ZAP Scanning Report

Site: https://exchangerate.host

Generated on Wed, 20 Sep 2023 16:09:48

ZAP Version: 2.13.0

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	1
Informational	5
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	4
Cross-Domain Misconfiguration	Medium	17
Missing Anti-clickjacking Header	Medium	4
Vulnerable JS Library	Medium	1
X-Content-Type-Options Header Missing	Low	17
Information Disclosure - Suspicious Comments	Informational	15
Modern Web Application	Informational	4
Re-examine Cache-control Directives	Informational	5
Retrieved from Cache	Informational	5
User Agent Fuzzer	Informational	40

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://exchangerate.host
Method	GET
Attack	
Evidence	

Other Info	
URL	https://exchangerate.host/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://exchangerate.host/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://exchangerate.host/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	4
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://exchangerate.host
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://exchangerate.host/

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://exchangerate.host/apple-touch-icon.png
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://exchangerate.host/assets/js/bootstrap.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://exchangerate.host/assets/js/main.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://exchangerate.host/assets/js/vendor/jquery-1.12.4.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://exchangerate.host/css/app.83d337b5.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://exchangerate.host/favicon-16x16.png
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://exchangerate.host/favicon-32x32.png
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://exchangerate.host/favicon.ico
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://exchangerate.host/js/app-legacy.82d076da.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://exchangerate.host/js/app.9729c651.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://exchangerate.host/js/chunk-vendors-legacy.5ce3045d.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://exchangerate.host/js/chunk-vendors.596ac91f.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://exchangerate.host/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://exchangerate.host/site.webmanifest
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://exchangerate.host/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	17
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 include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
URL	https://exchangerate.host
Method	GET
Attack	
Evidence	
Other Info	
URL	https://exchangerate.host/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://exchangerate.host/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://exchangerate.host/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	4
	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.

Solution	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

Medium	Vulnerable JS Library
Description	The identified library jquery, version 1.12.4 is vulnerable.
URL	https://exchangerate.host/assets/js/vendor/jquery-1.12.4.min.js
Method	GET
Attack	
Evidence	jquery-1.12.4.min.js
Other Info	CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-23064
Instances	1
Solution	Please upgrade to the latest version of jquery.
Reference	https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://bugs.jquery.com/ticket/11974 https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://github.com/jquery/jquery.com/issues/162
CWE Id	829
WASC Id	
Plugin Id	10003

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://exchangerate.host
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://exchangerate.host/
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://exchangerate.host/apple-touch-icon.png
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://exchangerate.host/assets/js/bootstrap.min.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://exchangerate.host/assets/js/main.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://exchangerate.host/assets/js/vendor/jquery-1.12.4.min.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://exchangerate.host/css/app.83d337b5.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.
URL	https://exchangerate.host/favicon-16x16.png
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://exchangerate.host/favicon-32x32.png
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://exchangerate.host/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://exchangerate.host/js/app-legacy.82d076da.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://exchangerate.host/js/app.9729c651.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://exchangerate.host/js/chunk-vendors-legacy.5ce3045d.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://exchangerate.host/js/chunk-vendors.596ac91f.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://exchangerate.host/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://exchangerate.host/site.webmanifest
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://exchangerate.host/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.
Instances	17
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 - 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://exchangerate.host/assets/js/bootstrap.min.js
Method	GET
Attack	
Evidence	from
Other	The following pattern was used: \bFROM\b and was detected in the element starting with: "!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require

Info	("jquery"),require("popper.js")):"function"", see evidence field for the suspicious comment /snippet.
URL	https://exchangerate.host/assets/js/vendor/jquery-1.12.4.min.js
Method	GET
Attack	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected 2 times, the first in the element starting with: "}return c}function Q(a){var b;for(b in a)if(("data"!==b||!n.isEmptyObject(a[b]))&&"toJSON"!==b)return!1;return!0}function R(a,b,", see evidence field for the suspicious comment/snippet.
URL	https://exchangerate.host/assets/js/vendor/jquery-1.12.4.min.js
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.docu", see evidence field for the suspicious comment/snippet.
URL	https://exchangerate.host/js/app-legacy.82d076da.js
Method	GET
Attack	
Evidence	Bug
Other Info	The following pattern was used: \bBUG\b and was detected in the element starting with: "(function(){"use strict";var t={5308:function(t,e,a){a(7726),a(3473),a(2151),a(1286);var s=a(538),o=function(){var t=this,e=t._s", see evidence field for the suspicious comment/snippet.
URL	https://exchangerate.host/js/app.9729c651.js
Method	GET
Attack	
Evidence	Bug
Other Info	The following pattern was used: \bBUG\b and was detected in the element starting with: "(function(){"use strict";var t={5308:function(t,e,a){var s=a(538),o=function(){var t=this,e=t._self._c;return e("div",{attrs:{id", see evidence field for the suspicious comment/snippet.
URL	https://exchangerate.host/js/chunk-vendors-legacy.5ce3045d.js
Method	GET
Attack	
Evidence	bugs
Other Info	The following pattern was used: \bBUGS\b and was detected in the element starting with: "var r=Object.freeze({}),i=Array.isArray;function o(t){return void 0===t||null===t}function a(t){return void 0!==t&&null!==t}func", see evidence field for the suspicious comment/snippet.
URL	https://exchangerate.host/js/chunk-vendors-legacy.5ce3045d.js
Method	GET
Attack	
Evidence	FROM
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: " INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM", see evidence field for the suspicious comment/snippet.
URL	https://exchangerate.host/js/chunk-vendors-legacy.5ce3045d.js

Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "(function(e,r){"object"===i(n)?t.exports=r():e.moment=r()})(e,(function(){var e,n;function o(){return e.apply(null,arguments)}fu", see evidence field for the suspicious comment/snippet.
URL	https://exchangerate.host/js/chunk-vendors-legacy.5ce3045d.js
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in the element starting with: " */t.exports&&(t.exports=i),"undefined"!==typeof n.g&&(n.g.Prism=i),i.languages.markup={comment:{pattern:/<!--(?:(?!<!--)[\s\S])", see evidence field for the suspicious comment/snippet.
URL	https://exchangerate.host/js/chunk-vendors-legacy.5ce3045d.js
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "(self["webpackChunkexchangerate_host"]=self["webpackChunkexchangerate_host"]||[]).push([[998],{6934:function(t){t.exports=functi", see evidence field for the suspicious comment/snippet.
URL	https://exchangerate.host/js/chunk-vendors.596ac91f.js
Method	GET
Attack	
Evidence	bugs
Other Info	The following pattern was used: \bBUGS\b and was detected in the element starting with: "var r=Object.freeze({}),i=Array.isArray;function o(t){return void 0===t||null===t}function a(t){return void 0!==t&&null!==t}func", see evidence field for the suspicious comment/snippet.
URL	https://exchangerate.host/js/chunk-vendors.596ac91f.js
Method	GET
Attack	
Evidence	FROM
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: " INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM", see evidence field for the suspicious comment/snippet.
URL	https://exchangerate.host/js/chunk-vendors.596ac91f.js
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "(function(e,r){"object"===i(n)?t.exports=r():e.moment=r()})(e,(function(){var e,n;function o(){return e.apply(null,arguments)}fu", see evidence field for the suspicious comment/snippet.
URL	https://exchangerate.host/js/chunk-vendors.596ac91f.js
Method	GET
Attack	
Evidence	select

Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in the element starting with: " */t.exports&&(t.exports=i),"undefined"!==typeof n.g&&(n.g.Prism=i),i.languages.markup={comment:{pattern:/<!--(?:(?!<!--)[\s\S])", see evidence field for the suspicious comment/snippet.
URL	https://exchangerate.host/js/chunk-vendors.596ac91f.js
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "(self["webpackChunkexchangerate_host"]=self["webpackChunkexchangerate_host"]||[]).push([[998],{6934:function(t){t.exports=functi", see evidence field for the suspicious comment/snippet.
Instances	15
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	[200](200)
WASC Id	13
Plugin Id	[10027](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://exchangerate.host
Method	GET
Attack	
Evidence	<script>(function (w, d, s, l, i) { w[l] = w[l] || []; w[l].push({ 'gtm.start': new Date().getTime(), event: 'gtm.js' }); var f = d.getElementsByTagName(s)[0], j = d.createElement(s), dl = l != 'dataLayer' ? '&l=' + l : ''; j.async = true; j.src = 'https://www.googletagmanager.com/gtm.js?id=' + i + dl; f.parentNode.insertBefore(j, f); })(window, document, 'script', 'dataLayer', 'GTM-NT38NXL');</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://exchangerate.host/
Method	GET
Attack	
Evidence	<script>(function (w, d, s, l, i) { w[l] = w[l] || []; w[l].push({ 'gtm.start': new Date().getTime(), event: 'gtm.js' }); var f = d.getElementsByTagName(s)[0], j = d.createElement(s), dl = l != 'dataLayer' ? '&l=' + l : ''; j.async = true; j.src = 'https://www.googletagmanager.com/gtm.js?id=' + i + dl; f.parentNode.insertBefore(j, f); })(window, document, 'script', 'dataLayer', 'GTM-NT38NXL');</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://exchangerate.host/robots.txt
Method	GET
Attack	
Evidence	<script>(function (w, d, s, l, i) { w[l] = w[l] || []; w[l].push({ 'gtm.start': new Date().getTime(), event: 'gtm.js' }); var f = d.getElementsByTagName(s)[0], j = d.createElement(s), dl = l != 'dataLayer' ? '&l=' + l : ''; j.async = true; j.src = 'https://www.googletagmanager.com/gtm.js?id=' + i + dl; f.parentNode.insertBefore(j, f); })(window, document, 'script', 'dataLayer', 'GTM-NT38NXL');</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://exchangerate.host/sitemap.xml
Method	GET
Attack	
Evidence	<script>(function (w, d, s, l, i) { w[l] = w[l] || []; w[l].push({ 'gtm.start': new Date().getTime(), event: 'gtm.js' }); var f = d.getElementsByTagName(s)[0], j = d.createElement(s), dl = l != 'dataLayer' ? '&l=' + l : ''; j.async = true; j.src = 'https://www.googletagmanager.com/gtm.js?id=' + i + dl; f.parentNode.insertBefore(j, f); })(window, document, 'script', 'dataLayer', 'GTM-NT38NXL');</script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	4
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://exchangerate.host
Method	GET
Attack	
Evidence	public, max-age=0, must-revalidate
Other Info	
URL	https://exchangerate.host/
Method	GET
Attack	
Evidence	public, max-age=0, must-revalidate
Other Info	
URL	https://exchangerate.host/robots.txt
Method	GET
Attack	
Evidence	max-age=18000
Other Info	
URL	https://exchangerate.host/site.webmanifest
Method	GET
Attack	
Evidence	public, max-age=0, must-revalidate
Other	

Info	
URL	https://exchangerate.host/sitemap.xml
Method	GET
Attack	
Evidence	public, max-age=0, must-revalidate
Other Info	
Instances	5
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://exchangerate.host
Method	GET
Attack	
Evidence	Age: 19217123
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://exchangerate.host/
Method	GET
Attack	
Evidence	Age: 19217122
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://exchangerate.host/
Method	GET
Attack	
Evidence	Age: 19217123
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://exchangerate.host/site.webmanifest
Method	GET
Attack	

Evidence	Age: 19215518
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://exchangerate.host/sitemap.xml
Method	GET
Attack	
Evidence	Age: 19211134
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
Instances	5
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)](http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html)
CWE Id	
WASC Id	
Plugin Id	[10050](10050)

Informational	**User Agent Fuzzer**
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	https://exchangerate.host/js/app-legacy.82d076da.js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://exchangerate.host/js/app-legacy.82d076da.js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://exchangerate.host/js/app-legacy.82d076da.js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36

Evidence	
Other Info	
URL	https://exchangerate.host/js/app-legacy.82d076da.js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://exchangerate.host/js/app-legacy.82d076da.js
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://exchangerate.host/js/app-legacy.82d076da.js
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://exchangerate.host/js/app-legacy.82d076da.js
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://exchangerate.host/js/app-legacy.82d076da.js
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://exchangerate.host/js/app-legacy.82d076da.js
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://exchangerate.host/js/app.9729c651.js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	

Other Info	
URL	https://exchangerate.host/js/app.9729c651.js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://exchangerate.host/js/app.9729c651.js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://exchangerate.host/js/app.9729c651.js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://exchangerate.host/js/app.9729c651.js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://exchangerate.host/js/app.9729c651.js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://exchangerate.host/js/app.9729c651.js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://exchangerate.host/js/app.9729c651.js
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	

Other Info	
URL	https://exchangerate.host/js/app.9729c651.js
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://exchangerate.host/js/app.9729c651.js
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://exchangerate.host/js/app.9729c651.js
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://exchangerate.host/js/app.9729c651.js
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://exchangerate.host/js/chunk-vendors-legacy.5ce3045d.js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://exchangerate.host/js/chunk-vendors-legacy.5ce3045d.js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://exchangerate.host/js/chunk-vendors-legacy.5ce3045d.js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other	

Info	
URL	https://exchangerate.host/js/chunk-vendors-legacy.5ce3045d.js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://exchangerate.host/js/chunk-vendors-legacy.5ce3045d.js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://exchangerate.host/js/chunk-vendors-legacy.5ce3045d.js
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://exchangerate.host/js/chunk-vendors-legacy.5ce3045d.js
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://exchangerate.host/js/chunk-vendors-legacy.5ce3045d.js
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://exchangerate.host/js/chunk-vendors-legacy.5ce3045d.js
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://exchangerate.host/js/chunk-vendors.596ac91f.js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other	

Info	
URL	https://exchangerate.host/js/chunk-vendors.596ac91f.js
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://exchangerate.host/js/chunk-vendors.596ac91f.js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://exchangerate.host/js/chunk-vendors.596ac91f.js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://exchangerate.host/js/chunk-vendors.596ac91f.js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://exchangerate.host/js/chunk-vendors.596ac91f.js
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://exchangerate.host/js/chunk-vendors.596ac91f.js
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://exchangerate.host/js/chunk-vendors.596ac91f.js
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other	

Info	
URL	https://exchangerate.host/js/chunk-vendors.596ac91f.js
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://exchangerate.host/js/chunk-vendors.596ac91f.js
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	40
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104