ZAP Scanning Report

OWASP ZAP Spidering and Active Scanning

Sites: https://ka-f.fontawesome.com https://cdn.quilljs.com https://kit.fontawesome.com https://luna-hyperion-tech-f8b6991d9822.herokuapp.com

Generated on Thu, 28 Sept 2023 23:06:16

ZAP Version: 2.13.0

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	5
Informational	5

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	3
Cross-Domain Misconfiguration	Medium	9
Hidden File Found	Medium	4
Missing Anti-clickjacking Header	Medium	3
Cross-Domain JavaScript Source File Inclusion	Low	9
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	7
Strict-Transport-Security Header Not Set	Low	16
Timestamp Disclosure - Unix	Low	1
X-Content-Type-Options Header Missing	Low	12
Information Disclosure - Sensitive Information in URL	Informational	4
Information Disclosure - Suspicious Comments	Informational	10
Modern Web Application	Informational	3
Re-examine Cache-control Directives	Informational	3
Retrieved from Cache	Informational	6

Alert Detail

Medium	Content Security Policy (CSP) Header Not Set
	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

Description	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://luna-hyperion-tech-f8b6991d9822.herokuapp.com/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/sitemap.xml
Method	GET
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 http://www.w3.org/TR/CSP/ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/
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://cdn.quilljs.com/1.3.6/quill.js
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://cdn.quilljs.com/1.3.6/quill.min.js
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://ka-f.fontawesome.com/releases/v6.4.2/css/free-v4-font-face.min.css?token=c25dad79f1
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://ka-f.fontawesome.com/releases/v6.4.2/css/free-v4-shims.min.css?token=c25dad79f1
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://ka-f.fontawesome.com/releases/v6.4.2/css/free-v5-font-face.min.css?token=c25dad79f1
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://ka-f.fontawesome.com/releases/v6.4.2/css/free.min.css?token=c25dad79f1
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://kit.fontawesome.com/c25dad79f1.js
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://luna-hyperion-tech-f8b6991d9822.herokuapp.com/robots.txt
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://luna-hyperion-tech-f8b6991d9822.herokuapp.com/sitemap.xml
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.
Instances	9
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	**Hidden File Found**
Description	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/._darcs
Method	GET

Attack	
Evidence	HTTP/1.1 200 OK
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/.bzr
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/.hg
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/BitKeeper
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	
Instances	4
Solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.
Reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html
CWE Id	538
WASC Id	13
Plugin Id	40035

Medium	Missing Anti-clickjacking Header
Description	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/robots.txt
Method	GET
Attack	
Evidence	
Other	

Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	3
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	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/
Method	GET
Attack	
Evidence	<script src="//cdn.quilljs.com/1.3.6/quill.js"></script>
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/
Method	GET
Attack	
Evidence	<script src="//cdn.quilljs.com/1.3.6/quill.min.js"></script>
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/
Method	GET
Attack	
Evidence	<script src="https://kit.fontawesome.com/c25dad79f1.js" crossorigin="anonymous"></script>
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/robots.txt
Method	GET
Attack	
Evidence	<script src="//cdn.quilljs.com/1.3.6/quill.js"></script>
Other Info	

URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/robots.txt
Method	GET
Attack	
Evidence	<script src="//cdn.quilljs.com/1.3.6/quill.min.js"></script>
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/robots.txt
Method	GET
Attack	
Evidence	<script src="https://kit.fontawesome.com/c25dad79f1.js" crossorigin="anonymous"></script>
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/sitemap.xml
Method	GET
Attack	
Evidence	<script src="//cdn.quilljs.com/1.3.6/quill.js"></script>
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/sitemap.xml
Method	GET
Attack	
Evidence	<script src="//cdn.quilljs.com/1.3.6/quill.min.js"></script>
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/sitemap.xml
Method	GET
Attack	
Evidence	<script src="https://kit.fontawesome.com/c25dad79f1.js" crossorigin="anonymous"></script>
Other Info	
Instances	9
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	**Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)**
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/
Method	GET
Attack	

Evidence	X-Powered-By: Express
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/favicon.ico
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/polyfills.7385c14d04879b7c.js
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/robots.txt
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/runtime.d93af9f6b74814cc.js
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/sitemap.xml
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/styles.cef175af30d0fd8e.css
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
Instances	7
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

CWE Id	200
WASC Id	13
Plugin Id	10037

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://cdn.quilljs.com/1.3.6/quill.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://cdn.quilljs.com/1.3.6/quill.min.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ka-f.fontawesome.com/releases/v6.4.2/css/free-v4-font-face.min.css?token=c25dad79f1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ka-f.fontawesome.com/releases/v6.4.2/css/free-v4-shims.min.css?token=c25dad79f1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ka-f.fontawesome.com/releases/v6.4.2/css/free-v5-font-face.min.css?token=c25dad79f1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ka-f.fontawesome.com/releases/v6.4.2/css/free.min.css?token=c25dad79f1
Method	GET
Attack	
Evidence	
Other	

Info	
URL	https://kit.fontawesome.com/c25dad79f1.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/favicon.ico
Method	GET
Attack	
Evidence	
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/main.c0ea5266c81453e1.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/polyfills.7385c14d04879b7c.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/runtime.d93af9f6b74814cc.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/scripts.a031a3392433bc9f.js

Method	GET
Attack	
Evidence	
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/styles.cef175af30d0fd8e.css
Method	GET
Attack	
Evidence	
Other Info	
Instances	16
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 http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security http://caniuse.com/stricttransportsecurity http://tools.ietf.org/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://luna-hyperion-tech-f8b6991d9822.herokuapp.com/
Method	GET
Attack	
Evidence	1695933183
Other Info	1695933183, which evaluates to: 2023-09-28 22:33:03
Instances	1
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200
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://ka-f.fontawesome.com/releases/v6.4.2/css/free-v4-font-face.min.css?token=c25dad79f1
Method	GET
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://ka-f.fontawesome.com/releases/v6.4.2/css/free-v4-shims.min.css?token=c25dad79f1
Method	GET
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://ka-f.fontawesome.com/releases/v6.4.2/css/free-v5-font-face.min.css?token=c25dad79f1
Method	GET
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://ka-f.fontawesome.com/releases/v6.4.2/css/free.min.css?token=c25dad79f1
Method	GET
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://kit.fontawesome.com/c25dad79f1.js
Method	GET
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://luna-hyperion-tech-f8b6991d9822.herokuapp.com/
Method	GET

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://luna-hyperion-tech-f8b6991d9822.herokuapp.com/favicon.ico
Method	GET
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://luna-hyperion-tech-f8b6991d9822.herokuapp.com/polyfills.7385c14d04879b7c.js
Method	GET
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://luna-hyperion-tech-f8b6991d9822.herokuapp.com/robots.txt
Method	GET
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://luna-hyperion-tech-f8b6991d9822.herokuapp.com/runtime.d93af9f6b74814cc.js
Method	GET
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://luna-hyperion-tech-f8b6991d9822.herokuapp.com/sitemap.xml
Method	GET
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://luna-hyperion-tech-f8b6991d9822.herokuapp.com/styles.cef175af30d0fd8e.css
Method	GET
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	12
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	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

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://ka-f.fontawesome.com/releases/v6.4.2/css/free-v4-font-face.min.css?token=c25dad79f1
Method	GET
Attack	
Evidence	token
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: token token
URL	https://ka-f.fontawesome.com/releases/v6.4.2/css/free-v4-shims.min.css?token=c25dad79f1
Method	GET
Attack	
Evidence	token
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: token token
URL	https://ka-f.fontawesome.com/releases/v6.4.2/css/free-v5-font-face.min.css?token=c25dad79f1
Method	GET
Attack	
Evidence	token
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: token token
URL	https://ka-f.fontawesome.com/releases/v6.4.2/css/free.min.css?token=c25dad79f1
Method	GET
Attack	
Evidence	token
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: token token
Instances	4

Solution	Do not pass sensitive information in URIs.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10024

Informational	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	https://cdn.quilljs.com/1.3.6/quill.js
Method	GET
Attack	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected in the element starting with: " // IE11 has bug with Text nodes", see evidence field for the suspicious comment/snippet.
URL	https://cdn.quilljs.com/1.3.6/quill.js
Method	GET
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected 27 times, the first in the element starting with: "var debug = (0, _logger2.default)('quill');", see evidence field for the suspicious comment/snippet.
URL	https://cdn.quilljs.com/1.3.6/quill.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 6 times, the first in the element starting with: "function _toConsumableArray(arr) { if (Array.isArray(arr)) { for (var i = 0, arr2 = Array(arr.length); i < arr.length; i++) { ar", see evidence field for the suspicious comment/snippet.
URL	https://cdn.quilljs.com/1.3.6/quill.js
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected 40 times, the first in the element starting with: " query: Registry.query,", see evidence field for the suspicious comment/snippet.
URL	https://cdn.quilljs.com/1.3.6/quill.js
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 48 times, the first in the element starting with: " function Picker(select) {", see evidence field for the suspicious comment/snippet.
URL	https://cdn.quilljs.com/1.3.6/quill.js
Method	GET

Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 10 times, the first in the element starting with: " // TODO use WeakMap", see evidence field for the suspicious comment/snippet.
URL	https://cdn.quilljs.com/1.3.6/quill.js
Method	GET
Attack	
Evidence	USER
Other Info	The following pattern was used: \bUSER\b and was detected 60 times, the first in the element starting with: " var source = arguments.length > 0 && arguments[0] !== undefined ? arguments[0] : _emitter4.default.sources.USER;", see evidence field for the suspicious comment/snippet.
URL	https://cdn.quilljs.com/1.3.6/quill.js
Method	GET
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected 3 times, the first in the element starting with: " // maintain two arrays for circular references, where corresponding parents", see evidence field for the suspicious comment/snippet.
URL	https://cdn.quilljs.com/1.3.6/quill.min.js
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "!function(t,e){"object"==typeof exports&&"object"==typeof module?module.exports=e():" function"==typeof define&&define.amd?define", see evidence field for the suspicious comment/snippet.
URL	https://kit.fontawesome.com/c25dad79f1.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "! function(t){"function"==typeof define&&define.amd?define("kit-loader",t):t()}((function(){"use strict";function t(t,e){var n=Ob", see evidence field for the suspicious comment/snippet.
Instances	10
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	200
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://luna-hyperion-tech-f8b6991d9822.herokuapp.com/
Method	GET

Attack	
Evidence	<script src="https://kit.fontawesome.com/c25dad79f1.js" crossorigin="anonymous"></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://luna-hyperion-tech-f8b6991d9822.herokuapp.com/robots.txt
Method	GET
Attack	
Evidence	<script src="https://kit.fontawesome.com/c25dad79f1.js" crossorigin="anonymous"></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://luna-hyperion-tech-f8b6991d9822.herokuapp.com/sitemap.xml
Method	GET
Attack	
Evidence	<script src="https://kit.fontawesome.com/c25dad79f1.js" crossorigin="anonymous"></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://luna-hyperion-tech-f8b6991d9822.herokuapp.com/
Method	GET
Attack	
Evidence	public, max-age=0
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/robots.txt
Method	GET
Attack	
Evidence	public, max-age=0
Other Info	
URL	https://luna-hyperion-tech-f8b6991d9822.herokuapp.com/sitemap.xml
Method	GET
Attack	
Evidence	public, max-age=0
Other Info	

Instances	3
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://cdn.quilljs.com/1.3.6/quill.js
Method	GET
Attack	
Evidence	Age: 71
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://cdn.quilljs.com/1.3.6/quill.min.js
Method	GET
Attack	
Evidence	Age: 190
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://ka-f.fontawesome.com/releases/v6.4.2/css/free-v4-font-face.min.css?token=c25dad79f1
Method	GET
Attack	
Evidence	Hit from cloudfront
Other Info	
URL	https://ka-f.fontawesome.com/releases/v6.4.2/css/free-v4-shims.min.css?token=c25dad79f1
Method	GET
Attack	
Evidence	Hit from cloudfront
Other Info	
URL	https://ka-f.fontawesome.com/releases/v6.4.2/css/free-v5-font-face.min.css?token=c25dad79f1
Method	GET
Attack	

Evidence	Hit from cloudfront
Other Info	
URL	https://ka-f.fontawesome.com/releases/v6.4.2/css/free.min.css?token=c25dad79f1
Method	GET
Attack	
Evidence	Hit from cloudfront
Other Info	
Instances	6
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 http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)
CWE Id	
WASC Id	
Plugin Id	10050