ZAP Scanning Report

Sites: http://davfds89h1pfc.cloudfront.net https://davfds89h1pfc.cloudfront.net

Generated on Fri, 11 Apr 2025 08:36:15

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	7
Informational	5
False Positives:	0

Summary of Sequences

For each step: result (Pass/Fail) - risk (of highest alert(s) for the step, if any).

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	3
Missing Anti-clickjacking Header	Medium	2
HTTPS Content Available via HTTP	Low	8

Insufficient Site Isolation Against Spectre Vulnerability	Low	10
Permissions Policy Header Not Set	Low	4
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	9
Strict-Transport-Security Header Not Set	Low	9
Timestamp Disclosure - Unix	Low	13
X-Content-Type-Options Header Missing	Low	8
Information Disclosure - Suspicious Comments	Informational	1
Modern Web Application	Informational	3
Re-examine Cache-control Directives	Informational	4
Retrieved from Cache	Informational	8
Storable and Cacheable Content	Informational	9

Alert Detail

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 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://davfds89h1pfc.cloudfront.net
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://davfds89h1pfc.cloudfront.net/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html 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	**Missing Anti-clickjacking Header**
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	https://davfds89h1pfc.cloudfront.net
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/
Method	GET
Parameter	x-frame-options

Attack	
Evidence	
Other Info	
Instances	2
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. 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) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use 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	**HTTPS Content Available via HTTP**
Description	Content which was initially accessed via HTTPS (i.e.: using SSL/TLS encryption) is also accessible via HTTP (without encryption).
URL	https://davfds89h1pfc.cloudfront.net
Method	GET
Parameter	
Attack	
Evidence	http://davfds89h1pfc.cloudfront.net
Other Info	ZAP attempted to connect via: http://davfds89h1pfc.cloudfront.net
URL	https://davfds89h1pfc.cloudfront.net/
Method	GET
Parameter	
Attack	
Evidence	http://davfds89h1pfc.cloudfront.net/
Other Info	ZAP attempted to connect via: http://davfds89h1pfc.cloudfront.net/
URL	https://davfds89h1pfc.cloudfront.net/favicon.ico
Method	GET

Parameter	
Attack	
Evidence	http://davfds89h1pfc.cloudfront.net/favicon.ico
Other Info	ZAP attempted to connect via: http://davfds89h1pfc.cloudfront.net/favicon.ico
URL	https://davfds89h1pfc.cloudfront.net/logo192.png
Method	GET
Parameter	
Attack	
Evidence	http://davfds89h1pfc.cloudfront.net/logo192.png
Other Info	ZAP attempted to connect via: http://davfds89h1pfc.cloudfront.net/logo192.png
URL	https://davfds89h1pfc.cloudfront.net/manifest.json
Method	GET
Parameter	
Attack	
Evidence	http://davfds89h1pfc.cloudfront.net/manifest.json
Other Info	ZAP attempted to connect via: http://davfds89h1pfc.cloudfront.net/manifest.json
URL	https://davfds89h1pfc.cloudfront.net/robots.txt
Method	GET
Parameter	
Attack	
Evidence	http://davfds89h1pfc.cloudfront.net/robots.txt
Other Info	ZAP attempted to connect via: http://davfds89h1pfc.cloudfront.net/robots.txt
URL	https://davfds89h1pfc.cloudfront.net/static/css/main.ca65008d.css
Method	GET
Parameter	
Attack	
Evidence	http://davfds89h1pfc.cloudfront.net/static/css/main.ca65008d.css
Other Info	ZAP attempted to connect via: http://davfds89h1pfc.cloudfront.net/static/css/main.ca65008d.css

URL	https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Method	GET
Parameter	
Attack	
Evidence	http://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Other Info	ZAP attempted to connect via: http://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Instances	8
Solution	Ensure that your web server, application server, load balancer, etc. is configured to only serve such content via HTTPS. Consider implementing HTTP Strict Transport Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html 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	311
WASC Id	4
Plugin Id	10047

Low	**Insufficient Site Isolation Against Spectre Vulnerability**
Description	Cross-Origin-Resource-Policy header is an opt-in header designed to counter side-channels attacks like Spectre. Resource should be specifically set as shareable amongst different origins.
URL	https://davfds89h1pfc.cloudfront.net
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	

Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/favicon.ico
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/logo192.png
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/manifest.json
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/robots.txt
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net
Method	GET

Parameter	Cross-Origin-Embedder-Policy
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/
Method	GET
Parameter	Cross-Origin-Embedder-Policy
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net
Method	GET
Parameter	Cross-Origin-Opener-Policy
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/
Method	GET
Parameter	Cross-Origin-Opener-Policy
Attack	
Evidence	
Other Info	
Instances	10
Solution	Ensure that the application/web server sets the Cross-Origin-Resource-Policy header appropriately, and that it sets the Cross-Origin-Resource-Policy header to 'same-origin' for all web pages. 'same-site' is considered as less secured and should be avoided. If resources must be shared, set the header to 'cross-origin'. If possible, ensure that the end user uses a standards-compliant and modern web browser that supports the Cross-Origin-Resource-Policy header (https://caniuse.com/mdn-http_headers_cross-origin-resource-policy).

Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Cross-Origin_Resource_Policy
CWE Id	693
WASC Id	14
Plugin Id	90004

Low	**Permissions Policy Header Not Set**
Description	Permissions Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Permissions Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
URL	https://davfds89h1pfc.cloudfront.net
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
Instances	4
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Permissions-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Permissions-Policy https://developer.chrome.com/blog/feature-policy/ https://scotthelme.co.uk/a-new-security-header-feature-policy/ https://w3c.github.io/webappsec-feature-policy/ https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	693
WASC Id	15
Plugin Id	10063

Low	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	https://davfds89h1pfc.cloudfront.net
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/favicon.ico

Method	GET
Parameter	
Attack	
Evidence	AmazonS3
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/logo192.png
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/manifest.json
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/robots.txt
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	AmazonS3

Other Info	
URL	https://davfds89h1pfc.cloudfront.net/static/css/main.ca65008d.css
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
Other Info	
Instances	9
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	497
WASC Id	13
Plugin Id	10036

Low	**Strict-Transport-Security Header Not Set**
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	https://davfds89h1pfc.cloudfront.net
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://davfds89h1pfc.cloudfront.net/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/favicon.ico
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/logo192.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/manifest.json
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/robots.txt
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/static/css/main.ca65008d.css
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	9
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html 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://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Method	GET
Parameter	
Attack	
Evidence	1508970993
Other Info	1508970993, which evaluates to: 2017-10-25 22:36:33.
URL	https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Method	GET
Parameter	
Attack	
Evidence	1537002063
Other Info	1537002063, which evaluates to: 2018-09-15 09:01:03.
URL	https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Method	GET
Parameter	
Attack	
Evidence	1541459225
Other Info	1541459225, which evaluates to: 2018-11-05 23:07:05.
URL	https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Method	GET
Parameter	
Attack	
Evidence	1555081692
Other Info	1555081692, which evaluates to: 2019-04-12 15:08:12.
URL	https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js

Method	GET
Parameter	
Attack	
Evidence	1695183700
Other Info	1695183700, which evaluates to: 2023-09-20 04:21:40.
URL	https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Method	GET
Parameter	
Attack	
Evidence	1747873779
Other Info	1747873779, which evaluates to: 2025-05-22 00:29:39.
URL	https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Method	GET
Parameter	
Attack	
Evidence	1779033703
Other Info	1779033703, which evaluates to: 2026-05-17 16:01:43.
URL	https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Method	GET
Parameter	
Attack	
Evidence	1899447441
Other Info	1899447441, which evaluates to: 2030-03-11 08:17:21.
URL	https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Method	GET
Parameter	
Attack	
Evidence	1925078388

Other Info	1925078388, which evaluates to: 2031-01-01 23:59:48.
URL	https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Method	GET
Parameter	
Attack	
Evidence	1955562222
Other Info	1955562222, which evaluates to: 2031-12-20 19:43:42.
URL	https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Method	GET
Parameter	
Attack	
Evidence	1986661051
Other Info	1986661051, which evaluates to: 2032-12-14 18:17:31.
URL	https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Method	GET
Parameter	
Attack	
Evidence	1996064986
Other Info	1996064986, which evaluates to: 2033-04-02 14:29:46.
URL	https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Method	GET
Parameter	
Attack	
Evidence	2024104815
Other Info	2024104815, which evaluates to: 2034-02-21 03:20:15.
Instances	13
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
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 older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://davfds89h1pfc.cloudfront.net
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://davfds89h1pfc.cloudfront.net/
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://davfds89h1pfc.cloudfront.net/favicon.ico
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://davfds89h1pfc.cloudfront.net/logo192.png

Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://davfds89h1pfc.cloudfront.net/manifest.json
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://davfds89h1pfc.cloudfront.net/robots.txt
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://davfds89h1pfc.cloudfront.net/static/css/main.ca65008d.css
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js

Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	8
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-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 does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Method	GET
Parameter	
Attack	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected in likely comment: "//fb.me/use-check-prop-types");throw s.name="Invariant Violation",s}}function t(){return e}e.isRequired=e;var n={array:e,bigint:", see evidence field for the suspicious comment/snippet.
Instances	1
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	615
WASC Id	13

Plugin Id	10027

Informational	**Modern Web Application**
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	https://davfds89h1pfc.cloudfront.net
Method	GET
Parameter	
Attack	
Evidence	<script defer="defer" src="/static/js/main.86ec999b.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://davfds89h1pfc.cloudfront.net/
Method	GET
Parameter	
Attack	
Evidence	<script defer="defer" src="/static/js/main.86ec999b.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://davfds89h1pfc.cloudfront.net/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	<script defer="defer" src="/static/js/main.86ec999b.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	3
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 proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://davfds89h1pfc.cloudfront.net
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/manifest.json
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/robots.txt
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
Instances	4

Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
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://davfds89h1pfc.cloudfront.net
Method	GET
Parameter	
Attack	
Evidence	Hit from cloudfront
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/
Method	GET
Parameter	
Attack	
Evidence	Hit from cloudfront
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/favicon.ico
Method	GET
Parameter	
Attack	
Evidence	Hit from cloudfront

Other Info	
URL	https://davfds89h1pfc.cloudfront.net/logo192.png
Method	GET
Parameter	
Attack	
Evidence	Hit from cloudfront
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/manifest.json
Method	GET
Parameter	
Attack	
Evidence	Hit from cloudfront
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/robots.txt
Method	GET
Parameter	
Attack	
Evidence	Hit from cloudfront
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/static/css/main.ca65008d.css
Method	GET
Parameter	
Attack	
Evidence	Hit from cloudfront
Other Info	
URL	https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Method	GET
Parameter	

Attack	
Evidence	Hit from cloudfront
Other Info	
Instances	8
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	**Storable and Cacheable Content**
Description	The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the cache, rather than from the origin server by the caching servers, in response to similar requests from other users. 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 "shared" 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://davfds89h1pfc.cloudfront.net
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.

URL	https://davfds89h1pfc.cloudfront.net/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://davfds89h1pfc.cloudfront.net/favicon.ico
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://davfds89h1pfc.cloudfront.net/logo192.png
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://davfds89h1pfc.cloudfront.net/manifest.json
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://davfds89h1pfc.cloudfront.net/robots.txt
Method	GET

Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://davfds89h1pfc.cloudfront.net/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://davfds89h1pfc.cloudfront.net/static/css/main.ca65008d.css
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://davfds89h1pfc.cloudfront.net/static/js/main.86ec999b.js
Method	GET
Parameter	
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
Instances	9
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://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html
CWE Id	524
WASC Id	13
Plugin Id	10049

Sequence Details

With the associated active scan results.