ZAP by Checkmarx Scanning Report

Site: http://127.0.0.1:8000

Generated on Wed, 4 Dec 2024 11:49:50

ZAP Version: 2.15.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	4
Informational	5

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	4
Missing Anti-clickjacking Header	Medium	2
Vulnerable JS Library	Medium	1
Big Redirect Detected (Potential Sensitive Information Leak)	Low	2
Cookie No HttpOnly Flag	Low	3
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	5
X-Content-Type-Options Header Missing	Low	15
Authentication Request Identified	Informational	1
Information Disclosure - Suspicious Comments	Informational	5
Modern Web Application	Informational	2
Session Management Response Identified	Informational	33
User Agent Fuzzer	Informational	24

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	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:8000/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:8000/storage/default.jpg
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 protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	http://127.0.0.1:8000/
Method	GET

Attack	
Evidence	
Other Info	
URL	http://127.0.0.1:8000/login
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

Medium	**Vulnerable JS Library**
Description	The identified library jquery, version 3.4.1 is vulnerable.
URL	http://127.0.0.1:8000/app-assets/vendors/js/vendors.min.js
Method	GET
Attack	
Evidence	/*! jQuery v3.4.1
Other Info	CVE-2020-11023 CVE-2020-11022
Instances	1
Solution	Please upgrade to the latest version of jquery.
Reference	https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
CWE Id	829
WASC Id	
Plugin Id	10003

Low	**Big Redirect Detected (Potential Sensitive Information Leak)**
Description	The server has responded with a redirect that seems to provide a large response. This may indicate that although the server sent a redirect it also responded with body content (which may include sensitive details, PII, etc.).
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	
Other Info	Location header URI length: 27 [http://127.0.0.1:8000/login]. Predicted response size: 327. Response Body Length: 354.

URL	http://127.0.0.1:8000/login
Method	POST
Attack	
Evidence	
Other Info	Location header URI length: 27 [http://127.0.0.1:8000/login]. Predicted response size: 327. Response Body Length: 354.
Instances	2
Solution	Ensure that no sensitive information is leaked via redirect responses. Redirect responses should have almost no content.
Reference	
CWE Id	201
WASC Id	13
Plugin Id	10044

Low	**Cookie No HttpOnly Flag**
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://127.0.0.1:8000/login
Method	POST
Attack	
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
Instances	3
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

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://127.0.0.1:8000/
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.2.12
Other Info	
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.2.12
Other Info	
URL	http://127.0.0.1:8000/sitemap.xml
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.2.12
Other Info	
URL	http://127.0.0.1:8000/storage/default.jpg
Method	GET
Attack	
Evidence	X-Powered-By: PHP/8.2.12
Other Info	
URL	http://127.0.0.1:8000/login
Method	POST
Attack	
Evidence	X-Powered-By: PHP/8.2.12
Other Info	
Instances	5
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	**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://127.0.0.1:8000/
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://127.0.0.1:8000/app-assets/css/bootstrap-extended.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://127.0.0.1:8000/app-assets/css/bootstrap.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://127.0.0.1:8000/app-assets/css/colors.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://127.0.0.1:8000/app-assets/css/components.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://127.0.0.1:8000/app-assets/css/core/colors/palette-gradient.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://127.0.0.1:8000/app-assets/css/core/menu/menu-types/vertical-menu.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://127.0.0.1:8000/app-assets/css/pages/authentication.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://127.0.0.1:8000/app-assets/fonts/feather/fonts/feather.woff?t=1525787366991
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://127.0.0.1:8000/app-assets/images/pages/vuexy-login-bg.jpg
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://127.0.0.1:8000/app-assets/vendors/css/vendors.min.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://127.0.0.1:8000/app-assets/vendors/js/vendors.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	http://127.0.0.1:8000/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://127.0.0.1:8000/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	http://127.0.0.1:8000/storage/logos/bufuwpV4IeWCycFhqug6T4Hac5Jv29U77KyayeN4.jpg
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	15
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://127.0.0.1:8000/login
Method	POST
Attack	
Evidence	password

Other Info	userParam=email userValue=zaproxy@example.com passwordParam=password referer=http://127.0.0.1:8000/login csrfToken=_token
Instances	1
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://127.0.0.1:8000/app-assets/vendors/js/vendors.min.js
Method	GET
Attack	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected in the element starting with: "!function(a,b,c,d){"use strict";function e(a,b,c){return setTimeout(j(a,c),b)}function f(a,b,c){return Array.isArray(a)?(g(a,c[b", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:8000/app-assets/vendors/js/vendors.min.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 2 times, the first in the element starting with: " !function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require("jquery"),require("popper.js")):"function", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:8000/app-assets/vendors/js/vendors.min.js
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: " * Requires jQuery v1.7 or later", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:8000/app-assets/vendors/js/vendors.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(t,e){"object"==typeof exports&&"undefined"!=typeof module?module.exports=e():"function"==typeof define&&define.amd?def", see evidence field for the suspicious comment/snippet.
URL	http://127.0.0.1:8000/app-assets/vendors/js/vendors.min.js
Method	GET
Attack	
Evidence	username
Other	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?

Info	module.exports=e.document?t(e,!0):function(", see evidence field for the suspicious comment/snippet.
Instances	5
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://127.0.0.1:8000/
Method	GET
Attack	
Evidence	<script src="/app-assets/vendors/js/vendors.min.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://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	<script src="/app-assets/vendors/js/vendors.min.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	**Session Management Response Identified**
Description	The given response has been identified as containing a session management token. The 'Other
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	eyJpdiI6IkMvSmZWVkgySG5CYlMydXd2dVM2WlE9PSIsInZhbHVlIjoiVG04aHRpZElKb3VzZzR
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	eyJpdiI6IlJ6NzliMWtadXJMbHh5SVoreUtBTmc9PSIsInZhbHVlIjoiUTFNYXA2ajRxUHVTTXgwcn
Other Info	cookie:laravel_session cookie:XSRF-TOKEN

URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	eyJpdiI6IlcweGVWWW8vaEt0LzFBMlMySXFpRlE9PSIsInZhbHVlIjoiWXF4RU9NZVJvMCtqQm
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	eyJpdiI6IlhwdGI0aG1zVVFhWHpZV0VNVkJheUE9PSIsInZhbHVlIjoibXFFWVMvN3J5ZTRWdW
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	eyJpdiI6IlplUXdyU2tRbDhnaDkzaVVGR0FMUlE9PSIsInZhbHVlIjoiTUJUU0tEUUovcnpmd2w0Z
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	eyJpdiI6InBUcTBNRWVqb2VZV29neVdmS0Q2S0E9PSIsInZhbHVlIjoicTUxTnEvb1JGRVg1dXZ
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	eyJpdiI6InZvUXZMVm5YUXhBTnp1WmRRQzVrTEE9PSIsInZhbHVlIjoiY3RLSzRJSUhubjU1elF
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	eyJpdiI6InlJYmlUc0paZnEvMlFQeW9EY3BwQlE9PSIsInZhbHVlIjoiZVBkR2ZYSjl6dDdJaE9DbF
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/
Method	GET
Attack	
Evidence	eyJpdiI6InlVT1FvQk8veGlFUW0vSVFNY1U0UkE9PSIsInZhbHVlIjoiRTdDRUtYaVdGNkpMaUly
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Method	GET

Attack	
Evidence	eyJpdiI6IjJhR3FVTGR1YzBEWVd6Vm9ZSGVRV3c9PSIsInZhbHVlIjoiRTBoM3NqUUtTaElpZUI
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	eyJpdiI6Ik55aFhwRWNXUDlaS2w3L3d1b3BlRlE9PSIsInZhbHVlIjoieXpJMTVtSnJDWWx2OEp4
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	eyJpdiI6IkNZOHd0OGs2TFJLMCtjeGNPOU5XNnc9PSIsInZhbHVlIjoiUWQ2Uk1qK1U3UDErMn
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	eyJpdiI6Ikw1WDFmdzNUNXVEQktnSnp5MSsvcnc9PSIsInZhbHVlIjoib1JXVnJ6ZG9pNTgxVmx
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	eyJpdiI6IlAxTWFjenBDQXI0bHpCUWtxVXNEcWc9PSIsInZhbHVlIjoiWHJ4UWNZTm0zUXN6Sn
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	eyJpdiI6IlBqVVVWL3Jodk9iL0pDQnJxMDNwdmc9PSIsInZhbHVlIjoiemhBeHJvN1JvaVc5YkFZb
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	eyJpdiI6IlI1UE1XTWNPSWFUQVdHazJ1Y3JkTFE9PSIsInZhbHVlIjoiM1F4RFFQVVJmdmtVMF
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Method	GET
Attack	

Evidence	eyJpdiI6IlNPbkFVTlFScEdOR3hDTkRRaW9STkE9PSIsInZhbHVlIjoiOXZkYTJsbjNSdVlBbEdiO
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	eyJpdiI6IlhIR09HTG1GUlRhMEJ4RUIxeTVwSVE9PSIsInZhbHVlIjoiZWNFOVZiSGMvSEVTL21
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	eyJpdiI6ImhCdEtQdDl1VWwrODlJcHM4c1FpVUE9PSIsInZhbHVlIjoiV2dIOXJZT29FeHRyYis3e
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	eyJpdiI6InB5Wk83c0FTZC9YRzNKMHBST0hNQnc9PSIsInZhbHVlIjoiSFU5OE9aTnVlVmxIQXJ
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	eyJpdiI6InNGZmpTQWdtQlJVL29RV3hiL0ZMN0E9PSIsInZhbHVlIjoiZUlIY0M0WmhnV08xTmtw
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	eyJpdiI6InRDOHIwRElLVUUranp2aXU0MWNPcmc9PSIsInZhbHVlIjoiN3dBMkZmaVVuOWtDW
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	eyJpdiI6InlwaXhGeGFrc0ZHKzk0cGN3Z3VTZnc9PSIsInZhbHVlIjoid2p1eFBMNDdZczhYQWpE
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Method	POST
Attack	
Evidence	eyJpdiI6IlNteFVyby9pNTBFTnplS3BRenZyUEE9PSIsInZhbHVlIjoieitFMVBTSnFraC8reEkvL25E
Other	

Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Method	POST
Attack	
Evidence	eyJpdiI6ImtCR1hjd0QyeCt2RVBPalhSRThUbmc9PSIsInZhbHVlIjoiaE5YeHJ4NTdIcVFFdHNIO
Other Info	cookie:laravel_session cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	eyJpdiI6IkNZOHd0OGs2TFJLMCtjeGNPOU5XNnc9PSIsInZhbHVlIjoiUWQ2Uk1qK1U3UDErMr
Other Info	cookie:laravel_session
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	eyJpdiI6Ikw1WDFmdzNUNXVEQktnSnp5MSsvcnc9PSIsInZhbHVlIjoib1JXVnJ6ZG9pNTgxVmx
Other Info	cookie:laravel_session
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	eyJpdiI6IlI1UE1XTWNPSWFUQVdHazJ1Y3JkTFE9PSIsInZhbHVlIjoiM1F4RFFQVVJmdmtVMF
Other Info	cookie:laravel_session
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	eyJpdiI6InB5Wk83c0FTZC9YRzNKMHBST0hNQnc9PSIsInZhbHVlIjoiSFU5OE9aTnVlVmxIQXJ
Other Info	cookie:laravel_session
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	eyJpdiI6IjdMMDdWbGRPMzZiREJTT2VsNS9Rd2c9PSIsInZhbHVlIjoiVWJRZmVWWjkweU42Zj 3D
Other Info	cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	eyJpdiI6Ik9EY0xhSmhCTkxWaXJuakQxSVprUkE9PSIsInZhbHVlIjoiNmlyNVNsY2p6a3U3VWU
Other Info	cookie:XSRF-TOKEN

URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	eyJpdiI6ImcvOEtRYlhORVhCWGxFVnpYYW5VRHc9PSIsInZhbHVlIjoiaGVERkdOZkhQSXI1Mr
Other Info	cookie:XSRF-TOKEN
URL	http://127.0.0.1:8000/login
Method	GET
Attack	
Evidence	eyJpdiI6Imh6a1NRS0xFSC94ODgwSjR6ZGhaa2c9PSIsInZhbHVlIjoianU5WmlUbVo1MWQrdk5
Other Info	cookie:XSRF-TOKEN
Instances	33
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id
CWE Id	
WASC Id	
Plugin Id	10112

Informational	**User 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://127.0.0.1:8000/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:8000/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:8000/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:8000/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	

Other Info	
URL	http://127.0.0.1:8000/
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	http://127.0.0.1:8000/
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	http://127.0.0.1:8000/
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://127.0.0.1:8000/
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:8000/
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:8000/
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://127.0.0.1:8000/
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://127.0.0.1:8000/
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://127.0.0.1:8000/login
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://127.0.0.1:8000/login
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://127.0.0.1:8000/login
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://127.0.0.1:8000/login
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://127.0.0.1:8000/login
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	http://127.0.0.1:8000/login
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	http://127.0.0.1:8000/login
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://127.0.0.1:8000/login
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://127.0.0.1:8000/login
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://127.0.0.1:8000/login
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://127.0.0.1:8000/login
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://127.0.0.1:8000/login
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	24
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	

Plugin Id	10104