admin-frontend-zap-proxy-Alerts

Sites: https://cdnjs.cloudflare.com https://api.nepcha.com http://localhost:8880 http://localhost:9991

Generated on Tue, 26 Mar 2024 21:46:21

ZAP Version: 2.14.0

ZAP is supported by the Crash Override Open Source Fellowship

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	3
Low	5
Informational	5
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
External Redirect	High	2
CSP: Wildcard Directive	Medium	1
Content Security Policy (CSP) Header Not Set	Medium	4
Missing Anti-clickjacking Header	Medium	2
Application Error Disclosure	Low	5
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	10
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	8
Strict-Transport-Security Header Not Set	Low	1
X-Content-Type-Options Header Missing	Low	9
Authentication Request Identified	Informational	6
Information Disclosure - Suspicious Comments	Informational	4
Modern Web Application	Informational	2
Retrieved from Cache	Informational	41
User Agent Fuzzer	Informational	14

Alert Detail

High	External Redirect
	URL redirectors represent common functionality employed by web sites to forward an incoming request to an alternate resource. This can be done for a variety of reasons and is

Description	often done to allow resources to be moved within the directory structure and to avoid breaking functionality for users that request the resource at its previous location. URL redirectors may also be used to implement load balancing, leveraging abbreviated URLs or recording outgoing links. It is this last implementation which is often used in phishing attacks as described in the example below. URL redirectors do not necessarily represent a direct security vulnerability but can be abused by attackers trying to social engineer victims into believing that they are navigating to a site other than the true destination.
URL	http://localhost:9991/assets
Method	GET
Attack	5513407466007019180.owasp.org
Evidence	5513407466007019180.owasp.org
Other Info	The response contains a redirect in its Location header which allows an external Url to be set.
URL	http://localhost:9991/img
Method	GET
Attack	5513407466007019180.owasp.org
Evidence	5513407466007019180.owasp.org
Other Info	The response contains a redirect in its Location header which allows an external Url to be set.
Instances	2
Solution	Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." Use an allow list of approved URLs or domains to be used for redirection. Use an intermediate disclaimer page that provides the user with a clear warning that they are leaving your site. Implement a long timeout before the redirect occurs, or force the user to click on the link. Be careful to avoid XSS problems when generating the disclaimer page. When the set of acceptable objects, such as filenames or URLs, is limited or known, create a mapping from a set of fixed input values (such as numeric IDs) to the actual filenames or URLs, and reject all other inputs. For example, ID 1 could map to "/login.asp" and ID 2 could map to "https://www.example.com/". Features such as the ESAPI AccessReferenceMap provide this capability. Understand all the potential areas where untrusted inputs can enter your software: parameters or arguments, cookies, anything read from the network, environment variables, reverse DNS lookups, query results, request headers, URL components, e-mail, files, databases, and any external systems that provide data to the application. Remember that such inputs may be obtained indirectly through API calls. Many open redirect problems occur because the programmer assumed that certain inputs could not be modified, such as cookies and hidden form fields.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/601.html
CWE Id	601

WASC Id	38
Plugin Id	20019

Medium	CSP: Wildcard Directive
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	http://localhost:8880/api/api/customers/$
Method	GET
Attack	
Evidence	default-src 'none'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	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	http://localhost:9991
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:9991/
Method	GET
Attack	
Evidence	
Other Info	

URL	http://localhost:9991/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:9991/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 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 include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
URL	http://localhost:9991
Method	GET
Attack	
Evidence	
Other Info	
URL	http://localhost:9991/
Method	GET
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	**Application Error Disclosure**
Description	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.
URL	http://localhost:8880/api/courses/$
Method	GET
Attack	
Evidence	HTTP/1.1 500 Internal Server Error
Other Info	
URL	http://localhost:8880/api/courses/create
Method	GET
Attack	
Evidence	HTTP/1.1 500 Internal Server Error
Other Info	
URL	http://localhost:8880/api/customers/$
Method	GET
Attack	
Evidence	HTTP/1.1 500 Internal Server Error
Other Info	
URL	http://localhost:8880/api/enrollment
Method	GET
Attack	
Evidence	HTTP/1.1 500 Internal Server Error
Other Info	
URL	http://localhost:8880/api/users/login
Method	POST
Attack	
Evidence	HTTP/1.1 500 Internal Server Error
Other Info	
Instances	5

Solution	Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.
Reference	
CWE Id	[200](200)
WASC Id	13
Plugin Id	[90022](90022)

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	http://localhost:8880/api/api/customers/$
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost:8880/api/courses
Method	GET
Attack	
Evidence	x-powered-by: Express
Other Info	
URL	http://localhost:8880/api/courses/$
Method	GET
Attack	
Evidence	x-powered-by: Express
Other Info	
URL	http://localhost:8880/api/courses/create
Method	GET
Attack	
Evidence	x-powered-by: Express
Other Info	
URL	http://localhost:8880/api/customers
Method	GET
Attack	
Evidence	x-powered-by: Express
Other Info	
URL	http://localhost:8880/api/customers/$
Method	GET
Attack	

Evidence	x-powered-by: Express
Other Info	
URL	http://localhost:8880/api/enrollment
Method	GET
Attack	
Evidence	x-powered-by: Express
Other Info	
URL	http://localhost:8880/api/users/login
Method	GET
Attack	
Evidence	x-powered-by: Express
Other Info	
URL	http://localhost:8880/api/users/login
Method	OPTIONS
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	http://localhost:8880/api/users/login
Method	POST
Attack	
Evidence	x-powered-by: Express
Other Info	
Instances	10
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10037

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	http://localhost:9991
Method	GET
Attack	
Evidence	nginx/1.25.4

Other Info	
URL	http://localhost:9991/
Method	GET
Attack	
Evidence	nginx/1.25.4
Other Info	
URL	http://localhost:9991/assets/index-f60dc4fb.js
Method	GET
Attack	
Evidence	nginx/1.25.4
Other Info	
URL	http://localhost:9991/assets/index-f63d4ef4.css
Method	GET
Attack	
Evidence	nginx/1.25.4
Other Info	
URL	http://localhost:9991/img/favicon.png
Method	GET
Attack	
Evidence	nginx/1.25.4
Other Info	
URL	http://localhost:9991/img/pattern.png
Method	GET
Attack	
Evidence	nginx/1.25.4
Other Info	
URL	http://localhost:9991/robots.txt
Method	GET
Attack	
Evidence	nginx/1.25.4
Other Info	
URL	http://localhost:9991/sitemap.xml
Method	GET
Attack	
Evidence	nginx/1.25.4
Other Info	

Instances	8
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	200
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://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	
Other Info	
Instances	1
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	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	http://localhost:8880/api/courses
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	http://localhost:8880/api/customers
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	http://localhost:8880/api/users/login
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	http://localhost:9991
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	http://localhost:9991/
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	http://localhost:9991/assets/index-f60dc4fb.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	http://localhost:9991/assets/index-f63d4ef4.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	http://localhost:9991/img/favicon.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	http://localhost:9991/img/pattern.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.
Instances	9
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	**Authentication Request Identified**
Description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	http://localhost:8880/api/users/login
Method	POST
Attack	
Evidence	password
Other Info	userParam=email userValue=RjXnHvOY passwordParam=password referer=http://localhost:9991/
URL	http://localhost:8880/api/users/login
Method	POST
Attack	
Evidence	password
Other Info	userParam=email userValue=RjXnHvOYGfYshwMq passwordParam=password referer=http://localhost:9991/
URL	http://localhost:8880/api/users/login
Method	POST
Attack	
Evidence	password
Other	userParam=email userValue=RjXnHvOYGfYshwMqnfctfBTU passwordParam=password

Info	referer=http://localhost:9991/
URL	http://localhost:8880/api/users/login
Method	POST
Attack	
Evidence	password
Other Info	userParam=email userValue=RjXnHvOYGfYshwMqnfctfBTUyOjChpcC passwordParam=password referer=http://localhost:9991/
URL	http://localhost:8880/api/users/login
Method	POST
Attack	
Evidence	password
Other Info	userParam=email userValue=RjXnHvOYGfYshwMqnfctfBTUyOjChpcCdLSHgwfN passwordParam=password referer=http://localhost:9991/
URL	http://localhost:8880/api/users/login
Method	POST
Attack	
Evidence	password
Other Info	userParam=email userValue=RjXnHvOYGfYshwMqnfctfBTUyOjChpcCdLSHgwfNKqDLrjes passwordParam=password referer=http://localhost:9991/
Instances	6
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

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	http://localhost:9991/assets/index-f60dc4fb.js
Method	GET
Attack	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected in the element starting with: "*/(function(e){(function(){var t={}.hasOwnProperty;function r(){for(var a=[],s=0;s<arguments.length;s++){var u=arguments[s];if(u", see evidence field for the suspicious comment/snippet.
URL	http://localhost:9991/assets/index-f60dc4fb.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 3 times, the first in the element starting with: " */function ll(){return ll=Object.assign?Object.assign.bind():function(e){for(var t=1;t<arguments.length;t++){var r=arguments[t]", see evidence field for the suspicious comment/snippet.
URL	http://localhost:9991/assets/index-f60dc4fb.js
Method	GET

Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 8 times, the first in the element starting with: "`+s[p].replace(" at new "," at ");return e.displayName&&S.includes("<anonymous>")&&(S=S.replace("<anonymous>",e.displayName)),S}", see evidence field for the suspicious comment/snippet.
URL	http://localhost:9991/assets/index-f60dc4fb.js
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: " user-select: none", see evidence field for the suspicious comment/snippet.
Instances	4
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	http://localhost:9991
Method	GET
Attack	
Evidence	<script defer data-site="YOUR_DOMAIN_HERE" src="https://api.nepcha.com/js/nepcha-analytics.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	http://localhost:9991/
Method	GET
Attack	
Evidence	<script defer data-site="YOUR_DOMAIN_HERE" src="https://api.nepcha.com/js/nepcha-analytics.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	2
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**Retrieved from Cache**
	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,

Description	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://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 2782
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 2785
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 2789
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 2791
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 2797
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 2801
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 2804

Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 2808
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 2813
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 2817
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 2819
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 4138
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 4141
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 4145
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.

URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 4147
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 4151
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 4153
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 4155
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 4157
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 4160
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 4164
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET

Attack	
Evidence	Age: 4166
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 4169
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 4173
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 4175
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://api.nepcha.com/js/nepcha-analytics.js
Method	GET
Attack	
Evidence	Age: 4177
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.2.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 343494
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.2.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 343497
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.2.0/css/all.min.css
Method	GET
Attack	

Evidence	Age: 343501
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.2.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 343503
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.2.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 343507
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.2.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 343509
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.2.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 343511
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.2.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 343513
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.2.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 343516
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.2.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 343520
Other	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is

Info	in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.2.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 343522
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.2.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 343525
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.2.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 343529
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.2.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 343531
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.2.0/css/all.min.css
Method	GET
Attack	
Evidence	Age: 343534
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
Instances	41
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	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	http://localhost:9991/robots.txt
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:9991/robots.txt
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:9991/robots.txt
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:9991/robots.txt
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:9991/robots.txt
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	http://localhost:9991/robots.txt
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	http://localhost:9991/robots.txt

Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://localhost:9991/sitemap.xml
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://localhost:9991/sitemap.xml
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://localhost:9991/sitemap.xml
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://localhost:9991/sitemap.xml
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://localhost:9991/sitemap.xml
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	http://localhost:9991/sitemap.xml
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	http://localhost:9991/sitemap.xml

Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	14
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104