ZAP Scanning Report - https://moeachat.petercpg.info/

Automated report generated by OWASP ZAP Automation Framework

Site: https://moeachat.petercpg.info

Generated on Tue, 10 Nov 2026 08:24:40

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	2
Informational	4
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
CSP: Failure to Define Directive with No Fallback	Medium	2
CSP: Wildcard Directive	Medium	2
CSP: script-src unsafe-hashes	Medium	2
CSP: style-src unsafe-inline	Medium	4
Strict-Transport-Security Header Not Set	Low	Systemic
X-Content-Type-Options Header Missing	Low	1
CSP: Header & Meta	Informational	2
Modern Web Application	Informational	2
Re-examine Cache-control Directives	Informational	4
Retrieved from Cache	Informational	Systemic

Alert Detail

Medium	CSP: Failure to Define Directive with No Fallback
Description	The Content Security Policy fails to define one of the directives that has no fallback. Missing /excluding them is the same as allowing anything.
URL	https://moeachat.petercpg.info/
Node	

Name	https://moeachat.petercpg.info/
Method	GET
Attack	
Evidence	script-src 'self'
Other Info	The directive(s): form-action is/are among the directives that do not fallback to default-src.
URL	https://moeachat.petercpg.info/sitemap.xml
Node Name	https://moeachat.petercpg.info/sitemap.xml
Method	GET
Attack	
Evidence	script-src 'self'
Other Info	The directive(s): form-action is/are among the directives that do not fallback to default-src.
Instances	2
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://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

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	https://moeachat.petercpg.info/
Node Name	https://moeachat.petercpg.info/
Method	GET
Attack	
Evidence	script-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src
URL	https://moeachat.petercpg.info/sitemap.xml
Node Name	https://moeachat.petercpg.info/sitemap.xml
Method	GET
Attack	
Evidence	script-src 'self'

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src
Instances	2
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://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	**CSP: script-src unsafe-hashes**
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	https://moeachat.petercpg.info/
Node Name	https://moeachat.petercpg.info/
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-hashes'; script-src-elem 'self' 'unsafe-hashes'; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:; frame-ancestors 'self'; form-action 'self';
Other Info	script-src includes unsafe-hashes, an attacker will be able to use any of the code covered by such hashes.
URL	https://moeachat.petercpg.info/sitemap.xml
Node Name	https://moeachat.petercpg.info/sitemap.xml
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-hashes'; script-src-elem 'self' 'unsafe-hashes'; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:; frame-ancestors 'self'; form-action 'self';
Other Info	script-src includes unsafe-hashes, an attacker will be able to use any of the code covered by such hashes.
Instances	2
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/CSP3/#unsafe-hashes-usage https://content-security-policy.com/examples/allow-inline-script/
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	CSP: style-src unsafe-inline
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	https://moeachat.petercpg.info/
Node Name	https://moeachat.petercpg.info/
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-hashes'; script-src-elem 'self' 'unsafe-hashes'; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:; frame-ancestors 'self'; form-action 'self';
Other Info	style-src includes unsafe-inline.
URL	https://moeachat.petercpg.info/
Node Name	https://moeachat.petercpg.info/
Method	GET
Attack	
Evidence	script-src 'self'
Other Info	style-src includes unsafe-inline.
URL	https://moeachat.petercpg.info/sitemap.xml
Node Name	https://moeachat.petercpg.info/sitemap.xml
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-hashes'; script-src-elem 'self' 'unsafe-hashes'; style-src 'self' 'unsafe-inline'; img-src 'self' data:; font-src 'self' data:; frame-ancestors 'self'; form-action 'self';
Other Info	style-src includes unsafe-inline.
URL	https://moeachat.petercpg.info/sitemap.xml
Node Name	https://moeachat.petercpg.info/sitemap.xml
Method	GET
Attack	
Evidence	script-src 'self'
Other Info	style-src includes unsafe-inline.
Instances	4
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy

Reference	https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

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://moeachat.petercpg.info/
Node Name	https://moeachat.petercpg.info/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://moeachat.petercpg.info/robots.txt
Node Name	https://moeachat.petercpg.info/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://moeachat.petercpg.info/static/icon_76x76.png
Node Name	https://moeachat.petercpg.info/static/icon_76x76.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://moeachat.petercpg.info/static/images/favicon/favicon-default-16x16.png
Node Name	https://moeachat.petercpg.info/static/images/favicon/favicon-default-16x16.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://moeachat.petercpg.info/static/images/favicon/favicon-default-24x24.png
Node Name	https://moeachat.petercpg.info/static/images/favicon/favicon-default-24x24.png

Method	GET
Attack	
Evidence	
Other Info	
Instances	Systemic
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://moeachat.petercpg.info/robots.txt
Node Name	https://moeachat.petercpg.info/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.
Instances	1
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	**CSP: Header & Meta**

Description	The message contained both CSP specified via header and via Meta tag. It was not possible to union these policies in order to perform an analysis. Therefore, they have been evaluated individually.
URL	https://moeachat.petercpg.info/
Node Name	https://moeachat.petercpg.info/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://moeachat.petercpg.info/sitemap.xml
Node Name	https://moeachat.petercpg.info/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	2
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://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Informational	**Modern Web Application**
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	https://moeachat.petercpg.info/
Node Name	https://moeachat.petercpg.info/
Method	GET
Attack	
Evidence	<script id="publicPathInWindowScript"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://moeachat.petercpg.info/sitemap.xml
Node Name	https://moeachat.petercpg.info/sitemap.xml
Method	GET
Attack	
Evidence	<script id="publicPathInWindowScript"></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	**Re-examine Cache-control Directives**
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://moeachat.petercpg.info/
Node Name	https://moeachat.petercpg.info/
Method	GET
Attack	
Evidence	no-cache, max-age=31556926, public
Other Info	
URL	https://moeachat.petercpg.info/robots.txt
Node Name	https://moeachat.petercpg.info/robots.txt
Method	GET
Attack	
Evidence	max-age=432000
Other Info	
URL	https://moeachat.petercpg.info/sitemap.xml
Node Name	https://moeachat.petercpg.info/sitemap.xml
Method	GET
Attack	
Evidence	no-cache, max-age=31556926, public
Other Info	
URL	https://moeachat.petercpg.info/static/manifest.json
Node Name	https://moeachat.petercpg.info/static/manifest.json
Method	GET
Attack	
Evidence	max-age=31556926, public
Other Info	
Instances	4

Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

Informational	**Retrieved from Cache**
Description	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	https://moeachat.petercpg.info/robots.txt
Node Name	https://moeachat.petercpg.info/robots.txt
Method	GET
Attack	
Evidence	Age: 6281
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://moeachat.petercpg.info/static/icon_76x76.png
Node Name	https://moeachat.petercpg.info/static/icon_76x76.png
Method	GET
Attack	
Evidence	Age: 11082
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://moeachat.petercpg.info/static/images/favicon/favicon-default-16x16.png
Node Name	https://moeachat.petercpg.info/static/images/favicon/favicon-default-16x16.png
Method	GET
Attack	
Evidence	Age: 11081
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://moeachat.petercpg.info/static/images/favicon/favicon-default-24x24.png
Node Name	https://moeachat.petercpg.info/static/images/favicon/favicon-default-24x24.png
Method	GET
Attack	
Evidence	Age: 11082

Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://moeachat.petercpg.info/static/images/favicon/favicon-default-96x96.png
Node Name	https://moeachat.petercpg.info/static/images/favicon/favicon-default-96x96.png
Method	GET
Attack	
Evidence	Age: 11082
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
Instances	Systemic
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://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.rfc-editor.org/rfc/rfc9110.html
CWE Id	525
WASC Id	
Plugin Id	10050