/allowlist
	Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to
URL	https://www.google.com/search?q=canva.com&oq=canva. com&gs_lcrp=EgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE&sou 8	
	Method	GET
	Attack	
	Evidence	object-src 'none';base-uri 'self';script-src 'nonce-7rYghCGK4vbA6bwZcWwEsQ' 'strict-dynamic' eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/cdt1
	Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to
URL	https://www.google.com/search?q=canva.com&oq=canva. com&gs_lcrp=EgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE&sou 8&sei=xB8daOXfHK-R4-EPzemMwAE	
	Method	GET
	Attack	
	Evidence	object-src 'none';base-uri 'self';script-src 'nonce-iG-ajMXaD2pfZF1Sl9odpA' 'strict-dynamic' 'rep eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/cdt1
	Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to
Instances	10	
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set Policy header.	
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variet	
CWE Id	693	
WASC Id	15	
Plugin Id	10055	

Medium	CSP: Wildcard Directive	
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate cer Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attack everything from data theft to site defacement or distribution of malware. CSP provides a set of s that allow website owners to declare approved sources of content that browsers should be allow page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable obj applets, ActiveX, audio and video files.	
URL	https://chromewebstore.google.com/	
	Method	GET
	Attack	
	Evidence	require-trusted-types-for 'script';report-uri /_/ChromeWebStoreConsumerFeUi/cspreport
	Other	The following directives either allow wildcard sources (or ancestors), are not defined, or are ove

Info	script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	script-src 'report-sample' 'nonce-dbVRdrpgV3yImHOgsq7drQ' 'unsafe-inline';object-src 'none';ba /ChromeWebStoreConsumerFeUi/cspreport;worker-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are ove style-src, img-src, connect-src, frame-src, font-src, media-src, manifest-src
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	script-src 'unsafe-inline' 'unsafe-eval' blob: data: 'self' https://apis.google.com https://ssl.gstatic.c com https://www.googletagmanager.com https://www.gstatic.com https://www.google-analytics. google.com/inapp/ https://www.google.com/tools/feedback/ https://www.gstatic.com/inproduct_h gstatic.com/support/content/ https://www.googleapis.com/appsmarket/v2/installedApps/;report-u /ChromeWebStoreConsumerFeUi/cspreport/allowlist
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are ove style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src
URL	https://www.google.com/search?q=canva.com&oq=canva. com&gs_lcrp=EgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE&sou 8
Method	GET
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-7rYghCGK4vbA6bwZcWwEsQ' 'strict-dynamic' eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/cdt1
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are ove style-src, img-src, connect-src, frame-src, font-src, media-src, manifest-src, worker-src
URL	https://www.google.com/search?q=canva.com&oq=canva. com&gs_lcrp=EgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE&sou 8&sei=xB8daOXfHK-R4-EPzemMwAE
Method	GET
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-iG-ajMXaD2pfZF1Sl9odpA' 'strict-dynamic' 'rep eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/cdt1
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are ove style-src, img-src, connect-src, frame-src, font-src, media-src, manifest-src, worker-src
Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variet
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	CSP: script-src unsafe-eval
	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate cer Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attack

Description		everything from data theft to site defacement or distribution of malware. CSP provides a set of s that allow website owners to declare approved sources of content that browsers should be allow page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable obje applets, ActiveX, audio and video files.
	URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/7sbwg /0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
	Method	GET
	Attack	
	Evidence	default-src 'none'; script-src 'nonce-KqXPejJer189nz9s' 'unsafe-eval'; script-src-attr 'none'; work 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; form-ac 'self'
	Other Info	script-src includes unsafe-eval.
	URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/7sbwg /0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
	Method	GET
	Attack	
	Evidence	default-src 'none'; script-src 'nonce-KqXPejJer189nz9s' 'unsafe-eval'; script-src-attr 'none'; work 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; form-ac 'self'; sandbox allow-same-origin allow-scripts allow-popups allow-forms
	Other Info	script-src includes unsafe-eval.
	URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/iu289 /0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
	Method	GET
	Attack	
	Evidence	default-src 'none'; script-src 'nonce-UWDhdRC48bH6c094' 'unsafe-eval'; script-src-attr 'none'; w src 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; form uri 'self'
	Other Info	script-src includes unsafe-eval.
	URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/iu289 /0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
	Method	GET
	Attack	
	Evidence	default-src 'none'; script-src 'nonce-UWDhdRC48bH6c094' 'unsafe-eval'; script-src-attr 'none'; w src 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; form uri 'self'; sandbox allow-same-origin allow-scripts allow-popups allow-forms
	Other Info	script-src includes unsafe-eval.
	URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/ixl4x /0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
	Method	GET
	Attack	
	Evidence	default-src 'none'; script-src 'nonce-xtUXrNYr2ZQmNM0g' 'unsafe-eval'; script-src-attr 'none'; wo src 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; form uri 'self'
	Other Info	script-src includes unsafe-eval.
	URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/ixl4x /0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/

Method	GET
Attack	
Evidence	default-src 'none'; script-src 'nonce-xtUXrNYr2ZQmNM0g' 'unsafe-eval'; script-src-attr 'none'; wo src 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; forn uri 'self'; sandbox allow-same-origin allow-scripts allow-popups allow-forms
Other Info	script-src includes unsafe-eval.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/o8ic5 /0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	default-src 'none'; script-src 'nonce-U7QbVnQRiLJw0j9C' 'unsafe-eval'; script-src-attr 'none'; wo 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; form-ac 'self'
Other Info	script-src includes unsafe-eval.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/o8ic5 /0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	default-src 'none'; script-src 'nonce-U7QbVnQRiLJw0j9C' 'unsafe-eval'; script-src-attr 'none'; wo 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; form-ac 'self'; sandbox allow-same-origin allow-scripts allow-popups allow-forms
Other Info	script-src includes unsafe-eval.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/u2hhw /0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	default-src 'none'; script-src 'nonce-ESUe9ETIU75F8KmH' 'unsafe-eval'; script-src-attr 'none'; w src 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; forn uri 'self'
Other Info	script-src includes unsafe-eval.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/u2hhw /0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	default-src 'none'; script-src 'nonce-ESUe9ETIU75F8KmH' 'unsafe-eval'; script-src-attr 'none'; w src 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; forn uri 'self'; sandbox allow-same-origin allow-scripts allow-popups allow-forms
Other Info	script-src includes unsafe-eval.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	script-src 'unsafe-inline' 'unsafe-eval' blob: data: 'self' https://apis.google.com https://ssl.gstatic.c com https://www.googletagmanager.com https://www.gstatic.com https://www.google-analytics. google.com/inapp/ https://www.google.com/tools/feedback/ https://www.gstatic.com/inproduct_h gstatic.com/support/content/ https://www.googleapis.com/appsmarket/v2/installedApps/;report-u /ChromeWebStoreConsumerFeUi/cspreport/allowlist

Other Info	script-src includes unsafe-eval.
URL	https://www.google.com/search?q=canva.com&oq=canva.com&gs_lcrp=EgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE&sou 8
Method	GET
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-7rYghCGK4vbA6bwZcWwEsQ' 'strict-dynamic' eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/cdt1
Other Info	script-src includes unsafe-eval.
URL	https://www.google.com/search?q=canva.com&oq=canva.com&gs_lcrp=EgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE&sou 8&sei=xB8daOXfHK-R4-EPzemMwAE
Method	GET
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-iG-ajMXaD2pfZF1Sl9odpA' 'strict-dynamic' 'rep eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/cdt1
Other Info	script-src includes unsafe-eval.
Instances	13
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variet
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	CSP: script-src unsafe-inline
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	require-trusted-types-for 'script';report-uri /_/ChromeWebStoreConsumerFeUi/cspreport
Other Info	script-src includes unsafe-inline.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
	script-src 'unsafe-inline' 'unsafe-eval' blob: data: 'self' https://apis.google.com https://ssl. gstatic.com https://www.google.com https://www.googletagmanager.com https://www.

Evidence	gstatic.com https://www.google-analytics.com https://support.google.com/inapp/ https://www.google.com/tools/feedback/ https://www.gstatic.com/inproduct_help/ https://www.gstatic.com/support/content/ https://www.googleapis.com/appsmarket/v2 /installedApps/;report-uri /_/ChromeWebStoreConsumerFeUi/cspreport/allowlist
Other Info	script-src includes unsafe-inline.
Instances	2
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security /csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	CSP: style-src unsafe-inline
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate cer Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attack everything from data theft to site defacement or distribution of malware. CSP provides a set of s that allow website owners to declare approved sources of content that browsers should be allow page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable obje applets, ActiveX, audio and video files.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/7sbwg /0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	default-src 'none'; script-src 'nonce-KqXPejJer189nz9s' 'unsafe-eval'; script-src-attr 'none'; work 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; form-ac 'self'
Other Info	style-src includes unsafe-inline.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/7sbwg /0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	default-src 'none'; script-src 'nonce-KqXPejJer189nz9s' 'unsafe-eval'; script-src-attr 'none'; work 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; form-ac 'self'; sandbox allow-same-origin allow-scripts allow-popups allow-forms
Other Info	style-src includes unsafe-inline.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/iu289 /0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	default-src 'none'; script-src 'nonce-UWDhdRC48bH6c094' 'unsafe-eval'; script-src-attr 'none'; w src 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; forn uri 'self'
Other Info	style-src includes unsafe-inline.

URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/iu289/0x4AAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	default-src 'none'; script-src 'nonce-UWDhdRC48bH6c094' 'unsafe-eval'; script-src-attr 'none'; w src 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; forn uri 'self'; sandbox allow-same-origin allow-scripts allow-popups allow-forms
Other Info	style-src includes unsafe-inline.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/ixl4x/0x4AAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	default-src 'none'; script-src 'nonce-xtUXrNYr2ZQmNM0g' 'unsafe-eval'; script-src-attr 'none'; wo src 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; forn uri 'self'
Other Info	style-src includes unsafe-inline.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/ixl4x/0x4AAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	default-src 'none'; script-src 'nonce-xtUXrNYr2ZQmNM0g' 'unsafe-eval'; script-src-attr 'none'; wo src 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; forn uri 'self'; sandbox allow-same-origin allow-scripts allow-popups allow-forms
Other Info	style-src includes unsafe-inline.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/o8ic5/0x4AAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	default-src 'none'; script-src 'nonce-U7QbVnQRiLJw0j9C' 'unsafe-eval'; script-src-attr 'none'; wo 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; form-ac 'self'
Other Info	style-src includes unsafe-inline.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/o8ic5/0x4AAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	default-src 'none'; script-src 'nonce-U7QbVnQRiLJw0j9C' 'unsafe-eval'; script-src-attr 'none'; wo 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; form-ac 'self'; sandbox allow-same-origin allow-scripts allow-popups allow-forms
Other Info	style-src includes unsafe-inline.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/u2hhw/0x4AAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	default-src 'none'; script-src 'nonce-ESUe9ETIU75F8KmH' 'unsafe-eval'; script-src-attr 'none'; w src 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; forn

		uri 'self'
	Other Info	style-src includes unsafe-inline.
	URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/u2hhw/0x4AAAAAADnPlDROrmt1Wwj/dark/fbE/new/normal/auto/
	Method	GET
	Attack	
	Evidence	default-src 'none'; script-src 'nonce-ESUe9ETIU75F8KmH' 'unsafe-eval'; script-src-attr 'none'; w src 'unsafe-inline'; img-src 'self'; connect-src 'self'; frame-src 'self' blob:; child-src 'self' blob:; forn uri 'self'; sandbox allow-same-origin allow-scripts allow-popups allow-forms
	Other Info	style-src includes unsafe-inline.
	URL	https://chromewebstore.google.com/
	Method	GET
	Attack	
	Evidence	require-trusted-types-for 'script';report-uri /_/ChromeWebStoreConsumerFeUi/cspreport
	Other Info	style-src includes unsafe-inline.
	URL	https://chromewebstore.google.com/
	Method	GET
	Attack	
	Evidence	script-src 'report-sample' 'nonce-dbVRdrpgV3yImHOgsq7drQ' 'unsafe-inline';object-src 'none';ba /ChromeWebStoreConsumerFeUi/cspreport;worker-src 'self'
	Other Info	style-src includes unsafe-inline.
	URL	https://chromewebstore.google.com/
	Method	GET
	Attack	
	Evidence	script-src 'unsafe-inline' 'unsafe-eval' blob: data: 'self' https://apis.google.com https://ssl.gstatic.c com https://www.googletagmanager.com https://www.gstatic.com https://www.google-analytics. google.com/inapp/ https://www.google.com/tools/feedback/ https://www.gstatic.com/inproduct_h gstatic.com/support/content/ https://www.googleapis.com/appsmarket/v2/installedApps/;report-u /ChromeWebStoreConsumerFeUi/cspreport/allowlist
	Other Info	style-src includes unsafe-inline.
	URL	https://www.google.com/search?q=canva.com&oq=canva.com&gs_lcrp=EgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE&sou 8
	Method	GET
	Attack	
	Evidence	object-src 'none';base-uri 'self';script-src 'nonce-7rYghCGK4vbA6bwZcWwEsQ' 'strict-dynamic' eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/cdt1
	Other Info	style-src includes unsafe-inline.
	URL	https://www.google.com/search?q=canva.com&oq=canva.com&gs_lcrp=EgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE&sou 8&sei=xB8daOXfHK-R4-EPzemMwAE
	Method	GET
	Attack	

Evidence	object-src 'none';base-uri 'self';script-src 'nonce-iG-ajMXaD2pfZF1SI9odpA' 'strict-dynamic' 'repo eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/cdt1
Other Info	style-src includes unsafe-inline.
Instances	15
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variet
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	Content Security Policy (CSP) Header Not Set
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate cer types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks for everything from data theft to site defacement or distribution of malware. CSP provides a set standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1673999601&target=OPTIMIZATION_TARGET_PAGE_VISIBILITY
Method	GET
Attack	
Evidence	
Other Info	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1679317318&target=OPTIMIZATION_TARGET_LANGUAGE_DETECTION
Method	GET
Attack	
Evidence	
Other Info	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1696267841&target=OPTIMIZATION_TARGET_OMNIBOX_URL_SCORING
Method	GET
Attack	
Evidence	
Other Info	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1728324084&target=OPTIMIZATION_TARGET_OMNIBOX_ON_DEVICE_TAIL_SUGGI
Method	GET
Attack	
Evidence	
Other	

	Info	
URL		https://optimizationguide-pa.googleapis.com/downloads?name=1744643027&target=OPTIMIZATION_TARGET_GEOLOCATION_PERMISSION_PRED
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		https://optimizationguide-pa.googleapis.com/downloads?name=1744643050&target=OPTIMIZATION_TARGET_NOTIFICATION_PERMISSION_PREDI
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		https://optimizationguide-pa.googleapis.com/downloads?name=1744729555&target=OPTIMIZATION_TARGET_CLIENT_SIDE_PHISHING
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		https://optimizationguide-pa.googleapis.com/downloads?name=240731042075&target=OPTIMIZATION_TARGET_SEGMENTATION_COMPOSE_PRO
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		https://optimizationguide-pa.googleapis.com/downloads?name=5&target=OPTIMIZATION_TARGET_PAGE_TOPICS_V2
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		https://www.canva.com/
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		https://www.google.com/sorry/index?continue=https://www.google.com/search%3Fq%3Dcanva.26oq%3Dcanva.com%26gs_lcrp%3DEgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE%26sourceid%3Dchrome%26ie%3DUTF-8%26sei%3DxB8daOXfHK-R4-EPzemMwAE&q=EgS2sN70GMi_9MAGIjAaBowNa3-eeVgj-e2FOxtvdzFSUA-SHTcJ5-a3xXNnKk6SJFPWzEcBx8ukuf03gHkyAnJSWgFD

	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		https://ogads-pa.clients6.google.com/$rpc/google.internal.onegoogle.asyncdata.v1.AsyncDataS /GetAsyncData
	Method	OPTIONS
	Attack	
	Evidence	
	Other Info	
URL		https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/flow/ov1/1388196947:1746735 yqCLWYtveBHybMLA-jPKMF2TPxac8KSy1xtButNu5s/93cbfe660a72fd41/O34_hNn2qXejUd.K(cK21v9e40a9X57HLRvXQI-1746739149-1.2.1.1-vAzecFFGR.iCAbIlfQ.0SsRo9muUQaIH55. EBFi8S3NEuRMzvl_xzOlaBfyEaLU5
	Method	POST
	Attack	
	Evidence	
	Other Info	
URL		https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/flow/ov1/240796764:17467350 nYnFH-Wa28az9wo4YlkN6TCVDjdGu_vfFeOOoXi5g4c/93cc00347a584b92 /ZkreTcQ4xd6T4VePf9vr2mWgw29K.ep56IPvHwaaO0A-1746739223-1.2.1.1-AQ.whSBgj_5DF 11EOgH7d7N.hTfu0PD_0K9hj6_OGPerxppP86a6zKRxybQ
	Method	POST
	Attack	
	Evidence	
	Other Info	
URL		https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/flow/ov1/511391438:17467351 1M74wKbCNT8GikpaeUAjS1ErZFS3B9_61rraghRsbHw/93cc02a2483e4b92 /JVSGtt6yLfW6r2d0cjuQJhZo..EZXG4fIG8v0kWkTkQ-1746739323-1.2.1.1- lXYYKSTaWcftYk1o02Nu8BROfeXTgidd3Z2PFkvKAMJ2A0k390ihVI7l_N1gdIp_
	Method	POST
	Attack	
	Evidence	
	Other Info	
URL		https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/flow/ov1/896151768:17467388 97cmr9eaID72RJyTn_AWe8UdmrwiejaAcADzdMVt7VA/93cc022b2833fd41 /NRXphi_JjY2VguRoeNqUmwDZzcARbT7_zh2zekCVgBg-1746739304-1.2.1.1- mK5y4uzXjblALRfUpIWmoXX2BNHfA3Xq.9w1so8nbp4Rolc2RSfYjHmvlA36H_yU
	Method	POST
	Attack	
	Evidence	
	Other Info	
		https://www.canva.com/cdn-cgi/challenge-platform/h/b/flow/ov1/1327657077:1746735050:

URL	isxRI0jRERaOzmJVhu9JDoarSxgWCd8qeLykqL2RsWg/93cbfe582e8df936/_70l9JZpnN. pt5ea5RVLEjRStH.UJGIfWRxcvYz6FxU-1746739147-1.2.1.1- iq7K10KwWCHJWoiEkXBQzTSZKCfe4XdpHJdz_CixhflVZ0d95dtVyO8Dalk8n.Wt	
Method	POST	
Attack		
Evidence		
Other Info		
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/flow/ov1/1960686401:1746738662: wprkCVg75v0xBwbjx16-xqThwqHQGk-r15UqiTYWwXY/93cc0222de9287ef/WiZXTedEFKLBcx. S4zSPKqGYqfwuA27o6Lx5X.wK6KE-1746739302-1.2.1.1- rvpgaz2YqR_0Ya3wKUefTsMkyKexh7mlXumFyYeExf4Bhz_fsyKuBNJ6hRlRKXVk	
Method	POST	
Attack		
Evidence		
Other Info		
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/flow/ov1/2073612182:1746735081: rb5YkuhDOb5Yc34qZP79RZ_mL-wW4jEjs0OPyP5eUrl/93cc029418493f63 /XL1JQQ_nkqrsoT6JfELgwl8HVsrnYLfBqBtKN2ed_nY-1746739320-1.2.1.1- p2CAV3tFtDOqM_tfdBDr_qIH1KQeZB5acc4_MkVmLLQG1BWO6_Z45suUh9WCTnbv	
Method	POST	
Attack		
Evidence		
Other Info		
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/flow/ov1/341960750:1746738712: 4ZeG8FSffZYZml9hWo_QL9sL_yK9K-IohViu0zAZoP0/93cc00257f1c5d17 /q5W3IClQjsMOePxVzyS5wFKZe2KIVgrp3P94K7K81Yg-1746739221-1.2.1.1-8L0UGwO4Gwb(7tf9P_EXtO4NR8RW.JMJEiqv5qWdsl1_Ex5jq84AEeuBj_Llo	
Method	POST	
Attack		
Evidence		
Other Info		
Instances	20	
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Con Security-Policy header.	
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Poli https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/	
CWE Id	693	
WASC Id	15	
Plugin Id	10038	

Medium	Cross-Domain Misconfiguration

Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
URL	https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.F939Du45chc.O/m=gapi_iframes,googleapis_client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo8uI5v7Xlp-b-Z4Th_hAAVtm2lZOw/cb=gapi.loaded_0
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/webfonts/fa-solid-900.woff2
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://challenges.cloudflare.com/turnstile/v0/b/701fd2559006/api.js?onload=OUxOl5&render=explicit
Method	GET
Attack	
Evidence	access-control-allow-origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://fonts.googleapis.com/css2?family=Google+Sans+Text_old:wght@400;500;700
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from

Info		authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL		https://fonts.gstatic.com/s/googlesans/v58/4UaRrENHsxJlGDuGo1OIlJfC6l_24rlCK1Yo_Iq2vgCI.woff2
	Method	GET
	Attack	
	Evidence	Access-Control-Allow-Origin: *
	Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL		https://fonts.gstatic.com/s/productsans/v9/pxiDypQkot1TnFhsFMOfGShVF9eO.woff2
	Method	GET
	Attack	
	Evidence	Access-Control-Allow-Origin: *
	Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL		https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmWUlfBBc4.woff2
	Method	GET
	Attack	
	Evidence	Access-Control-Allow-Origin: *
	Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL		https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717689176015
	Method	GET
	Attack	
	Evidence	Access-Control-Allow-Origin: *
	Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL		https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js
	Method	GET
	Attack	
	Evidence	Access-Control-Allow-Origin: *
		The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser

Other Info	implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Instances	10
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet. html5_overly_permissive_cors_policy
CWE Id	264
WASC Id	14
Plugin Id	10098

Medium	Missing Anti-clickjacking Header
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-S Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/7sbwg /0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/iu289 /0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/ixl4x /0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/o8ic5 /0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/u2hhw /0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/

	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		https://optimizationguide-pa.googleapis.com/downloads?name=1673999601&target=OPTIMIZATION_TARGET_PAGE_VISIBILITY
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		https://optimizationguide-pa.googleapis.com/downloads?name=1679317318&target=OPTIMIZATION_TARGET_LANGUAGE_DETECTION
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		https://optimizationguide-pa.googleapis.com/downloads?name=1696267841&target=OPTIMIZATION_TARGET_OMNIBOX_URL_SCORING
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		https://optimizationguide-pa.googleapis.com/downloads?name=1728324084&target=OPTIMIZATION_TARGET_OMNIBOX_ON_DEVICE_TAIL_SUGGE
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		https://optimizationguide-pa.googleapis.com/downloads?name=1744643027&target=OPTIMIZATION_TARGET_GEOLOCATION_PERMISSION_PRED
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		https://optimizationguide-pa.googleapis.com/downloads?name=1744643050&target=OPTIMIZATION_TARGET_NOTIFICATION_PERMISSION_PREDI
	Method	GET
	Attack	
	Evidence	
	Other Info	

	URL	https://optimizationguide-pa.googleapis.com/downloads?name=1744729555&target=OPTIMIZATION_TARGET_CLIENT_SIDE_PHISHING
	Method	GET
	Attack	
	Evidence	
	Other Info	
	URL	https://optimizationguide-pa.googleapis.com/downloads?name=240731042075&target=OPTIMIZATION_TARGET_SEGMENTATION_COMPOSE_PRO
	Method	GET
	Attack	
	Evidence	
	Other Info	
	URL	https://optimizationguide-pa.googleapis.com/downloads?name=5&target=OPTIMIZATION_TARGET_PAGE_TOPICS_V2
	Method	GET
	Attack	
	Evidence	
	Other Info	
	URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/flow/ov1/1388196947:1746735 yqCLWYtveBHybMLA-jPKMF2TPxac8KSy1xtButNu5s/93cbfe660a72fd41/O34_hNn2qXejUd.Kc cK21v9e40a9X57HLRvXQI-1746739149-1.2.1.1-vAzecFFGR.iCAbIlfQ.0SsRo9muUQaIH55. EBFi8S3NEuRMzvl_xzOlaBfyEaLU5
	Method	POST
	Attack	
	Evidence	
	Other Info	
	URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/flow/ov1/240796764:17467350 nYnFH-Wa28az9wo4YlkN6TCVDjdGu_vfFeOOoXi5g4c/93cc00347a584b92 /ZkreTcQ4xd6T4VePf9vr2mWgw29K.ep56IPvHwaaO0A-1746739223-1.2.1.1-AQ.whSBgj_5DF 11EOgH7d7N.hTfu0PD_0K9hj6_OGPerxppP86a6zKRxybQ
	Method	POST
	Attack	
	Evidence	
	Other Info	
	URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/flow/ov1/511391438:17467351 1M74wKbCNT8GikpaeUAjS1ErZFS3B9_61rraghRsbHw/93cc02a2483e4b92 /JVSGtt6yLfW6r2d0cjuQJhZo..EZXG4flG8v0kWkTkQ-1746739323-1.2.1.1- IXYYKSTaWcftYk1o02Nu8BROfeXTgidd3Z2PFkvKAMJ2A0k390ihVI7I_N1gdIp_
	Method	POST
	Attack	
	Evidence	
	Other Info	

	URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/flow/ov1/896151768:17467388 97cmr9eaID72RJyTn_AWe8UdmrwiejaAcADzdMVt7VA/93cc022b2833fd41 /NRXphi_JjY2VguRoeNqUmwDZzcARbT7_zh2zekCVgBg-1746739304-1.2.1.1- mK5y4uzXjblALRfUpIWmoXX2BNHfA3Xq.9w1so8nbp4Rolc2RSfYjHmvlA36H_yU
	Method	POST
	Attack	
	Evidence	
	Other Info	
	URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/flow/ov1/1327657077:1746735050: isxRI0jRERaOzmJVhu9JDoarSxgWCd8qeLykqL2RsWg/93cbfe582e8df936/_70l9JZpnN. pt5ea5RVLEjRStH.UJGIfWRxcvYz6FxU-1746739147-1.2.1.1- iq7K10KwWCHJWoiEkXBQzTSZKCfe4XdpHJdz_CixhflVZ0d95dtVyO8Dalk8n.Wt
	Method	POST
	Attack	
	Evidence	
	Other Info	
	URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/flow/ov1/1960686401:1746738662: wprkCVg75v0xBwbjx16-xqThwqHQGk-r15UqiTYWwXY/93cc0222de9287ef/WiZXTedEFKLBcx. S4zSPKqGYqfwuA27o6Lx5X.wK6KE-1746739302-1.2.1.1- rvpgaz2YqR_0Ya3wKUefTsMkyKexh7mIXumFyYeExf4Bhz_fsyKuBNJ6hRlRKXVk
	Method	POST
	Attack	
	Evidence	
	Other Info	
	URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/flow/ov1/2073612182:1746735081: rb5YkuhDOb5Yc34qZP79RZ_mL-wW4jEjs0OPyP5eUrI/93cc029418493f63 /XL1JQQ_nkqrsoT6JfELgwl8HVsrnYLfBqBtKN2ed_nY-1746739320-1.2.1.1- p2CAV3tFtDOqM_tfdBDr_qIH1KQeZB5acc4_MkVmLLQG1BWO6_Z45suUh9WCTnbv
	Method	POST
	Attack	
	Evidence	
	Other Info	
	URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/flow/ov1/341960750:1746738712: 4ZeG8FSffZYZml9hWo_QL9sL_yK9K-IohViu0zAZoP0/93cc00257f1c5d17 /q5W3lClQjsMOePxVzyS5wFKZe2KIVgrp3P94K7K81Yg-1746739221-1.2.1.1-8L0UGwO4Gwb 7tf9P_EXtO4NR8RW.JMJEiqv5qWdsl1_Ex5jq84AEeuBj_Llo
	Method	POST
	Attack	
	Evidence	
	Other Info	
Instances		22
Solution		Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP header Ensure one of them is set on all web pages returned by your site/app.

	If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you shou DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Low	CSP: Notices
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate cer Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attack everything from data theft to site defacement or distribution of malware. CSP provides a set of s that allow website owners to declare approved sources of content that browsers should be allow page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable obje applets, ActiveX, audio and video files.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	require-trusted-types-for 'script';report-uri /_/ChromeWebStoreConsumerFeUi/cspreport
Other Info	Warnings: The report-uri directive has been deprecated in favor of the new report-to directive
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	script-src 'report-sample' 'nonce-dbVRdrpgV3yImHOgsq7drQ' 'unsafe-inline';object-src 'none';ba /ChromeWebStoreConsumerFeUi/cspreport;worker-src 'self'
Other Info	Warnings: The report-uri directive has been deprecated in favor of the new report-to directive Th has been deprecated in favor of the new report-to directive
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	script-src 'unsafe-inline' 'unsafe-eval' blob: data: 'self' https://apis.google.com https://ssl.gstatic.c com https://www.googletagmanager.com https://www.gstatic.com https://www.google-analytics. google.com/inapp/ https://www.google.com/tools/feedback/ https://www.gstatic.com/inproduct_h gstatic.com/support/content/ https://www.googleapis.com/appsmarket/v2/installedApps/;report-u /ChromeWebStoreConsumerFeUi/cspreport/allowlist
Other Info	Warnings: The report-uri directive has been deprecated in favor of the new report-to directive Th has been deprecated in favor of the new report-to directive The report-uri directive has been de new report-to directive
URL	https://www.google.com/search?q=canva.com&oq=canva. com&gs_lcrp=EgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE&sou 8
Method	GET
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-7rYghCGK4vbA6bwZcWwEsQ' 'strict-dynamic' eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/cdt1
Other Info	Warnings: The report-uri directive has been deprecated in favor of the new report-to directive
URL	https://www.google.com/search?q=canva.com&oq=canva. com&gs_lcrp=EgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE&sou 8&sei=xB8daOXfHK-R4-EPzemMwAE

Method	GET
Attack	
Evidence	object-src 'none';base-uri 'self';script-src 'nonce-iG-ajMXaD2pfZF1SI9odpA' 'strict-dynamic' 'repo eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/cdt1
Other Info	Warnings: The report-uri directive has been deprecated in favor of the new report-to directive

Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variet
CWE Id	693
WASC Id	15
Plugin Id	10055

Low	Cookie with SameSite Attribute None
Description	A cookie has been set with its SameSite attribute set to "none", which means that the cookie ca a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site requ script inclusion, and timing attacks.

URL	https://www.canva.com/
Method	GET
Attack	
Evidence	Set-Cookie: __cf_bm
Other Info	
URL	https://www.google.com/search?q=canva.com&oq=canva. com&gs_lcrp=EgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE&sou 8
Method	GET
Attack	
Evidence	Set-Cookie: NID
Other Info	
URL	https://www.google.com/search?q=canva.com&oq=canva. com&gs_lcrp=EgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE&sou 8&sei=xB8daOXfHK-R4-EPzemMwAE
Method	GET
Attack	
Evidence	Set-Cookie: NID
Other Info	
URL	https://play.google.com/log?format=json&hasfast=true
Method	POST
Attack	
Evidence	Set-Cookie: NID
Other	

Info	
Instances	4
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Low	Cross-Domain JavaScript Source File Inclusion
Description	The page includes one or more script files from a third-party domain.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	<script noCollect src="https://www.gstatic.com/_/mss/boq-chrome-webstore/_/js/k=boq-chrome-webstore.ChromeWebStoreConsumerFeUi.en_US.GZv8TRD6ktk.es5.O/am=eFQADLgFAAE/d=1/excm=_b,_tp,discoverview/ed=1/dg=0/wt=2/ujg=1/rs=AEP720I0aXr2vcE4r6yw95Kzg6qLRWHu6w/m=_b,_tp" defer id="base-js" fetchpriority="high" nonce="dbVRdrpgV3yImHOgsq7drQ"></script>
Other Info	
Instances	1
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Plugin Id	10017

Low	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web serv web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered ov protocol and is specified in RFC 6797.
URL	https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.F939Du45chc.O/m=gapi_iframes,g /rs=AHpOoo8uI5v7XIp-b-Z4Th_hAAVtm2lZOw/cb=gapi.loaded_0
Method	GET
Attack	
Evidence	
Other Info	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93
Method	GET
Attack	
Evidence	
Other Info	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93
Method	GET
Attack	

Evidence		
Other Info		
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/pat/93cbfe660a72fd41/174673 /df44fc308dc19b6a135f6cdd3527af42e762c27690d5114e2e6319ce6c29a4c4/_yBHVJHasevNY	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/pat/93cc00347a584b92/17467 /f19dbfa9237ba7f30923b920915fded504a7812406d64eabe45c374068815ae0/dRlBfM-T3FtDKj	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/pat/93cc022b2833fd41/174673 /626ca5b2b453aafb37d57a92ebc439bbcbb8758d59617e08a4e1b2a40c0d5503/Cx66enWNmp	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/pat/93cc02a2483e4b92/17467 /3c048e3d28cad8aaf44fd4839692557cb7a0c68a6d002c2c42cbec1d7cf37eba/xqal3f_XYoQyEr	
Method	GET	

Attack		
Evidence		
Other Info		
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/pat/93cc033b099afd41/174673 /ec5489d0a80ea3fb16569c57099a7bc956c37cc4a9b059e72c48bea867786467/oUN9p7LQGol-	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/7sbwg/0 /normal/auto/	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/iu289/0x /normal/auto/	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/ixl4x/0x4 /auto/	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/o8ic5/0x /normal/auto/	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/u2hhw/0 /normal/auto/	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://challenges.cloudflare.com/turnstile/v0/b/701fd2559006/api.js?onload=OUxOl5&render=e	

Method	GET	
Attack		
Evidence		
Other Info		
URL	https://chrome.google.com/webstore?hl=en	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://chromewebstore.google.com/	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://content-autofill.googleapis.com/v1/pages/ChRDaHJvbWUvMTM2LjAuNzEwMy45MhIZCl alt=proto	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://fonts.gstatic.com/s/googlesans/v58/4UaRrENHsxJlGDuGo1OIlJfC6l_24rlCK1Yo_Iq2vgC	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://fonts.gstatic.com/s/productsans/v9/pxiDypQkot1TnFhsFMOfGShVF9eO.woff2	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmWUlfBBc4.woff2	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1673999601&target=OPTIMIZA	
Method	GET	

Attack		
Evidence		
Other Info		
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1679317318&target=OPTIMIZA	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1696267841&target=OPTIMIZA	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1728324084&target=OPTIMIZATION_TARGET_OMNIBOX_ON_DEVICE_TAIL_SUGGI	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1744643027&target=OPTIMIZATION_TARGET_GEOLOCATION_PERMISSION_PRED	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1744643050&target=OPTIMIZATION_TARGET_NOTIFICATION_PERMISSION_PREDI	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1744729555&target=OPTIMIZA	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://optimizationguide-pa.googleapis.com/downloads?name=240731042075&target=OPTIMIZATION_TARGET_SEGMENTATION_COMPOSE_PRO	

	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		https://optimizationguide-pa.googleapis.com/downloads?name=5&target=OPTIMIZATION_TAR
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717€
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		https://www.google.com/async/newtab_promos
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		https://www.google.com/recaptcha/api.js
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		https://www.google.com/shared_dict/srp/9b2f0e32aa58bed3086962cef882a7badfe7e540019b4
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		https://www.google.com/sorry/index?continue=https://www.google.com/search%3Fq%3Dcanva. 3DEgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE%26sourceid%3 3DxB8daOXfHK-R4-EPzemMwAE&q=EgS2sN70GMi_9MAGIjAaBowNa3-eeVgj-e2FOxtvdzFSl a3xXNnKk6SJFPWzEcBx8ukuf03gHkyAnJSWgFD
	Method	GET
	Attack	
	Evidence	
	Other Info	
		https://www.gstatic.com/_/mss/boq-chrome-webstore/_/js/k=boq-chrome-webstore.ChromeWeb

URL	/am=eFQADLgFAAE/d=1/excm=_b,_tp,discoverview/ed=1/dg=0/wt=2/ujg=1/rs=AEP720I0aXr2v
Method	GET
Attack	
Evidence	
Other Info	
URL	https://www.gstatic.com/_/mss/boq-chrome-webstore/_/js/k=boq-chrome-webstore.ChromeWeb /ck=boq-chrome-webstore.ChromeWebStoreConsumerFeUi.lVmjoB1179s.L.B1.O/am=eFQADL discoverview/ed=1/wt=2/ujg=1/rs=AEP720KkMP-e4Q8FpcjA_Oklqo-Cw1JNJA/ee=EVNhjf:pw70 ZDZcre;LBgRLc:SdcwHb;Me32dd:MEeYgc;NJ1rfe:qTnoBf;NPKaK:SdcwHb;NSEoX:lazG7b;Pjp ScI3Yc:e7Hzgb;Uvc8o:VDovNc;YIZmRd:A1yn5d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfS lOO0Vd:OTA3Ae;oGtAuc:sOXFj;pXdRYb:MdUzUe;qafBPd:yDVVkb;qddgKe:xQtZb;wR5FRb:YA zxnPse:duFQFc/m=ws9Tlc,n73qwf,aW3pY,UUJqVe,IZT63,e5qFLc,O1Gjze,ebZ3mb,gll2M,ml3L ZwDk9d,RyvaUb,YYmHzb,p8L0ob,MT4Hub,h4ilFc,erhsIc,ataMLc,NCodtd,O6y8ed,MpJwZc,PrF KUM7Z,qTnoBf,duFQFc,sI9bWe,lwddkf,gychg,w9hDv,RMhBfe,CfLNpd,SdcwHb,pw70Gc,mdR7 kjKdXe,JNoxi,BVgquf,QIhFr,YA1iG,V9amgb,hKSk3e,hc6Ubd,SpsfSb,Z5uLle,BBI74,MdUzUe,zb
Method	GET
Attack	
Evidence	
Other Info	
URL	https://www.gstatic.com/_/mss/boq-chrome-webstore/_/js/k=boq-chrome-webstore.ChromeWeb /ck=boq-chrome-webstore.ChromeWebStoreConsumerFeUi.lVmjoB1179s.L.B1.O/am=eFQADL EFQ78c,FdMhB,IZT63,JNoxi,KUM7Z,LEikZe,MI6k7c,MT4Hub,MdUzUe,MpJwZc,NCodtd,NwH0 QvLWAb,RMhBfe,RyvaUb,SdcwHb,SpsfSb,UUJqVe,Uas9Hd,Ulmmrd,V3dDOb,V9amgb,XVMN aW3pY,ataMLc,byfTOb,duFQFc,e5qFLc,ebZ3mb,erhsIc,gll2M,gychg,h4ilFc,hKSk3e,hc6Ubd,kjI n73qwf,p8L0ob,pjICDe,pw70Gc,qTnoBf,sI9bWe,w9hDv,ws9Tlc,xQtZb,xUdipf,zbML3c,zr1jrb/exc /rs=AEP720KkMP-e4Q8FpcjA_Oklqo-Cw1JNJA/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;JsbNhc:Xd MEeYgc;NJ1rfe:qTnoBf;NPKaK:SdcwHb;NSEoX:lazG7b;Pjplud:EEDORb;QGR0gd:Mlhmy;SNU YIZmRd:A1yn5d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;dowIGb:ebZ3mb;eBAeSb:zbM sOXFj;pXdRYb:MdUzUe;qafBPd:yDVVkb;qddgKe:xQtZb;wR5FRb:YA1iG:xqZigf:BBI74;yEQyxe /m=HsQQib,cephkf,i8oNZb,RilNWe,MH0hJe,AWpPDd,QVysJe,rm99Nc,ZvHseb,PIVayb,LBaJxk w9C4d,FkSse,LcrBLd,EKHvcb,VBl5Ff,Y8VT6d
Method	GET
Attack	
Evidence	
Other Info	
URL	https://www.gstatic.com/og/_/js/k=og.qtm.en_US.jS_CZIDYjaI.2019.O/rt=j/m=q_dnp,qmd,qcwid, qalo,qebr,qein,qhaw,qhawgm3,qhba,qhbr,qhbrgm3,qhch,qhchgm3,qhga,qhid,qhidgm3,qhin,qhl /rs=AA2YrTsB9Qz4OH5RFhAQLL8W1kIQz_J3Rg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://www.gstatic.com/og/_/js/k=og.qtm.en_US.jS_CZIDYjaI.2019.O/rt=j/m=qabr,q_dnp,qcwid qhba,qhbr,qhch,qhga,qhid,qhin/d=1/ed=1/rs=AA2YrTsB9Qz4OH5RFhAQLL8W1kIQz_J3Rg
Method	GET
Attack	
Evidence	
Other	

	Info
URL	https://www.gstatic.com/og/_/ss/k=og.qtm.kh2ijRv0MlA.L.W.O/m=qcwid/excm=qaaw,qadd,qaid,/ed=1/ct=zgms/rs=AA2YrTtnuxIkMiC5WsBVsg4Kr_L_CPAqfg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://www.gstatic.com/og/_/ss/k=og.qtm.kh2ijRv0MlA.L.W.O/m=qmd,qcwid/excm=qaaw,qabr,qhbr,qhbrgm3,qhch,qhchgm3,qhga,qhid,qhidgm3,qhin,qhlo,qhlogm3,qhmn,qhpc,qhsf,qhsfgm3,/rs=AA2YrTtnuxIkMiC5WsBVsg4Kr_L_CPAqfg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ogads-pa.clients6.google.com/$rpc/google.internal.onegoogle.asyncdata.v1.AsyncDataS
Method	OPTIONS
Attack	
Evidence	
Other Info	
URL	https://play.google.com/log?format=json&hasfast=true
Method	OPTIONS
Attack	
Evidence	
Other Info	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/flow/ov1/1388196947:1746735jPKMF2TPxac8KSy1xtButNu5s/93cbfe660a72fd41/O34_hNn2qXejUd.Kq_FYI.cK21v9e40a9X5iCAbIlfQ.0SsRo9muUQaIH55.EBFi8S3NEuRMzvI_xzOIaBfyEaLU5
Method	POST
Attack	
Evidence	
Other Info	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/flow/ov1/240796764:17467350Wa28az9wo4YlkN6TCVDjdGu_vfFeOOoXi5g4c/93cc00347a584b92/ZkreTcQ4xd6T4VePf9vr2nAQ.whSBgj_5DFZ9Pe.11EOgH7d7N.hTfu0PD_0K9hj6_OGPerxppP86a6zKRxybQ
Method	POST

	Attack	
	Evidence	
	Other Info	
URL		https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/flow/ov1/511391438:17467351 1M74wKbCNT8GikpaeUAjS1ErZFS3B9_61rraghRsbHw/93cc02a2483e4b92/JVSGtt6yLfW6r2d 1.2.1.1-lXYYKSTaWcftYk1o02Nu8BROfeXTgidd3Z2PFkvKAMJ2A0k390ihVI7l_N1gdIp_
	Method	POST
	Attack	
	Evidence	
	Other Info	
URL		https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/flow/ov1/573113744:17467388 9PHjCRGIImUmAAz2a3RJK6YpnBiLTNzvlM5PXX_c/93cc033b099afd41/ZDJyYttfPtX0UY.d_gN 1.2.1.1-s_d2WBJniKIqJLKvK0Tr7y341M4RhZdAIezfanZVk0cXk5aalZZ11.Uw7CwVuQfM
	Method	POST
	Attack	
	Evidence	
	Other Info	
URL		https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/flow/ov1/896151768:17467388 97cmr9eaID72RJyTn_AWe8UdmrwiejaAcADzdMVt7VA/93cc022b2833fd41/NRXphi_JjY2VguR 1746739304-1.2.1.1-mK5y4uzXjblALRfUpIWmoXX2BNHfA3Xq.9w1so8nbp4Rolc2RSfYjHmvlA3
	Method	POST
	Attack	
	Evidence	
	Other Info	
URL		https://chromewebstore.googleapis.com/v2/items/-/storeMetadata:batchGet
	Method	POST
	Attack	
	Evidence	
	Other Info	
URL		https://optimizationguide-pa.googleapis.com/v1:GetModels?key=AIzaSyBqJZh-7pA44blAaAkH6
	Method	POST
	Attack	
	Evidence	
	Other Info	
URL		https://play.google.com/log?format=json&hasfast=true
	Method	POST
	Attack	
	Evidence	
	Other Info	

URL	https://play.google.com/log?hasfast=true&authuser=0&format=json
Method	POST
Attack	
Evidence	
Other Info	
URL	https://update.googleapis.com/service/update2/json
Method	POST
Attack	
Evidence	
Other Info	
URL	https://update.googleapis.com/service/update2/json?cup2key=15:L3EYilNTE1rHeFFg6qYdPP0kFnFgf0wKFsDwgTGHerE&cup2hreq=a7b4bba51a2cf88b3a1456
Method	POST
Attack	
Evidence	
Other Info	
URL	https://www.canva.com/cdn-cgi/rum
Method	POST
Attack	
Evidence	
Other Info	

Instances	59
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Stri
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

Low	Timestamp Disclosure - Unix
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.F939Du45chc.O/m=gapi_iframes,go/rs=AHpOoo8uI5v7Xlp-b-Z4Th_hAAVtm2lZOw/cb=gapi.loaded_0
Method	GET
Attack	
Evidence	1518500249
Other Info	1518500249, which evaluates to: 2018-02-13 10:37:29.
URL	https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.F939Du45chc.O/m=gapi_iframes,go/rs=AHpOoo8uI5v7Xlp-b-Z4Th_hAAVtm2lZOw/cb=gapi.loaded_0

Method	GET	
Attack		
Evidence	1732584193	
Other Info	1732584193, which evaluates to: 2024-11-26 06:23:13.	
URL	https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.F939Du45chc.O/m=gapi_iframes,g /rs=AHpOoo8uI5v7Xlp-b-Z4Th_hAAVtm2lZOw/cb=gapi.loaded_0	
Method	GET	
Attack		
Evidence	1859775393	
Other Info	1859775393, which evaluates to: 2028-12-07 09:16:33.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93	
Method	GET	
Attack		
Evidence	1508970993	
Other Info	1508970993, which evaluates to: 2017-10-26 03:36:33.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93	
Method	GET	
Attack		
Evidence	1537002063	
Other Info	1537002063, which evaluates to: 2018-09-15 14:01:03.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93	
Method	GET	
Attack		
Evidence	1541459225	
Other Info	1541459225, which evaluates to: 2018-11-06 04:07:05.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93	
Method	GET	
Attack		
Evidence	1555081692	
Other Info	1555081692, which evaluates to: 2019-04-12 20:08:12.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93	
Method	GET	
Attack		
Evidence	1695183700	
Other Info	1695183700, which evaluates to: 2023-09-20 09:21:40.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93	
Method	GET	

Attack		
Evidence	1746735080	
Other Info	1746735080, which evaluates to: 2025-05-09 01:11:20.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93	
Method	GET	
Attack		
Evidence	1747873779	
Other Info	1747873779, which evaluates to: 2025-05-22 05:29:39.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93	
Method	GET	
Attack		
Evidence	1779033703	
Other Info	1779033703, which evaluates to: 2026-05-17 21:01:43.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93	
Method	GET	
Attack		
Evidence	1899447441	
Other Info	1899447441, which evaluates to: 2030-03-11 13:17:21.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93	
Method	GET	
Attack		
Evidence	1925078388	
Other Info	1925078388, which evaluates to: 2031-01-02 04:59:48.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93	
Method	GET	
Attack		
Evidence	1955562222	
Other Info	1955562222, which evaluates to: 2031-12-21 00:43:42.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93	
Method	GET	
Attack		
Evidence	1986661051	
Other Info	1986661051, which evaluates to: 2032-12-14 23:17:31.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93	
Method	GET	
Attack		
Evidence	1996064986	

Other Info	1996064986, which evaluates to: 2033-04-02 19:29:46.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93	
Method	GET	
Attack		
Evidence	2024104815	
Other Info	2024104815, which evaluates to: 2034-02-21 08:20:15.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93	
Method	GET	
Attack		
Evidence	1508970993	
Other Info	1508970993, which evaluates to: 2017-10-26 03:36:33.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93	
Method	GET	
Attack		
Evidence	1537002063	
Other Info	1537002063, which evaluates to: 2018-09-15 14:01:03.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93	
Method	GET	
Attack		
Evidence	1541459225	
Other Info	1541459225, which evaluates to: 2018-11-06 04:07:05.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93	
Method	GET	
Attack		
Evidence	1555081692	
Other Info	1555081692, which evaluates to: 2019-04-12 20:08:12.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93	
Method	GET	
Attack		
Evidence	1695183700	
Other Info	1695183700, which evaluates to: 2023-09-20 09:21:40.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93	
Method	GET	
Attack		
Evidence	1746735059	
Other Info	1746735059, which evaluates to: 2025-05-09 01:10:59.	

URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c
Method	GET
Attack	
Evidence	1747873779
Other Info	1747873779, which evaluates to: 2025-05-22 05:29:39.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c
Method	GET
Attack	
Evidence	1779033703
Other Info	1779033703, which evaluates to: 2026-05-17 21:01:43.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c
Method	GET
Attack	
Evidence	1899447441
Other Info	1899447441, which evaluates to: 2030-03-11 13:17:21.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c
Method	GET
Attack	
Evidence	1925078388
Other Info	1925078388, which evaluates to: 2031-01-02 04:59:48.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c
Method	GET
Attack	
Evidence	1955562222
Other Info	1955562222, which evaluates to: 2031-12-21 00:43:42.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c
Method	GET
Attack	
Evidence	1986661051
Other Info	1986661051, which evaluates to: 2032-12-14 23:17:31.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c
Method	GET
Attack	
Evidence	1996064986
Other Info	1996064986, which evaluates to: 2033-04-02 19:29:46.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c
Method	GET

Attack		
Evidence	2024104815	
Other Info	2024104815, which evaluates to: 2034-02-21 08:20:15.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence	1508970993	
Other Info	1508970993, which evaluates to: 2017-10-26 03:36:33.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence	1537002063	
Other Info	1537002063, which evaluates to: 2018-09-15 14:01:03.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence	1541459225	
Other Info	1541459225, which evaluates to: 2018-11-06 04:07:05.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence	1555081692	
Other Info	1555081692, which evaluates to: 2019-04-12 20:08:12.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence	1695183700	
Other Info	1695183700, which evaluates to: 2023-09-20 09:21:40.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence	1746738877	
Other Info	1746738877, which evaluates to: 2025-05-09 02:14:37.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		

	Evidence	1747873779
	Other Info	1747873779, which evaluates to: 2025-05-22 05:29:39.
URL		https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93d
	Method	GET
	Attack	
	Evidence	1779033703
	Other Info	1779033703, which evaluates to: 2026-05-17 21:01:43.
URL		https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93d
	Method	GET
	Attack	
	Evidence	1899447441
	Other Info	1899447441, which evaluates to: 2030-03-11 13:17:21.
URL		https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93d
	Method	GET
	Attack	
	Evidence	1925078388
	Other Info	1925078388, which evaluates to: 2031-01-02 04:59:48.
URL		https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93d
	Method	GET
	Attack	
	Evidence	1955562222
	Other Info	1955562222, which evaluates to: 2031-12-21 00:43:42.
URL		https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93d
	Method	GET
	Attack	
	Evidence	1986661051
	Other Info	1986661051, which evaluates to: 2032-12-14 23:17:31.
URL		https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93d
	Method	GET
	Attack	
	Evidence	1996064986
	Other Info	1996064986, which evaluates to: 2033-04-02 19:29:46.
URL		https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93d
	Method	GET
	Attack	
	Evidence	2024104815
	Other	

Info	2024104815, which evaluates to: 2034-02-21 08:20:15.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93
Method	GET
Attack	
Evidence	1508970993
Other Info	1508970993, which evaluates to: 2017-10-26 03:36:33.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93
Method	GET
Attack	
Evidence	1537002063
Other Info	1537002063, which evaluates to: 2018-09-15 14:01:03.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93
Method	GET
Attack	
Evidence	1541459225
Other Info	1541459225, which evaluates to: 2018-11-06 04:07:05.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93
Method	GET
Attack	
Evidence	1555081692
Other Info	1555081692, which evaluates to: 2019-04-12 20:08:12.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93
Method	GET
Attack	
Evidence	1695183700
Other Info	1695183700, which evaluates to: 2023-09-20 09:21:40.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93
Method	GET
Attack	
Evidence	1746735155
Other Info	1746735155, which evaluates to: 2025-05-09 01:12:35.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93
Method	GET
Attack	
Evidence	1747873779
Other Info	1747873779, which evaluates to: 2025-05-22 05:29:39.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93

Method	GET	
Attack		
Evidence	1779033703	
Other Info	1779033703, which evaluates to: 2026-05-17 21:01:43.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence	1899447441	
Other Info	1899447441, which evaluates to: 2030-03-11 13:17:21.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence	1925078388	
Other Info	1925078388, which evaluates to: 2031-01-02 04:59:48.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence	1955562222	
Other Info	1955562222, which evaluates to: 2031-12-21 00:43:42.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence	1986661051	
Other Info	1986661051, which evaluates to: 2032-12-14 23:17:31.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence	1996064986	
Other Info	1996064986, which evaluates to: 2033-04-02 19:29:46.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence	2024104815	
Other Info	2024104815, which evaluates to: 2034-02-21 08:20:15.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	

Attack		
Evidence	1508970993	
Other Info	1508970993, which evaluates to: 2017-10-26 03:36:33.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93d	
Method	GET	
Attack		
Evidence	1537002063	
Other Info	1537002063, which evaluates to: 2018-09-15 14:01:03.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93d	
Method	GET	
Attack		
Evidence	1541459225	
Other Info	1541459225, which evaluates to: 2018-11-06 04:07:05.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93d	
Method	GET	
Attack		
Evidence	1555081692	
Other Info	1555081692, which evaluates to: 2019-04-12 20:08:12.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93d	
Method	GET	
Attack		
Evidence	1695183700	
Other Info	1695183700, which evaluates to: 2023-09-20 09:21:40.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93d	
Method	GET	
Attack		
Evidence	1746738856	
Other Info	1746738856, which evaluates to: 2025-05-09 02:14:16.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93d	
Method	GET	
Attack		
Evidence	1747873779	
Other Info	1747873779, which evaluates to: 2025-05-22 05:29:39.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93d	
Method	GET	
Attack		
Evidence	1779033703	

Other Info	1779033703, which evaluates to: 2026-05-17 21:01:43.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence	1899447441	
Other Info	1899447441, which evaluates to: 2030-03-11 13:17:21.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence	1925078388	
Other Info	1925078388, which evaluates to: 2031-01-02 04:59:48.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence	1955562222	
Other Info	1955562222, which evaluates to: 2031-12-21 00:43:42.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence	1986661051	
Other Info	1986661051, which evaluates to: 2032-12-14 23:17:31.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence	1996064986	
Other Info	1996064986, which evaluates to: 2033-04-02 19:29:46.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93c	
Method	GET	
Attack		
Evidence	2024104815	
Other Info	2024104815, which evaluates to: 2034-02-21 08:20:15.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/7sbwg0 /normal/auto/	
Method	GET	
Attack		
Evidence	1746739323	
Other		

Info	1746739323, which evaluates to: 2025-05-09 02:22:03.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/iu289/0x /normal/auto/
Method	GET
Attack	
Evidence	1746739223
Other Info	1746739223, which evaluates to: 2025-05-09 02:20:23.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/ixl4x/0x4 /auto/
Method	GET
Attack	
Evidence	1746739304
Other Info	1746739304, which evaluates to: 2025-05-09 02:21:44.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/o8ic5/0x /normal/auto/
Method	GET
Attack	
Evidence	1746739149
Other Info	1746739149, which evaluates to: 2025-05-09 02:19:09.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/u2hhw/0 /normal/auto/
Method	GET
Attack	
Evidence	1746739347
Other Info	1746739347, which evaluates to: 2025-05-09 02:22:27.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	1440571943
Other Info	1440571943, which evaluates to: 2015-08-26 11:52:23.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	1445290099
Other Info	1445290099, which evaluates to: 2015-10-20 02:28:19.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	1459197854

Other Info	1459197854, which evaluates to: 2016-03-29 01:44:14.	
URL	https://chromewebstore.google.com/	
Method	GET	
Attack		
Evidence	1492534915	
Other Info	1492534915, which evaluates to: 2017-04-18 22:01:55.	
URL	https://chromewebstore.google.com/	
Method	GET	
Attack		
Evidence	1494504039	
Other Info	1494504039, which evaluates to: 2017-05-11 17:00:39.	
URL	https://chromewebstore.google.com/	
Method	GET	
Attack		
Evidence	1500939635	
Other Info	1500939635, which evaluates to: 2017-07-25 04:40:35.	
URL	https://chromewebstore.google.com/	
Method	GET	
Attack		
Evidence	1505079174	
Other Info	1505079174, which evaluates to: 2017-09-11 02:32:54.	
URL	https://chromewebstore.google.com/	
Method	GET	
Attack		
Evidence	1506819887	
Other Info	1506819887, which evaluates to: 2017-10-01 06:04:47.	
URL	https://chromewebstore.google.com/	
Method	GET	
Attack		
Evidence	1512762074	
Other Info	1512762074, which evaluates to: 2017-12-09 00:41:14.	
URL	https://chromewebstore.google.com/	
Method	GET	
Attack		
Evidence	1529517641	
Other Info	1529517641, which evaluates to: 2018-06-20 23:00:41.	

URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	1531294590
Other Info	1531294590, which evaluates to: 2018-07-11 12:36:30.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	1537276554
Other Info	1537276554, which evaluates to: 2018-09-18 18:15:54.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	1559730861
Other Info	1559730861, which evaluates to: 2019-06-05 15:34:21.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	1563848740
Other Info	1563848740, which evaluates to: 2019-07-23 07:25:40.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	1565457055
Other Info	1565457055, which evaluates to: 2019-08-10 22:10:55.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	1569974566
Other Info	1569974566, which evaluates to: 2019-10-02 05:02:46.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	1573696625
Other Info	1573696625, which evaluates to: 2019-11-14 06:57:05.
URL	https://chromewebstore.google.com/
Method	GET

	Attack	
	Evidence	1574362961
	Other Info	1574362961, which evaluates to: 2019-11-22 00:02:41.
URL		https://chromewebstore.google.com/
	Method	GET
	Attack	
	Evidence	1575960051
	Other Info	1575960051, which evaluates to: 2019-12-10 11:40:51.
URL		https://chromewebstore.google.com/
	Method	GET
	Attack	
	Evidence	1595589093
	Other Info	1595589093, which evaluates to: 2020-07-24 16:11:33.
URL		https://chromewebstore.google.com/
	Method	GET
	Attack	
	Evidence	1601976924
	Other Info	1601976924, which evaluates to: 2020-10-06 14:35:24.
URL		https://chromewebstore.google.com/
	Method	GET
	Attack	
	Evidence	1602302139
	Other Info	1602302139, which evaluates to: 2020-10-10 08:55:39.
URL		https://chromewebstore.google.com/
	Method	GET
	Attack	
	Evidence	1603004986
	Other Info	1603004986, which evaluates to: 2020-10-18 12:09:46.
URL		https://chromewebstore.google.com/
	Method	GET
	Attack	
	Evidence	1607075079
	Other Info	1607075079, which evaluates to: 2020-12-04 14:44:39.
URL		https://chromewebstore.google.com/
	Method	GET
	Attack	

Evidence	1617680491	
Other Info	1617680491, which evaluates to: 2021-04-06 08:41:31.	
URL	https://chromewebstore.google.com/	
Method	GET	
Attack		
Evidence	1628057821	
Other Info	1628057821, which evaluates to: 2021-08-04 11:17:01.	
URL	https://chromewebstore.google.com/	
Method	GET	
Attack		
Evidence	1632294628	
Other Info	1632294628, which evaluates to: 2021-09-22 12:10:28.	
URL	https://chromewebstore.google.com/	
Method	GET	
Attack		
Evidence	1638419424	
Other Info	1638419424, which evaluates to: 2021-12-02 09:30:24.	
URL	https://chromewebstore.google.com/	
Method	GET	
Attack		
Evidence	1640929337	
Other Info	1640929337, which evaluates to: 2021-12-31 10:42:17.	
URL	https://chromewebstore.google.com/	
Method	GET	
Attack		
Evidence	1641190441	
Other Info	1641190441, which evaluates to: 2022-01-03 11:14:01.	
URL	https://chromewebstore.google.com/	
Method	GET	
Attack		
Evidence	1641600125	
Other Info	1641600125, which evaluates to: 2022-01-08 05:02:05.	
URL	https://chromewebstore.google.com/	
Method	GET	
Attack		
Evidence	1645871820	
Other		

Info	1645871820, which evaluates to: 2022-02-26 15:37:00.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	1657013770
Other Info	1657013770, which evaluates to: 2022-07-05 14:36:10.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	1658309495
Other Info	1658309495, which evaluates to: 2022-07-20 14:31:35.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	1658642128
Other Info	1658642128, which evaluates to: 2022-07-24 10:55:28.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	1663045409
Other Info	1663045409, which evaluates to: 2022-09-13 10:03:29.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	1663314304
Other Info	1663314304, which evaluates to: 2022-09-16 12:45:04.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	1664430433
Other Info	1664430433, which evaluates to: 2022-09-29 10:47:13.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	1665558597
Other Info	1665558597, which evaluates to: 2022-10-12 12:09:57.
URL	https://chromewebstore.google.com/

	Method	GET
	Attack	
	Evidence	1671599974
	Other Info	1671599974, which evaluates to: 2022-12-21 10:19:34.
URL		https://chromewebstore.google.com/
	Method	GET
	Attack	
	Evidence	1671705052
	Other Info	1671705052, which evaluates to: 2022-12-22 15:30:52.
URL		https://chromewebstore.google.com/
	Method	GET
	Attack	
	Evidence	1678171353
	Other Info	1678171353, which evaluates to: 2023-03-07 11:42:33.
URL		https://chromewebstore.google.com/
	Method	GET
	Attack	
	Evidence	1684319496
	Other Info	1684319496, which evaluates to: 2023-05-17 15:31:36.
URL		https://chromewebstore.google.com/
	Method	GET
	Attack	
	Evidence	1686287142
	Other Info	1686287142, which evaluates to: 2023-06-09 10:05:42.
URL		https://chromewebstore.google.com/
	Method	GET
	Attack	
	Evidence	1687166090
	Other Info	1687166090, which evaluates to: 2023-06-19 14:14:50.
URL		https://chromewebstore.google.com/
	Method	GET
	Attack	
	Evidence	1688992201
	Other Info	1688992201, which evaluates to: 2023-07-10 17:30:01.
URL		https://chromewebstore.google.com/
	Method	GET

Attack		
	Evidence	1690358666
	Other Info	1690358666, which evaluates to: 2023-07-26 13:04:26.
URL		https://chromewebstore.google.com/
	Method	GET
	Attack	
	Evidence	1693973103
	Other Info	1693973103, which evaluates to: 2023-09-06 09:05:03.
URL		https://chromewebstore.google.com/
	Method	GET
	Attack	
	Evidence	1713083763
	Other Info	1713083763, which evaluates to: 2024-04-14 13:36:03.
URL		https://chromewebstore.google.com/
	Method	GET
	Attack	
	Evidence	1717733407
	Other Info	1717733407, which evaluates to: 2024-06-07 09:10:07.
URL		https://chromewebstore.google.com/
	Method	GET
	Attack	
	Evidence	1732532491
	Other Info	1732532491, which evaluates to: 2024-11-25 16:01:31.
URL		https://www.canva.com/
	Method	GET
	Attack	
	Evidence	1746739146
	Other Info	1746739146, which evaluates to: 2025-05-09 02:19:06.
URL		https://www.canva.com/
	Method	GET
	Attack	
	Evidence	1746739147
	Other Info	1746739147, which evaluates to: 2025-05-09 02:19:07.
URL		https://www.canva.com/
	Method	GET
	Attack	
	Evidence	1746739221

Other Info	1746739221, which evaluates to: 2025-05-09 02:20:21.	
URL	https://www.canva.com/	
Method	GET	
Attack		
Evidence	1746739302	
Other Info	1746739302, which evaluates to: 2025-05-09 02:21:42.	
URL	https://www.canva.com/	
Method	GET	
Attack		
Evidence	1746739320	
Other Info	1746739320, which evaluates to: 2025-05-09 02:22:00.	
URL	https://www.canva.com/	
Method	GET	
Attack		
Evidence	1746739345	
Other Info	1746739345, which evaluates to: 2025-05-09 02:22:25.	
URL	https://www.canva.com/	
Method	GET	
Attack		
Evidence	1746739146	
Other Info	1746739146, which evaluates to: 2025-05-09 02:19:06.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cbfe582	
Method	GET	
Attack		
Evidence	1508970993	
Other Info	1508970993, which evaluates to: 2017-10-26 03:36:33.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cbfe582	
Method	GET	
Attack		
Evidence	1537002063	
Other Info	1537002063, which evaluates to: 2018-09-15 14:01:03.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cbfe582	
Method	GET	
Attack		
Evidence	1541459225	
Other Info	1541459225, which evaluates to: 2018-11-06 04:07:05.	

URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cbfe582
Method	GET
Attack	
Evidence	1555081692
Other Info	1555081692, which evaluates to: 2019-04-12 20:08:12.
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cbfe582
Method	GET
Attack	
Evidence	1695183700
Other Info	1695183700, which evaluates to: 2023-09-20 09:21:40.
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cbfe582
Method	GET
Attack	
Evidence	1746735050
Other Info	1746735050, which evaluates to: 2025-05-09 01:10:50.
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cbfe582
Method	GET
Attack	
Evidence	1747873779
Other Info	1747873779, which evaluates to: 2025-05-22 05:29:39.
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cbfe582
Method	GET
Attack	
Evidence	1779033703
Other Info	1779033703, which evaluates to: 2026-05-17 21:01:43.
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cbfe582
Method	GET
Attack	
Evidence	1899447441
Other Info	1899447441, which evaluates to: 2030-03-11 13:17:21.
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cbfe582
Method	GET
Attack	
Evidence	1925078388
Other Info	1925078388, which evaluates to: 2031-01-02 04:59:48.
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cbfe582
Method	GET

	Attack	
	Evidence	1955562222
	Other Info	1955562222, which evaluates to: 2031-12-21 00:43:42.
URL		https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cbfe582
	Method	GET
	Attack	
	Evidence	1986661051
	Other Info	1986661051, which evaluates to: 2032-12-14 23:17:31.
URL		https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cbfe582
	Method	GET
	Attack	
	Evidence	1996064986
	Other Info	1996064986, which evaluates to: 2033-04-02 19:29:46.
URL		https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cbfe582
	Method	GET
	Attack	
	Evidence	2024104815
	Other Info	2024104815, which evaluates to: 2034-02-21 08:20:15.
URL		https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc00257
	Method	GET
	Attack	
	Evidence	1508970993
	Other Info	1508970993, which evaluates to: 2017-10-26 03:36:33.
URL		https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc00257
	Method	GET
	Attack	
	Evidence	1537002063
	Other Info	1537002063, which evaluates to: 2018-09-15 14:01:03.
URL		https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc00257
	Method	GET
	Attack	
	Evidence	1541459225
	Other Info	1541459225, which evaluates to: 2018-11-06 04:07:05.
URL		https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc00257
	Method	GET
	Attack	

Evidence	1555081692	
Other Info	1555081692, which evaluates to: 2019-04-12 20:08:12.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc00257	
Method	GET	
Attack		
Evidence	1695183700	
Other Info	1695183700, which evaluates to: 2023-09-20 09:21:40.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc00257	
Method	GET	
Attack		
Evidence	1746738712	
Other Info	1746738712, which evaluates to: 2025-05-09 02:11:52.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc00257	
Method	GET	
Attack		
Evidence	1747873779	
Other Info	1747873779, which evaluates to: 2025-05-22 05:29:39.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc00257	
Method	GET	
Attack		
Evidence	1779033703	
Other Info	1779033703, which evaluates to: 2026-05-17 21:01:43.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc00257	
Method	GET	
Attack		
Evidence	1899447441	
Other Info	1899447441, which evaluates to: 2030-03-11 13:17:21.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc00257	
Method	GET	
Attack		
Evidence	1925078388	
Other Info	1925078388, which evaluates to: 2031-01-02 04:59:48.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc00257	
Method	GET	
Attack		
Evidence	1955562222	
Other		

Info	1955562222, which evaluates to: 2031-12-21 00:43:42.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc00257	
Method	GET	
Attack		
Evidence	1986661051	
Other Info	1986661051, which evaluates to: 2032-12-14 23:17:31.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc00257	
Method	GET	
Attack		
Evidence	1996064986	
Other Info	1996064986, which evaluates to: 2033-04-02 19:29:46.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc00257	
Method	GET	
Attack		
Evidence	2024104815	
Other Info	2024104815, which evaluates to: 2034-02-21 08:20:15.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc0222c	
Method	GET	
Attack		
Evidence	1508970993	
Other Info	1508970993, which evaluates to: 2017-10-26 03:36:33.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc0222c	
Method	GET	
Attack		
Evidence	1537002063	
Other Info	1537002063, which evaluates to: 2018-09-15 14:01:03.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc0222c	
Method	GET	
Attack		
Evidence	1541459225	
Other Info	1541459225, which evaluates to: 2018-11-06 04:07:05.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc0222c	
Method	GET	
Attack		
Evidence	1555081692	
Other Info	1555081692, which evaluates to: 2019-04-12 20:08:12.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc0222c	

Method	GET	
Attack		
Evidence	1695183700	
Other Info	1695183700, which evaluates to: 2023-09-20 09:21:40.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc0222c	
Method	GET	
Attack		
Evidence	1746738662	
Other Info	1746738662, which evaluates to: 2025-05-09 02:11:02.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc0222c	
Method	GET	
Attack		
Evidence	1747873779	
Other Info	1747873779, which evaluates to: 2025-05-22 05:29:39.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc0222c	
Method	GET	
Attack		
Evidence	1779033703	
Other Info	1779033703, which evaluates to: 2026-05-17 21:01:43.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc0222c	
Method	GET	
Attack		
Evidence	1899447441	
Other Info	1899447441, which evaluates to: 2030-03-11 13:17:21.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc0222c	
Method	GET	
Attack		
Evidence	1925078388	
Other Info	1925078388, which evaluates to: 2031-01-02 04:59:48.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc0222c	
Method	GET	
Attack		
Evidence	1955562222	
Other Info	1955562222, which evaluates to: 2031-12-21 00:43:42.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc0222c	
Method	GET	

Attack		
Evidence	1960686401	
Other Info	1960686401, which evaluates to: 2032-02-18 08:06:41.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc0222c	
Method	GET	
Attack		
Evidence	1986661051	
Other Info	1986661051, which evaluates to: 2032-12-14 23:17:31.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc0222c	
Method	GET	
Attack		
Evidence	1996064986	
Other Info	1996064986, which evaluates to: 2033-04-02 19:29:46.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc0222c	
Method	GET	
Attack		
Evidence	2024104815	
Other Info	2024104815, which evaluates to: 2034-02-21 08:20:15.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc02941	
Method	GET	
Attack		
Evidence	1508970993	
Other Info	1508970993, which evaluates to: 2017-10-26 03:36:33.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc02941	
Method	GET	
Attack		
Evidence	1537002063	
Other Info	1537002063, which evaluates to: 2018-09-15 14:01:03.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc02941	
Method	GET	
Attack		
Evidence	1541459225	
Other Info	1541459225, which evaluates to: 2018-11-06 04:07:05.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc02941	
Method	GET	
Attack		
Evidence	1555081692	

	Other Info	1555081692, which evaluates to: 2019-04-12 20:08:12.
URL		https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc02941
	Method	GET
	Attack	
	Evidence	1695183700
	Other Info	1695183700, which evaluates to: 2023-09-20 09:21:40.
URL		https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc02941
	Method	GET
	Attack	
	Evidence	1746735081
	Other Info	1746735081, which evaluates to: 2025-05-09 01:11:21.
URL		https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc02941
	Method	GET
	Attack	
	Evidence	1747873779
	Other Info	1747873779, which evaluates to: 2025-05-22 05:29:39.
URL		https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc02941
	Method	GET
	Attack	
	Evidence	1779033703
	Other Info	1779033703, which evaluates to: 2026-05-17 21:01:43.
URL		https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc02941
	Method	GET
	Attack	
	Evidence	1899447441
	Other Info	1899447441, which evaluates to: 2030-03-11 13:17:21.
URL		https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc02941
	Method	GET
	Attack	
	Evidence	1925078388
	Other Info	1925078388, which evaluates to: 2031-01-02 04:59:48.
URL		https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc02941
	Method	GET
	Attack	
	Evidence	1955562222
	Other Info	1955562222, which evaluates to: 2031-12-21 00:43:42.

	URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc02941
	Method	GET
	Attack	
	Evidence	1986661051
	Other Info	1986661051, which evaluates to: 2032-12-14 23:17:31.
	URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc02941
	Method	GET
	Attack	
	Evidence	1996064986
	Other Info	1996064986, which evaluates to: 2033-04-02 19:29:46.
	URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc02941
	Method	GET
	Attack	
	Evidence	2024104815
	Other Info	2024104815, which evaluates to: 2034-02-21 08:20:15.
	URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc032e9
	Method	GET
	Attack	
	Evidence	1508970993
	Other Info	1508970993, which evaluates to: 2017-10-26 03:36:33.
	URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc032e9
	Method	GET
	Attack	
	Evidence	1537002063
	Other Info	1537002063, which evaluates to: 2018-09-15 14:01:03.
	URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc032e9
	Method	GET
	Attack	
	Evidence	1541459225
	Other Info	1541459225, which evaluates to: 2018-11-06 04:07:05.
	URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc032e9
	Method	GET
	Attack	
	Evidence	1555081692
	Other Info	1555081692, which evaluates to: 2019-04-12 20:08:12.
	URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc032e9
	Method	GET

Attack		
Evidence	1695183700	
Other Info	1695183700, which evaluates to: 2023-09-20 09:21:40.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc032e9	
Method	GET	
Attack		
Evidence	1746738763	
Other Info	1746738763, which evaluates to: 2025-05-09 02:12:43.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc032e9	
Method	GET	
Attack		
Evidence	1747873779	
Other Info	1747873779, which evaluates to: 2025-05-22 05:29:39.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc032e9	
Method	GET	
Attack		
Evidence	1779033703	
Other Info	1779033703, which evaluates to: 2026-05-17 21:01:43.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc032e9	
Method	GET	
Attack		
Evidence	1899447441	
Other Info	1899447441, which evaluates to: 2030-03-11 13:17:21.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc032e9	
Method	GET	
Attack		
Evidence	1925078388	
Other Info	1925078388, which evaluates to: 2031-01-02 04:59:48.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc032e9	
Method	GET	
Attack		
Evidence	1955562222	
Other Info	1955562222, which evaluates to: 2031-12-21 00:43:42.	
URL	https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc032e9	
Method	GET	
Attack		

	Evidence	1986661051
	Other Info	1986661051, which evaluates to: 2032-12-14 23:17:31.
URL		https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc032e9
	Method	GET
	Attack	
	Evidence	1996064986
	Other Info	1996064986, which evaluates to: 2033-04-02 19:29:46.
URL		https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc032e9
	Method	GET
	Attack	
	Evidence	2024104815
	Other Info	2024104815, which evaluates to: 2034-02-21 08:20:15.
URL		https://www.gstatic.com/_/mss/boq-chrome-webstore/_/js/k=boq-chrome-webstore.ChromeWeb /ck=boq-chrome-webstore.ChromeWebStoreConsumerFeUi.IVmjoB1179s.L.B1.O/am=eFQADL discoverview/ed=1/wt=2/ujg=1/rs=AEP720KkMP-e4Q8FpcjA_Oklqo-Cw1JNJA/ee=EVNhjf:pw7(ZDZcre;LBgRLc:SdcwHb;Me32dd:MEeYgc;NJ1rfe:qTnoBf;NPKaK:SdcwHb;NSEoX:lazG7b;Pjp ScI3Yc:e7Hzgb;Uvc8o:VDovNc;YIZmRd:A1yn5d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfS lOO0Vd:OTA3Ae;oGtAuc:sOXFj;pXdRYb:MdUzUe;qafBPd:yDVVkb;qddgKe:xQtZb;wR5FRb:YA zxnPse:duFQFc/m=ws9Tlc,n73qwf,aW3pY,UUJqVe,IZT63,e5qFLc,O1Gjze,ebZ3mb,gIl2M,mI3L ZwDk9d,RyvaUb,YYmHzb,p8L0ob,MT4Hub,h4ilFc,erhsIc,ataMLc,NCodtd,O6y8ed,MpJwZc,PrF KUM7Z,qTnoBf,duFQFc,sI9bWe,lwddkf,gychg,w9hDv,RMhBfe,CfLNpd,SdcwHb,pw70Gc,mdR7 kjKdXe,JNoxi,BVgquf,QIhFr,YA1iG,V9amgb,hKSk3e,hc6Ubd,SpsfSb,Z5uLle,BBl74,MdUzUe,zb
	Method	GET
	Attack	
	Evidence	1518500249
	Other Info	1518500249, which evaluates to: 2018-02-13 10:37:29.
URL		https://www.gstatic.com/_/mss/boq-chrome-webstore/_/js/k=boq-chrome-webstore.ChromeWeb /ck=boq-chrome-webstore.ChromeWebStoreConsumerFeUi.IVmjoB1179s.L.B1.O/am=eFQADL discoverview/ed=1/wt=2/ujg=1/rs=AEP720KkMP-e4Q8FpcjA_Oklqo-Cw1JNJA/ee=EVNhjf:pw7(ZDZcre;LBgRLc:SdcwHb;Me32dd:MEeYgc;NJ1rfe:qTnoBf;NPKaK:SdcwHb;NSEoX:lazG7b;Pjp ScI3Yc:e7Hzgb;Uvc8o:VDovNc;YIZmRd:A1yn5d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfS lOO0Vd:OTA3Ae;oGtAuc:sOXFj;pXdRYb:MdUzUe;qafBPd:yDVVkb;qddgKe:xQtZb;wR5FRb:YA zxnPse:duFQFc/m=ws9Tlc,n73qwf,aW3pY,UUJqVe,IZT63,e5qFLc,O1Gjze,ebZ3mb,gIl2M,mI3L ZwDk9d,RyvaUb,YYmHzb,p8L0ob,MT4Hub,h4ilFc,erhsIc,ataMLc,NCodtd,O6y8ed,MpJwZc,PrF KUM7Z,qTnoBf,duFQFc,sI9bWe,lwddkf,gychg,w9hDv,RMhBfe,CfLNpd,SdcwHb,pw70Gc,mdR7 kjKdXe,JNoxi,BVgquf,QIhFr,YA1iG,V9amgb,hKSk3e,hc6Ubd,SpsfSb,Z5uLle,BBl74,MdUzUe,zb
	Method	GET
	Attack	
	Evidence	1732584193
	Other Info	1732584193, which evaluates to: 2024-11-26 06:23:13.
URL		https://www.gstatic.com/_/mss/boq-chrome-webstore/_/js/k=boq-chrome-webstore.ChromeWeb /ck=boq-chrome-webstore.ChromeWebStoreConsumerFeUi.IVmjoB1179s.L.B1.O/am=eFQADL discoverview/ed=1/wt=2/ujg=1/rs=AEP720KkMP-e4Q8FpcjA_Oklqo-Cw1JNJA/ee=EVNhjf:pw7(ZDZcre;LBgRLc:SdcwHb;Me32dd:MEeYgc;NJ1rfe:qTnoBf;NPKaK:SdcwHb;NSEoX:lazG7b;Pjp ScI3Yc:e7Hzgb;Uvc8o:VDovNc;YIZmRd:A1yn5d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfS lOO0Vd:OTA3Ae;oGtAuc:sOXFj;pXdRYb:MdUzUe;qafBPd:yDVVkb;qddgKe:xQtZb;wR5FRb:YA zxnPse:duFQFc/m=ws9Tlc,n73qwf,aW3pY,UUJqVe,IZT63,e5qFLc,O1Gjze,ebZ3mb,gIl2M,mI3L ZwDk9d,RyvaUb,YYmHzb,p8L0ob,MT4Hub,h4ilFc,erhsIc,ataMLc,NCodtd,O6y8ed,MpJwZc,PrF

	KUM7Z,qTnoBf,duFQFc,sI9bWe,lwddkf,gychg,w9hDv,RMhBfe,CfLNpd,SdcwHb,pw70Gc,mdR7 kjKdXe,JNoxi,BVgquf,QIhFr,YA1iG,V9amgb,hKSk3e,hc6Ubd,SpsfSb,Z5uLle,BBl74,MdUzUe,zb
Method	GET
Attack	
Evidence	1859775393
Other Info	1859775393, which evaluates to: 2028-12-07 09:16:33.
URL	https://www.gstatic.com/og/_/js/k=og.qtm.en_US.jS_CZIDYjaI.2019.O/rt=j/m=q_dnp,qmd,qcwid, qalo,qebr,qein,qhaw,qhawgm3,qhba,qhbr,qhbrgm3,qhch,qhchgm3,qhga,qhid,qhidgm3,qhin,qhl /rs=AA2YrTsB9Qz4OH5RFhAQLL8W1kIQz_J3Rg
Method	GET
Attack	
Evidence	1518500249
Other Info	1518500249, which evaluates to: 2018-02-13 10:37:29.
URL	https://www.gstatic.com/og/_/js/k=og.qtm.en_US.jS_CZIDYjaI.2019.O/rt=j/m=q_dnp,qmd,qcwid, qalo,qebr,qein,qhaw,qhawgm3,qhba,qhbr,qhbrgm3,qhch,qhchgm3,qhga,qhid,qhidgm3,qhin,qhl /rs=AA2YrTsB9Qz4OH5RFhAQLL8W1kIQz_J3Rg
Method	GET
Attack	
Evidence	1732584193
Other Info	1732584193, which evaluates to: 2024-11-26 06:23:13.
URL	https://www.gstatic.com/og/_/js/k=og.qtm.en_US.jS_CZIDYjaI.2019.O/rt=j/m=q_dnp,qmd,qcwid, qalo,qebr,qein,qhaw,qhawgm3,qhba,qhbr,qhbrgm3,qhch,qhchgm3,qhga,qhid,qhidgm3,qhin,qhl /rs=AA2YrTsB9Qz4OH5RFhAQLL8W1kIQz_J3Rg
Method	GET
Attack	
Evidence	1859775393
Other Info	1859775393, which evaluates to: 2028-12-07 09:16:33.
URL	https://www.gstatic.com/og/_/js/k=og.qtm.en_US.jS_CZIDYjaI.2019.O/rt=j/m=qabr,q_dnp,qcwid, qhba,qhbr,qhch,qhga,qhid,qhin/d=1/ed=1/rs=AA2YrTsB9Qz4OH5RFhAQLL8W1kIQz_J3Rg
Method	GET
Attack	
Evidence	1518500249
Other Info	1518500249, which evaluates to: 2018-02-13 10:37:29.
URL	https://www.gstatic.com/og/_/js/k=og.qtm.en_US.jS_CZIDYjaI.2019.O/rt=j/m=qabr,q_dnp,qcwid, qhba,qhbr,qhch,qhga,qhid,qhin/d=1/ed=1/rs=AA2YrTsB9Qz4OH5RFhAQLL8W1kIQz_J3Rg
Method	GET
Attack	
Evidence	1732584193
Other Info	1732584193, which evaluates to: 2024-11-26 06:23:13.
URL	https://www.gstatic.com/og/_/js/k=og.qtm.en_US.jS_CZIDYjaI.2019.O/rt=j/m=qabr,q_dnp,qcwid, qhba,qhbr,qhch,qhga,qhid,qhin/d=1/ed=1/rs=AA2YrTsB9Qz4OH5RFhAQLL8W1kIQz_J3Rg
Method	GET

	Attack	
	Evidence	1859775393
	Other Info	1859775393, which evaluates to: 2028-12-07 09:16:33.
URL		https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js
	Method	GET
	Attack	
	Evidence	1508970993
	Other Info	1508970993, which evaluates to: 2017-10-26 03:36:33.
URL		https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js
	Method	GET
	Attack	
	Evidence	1518500249
	Other Info	1518500249, which evaluates to: 2018-02-13 10:37:29.
URL		https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js
	Method	GET
	Attack	
	Evidence	1537002063
	Other Info	1537002063, which evaluates to: 2018-09-15 14:01:03.
URL		https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js
	Method	GET
	Attack	
	Evidence	1541459225
	Other Info	1541459225, which evaluates to: 2018-11-06 04:07:05.
URL		https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js
	Method	GET
	Attack	
	Evidence	1555081692
	Other Info	1555081692, which evaluates to: 2019-04-12 20:08:12.
URL		https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js
	Method	GET
	Attack	
	Evidence	1695183700
	Other Info	1695183700, which evaluates to: 2023-09-20 09:21:40.
URL		https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js
	Method	GET
	Attack	
	Evidence	1732584193

Other Info	1732584193, which evaluates to: 2024-11-26 06:23:13.	
URL	https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js	
Method	GET	
Attack		
Evidence	1747873779	
Other Info	1747873779, which evaluates to: 2025-05-22 05:29:39.	
URL	https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js	
Method	GET	
Attack		
Evidence	1779033703	
Other Info	1779033703, which evaluates to: 2026-05-17 21:01:43.	
URL	https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js	
Method	GET	
Attack		
Evidence	1859775393	
Other Info	1859775393, which evaluates to: 2028-12-07 09:16:33.	
URL	https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js	
Method	GET	
Attack		
Evidence	1899447441	
Other Info	1899447441, which evaluates to: 2030-03-11 13:17:21.	
URL	https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js	
Method	GET	
Attack		
Evidence	1925078388	
Other Info	1925078388, which evaluates to: 2031-01-02 04:59:48.	
URL	https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js	
Method	GET	
Attack		
Evidence	1955562222	
Other Info	1955562222, which evaluates to: 2031-12-21 00:43:42.	
URL	https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js	
Method	GET	
Attack		
Evidence	1981196515	
Other Info	1981196515, which evaluates to: 2032-10-12 17:21:55.	

URL	https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js
Method	GET
Attack	
Evidence	1986661051
Other Info	1986661051, which evaluates to: 2032-12-14 23:17:31.
URL	https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js
Method	GET
Attack	
Evidence	1996064986
Other Info	1996064986, which evaluates to: 2033-04-02 19:29:46.
URL	https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js
Method	GET
Attack	
Evidence	2024104815
Other Info	2024104815, which evaluates to: 2034-02-21 08:20:15.
URL	https://optimizationguide-pa.googleapis.com/v1:GetModels?key=AIzaSyBqJZh-7pA44blAaAkH6
Method	POST
Attack	
Evidence	1673999601
Other Info	1673999601, which evaluates to: 2023-01-18 04:53:21.
URL	https://optimizationguide-pa.googleapis.com/v1:GetModels?key=AIzaSyBqJZh-7pA44blAaAkH6
Method	POST
Attack	
Evidence	1679317318
Other Info	1679317318, which evaluates to: 2023-03-20 18:01:58.
URL	https://optimizationguide-pa.googleapis.com/v1:GetModels?key=AIzaSyBqJZh-7pA44blAaAkH6
Method	POST
Attack	
Evidence	1696267841
Other Info	1696267841, which evaluates to: 2023-10-02 22:30:41.
URL	https://optimizationguide-pa.googleapis.com/v1:GetModels?key=AIzaSyBqJZh-7pA44blAaAkH6
Method	POST
Attack	
Evidence	1728324084
Other Info	1728324084, which evaluates to: 2024-10-07 23:01:24.
URL	https://optimizationguide-pa.googleapis.com/v1:GetModels?key=AIzaSyBqJZh-7pA44blAaAkH6

Method	POST	
Attack		
Evidence	1744643027	
Other Info	1744643027, which evaluates to: 2025-04-14 20:03:47.	
URL	https://optimizationguide-pa.googleapis.com/v1:GetModels?key=AIzaSyBqJZh-7pA44blAaAkH6	
Method	POST	
Attack		
Evidence	1744643050	
Other Info	1744643050, which evaluates to: 2025-04-14 20:04:10.	
URL	https://optimizationguide-pa.googleapis.com/v1:GetModels?key=AIzaSyBqJZh-7pA44blAaAkH6	
Method	POST	
Attack		
Evidence	1744729555	
Other Info	1744729555, which evaluates to: 2025-04-15 20:05:55.	
URL	https://update.googleapis.com/service/update2/json?cup2key=15: L3EYilNTE1rHeFFg6qYdPP0kFnFgf0wKFsDwgTGHerE&cup2hreq=a7b4bba51a2cf88b3a1456	
Method	POST	
Attack		
Evidence	1744928549	
Other Info	1744928549, which evaluates to: 2025-04-18 03:22:29.	
Instances	241	
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregat	
Reference	https://cwe.mitre.org/data/definitions/200.html	
CWE Id	497	
WASC Id	13	
Plugin Id	10096	

Low	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows olde Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the re interpreted and displayed as a content type other than the declared content type. Current (early versions of Firefox will use the declared content type (if one is set), rather than performing MIME
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1? ray=93cbfe660a72fd41&lang=auto
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1? ray=93cc00347a584b92&lang=auto
Method	GET

	Attack	
	Evidence	
	Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.
	URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93cc022b2833fd41&lang=auto
	Method	GET
	Attack	
	Evidence	
	Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.
	URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93cc02a2483e4b92&lang=auto
	Method	GET
	Attack	
	Evidence	
	Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.
	URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93cc033b099afd41&lang=auto
	Method	GET
	Attack	
	Evidence	
	Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.
	URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/7sbwg/0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
	Method	GET
	Attack	
	Evidence	
	Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.
	URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/iu289/0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
	Method	GET
	Attack	
	Evidence	
	Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.
	URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/ixl4x/0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
	Method	GET
	Attack	

Evidence		
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/o8ic5 /0x4AAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/	
Method	GET	
Attack		
Evidence		
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/u2hhw /0x4AAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/	
Method	GET	
Attack		
Evidence		
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.	
URL	https://challenges.cloudflare.com/turnstile/v0/b/701fd2559006/api.js?onload=OUxOl5&render=e	
Method	GET	
Attack		
Evidence		
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.	
URL	https://optimizationguide-pa.googleapis.com/downloads? name=1673999601&target=OPTIMIZATION_TARGET_PAGE_VISIBILITY	
Method	GET	
Attack		
Evidence		
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.	
URL	https://optimizationguide-pa.googleapis.com/downloads? name=1679317318&target=OPTIMIZATION_TARGET_LANGUAGE_DETECTION	
Method	GET	
Attack		
Evidence		
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.	
URL	https://optimizationguide-pa.googleapis.com/downloads? name=1696267841&target=OPTIMIZATION_TARGET_OMNIBOX_URL_SCORING	
Method	GET	
Attack		
Evidence		
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe	

Other Info	issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1728324084&target=OPTIMIZATION_TARGET_OMNIBOX_ON_DEVICE_TAIL_SUGGI	
Method	GET	
Attack		
Evidence		
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1744643027&target=OPTIMIZATION_TARGET_GEOLOCATION_PERMISSION_PRED	
Method	GET	
Attack		
Evidence		
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1744643050&target=OPTIMIZATION_TARGET_NOTIFICATION_PERMISSION_PREDI	
Method	GET	
Attack		
Evidence		
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1744729555&target=OPTIMIZATION_TARGET_CLIENT_SIDE_PHISHING	
Method	GET	
Attack		
Evidence		
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=240731042075&target=OPTIMIZATION_TARGET_SEGMENTATION_COMPOSE_PRO	
Method	GET	
Attack		
Evidence		
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=5&target=OPTIMIZATION_TARGET_PAGE_TOPICS_V2	
Method	GET	
Attack		
Evidence		
Other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co	

Info	threshold this scan rule will not alert on client or server error responses.
URL	https://static.cloudflareinsights.com/beacon.min.js/vcd15cbe7772f49c399c6a5babf22c1241717(
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.
URL	https://www.google.com/search?q=canva.com&oq=canva. com&gs_lcrp=EgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE&sou 8
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/flow/ov1/1388196947:1746735 yqCLWYtveBHybMLA-jPKMF2TPxac8KSy1xtButNu5s/93cbfe660a72fd41/O34_hNn2qXejUd.Kc cK21v9e40a9X57HLRvXQI-1746739149-1.2.1.1-vAzecFFGR.iCAbIlfQ.0SsRo9muUQaIH55. EBFi8S3NEuRMzvl_xzOIaBfyEaLU5
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/flow/ov1/240796764:17467350 Wa28az9wo4YlkN6TCVDjdGu_vfFeOOoXi5g4c/93cc00347a584b92/ZkreTcQ4xd6T4VePf9vr2r ep56IPvHwaaO0A-1746739223-1.2.1.1-AQ.whSBgj_5DFZ9Pe.11EOgH7d7N. hTfu0PD_0K9hj6_OGPerxppP86a6zKRxybQ
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/flow/ov1/511391438:17467351 1M74wKbCNT8GikpaeUAjS1ErZFS3B9_61rraghRsbHw/93cc02a2483e4b92/JVSGtt6yLfW6r2d EZXG4flG8v0kWkTkQ-1746739323-1.2.1.1- IXYYKSTaWcftYk1o02Nu8BROfeXTgidd3Z2PFkvKAMJ2A0k390ihVI7I_N1gdIp_
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/flow/ov1/573113744:17467388 9PHjCRGlImUmAAz2a3RJK6YpnBiLTNzvlM5PXX_c/93cc033b099afd41/ZDJyYttfPtX0UY. d_gNGBzvj8loh8VCvh_MEQznXWFw-1746739347-1.2.1.1- s_d2WBJniKIqJLKvK0Tr7y341M4RhZdAIezfanZVk0cXk5aalZZ11.Uw7CwVuQfM

Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/flow/ov1/896151768:17467388 97cmr9eaID72RJyTn_AWe8UdmrwiejaAcADzdMVt7VA/93cc022b2833fd41 /NRXphi_JjY2VguRoeNqUmwDZzcARbT7_zh2zekCVgBg-1746739304-1.2.1.1- mK5y4uzXjblALRfUpIWmoXX2BNHfA3Xq.9w1so8nbp4Rolc2RSfYjHmvlA36H_yU
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.
URL	https://play.google.com/log?format=json&hasfast=true
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.
URL	https://play.google.com/log?hasfast=true&authuser=0&format=json
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe issues, in which case there is still concern for browsers sniffing pages away from their actual co threshold this scan rule will not alert on client or server error responses.
Instances	29
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it s Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that MIME-sniffing at all, or that can be directed by the web application/web server to not perform MI
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/com (v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	CSP: Header & Meta
Description	The message contained both CSP specified via header and via Meta tag. It was not possible to union these policies in order to perform an analysis. Therefore, they have been evaluated individually.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv /7sbwg/0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET

Attack	
Evidence	
Other Info	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/iu289/0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/ixl4x/0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/o8ic5/0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/u2hhw/0x4AAAAAAADnPIDROrmt1Wwj/dark/fbE/new/normal/auto/
Method	GET
Attack	
Evidence	
Other Info	
Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Informational	Content Security Policy (CSP) Report-Only Header Found
	The response contained a Content-Security-Policy-Report-Only header, this may indicate a work-in-progress implementation, or an oversight in promoting pre-Prod to Prod, etc.

Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://chromewebstore.google.com/
Method	GET
Attack	
Evidence	
Other Info	
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP2/ https://w3c.github.io/webappsec-csp/ https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Informational	Information Disclosure - Information in Browser sessionStorage
Description	Information was stored in browser sessionStorage. This is not unusual or necessarily unsafe - this informational alert has been raised to help you get a better understanding of what this app is doing. For more details see the Client tabs - this information was set directly in the browser and will therefore not necessarily appear in this form in any HTTP(S) messages.
URL	https://www.google.com/sorry/index?continue=https://www.google.com/search%3Fq%3Dcanva.com%26oq%3Dcanva.com%26gs_lcrp%3DEgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE%26sourceid%3Dchrome%26ie%3DUTF-8%26sei%3DxB8daOXfHK-R4-EPzemMwAE&q=EgS2sN70GMi_9MAGIjAaBowNa3-eeVgj-e2FOxtvdzFSUA-SHTcJ5-a3xXNnKk6SJFPWzEcBx8ukuf03gHkyAnJSWgFD
Method	GET
Attack	
Evidence	
Other Info	The following data (key=value) was set: _c;;i=p:*|l:9007199254740991_1 Note that this alert will only be raised once for each URL + key.
URL	https://www.google.com/sorry/index?continue=https://www.google.com/search%3Fq%3Dcanva.com%26oq%3Dcanva.com%26gs_lcrp%3DEgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE%26sourceid%3Dchrome%26ie%3DUTF-8%26sei%3DxB8daOXfHK-R4-EPzemMwAE&q=EgS2sN70GMi_9MAGIjAaBowNa3-eeVgj-e2FOxtvdzFSUA-SHTcJ5-a3xXNnKk6SJFPWzEcBx8ukuf03gHkyAnJSWgFD
Method	GET
Attack	
Evidence	
Other Info	The following data (key=value) was set: sg_pns;;xB8daOXfHK-R4-EPzemMwAE=p:m|l:0_" 1746739139366" Note that this alert will only be raised once for each URL + key.

Instances	2
Solution	This is an informational alert and no action is necessary.
Reference	
CWE Id	359
WASC Id	13
Plugin Id	120000

Informational	Information Disclosure - Sensitive Information in URL
Description	The request appeared to contain sensitive information leaked in the URL. This can violate PCI and most organizational compliance policies. You can configure the list of strings for this check to add or remove values specific to your environment.
URL	https://play.google.com/log?hasfast=true&authuser=0&format=json
Method	POST
Attack	
Evidence	authuser
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: user authuser
Instances	1
Solution	Do not pass sensitive information in URIs.
Reference	
CWE Id	598
WASC Id	13
Plugin Id	10024

Informational	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93cbfe660a72fd41&lang=auto
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//,h[hQ(222)](e instanceof Error)||!d[hQ(1172)]||g[hQ(301)](typeof d[hQ(1172)],hQ(1444))){if(g[hQ(301)](h", see suspicious comment/snippet.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93cc00347a584b92&lang=auto
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//,x[hu(464)](j) (415)](l,m)||!n[hu(1284)]||typeof o[hu(1284)]!==g[hu(548)])return![];x[hu(464)](s[hu(128", see evi suspicious comment/snippet.
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93cc02a2483e4b92&lang=auto
Method	GET
Attack	
Evidence	from

Other Info		The following pattern was used: \bFROM\b and was detected in likely comment: "//www.cloudfla utm_source=challenge&utm_campaign=~CzENa~chlApiOrigin~JPdLg~fLdNy~AiQkg~ZJzBm~z terms~turnsti", see evidence field for the suspicious comment/snippet.
URL		https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_api/v1?ray=93cc033b099afd41&lang=auto
Method		GET
Attack		
Evidence		from
Other Info		The following pattern was used: \bFROM\b and was detected in likely comment: "//,h[hy(1038)]((1393)](d,Error)||!d[hy(688)]||typeof d[hy(688)]!==hy(1147))return g[hy(755)](g[hy(939)]", see evid suspicious comment/snippet.
URL		https://challenges.cloudflare.com/turnstile/v0/b/701fd2559006/api.js?onload=OUxOl5&render=e
Method		GET
Attack		
Evidence		from
Other Info		The following pattern was used: \bFROM\b and was detected in likely comment: "//challenges.cl a=(o=e["base-url"])!==null&&o!==void 0?o:a}return a}function Rt(e,t,a,o,c,l,v,h){var s=", see evid suspicious comment/snippet.
URL		https://chromewebstore.google.com/
Method		GET
Attack		
Evidence		user
Other Info		The following pattern was used: \bUSER\b and was detected in likely comment: "//lh3.googleuse /z2F4pXDs72oDlRtp27y1F_AE1npf025cRzSSsGFnTI49Ll4gHmmaHrVPaOomCCSjfTdIYG5sM Ultima", see evidence field for the suspicious comment/snippet.
URL		https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc00257
Method		GET
Attack		
Evidence		from
Other Info		The following pattern was used: \bFROM\b and was detected in likely comment: "//,h[ig(1072)](e (620)))k[ig(691)][ig(694)][ig(780)](l,m)||(n[o]=[]),s[v][ig(981)](x);else return!![]}", see evidence field comment/snippet.
URL		https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc0222c
Method		GET
Attack		
Evidence		from
Other Info		The following pattern was used: \bFROM\b and was detected in likely comment: "//,h[hG(1044)] instanceof Error)||!d[hG(1212)]||typeof d[hG(1212)]!==g[hG(931)])return hG(1276)===hG(13", se suspicious comment/snippet.
URL		https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc02941
Method		GET
Attack		
Evidence		from
Other Info		The following pattern was used: \bFROM\b and was detected in likely comment: "//,h[gP(1132)](instanceof Error)||!d[gP(1295)]||typeof d[gP(1295)]!==g[gP(1370)]){if(g[gP(536)](gP(1085", see e suspicious comment/snippet.
URL		https://www.canva.com/cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cc032e9

Method	GET	
Attack		
Evidence	from	
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//,h[hl(732)](e) instanceof Error)||!d[hl(1012)]||g[hl(1408)](typeof d[hl(1012)],hl(1225)))return![];h[hl(", see evider suspicious comment/snippet.	
URL	https://www.google.com/search?q=canva.com&oq=canva.com&gs_lcrp=EgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE&sou	
Method	GET	
Attack		
Evidence	SELECT	
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "//g,"_").repla (K==66)K=typeof b!=="function"?98:95;else if(K==69)K=f<N.length?81:36;else if(K==7)K=12;el" the suspicious comment/snippet.	
URL	https://www.google.com/shared_dict/srp/9b2f0e32aa58bed3086962cef882a7badfe7e540019b4 dict	
Method	GET	
Attack		
Evidence	db	
Other Info	The following pattern was used: \bDB\b and was detected in likely comment: "//www.gstatic.com en_US.F5FYpWR84r8.2019.O/rt=j/m=_ac,_awd,ada,lldp,qads/exm=/d=1/ed=1/rs=AA2YrTtT5jd evidence field for the suspicious comment/snippet.	
URL	https://www.gstatic.com/_/mss/boq-chrome-webstore/_/js/k=boq-chrome-webstore.ChromeWeb en_US.GZv8TRD6ktk.es5.O/ck=boq-chrome-webstore.ChromeWebStoreConsumerFeUi.IVmjoF /am=eFQADLgFAAE/d=1/exm=_b,_tp/excm=_b,_tp.discoverview/ed=1/wt=2/ujg=1/rs=AEP720F e4Q8FpcjA_OkIqo-Cw1JNJA/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;JsbNhc:Xd8iUd;K5nYTd:ZDZc Me32dd:MEeYgc;NJ1rfe:qTnoBf;NPKaK:SdcwHb;NSEoX:IazG7b;Pjplud:EEDORb;QGR0gd:MIF ScI3Yc:e7Hzgb;Uvc8o:VDovNc;YlZmRd:A1yn5d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfS eBAeSb:zbML3c;iFQyKf:QIhFr;lOO0Vd:OTA3Ae;oGtAuc:sOXFj;pXdRYb:MdUzUe;qafBPd:yDV wR5FRb:YA1iG;xqZiqf:BBI74;yEQyxe:p8L0ob;yxTchf:KUM7Z;zxnPse:duFQFc/m=ws9Tlc,n73qf IZT63,e5qFLc,O1Gjze,ebZ3mb,gll2M,mI3LFb,byfTOb,lsjVmc,xUdipf,ZDZcre,OTA3Ae,ZwDk9d,f p8L0ob,MT4Hub,h4iIFc,erhsIc,ataMLc,NCodtd,O6y8ed,MpJwZc,PrPYRd,lazG7b,LEikZe,NwH0 KUM7Z,qTnoBf,duFQFc,sI9bWe,lwddkf,gychg,w9hDv,RMhBfe,CfLNpd,SdcwHb,pw70Gc,mdR7 A7fCU,xQtZb,FdMhB,MI6k7c,kjKdXe,JNoxi,BVgquf,QIhFr,YA1iG,V9amgb,hKSk3e,hc6Ubd,Sps MdUzUe,zbML3c,zr1jrb,QvLWAb,Uas9Hd,pjICDe	
Method	GET	
Attack		
Evidence	Db	
Other Info	The following pattern was used: \bDB\b and was detected in likely comment: "//www.google.con iv(c)}this.qa=c};_.k=jv.prototype;_.k.GC=1E4;_.k.Zn=!1;_.k.Fx=0;_.k.ft=null;_.k.HA=null", see ev suspicious comment/snippet.	
URL	https://www.gstatic.com/og/_/js/k=og.qtm.en_US.jS_CZIDYjaI.2019.O/rt=j/m=q_dnp,qmd,qcwid, /exm=qaaw,qabr,qadd,qaid,qalo,qebr,qein,qhaw,qhawgm3,qhba,qhbr,qhbrgm3,qhch,qhchgm3, qhlo,qhlogm3,qhmn,qhpc,qhsf,qhsfgm3,qhtt/d=1/ed=1/rs=AA2YrTsB9Qz4OH5RFhAQLL8W1kl	
Method	GET	
Attack		
Evidence	username	
Other Info	The following pattern was used: \bUSERNAME\b and was detected in likely comment: "//");e=b. password;c=c+(e&&d?e+":"+d+"@":e?e+"@":d?":"+d+"@":"")+(b.hostname||"");b.port&&(c+=":"+ see evidence field for the suspicious comment/snippet.	
URL	https://www.gstatic.com/og/_/js/k=og.qtm.en_US.jS_CZIDYjaI.2019.O/rt=j/m=qabr,q_dnp,qcwid /exm=qaaw,qadd,qaid,qein,qhaw,qhba,qhbr,qhch,qhga,qhid,qhin/d=1/ed=1 /rs=AA2YrTsB9Qz4OH5RFhAQLL8W1klQz_J3Rg	

Method	GET	
Attack		
Evidence	username	
Other Info	The following pattern was used: \bUSERNAME\b and was detected in likely comment: "//");e=b. password;c=c+(e&&d?e+":"+d+"@":e?e+"@":d?":"+d+"@":"")+(b.hostname||"");b.port&&(c+=":"+ see evidence field for the suspicious comment/snippet.	
URL	https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js	
Method	GET	
Attack		
Evidence	query	
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//cloud.googl /troubleshoot-recaptcha-issues#automated-query-error" target="_blank">our help page.</di for the suspicious comment/snippet.	
Instances	16	
Solution	Remove all comments that return information that may help an attacker and fix any underlying p	
Reference		
CWE Id	615	
WASC Id	13	
Plugin Id	10027	

Informational	Loosely Scoped Cookie	
Description	Cookies can be scoped by domain or path. This check is only concerned with domain scope.The scoped strictly to a subdomain e.g. www.nottrusted.com, or loosely scoped to a parent domain e scoped cookies are common in mega-applications like google.com and live.com. Cookies set fr scoped to a parent-level domain may be transmitted to the parent, or any subdomain of the pare	
URL	https://www.canva.com/	
Method	GET	
Attack		
Evidence		
Other Info	The origin domain used for comparison was: www.canva.com __cf_bm=8YDvy0pdPnlWoGeyG O3APTjHScD4AjYHwd_LrjYuzSEJCROa2pFT1NTcvWuNN2YGGHIX8f1FBOpj3B7cMAO.3stV3	
URL	https://www.google.com/search?q=canva.com&oq=canva.com&gs_lcrp=EgZjaHJvbWUyBggAE	
Method	GET	
Attack		
Evidence		
Other Info	The origin domain used for comparison was: www.google.com AEC=AVcja2e-gC8vv4GhzO64E _sFYai89oXmp5OD8Fc9wFmQhQfWKE3Z8Jg8gHtApG8n11VDGSc-a2rAdJ7nXIj_3rOs6EGSP oOw_DCD3L9gKz-z_Llg_Wo6YU1izg	
URL	https://www.google.com/search?q=canva.com&oq=canva.com&gs_lcrp=EgZjaHJvbWUyBggAE EPzemMwAE	
Method	GET	
Attack		
Evidence		
Other Info	The origin domain used for comparison was: www.google.com NID=523=Wln5_eS11oqdlly8n6C 96mNn1cLfzKF73myZEKM4n2pRfvyDcszLptO9A5o7O0KEJkc8MOond_f3xY0izfQAecCUEz- 3aVGwRhzJRzx1nqwY0wfvsvGl6UMGuHX7fHpJGhD5pHPNM66JTrYh42zkVHPWvXdVBVwos	
URL	https://play.google.com/log?format=json&hasfast=true	

Method	POST	
Attack		
Evidence		
Other Info	The origin domain used for comparison was: play.google.com NID=524=a47diNNjOx4JDgYKI_b oi1p9STqqWP4l3KHQG16cciSsLoyPXrGquRhkLKKL7ULIVsv7ZXqp0d7eylyPDJ4TX5-YJZtFqc	
URL	https://play.google.com/log?format=json&hasfast=true	
Method	POST	
Attack		
Evidence		
Other Info	The origin domain used for comparison was: play.google.com NID=524=AUyKDc7nO9DxVjlRRrs5igNjWR58Fgx8hARhoxgJwkfaSfaXRGvfntvfx6hxBKimeLbo fZolbv7rXY3tSkVY7tmV6c4Nc_c_9n2A9bdubg	
Instances	5	
Solution	Always scope cookies to a FQDN (Fully Qualified Domain Name).	
Reference	https://tools.ietf.org/html/rfc6265#section-4.1 https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Tes https://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies	
CWE Id	565	
WASC Id	15	
Plugin Id	90033	

Informational	Modern Web Application	
Description	The application appears to be a modern web application. If you need to explore it automatically	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/7sbwg/0	
Method	GET	
Attack		
Evidence	<script nonce="KqXPejJer189nz9s"> (function(){ window._cf_chl_opt={ cvId: '3', cZone: 'challen chlApiTimeoutEncountered: 0, chlApiOverrunBudgetMs:30000, chlTimeoutMs:120000,hjlH5: 'uE IXYYKSTaWcftYk1o02Nu8BROfeXTgidd3Z2PFkvKAMJ2A0k390ihVI7I_N1gdIp_', cFPWv: 'b', c l2cXCkvn4TmC7yWKh8NlMWG40VSOua7A8sRbKL6XUtAGbw5cxWXHmkDYew1CHzmf2dYW ejTVNPSnsVMKIoygzjBrYnk_hTfvIBcAcgyyfZxBwvoNZyj11MqCOiVe7GCWuD8912sEj.SjzGy2 CqxEgFwPg9oNJ63_qKPH2ZzB8BaZni1mostkU1shu0LoR8I7p3T13FP5v9dcAqbWBNjI6zJOqr 3NsprjYM56Su19MypPWn1xBit6N4ICKFwyaXsSBCw4RAs1CsBp9tg__qd80mHIEALGsLz7pY_ XbqTEj08uMM8vQWmfDOLJE451QLtQvedglwSoAw1L5tnt2I4O7sBL5OTSjrJ8YnF8NeLl3RpO DcgzHSg5YPptC_1WCKLic7596BVZyele4g4E239qVwvNMYKbu_okduLmdjE93wFkGhmnb5CE source: 'cloudflare-challenge', widgetId: '7sbwg', nextRcV: 'a56YdrgHMhg8avw24jaGzCL6gb0S postMessage({ source: 'cloudflare-challenge', widgetId: window._cf_chl_opt.chlApiWidgetId, eve	
Other Info	No links have been found while there are scripts, which is an indication that this is a modern we	
URL	https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/iu289/0x	
Method	GET	
Attack		
Evidence	<script nonce="UWDhdRC48bH6c094"> (function(){ window._cf_chl_opt={ cvId: '3', cZone: 'cha chlApiTimeoutEncountered: 0, chlApiOverrunBudgetMs:30000, chlTimeoutMs:120000,hjlH5: 'uz whSBgj_5DFZ9Pe.11EOgH7d7N.hTfu0PD_0K9hj6_OGPerxppP86a6zKRxybQ', cFPWv: 'b', cLt Ns9SQxI0OiqEuQMNGeJH2cfTiM403wW08rQwCnBRvzoghe5xFuJUVNZv6YfJ9BPnp5ULYvg8 CKO1YiXhZt3uxWMljN6mJgzxcB4h036W6YAY07gU6VjZaMbUTahcXigVnE0WFQbNy9qje0eS 2ybpS0IDuyZqx6mcqyF2shYvzDWauybndTfrdbTHM1tALrPD1GkdMGoIKuwoX469wot9QMc9c: jKnbfSOeeQiIEli5lO5wPjVoxmI9K0M2gYxiN0iZ2fwNToxn1or_029pOd3HPiW4743Sf3f2jou4Z2k rEVaxnJT0JMks7wuxlkojwOl9nnkTvlqse.SWHAVupQeOv1sxsJv62RGPxGv1ULCt6KSMwfhAB 10H_FWAvhNKKdbgYQmEMHDeR53kZJJeRXJYeCvvShhCLL0gmoMM9qze7JHsygehGLrQ2 cAZzPVolEffII8REhWp3qepSdfxgkNhxlxr8lDSigIB6VXSKr.LiK8p8ulln4607yu882QtE.kHnlwCF6 trigger: refreshTrigger, source: 'cloudflare-challenge', widgetId: 'iu289', nextRcV: 'dylu0.2Zm7iIN	

		window.parent.postMessage({ source: 'cloudflare-challenge', widgetId: window._cf_chl_opt.chlA /script>
	Other Info	No links have been found while there are scripts, which is an indication that this is a modern we
URL		https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/ixl4x/0x4
	Method	GET
	Attack	
	Evidence	<script nonce="xtUXrNYr2ZQmNM0g"> (function(){ window._cf_chl_opt={ cvId: '3', cZone: 'chall chlApiTimeoutEncountered: 0, chlApiOverrunBudgetMs:30000, chlTimeoutMs:120000,hjlH5: 'v4 mK5y4uzXjblALRfUpIWmoXX2BNHfA3Xq.9w1so8nbp4Rolc2RSfYjHmvlA36H_yU', cFPWv: 'b', Q2Nl3Bv3NgX4F6RB1nhAVG6is1LjAUfpmIPXsiujSdkTxB9WOXOfVeeZSlOvkIRhOa2dwvk_Vp 4IvSOuTyi8L6RfnkrxRhOCMwebwh9frZjRcqwsGv6h_FSR3gcn_A65iYW_kugJjP8GfeMEJrKGL Ysp1aSnn4IcpQFJcXeMaklV8Wf5zLwKbb1NZG7MXkuIEDDh9ejJtAv7WZj7EOUGOkgg6t7Y6K C8i_7Darwm8qNk_mqm0lMq2Koyg44a6KHezexd_Z4KjFrU4Af1TUP5dyo6I5dkncOHHSdkZC7J IFq8_wOHv9qw9WkoLAVy_w6EdepZz67fiH79unBcVzuNt4RdYW_PBKIEgUyBkEWUtl9_9EsM Hj7Vz8NvsOT6j17KRl5b_lDsKTfvtCGl3smN86hoghzsfS1ismApzxosiVcxnXvGNUB964Pxi48F_ 9a71LibRHO9BLua52ske9Q7NLBgjZUZK0v8eHGM_KW2ARrODw4Isvm84b4cs5TlA92euUfWr 'bZzZ_dAym2Wtsmymq9Zn1JWlLzMTDoyK7oT1I5pbFwg-1746739304-1.3.1.1-Vq5xG7Rdu32J _cf_chl_opt.chlApiWidgetId, event: 'food', seq: e.seq, }, '*'); } } window.addEventListener('messa
	Other Info	No links have been found while there are scripts, which is an indication that this is a modern we
URL		https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/o8ic5/0x
	Method	GET
	Attack	
	Evidence	<script nonce="U7QbVnQRiLJw0j9C"> (function(){ window._cf_chl_opt={ cvId: '3', cZone: 'chall chlApiTimeoutEncountered: 0, chlApiOverrunBudgetMs:30000, chlTimeoutMs:120000,hjlH5: 'oh iCAbIlfQ.0SsRo9muUQaIH55.EBFi8S3NEuRMzvl_xzOlaBfyEaLU5', cFPWv: 'b', cLt: 'n', chlApiF e_PD3DTl_PhFhZz2OpRex_BQ1JhkjPo3LjY4CAsrrv6txjpEZAaZO3soZ9t3vwBslsTHwxrrhn10v 1_DjgcmDhm_pyNEMhHnlsH3UweGMyaee255uewdSzdHvWsCTehVwrKtGiVtLErRfNXZgg0Fk 83_ivOSMp4tbzHscfNPMHpvtuZKgzBZFgAUvstikW7Ye2B6c3vMVWemzjCECJ7_v8ywR3iqQu ZlDD2OBJvgybjkNXMIixRj90hG2KNb48gBZfPh4QAPprOkZwXrGPkb0ia5vlupDQRFy2B78m21 b5g2TF7AX6xxjm8G17XWPKiuksD0M5Rdb0joOSs_FknsMY0QSiZn68w3b8W5Cm2eIYMtSHJ rKGTsnED9cDdqNYI3PCX7Xdul3C8K7KNRKRIFVVzAjFpfQvfBlDKDHbowirUtecx5OJgLHZCw jxoB9GBl14vavKDtpqYl6P7RNApEk2w6Ig5395a3MLgumJdo4SbzYPfs4LJ6X9VeRr78_cHZFPa trigger: refreshTrigger, source: 'cloudflare-challenge', widgetId: 'o8ic5', nextRcV: '7pVV3BOshG' window.parent.postMessage({ source: 'cloudflare-challenge', widgetId: window._cf_chl_opt.chlA /script>
	Other Info	No links have been found while there are scripts, which is an indication that this is a modern we
URL		https://challenges.cloudflare.com/cdn-cgi/challenge-platform/h/b/turnstile/if/ov2/av0/rcv/u2hhw/0
	Method	GET
	Attack	
	Evidence	<script nonce="ESUe9ETIU75F8KmH"> (function(){ window._cf_chl_opt={ cvId: '3', cZone: 'cha chlApiTimeoutEncountered: 0, chlApiOverrunBudgetMs:30000, chlTimeoutMs:120000,hjlH5: 'vQ s_d2WBJniKIqJLKvK0Tr7y341M4RhZdAIezfanZVk0cXk5aalZZ11.Uw7CwVuQfM', cFPWv: 'b', c 1hLb6fiRH6AcK2LgruKj2blr5UeuI4V.zxAkBsgIaeqk2L5RZvQN_VWfuqMoXssVmX3OC3Ij8gW6 uBSnhmihdzfeNdVwykE6b6Pu9aVMVsJo9jqehpQ1l6xr0NStu5DhQXeSpYHmAkH975kFJm.6IB BuPaEUzjWT8XlXLh_pPsF2BIIlKJG77Wh3m7gmBSpgLSeekQBzRNpFdkl0md7kD6Fi2EZIrjXv rL4IWKspFtAyMnVqqjNF4oBjDsH4QVJjv_mNEWGYOOzV1DLx94eivu01_6toO_B8IaqcXWEor Tw7cQ8Rl0UhTCrSI7oDNpjPawOqg6g3XP7tmi0TkszFs97M.503.iqeQTlRuuE6ECYcslpq1J1wJ srVr2H0wTYHtuVymW8rRGYGTzh88Je8bJ3NZ_ohAQHYw1eIDgeNadAwQ6EKnjLo5VPJNzg1 postMessage({ trigger: refreshTrigger, source: 'cloudflare-challenge', widgetId: 'u2hhw', nextRcV chlApiWidgetId) { window.parent.postMessage({ source: 'cloudflare-challenge', widgetId: windov ('__cfDebugTurnstileOutcome'); } }()); </script>
	Other Info	No links have been found while there are scripts, which is an indication that this is a modern we
URL		https://chromewebstore.google.com/

window.parent.postMessage({ source: 'cloudflare-challenge', widgetId: window._cf_chl_opt.chlA
/script>

<script nonce="xtUXrNYr2ZQmNM0g"> (function(){ window._cf_chl_opt={ cvId: '3', cZone: 'chall
chlApiTimeoutEncountered: 0, chlApiOverrunBudgetMs:30000, chlTimeoutMs:120000,hjlH5: 'v4
mK5y4uzXjblALRfUpIWmoXX2BNHfA3Xq.9w1so8nbp4Rolc2RSfYjHmvlA36H_yU', cFPWv: 'b',
Q2Nl3Bv3NgX4F6RB1nhAVG6is1LjAUfpmIPXsiujSdkTxB9WOXOfVeeZSlOvkIRhOa2dwvk_Vp
4IvSOuTyi8L6RfnkrxRhOCMwebwh9frZjRcqwsGv6h_FSR3gcn_A65iYW_kugJjP8GfeMEJrKGL
Ysp1aSnn4IcpQFJcXeMaklV8Wf5zLwKbb1NZG7MXkuIEDDh9ejJtAv7WZj7EOUGOkgg6t7Y6K
C8i_7Darwm8qNk_mqm0lMq2Koyg44a6KHezexd_Z4KjFrU4Af1TUP5dyo6I5dkncOHHSdkZC7J
IFq8_wOHv9qw9WkoLAVy_w6EdepZz67fiH79unBcVzuNt4RdYW_PBKIEgUyBkEWUtl9_9EsM
Hj7Vz8NvsOT6j17KRl5b_lDsKTfvtCGl3smN86hoghzsfS1ismApzxosiVcxnXvGNUB964Pxi48F_
9a71LibRHO9BLua52ske9Q7NLBgjZUZK0v8eHGM_KW2ARrODw4Isvm84b4cs5TlA92euUfWr
'bZzZ_dAym2Wtsmymq9Zn1JWlLzMTDoyK7oT1I5pbFwg-1746739304-1.3.1.1-Vq5xG7Rdu32J
_cf_chl_opt.chlApiWidgetId, event: 'food', seq: e.seq, }, '*'); } } window.addEventListener('messa

Method	GET	
Attack		
Evidence	Skip to main content	
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this	
URL	https://www.canva.com/	
Method	GET	
Attack		
Evidence	<script>(function(){window._cf_chl_opt={cvId: '3',cZone: "www.canva.com",cType: 'managed',cF J21GrJ9rRGGe_cw0NqwQskirTvbSmkDIbZUhgamOE4I",cFPWv: 'b',cITimeS: '1746739146',cT yDsY5_WBi3gJkQ55IVdRtWCHHTBtKVZGQ6MAfut6ds0zi5ESgWqtDFILvZ12dSzeGgCtgqzloV 5H2Klo4DuGW9nWml_93hoCAOaQV44Qebp_l1xuXtDPPsHlyHIVWfcXXISa1EGRHOeAHuFsv 45byKFD7B1oIpdV3b5eRDDdRVoyR88Ema6hT6dXQVv61uv1VPd6RacNU0tyA9QEsknJAubrl jESX8vCID5iWImSPn4OX29yxD0D1Tpi5Pvtw3UoRLRTn8tT.Kk7w99CjRncTzNY3UxU1vW_Zc Ev9sJNLy73DEdcVygiEtKyHMVqYdQ_C7olBq76Jo19DAfbzQjl70jN9_R2AtFW6iIbFatuN7t7mG EMh20o0IyShcXJvjkEa6BWq99Rtxm9jB54W48Nj3ea8INJF6wcMdbm0iKPoFCuyvOheV2l5OQl Iyao3rzgRdUlZv3dhpDIXbNhoXkfkrdd6PnwtiyozqB_V5kjV2M3IzRsV_F2HbdE0fwkHvMvzKYHr S36r9g8uHkgghCkCHHneHnEOAim6mSCrYE7wUsxXHxwQT04DLKLG1g6NWXadnZBXLIjlbal haLZvGnqKvpJWdIafgU1s3XF2KekAnERaP4gC6Lsl8IzXNXP.OW32dxmAkJe9393E6ulFR6Sn W6zqzpfzKRVPrh_qOe06Bgm5ZSKitXY6kTLfvSVk6NbCQPOV875v83c9En0VYRbn6Tgfbn0xs WrklMV_oEknx1Y72FEtlVhSBcFRAZZLYALMnSWLD3deLFpT2ecKXQYT70T4NivyKC5c41hVl w9xrV6QJboKPuT3k3mHOJa5YOHKYrOlljmvbr0iQ4IL_UOAuPMZKB3GenZFoVXgcnL6DHFxk w2J9YZNUrmmnbElxHcjN7qvHNbgGqpOkcEhNvUQzy3WOJdqS2kuTHMc3L6Fl3H6B_pGNec hHxeM4Cy5e64msTeqyQ3dYExstUlavtL8Ui8V0Lw3hRb2IjRrg9Vxh0jtq6Oey8TthM3rlFxXS6Nie /cdn-cgi/challenge-platform/h/b/orchestrate/chl_page/v1?ray=93cbfe5428043d98';window._cf_c location.pathname + window._cf_chl_opt.cOgUQuery + window._cf_chl_opt.cOgUHash;history. (cpo);}());</script>	
Other Info	No links have been found while there are scripts, which is an indication that this is a modern we	
URL	https://www.canva.com/	
Method	GET	
Attack		
Evidence	<script>(function(){window._cf_chl_opt={cvId: '3',cZone: "www.canva.com",cType: 'managed',cF VPkMXfj7M",cFPWv: 'b',cITimeS: '1746739147',cTplC: 0,cTplV: 5,cTplB: 'cf',fa: "\/?__cf_chl_f_tl hkFQtSZrcCU1IWxVpcnnhK5ikBIPyU7sJHpb7ko21IKp5XjlvQYFMWQr7xa8wURAfjatt7gAjWY7 PbAxbNxOrPIpH7o9J1dHQPLZuLs1f7aXR1jTVGF92Wb_NsrSgwkJc8KroT5Pg1ewDJNqYqynC XhSq0hoiP5NSR62RO3pSp0V9VZwypD3ypDq9PuZMym993geyiimJn6HuJKOvXYPovK4cIrOjl dkRfvIjYVPJqgRgwpkwY",mdrd: "3ff3mwkZrXjew7wnSdgYcNPwZVNVkY5bHJFv4N5gJhE-174(FlddvZ3_MNjmgIriJMVZmy8MYnV6y4yrIlsUGerm6OXt0R4qi4y6jtd.ynwZMZO_DB2N4C7oX3W N50oEONe505xofZ9bhELYmLOTy5BfdjffJiaCj3zLYGqrOecMxIMoB1M2nYsr39I5d5arN42i71qx QU9y_hoUtcl3ZYfUmQQK3pPAV07nqCvbInCkL8Do9nL6.lHx6z2S3JXPfpX74IC8C8VXBHR7X YGvPM7p7AJREbI3CsJzbUaY3xA4bQ1qNLe0D9C2PNHW35wx.DXaq2g689SwUqBJb8Ipyn8e WSqVktSs1Sf753KrpC2I70ZaWQ2C3LB9m7lrVL28hujxKFIa9eULKrls8ImU_V47tmrb4SG4uxbo HYZDlOhtofRc5B216n4_rGN_FuoCL2gLM8vswwSzn9u6Vd6uzkM4MCtFhiv9VO7pnDZxznlWX FDIA7KNkikmkyXAyTznpwlmI6lRwJoSyAMUWZ9apZH3VH8vFsVECaKFq2wSHThrKrCbMXa7 ieDuivfsysMScL8NIMMVA7Mv8kxgzqnTOuA4EmirgWFWzkFEa8mYlTfwv5u2fhkCSGoI8x_6Vc fHwCsbCGhpDdQ0dCAxOSdhK_2GOtFYyFTt_1rkwBmiHuaNJUWqzsSBoKVVOZRqMBe8VhE C3NhWcaUuglSE50mo4pFTnBysyMdtF1zQVs9GPzgB4L5WyE2qzZ6Vg7p2kc49pVIf2f2jbvoXa 89JBBAIwTdyRpHe5UJOO61s_vh84cpbCS1lkwgL0tvdyBpzBg08cwGGFq25UiQOO_SZTMm_l MGCtM0r_rQzT91_sr9BVvN_ZzIO9hbdltxgCvg6VkVDU1xyB0HSoNhMyaEqgs_4_oDVepe8bBl cjYdFVGY9Au6UFklRggfm67Cu42tOv4HWRpbgRfO0lTTCdYg3kY5DqLUQjV1T6npe3LroVUqC location.hash === '' && location.href.indexOf('#') !== -1 ? '#' : location.hash;window._cf_chl_opt. null, "\/?__cf_chl_rt_tk=hIRHc5fz6lDYnAd5EAYUfONr5h5U.L8_GUSg34bQuXs-1746739147-1.	
Other Info	No links have been found while there are scripts, which is an indication that this is a modern we	
URL	https://www.canva.com/	
Method	GET	

Attack	

Evidence	`<script>(function(){window._cf_chl_opt={cvId: '3',cZone: "www.canva.com",cType: 'managed',cF`
	 `FEpjn08YZuEeaZa48yeh2vDcG9CT9_GrECEiEh1Wp2U",cFPWv: 'b',cITimeS: '1746739221',cT`
	 `WHW2KWdm8R9pxZ1BBVmvZGKp7kSe0Dej73tOqrMALlS4IJM_NzKgWeAkY8xEjec3zLYALrr`
	 `n9LX_JR5mSeCqnCTghYJh9Z27IbPEkFZEhdORLysO_x9Crwu85Pyhb8ZJBU02XeQDo9OQFs`
	 `yMoAfTJj7DbNLxfnoL5GRispyWRVkfjmKL9mJ2q15Oty6cy83pqRrtlm_hNW4U6xg0Yl4_mHhQA`
	 `3LxruWRHpkfoRr5Hwy11pr5usjHO7wgNofEcrzFBeGDgwmsIsVknmlgV5Bgs2awCFSJBsNc.DE`
	 `tw44E3Ur_P90EACWoIKtfHhZ8_gOTAopEhaPixlRVL5DAuzsW_aqyIBIBeQYQU_XVWnDFnGr`
	 `j5yp69f9Amj5EUFHvhPfku2mLdJvJCs49lmvwRDe7keSP26JoDOvbAGsrcu6fWKr2alTJsxNHhp`
	 `8xcqco8dR1j2U13XchZ9pexCamiP9QhWlXhWm7jzVhm8beWbziI6.fFAP4gTSSN6lqbugB9PO9`
	 `mvL1m8ImEprUou6WSZowc4RiBubX0i4nd1fckZX8bo71w_impWUG0o3Ym6D6rbxjf7_J3MP_y`
	 `Kd5vJq15lk82pxFDc4Z4.KPqlYYKGjSF1ZjcU7Uc4cXfKHf05ABGW8Nv0qj.PMczOMWL4G_Ov(`
	 `c491YK_VayXsbUXcWUKAT0MqCt.MjkQ2lHaIpQBrD0Ts2v7jz0v0g67LNQRFmhEAGqLVOsf5I`
	 `ULKfYtnEJ0VV72mS91eiOSKtHykbb3gSSR6fMFhosANajhq66EQLabFwy.T6DvKTFMvgi6IE4G`
	 `rLEKeK2mqYiwbDnr296BdX1Xfw0hEq1LpSaJ.OpZ8wCRG4wn1aX_50VQau8qpxISZfg4pF4rzE`
	 `_Wz9GpusviREJn04G1rOL.U15lKSPE.KZe5UAtfh5qJ73axjgHouhBp.29Hc3BXWOWCDaJTkQ`
	 `jgvkAsGNW8momtAyPHmPM23JYcw_LtrjhQ19VQ.N4_hCc43JlHPO_FY.xDXEiU211r1PUL"};v`
	 `length - window._cf_chl_opt.cOgUHash.length).indexOf('?') !== -1 ? '?' : location.search;if (wind`
	 `_cf_chl_opt.cOgUHash);cpo.onload = function() {history.replaceState(null, null, ogU);}}documen`

Other Info	No links have been found while there are scripts, which is an indication that this is a modern we
URL	https://www.canva.com/
Method	GET
Attack	

Evidence	`<script>(function(){window._cf_chl_opt={cvId: '3',cZone: "www.canva.com",cType: 'managed',cF`
	 `lS1o1kSm6xwaBidakMpjrxioAYzwhkDQKDj21IcR6Sc",cFPWv: 'b',cITimeS: '1746739302',cTplC`
	 `K67itsqWx7iadj09WpOs5THLplvOm5e7a_2OAPzfCvmgb9Tq1MjorGjC94pKSXDMu9EHAjDokb`
	 `WPUpBwEwfHbgsVKbLRNc0U5AhxPdbMyaoLAnCopKn8YvjOc_MQ7Ekn7EVug72Alahh..QCe`
	 `EwOuD1RLLBk.NLNvVq_LjQczIeVL7_jVbKYE14rlaoO.kwmkfnHCneVUp1oqFjYf9j3B76Wbmjc(`
	 `PuiXLyYKF7IzbW6QXzq4GfFgP53EtroHMHtYZGrwe5gem..y3DXadX4JWHnN5ccT4fimH5gc",r`
	 `YQXxw2MH9iU_H_mkw_zpmbBl5efoXd4q8FVrRamvOl1b9pyICmGyAtzAygFuxmqZws7cABVk`
	 `gwTty4JaGDExaQ4Be7EHsGF8VkHbcPbBD.iWSFzgkLJqIYU6lzgokXfLTzwrmAQSx0XstoqXcF`
	 `Z6zrRSMmTfyO5GVk8SlufIsOskK1kfrkraZmLSVnTv3KDYRiwJ2CubqbRfbsfuIrSbGMHqQLAyU`
	 `Koln6MN66cYQfkowUrDpXh6aabLwTZBTV3oAafHLBex2rhcRIIrALMnraq1xeF4aV4dnHrkrmtAy`
	 `NNCE8Ky7JvHl0HfRMYsgyY6gMAsBipdxY5SgeId_aFHiJEZY3P2Ynq9GPyY7RcErB9zMT75HT`
	 `7nP5uWmZlm3Uv1ezoflZXbK3EGn9J6xPgrGmRiSa2FKcAKowHs.a16qmr9XlZzTpmsmErxAU/`
	 `UkCNc7ofY87paH7lOmOA1HSmsDOfPjzEM_91u7QbtHukmhUYvEx_ygVmKy8GjA63eSrYYwp`
	 `xbts611WTEZYSAvHRLBX17LVU0gqLDVRqxMc77GcjmiJDoU84gVt1llRht66xTU8SYI5SfREvV`
	 `IcojJcR_U0dQDPrnX9UAq2aNJhob2_cj3lm3DZZtnuJuNW7BDYz5a8OCss3zwK9eLRIIacG8hIE`
	 `2prcseLW2dswxfy9lL3yAQkZx._d32zeB75X8MdgsYHrSqnKUUryO36pTFboCza6r8zd6SxJA3gl`
	 `s2UgWOeW5XLd1IaCizPFOsPvw_Iyy_n0dZcs3DfkTk7QVHBDjk.JktMPaViQQ6IVasS2zendl.sh`
	 `_cf_chl_opt.cOgUHash = location.hash === '' && location.href.indexOf('#') !== -1 ? '#' : location.`
	 `history.replaceState(null, null, "V?__cf_chl_rt_tk=fSK31tE2cSQ8yeXBKfdMfa6Qfkca4XfYNiIBG(`

Other Info	No links have been found while there are scripts, which is an indication that this is a modern we
URL	https://www.canva.com/
Method	GET
Attack	

Evidence	`<script>(function(){window._cf_chl_opt={cvId: '3',cZone: "www.canva.com",cType: 'managed',cF`
	 `0vOYk0yYMnZ_2gSX9hBQA1Kw7M60QPtRa7n41uetjr0",cFPWv: 'b',cITimeS: '1746739320',cT`
	 `N5J06rGVCeJcEpVuPzdYaSN6ijW7xM0BeWeIJv0g8iW1qVQsX2eUURJdmf5Cu7SXHLADW8I`
	 `wCXGzdE2rNxYE1o1aQVsE8xaR5qUoW.nNVDqXLOnFwODztGWXNJAJzsJ6UGacUupu4N2y`
	 `LCLAV1Co58RR3is5sa5EWFH8ZpYmTV4mnph1SfSi6ZEI3sJCSAzvb9eAjC9Nh5GzbSzzKbng`
	 `IPSD4bRVoXey3A64lqYZjKRjrdEPnItxfqjx8E_aLsUDX0zcrRnvdrRfZmXJznNSUNv4JtVgOuJrU`
	 `JFXABgfcUjbcRcw_m6nbx2nn98YRmVscBQgmHBn6kHoM_B2S6.dHdLmPN7TyyhQ66yz2rcfE`
	 `wWj7UMuWcYVsdlpfk6T1Ea1seHx6bZ7SdRee6Fn4LXEU8y9SAqk7vUTe446ohXBHKfjcIyEDz`
	 `j14lboA1FhU5UgmpwyioZznR_pgxU9lMnvCJSVZuIcpY7VvinhIQvNsGY_bXC9iiQfHY3CwhXg6`
	 `PEivjUuIWt5wtvqjPFrn0xw_VG6HyHrYUXrfVwzhVDB56027FhbxplB2oeZwCh11KJW5a9QoBdl`
	 `eGIFvtYlD5UeU38uWjpgViuBrCaltsIE5XuzTxYqaNqU49mvZOaZWdDXikD9zbusCxSBXdrERV`
	 `SZZMbg6zyMVqhywF_Ui6htsWCWtWOh1R_U5d9buzusl7fT48PVJVPLXzImKsz7pFiZ7lupPfzg`
	 `ocVvUw8yMJj8BAcWUhCUCNZUp0cMgkVxLI.7mHqx6f4xW63RSVGU2.nJ7DayXyFbc61Ls3C(`

		0A1RpDVcjGAjwu8acP1W85r8Y72X0g9wAII2lEAedwIfRgcLAuB569pDcFB1RSAl4ia7KBUrm6u 1YTdlFXLsN46cVx05hvCm7SrmmvR49XK9.tHi.szkhi3u1yzwuFVi8LRJuEqaQHcqdH99P.y337C document.createElement('script');cpo.src = '/cdn-cgi/challenge-platform/h/b/orchestrate/chl_pag && window.history.replaceState) {var ogU = location.pathname + window._cf_chl_opt.cOgUQue getElementsByTagName('head')[0].appendChild(cpo);}());</script>
	Other Info	No links have been found while there are scripts, which is an indication that this is a modern we
URL		https://www.canva.com/
	Method	GET
	Attack	
	Evidence	<script>(function(){window._cf_chl_opt={cvId: '3',cZone: "www.canva.com",cType: 'managed',cF 2vlx3B0OnAUpHWme3Ps3gUGrrpv8H6mjlL96EYTe1q0",cFPWv: 'b',cITimeS: '1746739345',cT LZRCvkzqdE8Afy9Kg_k0rTqQVJa__iZWMQIMgghh0bmsUWkkjo_tlSsdbkQ1siDT7WnKQ5T7D pPBIoQA9zFVV3NswlzcjPnD8CX5Y7BBD2oZzBLh0setbQEKFRFN2ORJnRuGvQe5Y1fdOFUv 1mpxzPBKU3VRjtY56VMdfhVMo1FSXXAwm2Ulk_BLbNaddxM0iZ2tpqjMNUn6HexdM_pEpF8e F0eB9ty0nOxriJXTSP45Ew_Td2VeMEiOBh4YdwMj6u8yqIMGBQJO8XI.2Q2sswugjZDvRObdk SDXPpbNhHohP27Kw2IeqHOmFClPcqDYxcIM7rMb6djzX0tRAWBWwFKuOMmByLIL_RV_l8F 0uayyNbyikKw8TBGk8RguWX8fppPuxK7mcjseCYbI4Z5gATfLrLMY_T29Fo37n8A4qP3OPF8gl SRvhlyvfyTom4QDmb7BernbaDUkBgIorcq_Mw5b9yR3UiwBtNAuA.i110nF9rNxjXqfqR3w377zC 0E0q1HUAA1D4uTPp1Vir15Rye83QkgW_v9VH2exQMMkwilDrDmYLwEC9xJq5BLsgdXCgG9k 5zLVUfM7rdHBVOONSVOBAReXtzEoImqgbCGLVqxmaAcv6eAARGzTJ_eDZx0k1O1O4UKdv K93rNlAN186IaL5FehXwmQ_9ABRE5gtnZE2AsqoRgqeIi0E1owBZPBdkyfnZWTHUrjMGn_vsQ 6BG0WTBKX6kKvbHmFeMSOaq85qeafZg5wBsMQLhtatolqr6PoJ4gT9NwyxJohfAjT2s7umzk5 Joc3sAB1VDaBbxiyY_WseRkvwLx3lknsTiYOtHIb7CjEpMk2vf3eK0KO7hcvc5AciHUuiy_PbV0M WvpzAIX_uTIStdcwb6IDbbyCbdo2ec7yDrclOM_rx1vGv7FPRlDtDHMwAdDlHcLlqBcoiiM7YbSR jVOVsDiLmEwyOYihCYLxMytzqldB44.NgXT8ckyuyOQXEDqFiVyhSc6lxxhrg3bLglRGy7oaY4lp Es4kXC6x5j0vmD9yF9RLrmYUYzzoC8VnHbGKsUyKu7yA3KRFTbSkWiWrE6_21x4t_jiq1jaqeU '#' : location.hash;window._cf_chl_opt.cOgUQuery = location.search === '' && location.href.slice __cf_chl_rt_tk=gDaSPq_WcBResXPb7oj1cyuO6jHspFvRU_a9YcJO2zc-1746739345-1.0.1.1-2\
	Other Info	No links have been found while there are scripts, which is an indication that this is a modern we
URL		https://www.google.com/search?q=canva.com&oq=canva.com&gs_lcrp=EgZjaHJvbWUyBggAE
	Method	GET
	Attack	
	Evidence	<noscript><style>table,div,span,p{display:none}</style><meta content="0;url=/httpservice/retry/
	Other Info	A noScript tag has been found, which is an indication that the application works differently with .
URL		https://www.google.com/sorry/index?continue=https://www.google.com/search%3Fq%3Dcanva.
	Method	GET
	Attack	
	Evidence	<a href="#" onclick="document.getElementById('infoDiv').style.display='block';">Why did this ha
	Other Info	Links have been found that do not have traditional href attributes, which is an indication that this
Instances		14
Solution		This is an informational alert and so no changes are required.
Reference		
CWE Id		
WASC Id		
Plugin Id		10109

Informational	Re-examine Cache-control Directives

Description	The cache-control header has not been set properly or is missing, allowing the browser and pro... For static assets like css, js, or image files this might be intended, however, the resources shoul ensure that no sensitive content will be cached.
URL	https://content-autofill.googleapis.com/v1/pages /ChRDaHJvbWUvMTM2LjAuNzEwMy45MhIZCbUh2di5B6M5EgUNGV2o4iHqqpfJjEnCRA==?a
Method	GET
Attack	
Evidence	private,max-age=604800
Other Info	
URL	https://optimizationguide-pa.googleapis.com/downloads? name=1673999601&target=OPTIMIZATION_TARGET_PAGE_VISIBILITY
Method	GET
Attack	
Evidence	public, max-age=86400
Other Info	
URL	https://optimizationguide-pa.googleapis.com/downloads? name=1679317318&target=OPTIMIZATION_TARGET_LANGUAGE_DETECTION
Method	GET
Attack	
Evidence	public, max-age=86400
Other Info	
URL	https://optimizationguide-pa.googleapis.com/downloads? name=1696267841&target=OPTIMIZATION_TARGET_OMNIBOX_URL_SCORING
Method	GET
Attack	
Evidence	public, max-age=86400
Other Info	
URL	https://optimizationguide-pa.googleapis.com/downloads? name=1728324084&target=OPTIMIZATION_TARGET_OMNIBOX_ON_DEVICE_TAIL_SUGGI
Method	GET
Attack	
Evidence	public, max-age=86400
Other Info	
URL	https://optimizationguide-pa.googleapis.com/downloads? name=1744643027&target=OPTIMIZATION_TARGET_GEOLOCATION_PERMISSION_PRED
Method	GET
Attack	
Evidence	public, max-age=86400
Other Info	
URL	https://optimizationguide-pa.googleapis.com/downloads? name=1744643050&target=OPTIMIZATION_TARGET_NOTIFICATION_PERMISSION_PREDI

Method	GET	
Attack		
Evidence	public, max-age=86400	
Other Info		
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1744729555&target=OPTIMIZATION_TARGET_CLIENT_SIDE_PHISHING	
Method	GET	
Attack		
Evidence	public, max-age=86400	
Other Info		
URL	https://optimizationguide-pa.googleapis.com/downloads?name=240731042075&target=OPTIMIZATION_TARGET_SEGMENTATION_COMPOSE_PRO	
Method	GET	
Attack		
Evidence	public, max-age=86400	
Other Info		
URL	https://optimizationguide-pa.googleapis.com/downloads?name=5&target=OPTIMIZATION_TARGET_PAGE_TOPICS_V2	
Method	GET	
Attack		
Evidence	public, max-age=86400	
Other Info		
URL	https://www.google.com/async/ddljson?async=ntp:2	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://www.google.com/async/newtab_ogb?hl=en-US&async=fixed:0	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://www.google.com/async/newtab_promos	
Method	GET	
Attack		
Evidence		
Other Info		
URL	https://www.google.com/search?q=canva.com&oq=canva.com&gs_lcrp=EgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE&sou

	[8](#)
Method	GET
Attack	
Evidence	private
Other Info	
URL	[https://www.google.com/shared_dict/srp/9b2f0e32aa58bed3086962cef882a7badfe7e540019b4...dict](#)
Method	GET
Attack	
Evidence	public, max-age=31536000
Other Info	
Instances	15
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, mus... asset should be cached consider setting the directives "public, max-age, immutable".
Reference	[https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web...](#) [https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control](#) [https://grayduck.mn/2021/09/13/cache-control-recommendations/](#)
CWE Id	[525](#)
WASC Id	13
Plugin Id	[10015](#)

Informational	Retrieved from Cache	
Description	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.	
URL	[https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.F939Du45chc.O/m=gapi_iframes,googleapis_client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo8uI5v7Xlp-b-Z4Th_hAAVtm2lZOw/cb=gapi.loaded_0](#)	
Method	GET	
Attack		
Evidence	Age: 129241	
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.	
URL	[https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.F939Du45chc.O/m=gapi_iframes,googleapis_client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo8uI5v7Xlp-b-Z4Th_hAAVtm2lZOw/cb=gapi.loaded_0](#)	
Method	GET	
Attack		
Evidence	Age: 129284	
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.	
URL	[https://apis.google.com/_/scs/abc-static/_/js/k=gapi.gapi.en.F939Du45chc.O/m=gapi_iframes,googleapis_client/rt=j/sv=1/d=1/ed=1/rs=AHpOoo8uI5v7Xlp-b-Z4Th_hAAVtm2lZOw/cb=gapi.loaded_0](#)	

	Method	GET
	Attack	
	Evidence	Age: 129288
	Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL		https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/css/all.min.css
	Method	GET
	Attack	
	Evidence	Age: 547892
	Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL		https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.4.0/webfonts/fa-solid-900.woff2
	Method	GET
	Attack	
	Evidence	Age: 580688
	Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL		https://chrome.google.com/webstore?hl=en
	Method	GET
	Attack	
	Evidence	Age: 1652
	Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL		https://fonts.gstatic.com/s/googlesans/v58/4UaRrENHsxJlGDuGo1OIlJfC6l_24rlCK1Yo_Iq2vgCI.woff2
	Method	GET
	Attack	
	Evidence	Age: 128745
	Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL		https://fonts.gstatic.com/s/productsans/v9/pxiDypQkot1TnFhsFMOfGShVF9eO.woff2
	Method	GET
	Attack	
	Evidence	Age: 153533
	Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL		https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmWUlfBBc4.woff2
	Method	GET
	Attack	
	Evidence	Age: 14830
	Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL		https://www.gstatic.com/og/_/js/k=og.qtm.en_US.jS_CZIDYjaI.2019.O/rt=j/m=q_dnp,qmd, qcwid,qapid,qald,qads,q_dg/exm=qaaw,qabr,qadd,qaid,qalo,qebr,qein,qhaw,qhawgm3, qhba,qhbr,qhbrgm3,qhch,qhchgm3,qhga,qhid,qhidgm3,qhin,qhlo,qhlogm3,qhmn,qhpc,qhsf,

		qhsfgm3.qhtt/d=1/ed=1/rs=AA2YrTsB9Qz4OH5RFhAQLL8W1kIQz_J3Rg
	Method	GET
	Attack	
	Evidence	Age: 203898
	Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL		https://www.gstatic.com/og/_/js/k=og.qtm.en_US.jS_CZIDYjaI.2019.O/rt=j/m=q_dnp,qmd, qcwid,qapid,qald,qads,q_dg/exm=qaaw,qabr,qadd,qaid,qalo,qebr,qein,qhaw,qhawgm3, qhba,qhbr,qhbrgm3,qhch,qhchgm3,qhga,qhid,qhidgm3,qhin,qhlo,qhlogm3,qhmn,qhpc,qhsf, qhsfgm3.qhtt/d=1/ed=1/rs=AA2YrTsB9Qz4OH5RFhAQLL8W1kIQz_J3Rg
	Method	GET
	Attack	
	Evidence	Age: 203945
	Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL		https://www.gstatic.com/og/_/js/k=og.qtm.en_US.jS_CZIDYjaI.2019.O/rt=j/m=qabr,q_dnp, qcwid,qapid,qads,q_dg/exm=qaaw,qadd,qaid,qein,qhaw,qhba,qhbr,qhch,qhga,qhid,qhin/d=1 /ed=1/rs=AA2YrTsB9Qz4OH5RFhAQLL8W1kIQz_J3Rg
	Method	GET
	Attack	
	Evidence	Age: 204187
	Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL		https://www.gstatic.com/og/_/ss/k=og.qtm.kh2ijRv0MlA.L.W.O/m=qcwid/excm=qaaw,qadd, qaid,qein,qhaw,qhba,qhbr,qhch,qhga,qhid,qhin/d=1/ed=1/ct=zgms /rs=AA2YrTtnuxIkMiC5WsBVsg4Kr_L_CPAqfg
	Method	GET
	Attack	
	Evidence	Age: 138245
	Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL		https://www.gstatic.com/og/_/ss/k=og.qtm.kh2ijRv0MlA.L.W.O/m=qmd,qcwid/excm=qaaw, qabr,qadd,qaid,qalo,qebr,qein,qhaw,qhawgm3,qhba,qhbr,qhbrgm3,qhch,qhchgm3,qhga, qhid,qhidgm3,qhin,qhlo,qhlogm3,qhmn,qhpc,qhsf,qhsfgm3,qhtt/d=1/ed=1/ct=zgms /rs=AA2YrTtnuxIkMiC5WsBVsg4Kr_L_CPAqfg
	Method	GET
	Attack	
	Evidence	Age: 204383
	Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL		https://www.gstatic.com/og/_/ss/k=og.qtm.kh2ijRv0MlA.L.W.O/m=qmd,qcwid/excm=qaaw, qabr,qadd,qaid,qalo,qebr,qein,qhaw,qhawgm3,qhba,qhbr,qhbrgm3,qhch,qhchgm3,qhga, qhid,qhidgm3,qhin,qhlo,qhlogm3,qhmn,qhpc,qhsf,qhsfgm3,qhtt/d=1/ed=1/ct=zgms /rs=AA2YrTtnuxIkMiC5WsBVsg4Kr_L_CPAqfg
	Method	GET
	Attack	
	Evidence	Age: 204431
	Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.

URL	https://www.gstatic.com/recaptcha/releases/Hi8UmRMnhdOBM3IuViTkapUP/recaptcha__en.js
Method	GET
Attack	
Evidence	Age: 132707
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
Instances	16
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Reference	https://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231 https://www.rfc-editor.org/rfc/rfc9110.html
CWE Id	
WASC Id	
Plugin Id	10050

Informational	Session Management Response Identified
Description	The given response has been identified as containing a session management token. The 'Other Method. If the request is in a context which has a Session Management Method set to "Auto-De
URL	https://www.canva.com/
Method	GET
Attack	
Evidence	8YDvy0pdPnlWoGeyGumq3JB3A81pCDAmrrAZVTytsIs-1746739146-1.0.1.1-.O3APTjHScD4A 3stV3fUzDquhO07CssMbdp46UtLQ0XBp8.oL35s
Other Info	cookie:__cf_bm
URL	https://www.google.com/search?q=canva.com&oq=canva.com&gs_lcrp=EgZjaHJvbWUyBggAE
Method	GET
Attack	
Evidence	523=liwXJAnIh2BoJLvB1ya4IU1-_sFYai89oXmp5OD8Fc9wFmQhQfWKE3Z8Jg8gHtApG8n11\ h_ghlrg_7nqXr5nCDLKO5LOo_2NiduB_LP-Ufp-oOw_DCD3L9gKz-z_Llg_Wo6YU1izg
Other Info	cookie:NID cookie:AEC
URL	https://www.google.com/search?q=canva.com&oq=canva.com&gs_lcrp=EgZjaHJvbWUyBggAE R4-EPzemMwAE
Method	GET
Attack	
Evidence	523=WIn5_eS11oqdlly8n6OPeyA0itGubzFT5LRBkkWVd3jh8-96mNn1cLfzKF73myZEKM4n2pF 3aVGwRhzJRzx1nqwY0wfvsvGl6UMGuHX7fHpJGhD5pHPNM66JTrYh42zkVHPWvXdVBVwos

Other Info	cookie:NID	
URL	https://play.google.com/log?format=json&hasfast=true	
Method	POST	
Attack		
Evidence	524=AUyKDc7nO9DxVjlRRrs5igNjWR58Fgx8hARhoxgJwkfaSfaXRGvfntvfx6hxBKimeLboMVcf fZolbv7rXY3tSkVY7tmV6c4Nc_c_9n2A9bdubg	
Other Info	cookie:NID	
URL	https://play.google.com/log?format=json&hasfast=true	
Method	POST	
Attack		
Evidence	524=a47diNNjOx4JDgYKl_b9ImH6UmpCtAgtQN3OERYGuKFkg5hln--lfY3_sx-x1nBzzgdZDXYl YJZtFqcMGCWErAroAGjAXq0JiGhSIpsJbyFwRT9IxUg	
Other Info	cookie:NID	
URL	https://www.canva.com/	
Method	GET	
Attack		
Evidence	8YDvy0pdPnlWoGeyGumq3JB3A81pCDAmrrAZVTytsIs-1746739146-1.0.1.1-.O3APTjHScD4A 3stV3fUzDquhO07CssMbdp46UtLQ0XBp8.oL35s	
Other Info	cookie:__cf_bm	
Instances	6	
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.	
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id	
CWE Id		
WASC Id		
Plugin Id	10112	

Informational	User Controllable Charset
Description	This check looks at user-supplied input in query string parameters and POST data to identify wh meta tag charset declarations might be user-controlled. Such charset declarations should alway application. If an attacker can control the response charset, they could manipulate the HTML to attacks. For example, an attacker controlling the <meta> element charset value is able to declar able to include enough user-controlled payload early in the HTML document to have it interprete encoding their payload with UTF-7 the attacker is able to bypass any server-side XSS protection the page.
URL	https://www.google.com/search?q=canva.com&oq=canva. com&gs_lcrp=EgZjaHJvbWUyBggAEEUYOjIGCAEQRRg50gEIMzM3MGowajeoAgCwAgE&sou 8
Method	GET
Attack	
Evidence	
Other Info	A(n) [Content-Type HTTP header] tag [charset] attribute The user input found was: ie=UTF-8 Th controlled was: UTF-8
Instances	1
Solution	Force UTF-8 in all charset declarations. If user-input is required to decide a charset declaration, allowed list is used.

Reference	
CWE Id	[20](#)
WASC Id	20
Plugin Id	[10030](#)