cgust staging re-verify

Site: http://120.126.223.31

Generated on , 21 8 2026 18:24:26

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	3
Informational	2
False Positives:	0

	Risk Level	Number of Instances
Big Redirect Detected (Potential Sensitive Information Leak)	Low	4
Cookie No HttpOnly Flag	Low	14
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	38
Information Disclosure - Suspicious Comments	Informational	8
Session Management Response Identified	Informational	12

Alert Detail

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://120.126.223.31/login/dedicated_tutor
	POST
Evidence	
Other Info	Location header URI length: 43 [http://120.126.223.31/login/dedicated_tutor]. Predicted response size: 343. Response Body Length: 418.
URL	http://120.126.223.31/login/manager

	POST
Evidence	
Other Info	Location header URI length: 35 [http://120.126.223.31/login/manager]. Predicted response size: 335. Response Body Length: 386.
URL	http://120.126.223.31/login/mentor
	POST
Evidence	
Other Info	Location header URI length: 34 [http://120.126.223.31/login/mentor]. Predicted response size: 334. Response Body Length: 382.
URL	http://120.126.223.31/login/student
	POST
Evidence	
Other Info	Location header URI length: 35 [http://120.126.223.31/login/student]. Predicted response size: 335. Response Body Length: 386.
Instances	4
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://120.126.223.31
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://120.126.223.31/
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://120.126.223.31/captcha/flat?fsrHbg2F
	GET
Evidence	Set-Cookie: XSRF-TOKEN

Other Info	
URL	http://120.126.223.31/captcha/flat?iZcZFFZl
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://120.126.223.31/captcha/flat?L5qnkw3Y
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://120.126.223.31/captcha/flat?x42GjZTt
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://120.126.223.31/login/dedicated_tutor
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://120.126.223.31/login/manager
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://120.126.223.31/login/mentor
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://120.126.223.31/login/student
	GET
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	

URL	http://120.126.223.31/login/dedicated_tutor
	POST
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://120.126.223.31/login/manager
	POST
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://120.126.223.31/login/mentor
	POST
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
URL	http://120.126.223.31/login/student
	POST
Evidence	Set-Cookie: XSRF-TOKEN
Other Info	
Instances	14
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 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://120.126.223.31
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26

Other Info	
URL	http://120.126.223.31/captcha/flat?fsrHbg2F
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/captcha/flat?iZcZFFZl
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/captcha/flat?L5qnkw3Y
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/captcha/flat?x42GjZTt
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/css/fontawesome/6.2.0/fontawesome.free.css
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/css/jquery.tagsinput-revisited.css
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/css/theme/frontend/style.min.css
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	

URL	http://120.126.223.31/css/theme/sidebar/bootstrap/5.1.3/bootstrap.min.css
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/images/cgust-logo-sm.png
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/images/login-image.jpg
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/js/frontent-layout.js
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/js/jquery.tagsinput-revisited.js
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/js/jquery/jquery-3.5.1.min.js
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/js/theme/sidebar/bootstrap/5.1.3/bootstrap.bundle.min.js
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/js/theme/sidebar/sidebar.js

	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/login/dedicated_tutor
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/login/manager
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/login/mentor
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/login/student
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/modules/custom/css/alert.css
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/modules/custom/css/loading-cover.css
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/modules/custom/js/alert/alert.js
	GET

Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/modules/custom/js/alert/alert.precompiled.js
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/modules/custom/js/checkbox-group-required.js
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/modules/custom/js/loading-cover.js
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/modules/user/css/login.css
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/modules/user/js/login.js
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/robots.txt
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/sitemap.xml
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26

Other Info	
URL	http://120.126.223.31/vendor/handlebars/4.7.9/handlebars.runtime.min.js
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/vendor/select2/4.1.0-rc.0/css/select2.min.css
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/vendor/select2/4.1.0-rc.0/js/select2.min.js
	GET
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/login/dedicated_tutor
	POST
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/login/manager
	POST
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/login/mentor
	POST
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	
URL	http://120.126.223.31/login/student
	POST
Evidence	Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/8.1.26
Other Info	

Instances	38
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	497
WASC Id	13
Plugin Id	10036

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker.
URL	http://120.126.223.31/js/jquery.tagsinput-revisited.js
	GET
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "// If a user types a delimiter create a new tag", see evidence field for the suspicious comment/snippet.
URL	http://120.126.223.31/js/jquery/jquery-3.5.1.min.js
	GET
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in likely comment: "//, Rt={},Mt={},It="*/".concat("*"),Wt=E.createElement("a");function Ft(o){return function(e,t) {"string"!=typeof e&&(t=e,e="*");v", see evidence field for the suspicious comment/snippet.
URL	http://120.126.223.31/js/theme/sidebar/bootstrap/5.1.3/bootstrap.bundle.min.js
	GET
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "//popper.js.org)"); let e = this._element; "parent" === this._config.reference ? e = t : o(this._config.reference) ? e = r(this.", see evidence field for the suspicious comment/snippet.
URL	http://120.126.223.31/login/dedicated_tutor
	GET
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//120.126.223.31/modules/user/js/login.js"></script>", see evidence field for the suspicious comment/snippet.
URL	http://120.126.223.31/login/manager
	GET
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//120.126.223.31/modules/user/js/login.js"></script>", see evidence field for the suspicious comment/snippet.
URL	http://120.126.223.31/login/mentor

	GET
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//120.126.223.31/modules/user/js/login.js"></script>", see evidence field for the suspicious comment/snippet.
URL	http://120.126.223.31/login/student
	GET
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//120.126.223.31/modules/user/js/login.js"></script>", see evidence field for the suspicious comment/snippet.
URL	http://120.126.223.31/vendor/handlebars/4.7.9/handlebars.runtime.min.js
	GET
Evidence	FROM
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "/**! @license handlebars v4.7.9 Copyright (C) 2011-2019 by Yehuda Katz Permission is hereby granted, free of charge, to any", see evidence field for the suspicious comment/snippet.
Instances	8
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	615
WASC Id	13
Plugin Id	10027

Informational	**Session Management Response Identified**
Description	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	http://120.126.223.31
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	http://120.126.223.31/
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	http://120.126.223.31/login/dedicated_tutor

	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	http://120.126.223.31/login/manager
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	http://120.126.223.31/login/mentor
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	http://120.126.223.31/login/student
	GET
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	http://120.126.223.31/login/dedicated_tutor
	POST
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	http://120.126.223.31/login/manager
	POST
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	http://120.126.223.31/login/mentor
	POST
Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	http://120.126.223.31/login/student
	POST

Evidence	_session
Other Info	cookie:_session cookie:XSRF-TOKEN
URL	http://120.126.223.31/login/dedicated_tutor
	POST
Evidence	_session
Other Info	cookie:_session
URL	http://120.126.223.31/login/dedicated_tutor
	POST
Evidence	XSRF-TOKEN
Other Info	cookie:XSRF-TOKEN
Instances	12
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