Vulture Scan Report

Site: https://google-gruyere.appspot.com /3974280751157544293332683230779587133 88/

Generated on Sun, 7 Apr 2024 02:36:33

ZAP Version: 2.14.0

ZAP is supported by the Crash Override Open Source Fellowship

Summary of Alerts

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

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	15
Big Redirect Detected (Potential Sensitive Information Leak)	Low	2
Cookie No HttpOnly Flag	Low	2
Strict-Transport-Security Header Not Set	Low	16
X-Content-Type-Options Header Missing	Low	16
Information Disclosure - Suspicious Comments	Informational	1

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://google-gruyere.appspot.com/3974280751157544293332683230779587133 88/
Method	GET
Attack	
Evidence	
Other	

Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/editprofile.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/login
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/login?pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/logout
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/newaccount.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/newsnippet.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	

Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/saveprofile?action=update&color=%23ffffff&icon=ZAP&name=ZAP&oldpw=ZAP&private_snippet&pw=ZAP&web_site=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/snippets.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/snippets.gtl?uid=brie
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/snippets.gtl?uid=cheddar
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/upload.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/upload2
Method	POST

Attack	
Evidence	
Other Info	
Instances	15
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

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	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/newsnippet2?snippet
Method	GET
Attack	
Evidence	
Other Info	Location header URI length: 87 [https://google-gruyere.appspot.com/397428075115754429333268323077958713388/snippets.gtl]. Predicted response size: 387. Response Body Length: 2,436.
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/newsnippet2?snippet
Method	GET
Attack	
Evidence	
Other Info	Location header URI length: 87 [https://google-gruyere.appspot.com/397428075115754429333268323077958713388/snippets.gtl]. Predicted response size: 387. Response Body Length: 2,793.
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	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/login?pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	Set-Cookie: GRUYERE
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/logout
Method	GET
Attack	
Evidence	Set-Cookie: GRUYERE
Other Info	
Instances	2
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	**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://google-gruyere.appspot.com/397428075115754429333268323077958713388/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/editprofile.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/lib.js
Method	GET
Attack	
Evidence	
Other	

Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/login
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/login?pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/logout
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/newaccount.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/newsnippet.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/saveprofile?action=update&color=%23ffffff&icon=ZAP&name=ZAP&oldpw=ZAP&private_snippet&pw=ZAP&web_site=ZAP
Method	GET
Attack	

Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/snippets.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/snippets.gtl?uid=brie
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/snippets.gtl?uid=cheddar
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/upload.gtl
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/ZAP
Method	GET
Attack	
Evidence	
Other Info	
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/upload2
Method	POST
Attack	
Evidence	
Other Info	
Instances	16
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers 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	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/
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://google-gruyere.appspot.com/397428075115754429333268323077958713388/editprofile.gtl
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://google-gruyere.appspot.com/397428075115754429333268323077958713388/lib.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://google-gruyere.appspot.com/397428075115754429333268323077958713388/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	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/login?pw=ZAP&uid=ZAP

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://google-gruyere.appspot.com/397428075115754429333268323077958713388/logout
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://google-gruyere.appspot.com/397428075115754429333268323077958713388/newaccount.gtl
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://google-gruyere.appspot.com/397428075115754429333268323077958713388/newsnippet.gtl
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://google-gruyere.appspot.com/397428075115754429333268323077958713388/saveprofile?action=new&is_author=True&pw=ZAP&uid=ZAP
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://google-gruyere.appspot.com/397428075115754429333268323077958713388/saveprofile?action=update&color=%23ffffff&icon=ZAP&name=ZAP&oldpw=ZAP&private_snippet&pw=ZAP&web_site=ZAP
Method	GET
Attack	
Evidence	
Other	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

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://google-gruyere.appspot.com/397428075115754429333268323077958713388/snippets.gtl
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://google-gruyere.appspot.com/397428075115754429333268323077958713388/snippets.gtl?uid=brie
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://google-gruyere.appspot.com/397428075115754429333268323077958713388/snippets.gtl?uid=cheddar
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://google-gruyere.appspot.com/397428075115754429333268323077958713388/upload.gtl
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://google-gruyere.appspot.com/397428075115754429333268323077958713388/ZAP
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://google-gruyere.appspot.com/397428075115754429333268323077958713388/upload2
Method	POST
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	16
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	**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://google-gruyere.appspot.com/397428075115754429333268323077958713388/lib.js
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: " * Processes refresh response {'private_snippet':snippet, user:snippet, ...}", see evidence field for the suspicious comment/snippet.
Instances	1
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