ZAP by Checkmarx ZAP Scanning Report

Sites: http://example.com https://firefox.settings.services.mozilla.com https://content-signature-2.cdn.mozilla.net https://firefox-settings-attachments.cdn.mozilla.net https://example.com http://testphp.vulnweb.com

Generated on Wed, 11 Feb 2026 08:39:22

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	7
Informational	6
False Positives:	0

Insights

Level	Reason	Site	Description	Statistic
Low	Warning		ZAP errors logged - see the zap.log file for details	1
Low	Warning		ZAP warnings logged - see the zap.log file for details	12
Info	Informational		Percentage of network failures	1 %
Info	Informational	http://example.com	Percentage of responses with status code 2xx	100 %
Info	Informational	http://example.com	Percentage of endpoints with content type text/html	100 %
Info	Informational	http://example.com	Percentage of endpoints with method GET	100 %
Info	Informational	http://example.com	Count of total endpoints	1
Info	Informational	http://example.com	Percentage of slow responses	100 %
Info	Informational	http://testphp.vulnweb.com	Percentage of responses with status code 2xx	92 %

Info	Informational	http://testphp.vulnweb.com	Percentage of responses with status code 3xx	2 %
Info	Informational	http://testphp.vulnweb.com	Percentage of responses with status code 4xx	4 %
Info	Informational	http://testphp.vulnweb.com	Percentage of endpoints with content type application/x-shockwave-flash	2 %
Info	Informational	http://testphp.vulnweb.com	Percentage of endpoints with content type image/gif	4 %
Info	Informational	http://testphp.vulnweb.com	Percentage of endpoints with content type image/jpeg	10 %
Info	Informational	http://testphp.vulnweb.com	Percentage of endpoints with content type text/css	6 %
Info	Informational	http://testphp.vulnweb.com	Percentage of endpoints with content type text/html	77 %
Info	Informational	http://testphp.vulnweb.com	Percentage of endpoints with method GET	89 %
Info	Informational	http://testphp.vulnweb.com	Percentage of endpoints with method POST	10 %
Info	Informational	http://testphp.vulnweb.com	Count of total endpoints	48
Info	Informational	http://testphp.vulnweb.com	Percentage of slow responses	100 %
Info	Informational	https://content-signature-2.cdn.mozilla.net	Percentage of responses with status code 2xx	100 %
Info	Informational	https://content-signature-2.cdn.mozilla.net	Percentage of endpoints with content type binary/octet-stream	100 %
Info	Informational	https://content-signature-2.cdn.mozilla.net	Percentage of endpoints with method GET	100 %
Info	Informational	https://content-signature-2.cdn.mozilla.net	Count of total endpoints	1
Info	Informational	https://content-signature-2.cdn.mozilla.net	Percentage of slow responses	100 %
Info	Informational	https://example.com	Percentage of responses with status code 2xx	20 %
Info	Informational	https://example.com	Percentage of responses with status code 4xx	79 %
Info	Informational	https://example.com	Percentage of endpoints with content type text/html	100 %
Info	Informational	https://example.com	Percentage of endpoints with method GET	100 %
Info	Informational	https://example.com	Count of total endpoints	4
Info	Informational	https://example.com	Percentage of slow responses	96 %
Info	Informational	https://firefox-settings-attachments.cdn.mozilla.net	Percentage of responses with status code 2xx	100 %
Info	Informational	https://firefox-settings-attachments.cdn.mozilla.net	Percentage of endpoints with content type application/octet-stream	100 %
Info	Informational	https://firefox-settings-attachments.cdn.mozilla.net	Percentage of endpoints with method GET	100 %

Info	Informational	https://firefox-settings-attachments.cdn.mozilla.net	Count of total endpoints	1
Info	Informational	https://firefox-settings-attachments.cdn.mozilla.net	Percentage of slow responses	100 %
Info	Informational	https://firefox.settings.services.mozilla.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://firefox.settings.services.mozilla.com	Percentage of endpoints with content type application/json	100 %
Info	Informational	https://firefox.settings.services.mozilla.com	Percentage of endpoints with method GET	100 %
Info	Informational	https://firefox.settings.services.mozilla.com	Count of total endpoints	1
Info	Informational	https://firefox.settings.services.mozilla.com	Percentage of slow responses	100 %

Summary of Sequences

For each step: result (Pass/Fail) - risk (of highest alert(s) for the step, if any).

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	Systemic
Content Security Policy (CSP) Header Not Set	Medium	Systemic
Cross-Domain Misconfiguration	Medium	1
Missing Anti-clickjacking Header	Medium	Systemic
HTTPS Content Available via HTTP	Low	2
In Page Banner Information Leak	Low	3
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	Systemic
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	Systemic
Strict-Transport-Security Header Not Set	Low	7
Timestamp Disclosure - Unix	Low	5
X-Content-Type-Options Header Missing	Low	Systemic
Authentication Request Identified	Informational	1
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	Systemic
Modern Web Application	Informational	Systemic
Re-examine Cache-control Directives	Informational	3
Retrieved from Cache	Informational	Systemic
User Controllable HTML Element Attribute (Potential XSS)	Informational	2

Alert Detail

Medium	Absence of Anti-CSRF Tokens
Description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	http://testphp.vulnweb.com
Node Name	http://testphp.vulnweb.com
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/
Node Name	http://testphp.vulnweb.com/
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/disclaimer.php
Node Name	http://testphp.vulnweb.com/disclaimer.php
Method	GET
Parameter	

Attack	
Evidence	<form action="search.php?test=query" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/index.php
Node Name	http://testphp.vulnweb.com/index.php
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/login.php
Node Name	http://testphp.vulnweb.com/login.php
Method	GET
Parameter	
Attack	
Evidence	<form name="loginform" method="post" action="userinfo.php">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "pass" "uname"].
Instances	Systemic
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS.

	Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

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://testphp.vulnweb.com
Node Name	http://testphp.vulnweb.com
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/
Node Name	http://testphp.vulnweb.com/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/disclaimer.php
Node Name	http://testphp.vulnweb.com/disclaimer.php
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	http://testphp.vulnweb.com/robots.txt
Node Name	http://testphp.vulnweb.com/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Node Name	http://testphp.vulnweb.com/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://example.com
Node Name	https://example.com
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://example.com/
Node Name	https://example.com/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://example.com/favicon.ico
Node Name	https://example.com/favicon.ico
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
URL	https://example.com/robots.txt
Node Name	https://example.com/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://example.com/sitemap.xml
Node Name	https://example.com/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	Systemic
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/HTTP/Guides/CSP 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	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
URL	https://firefox.settings.services.mozilla.com/v1/
Node Name	https://firefox.settings.services.mozilla.com/v1/
Method	GET
Parameter	
Attack	
Evidence	access-control-allow-origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that

	is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Instances	1
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?category=HTML5&subcategory=Overly%20Permissive%20CORS%20Policy
CWE Id	264
WASC Id	14
Plugin Id	10098

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://testphp.vulnweb.com
Node Name	http://testphp.vulnweb.com
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/
Node Name	http://testphp.vulnweb.com/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/disclaimer.php
Node Name	http://testphp.vulnweb.com/disclaimer.php
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/index.php
Node Name	http://testphp.vulnweb.com/index.php

Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/login.php
Node Name	http://testphp.vulnweb.com/login.php
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://example.com
Node Name	https://example.com
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	https://example.com/
Node Name	https://example.com/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
Instances	Systemic
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/Reference/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Low	**HTTPS Content Available via HTTP**

Description	Content which was initially accessed via HTTPS (i.e.: using SSL/TLS encryption) is also accessible via HTTP (without encryption).
URL	https://example.com
Node Name	http://example.com
Method	GET
Parameter	
Attack	
Evidence	http://example.com
Other Info	ZAP attempted to connect via: http://example.com
URL	https://example.com/
Node Name	http://example.com/
Method	GET
Parameter	
Attack	
Evidence	http://example.com/
Other Info	ZAP attempted to connect via: http://example.com/
Instances	2
Solution	Ensure that your web server, application server, load balancer, etc. is configured to only serve such content via HTTPS. Consider implementing HTTP 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	311
WASC Id	4
Plugin Id	10047

Low	**In Page Banner Information Leak**
Description	The server returned a version banner string in the response content. Such information leaks may allow attackers to further target specific issues impacting the product and version in use.
URL	http://testphp.vulnweb.com/high
Node Name	http://testphp.vulnweb.com/high
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	There is a chance that the highlight in the finding is on a value in the headers, versus the actual matched string in the response body.
URL	http://testphp.vulnweb.com/robots.txt

Node Name	http://testphp.vulnweb.com/robots.txt
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	There is a chance that the highlight in the finding is on a value in the headers, versus the actual matched string in the response body.
URL	http://testphp.vulnweb.com/sitemap.xml
Node Name	http://testphp.vulnweb.com/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	There is a chance that the highlight in the finding is on a value in the headers, versus the actual matched string in the response body.
Instances	3
Solution	Configure the server to prevent such information leaks. For example: Under Tomcat this is done via the "server" directive and implementation of custom error pages. Under Apache this is done via the "ServerSignature" and "ServerTokens" directives.
Reference	https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/08-Testing_for_Error_Handling/
CWE Id	497
WASC Id	13
Plugin Id	10009

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://testphp.vulnweb.com/
Node Name	http://testphp.vulnweb.com/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Node Name	http://testphp.vulnweb.com/Mod_Rewrite_Shop/

Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/disclaimer.php
Node Name	http://testphp.vulnweb.com/disclaimer.php
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/hpp/
Node Name	http://testphp.vulnweb.com/hpp/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/privacy.php
Node Name	http://testphp.vulnweb.com/privacy.php
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
Instances	Systemic
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/shhh-dont-let-your-response-headers/
CWE Id	497
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://testphp.vulnweb.com/
Node Name	http://testphp.vulnweb.com/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Node Name	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/disclaimer.php
Node Name	http://testphp.vulnweb.com/disclaimer.php
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/robots.txt
Node Name	http://testphp.vulnweb.com/robots.txt
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Node Name	http://testphp.vulnweb.com/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	

URL	https://content-signature-2.cdn.mozilla.net/g/chains/202402/remote-settings.content-signature.mozilla.org-2026-03-08-09-54-23.chain
Node Name	https://content-signature-2.cdn.mozilla.net/g/chains/202402/remote-settings.content-signature.mozilla.org-2026-03-08-09-54-23.chain
Method	GET
Parameter	
Attack	
Evidence	AmazonS3
Other Info	
Instances	Systemic
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

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://content-signature-2.cdn.mozilla.net/g/chains/202402/remote-settings.content-signature.mozilla.org-2026-03-08-09-54-23.chain
Node Name	https://content-signature-2.cdn.mozilla.net/g/chains/202402/remote-settings.content-signature.mozilla.org-2026-03-08-09-54-23.chain
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://example.com
Node Name	https://example.com
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://example.com/
Node Name	https://example.com/
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	https://example.com/favicon.ico
Node Name	https://example.com/favicon.ico
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://example.com/robots.txt
Node Name	https://example.com/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://example.com/sitemap.xml
Node Name	https://example.com/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	7
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	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4
Method	GET
Parameter	
Attack	
Evidence	1600191811
Other Info	1600191811, which evaluates to: 2020-09-15 17:43:31.
URL	https://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4
Method	GET
Parameter	
Attack	
Evidence	1703946492
Other Info	1703946492, which evaluates to: 2023-12-30 14:28:12.
URL	https://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4
Method	GET
Parameter	
Attack	
Evidence	1773959826
Other Info	1773959826, which evaluates to: 2026-03-19 22:37:06.
URL	https://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4
Method	GET
Parameter	
Attack	
Evidence	1827377968
Other Info	1827377968, which evaluates to: 2027-11-28 04:59:28.
URL	https://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4

Node Name	https://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4
Method	GET
Parameter	
Attack	
Evidence	1889814595
Other Info	1889814595, which evaluates to: 2029-11-19 20:29:55.
Instances	5
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	497
WASC Id	13
Plugin Id	10096

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://testphp.vulnweb.com/
Node Name	http://testphp.vulnweb.com/
Method	GET
Parameter	x-content-type-options
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://testphp.vulnweb.com/Mod_Rewrite_Shop/
Node Name	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Method	GET
Parameter	x-content-type-options
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://testphp.vulnweb.com/disclaimer.php
Node Name	http://testphp.vulnweb.com/disclaimer.php

Method	GET
Parameter	x-content-type-options
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://testphp.vulnweb.com/hpp/
Node Name	http://testphp.vulnweb.com/hpp/
Method	GET
Parameter	x-content-type-options
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://testphp.vulnweb.com/index.php
Node Name	http://testphp.vulnweb.com/index.php
Method	GET
Parameter	x-content-type-options
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://content-signature-2.cdn.mozilla.net/g/chains/202402/remote-settings.content-signature.mozilla.org-2026-03-08-09-54-23.chain
Node Name	https://content-signature-2.cdn.mozilla.net/g/chains/202402/remote-settings.content-signature.mozilla.org-2026-03-08-09-54-23.chain
Method	GET
Parameter	x-content-type-options
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://example.com
Node Name	https://example.com
Method	GET

Parameter	x-content-type-options
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://example.com/
Node Name	https://example.com/
Method	GET
Parameter	x-content-type-options
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://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4
Method	GET
Parameter	x-content-type-options
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	Systemic
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://testphp.vulnweb.com/secured/newuser.php
Node Name	http://testphp.vulnweb.com/secured/newuser.php () (signup,uaddress,ucc,uemail,upass,upass2,uphone,urname,uuname)
Method	POST
Parameter	uemail
Attack	
Evidence	upass
Other Info	userParam=uemail userValue=ZAP passwordParam=upass referer=http://testphp.vulnweb.com/signup.php
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	Charset Mismatch (Header Versus Meta Content-Type Charset)
Description	This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set. An attacker could manipulate content on the page to be interpreted in an encoding of their choice. For example, if an attacker can control content at the beginning of the page, they could inject script using UTF-7 encoded text and manipulate some browsers into interpreting that text.
URL	http://testphp.vulnweb.com
Node Name	http://testphp.vulnweb.com
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	http://testphp.vulnweb.com/
Node Name	http://testphp.vulnweb.com/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	http://testphp.vulnweb.com/disclaimer.php

Node Name	http://testphp.vulnweb.com/disclaimer.php
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	http://testphp.vulnweb.com/index.php
Node Name	http://testphp.vulnweb.com/index.php
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	http://testphp.vulnweb.com/login.php
Node Name	http://testphp.vulnweb.com/login.php
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
Instances	Systemic
Solution	Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.
Reference	https://code.google.com/archive/p/browsersec/wikis/Part2.wiki#Character_set_handling_and_detection
CWE Id	436
WASC Id	15
Plugin Id	90011

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://testphp.vulnweb.com/AJAX/index.php
Node Name	http://testphp.vulnweb.com/AJAX/index.php
Method	GET
Parameter	
Attack	

Evidence	<a href="#" onclick="loadSomething('titles.php')">titles</a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/artists.php
Node Name	http://testphp.vulnweb.com/artists.php
Method	GET
Parameter	
Attack	
Evidence	<a href='#' onClick="window.open('./comment.php?aid=1','comment','width=500,height=400')">comment on this artist</a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/artists.php?artist=1
Node Name	http://testphp.vulnweb.com/artists.php (artist)
Method	GET
Parameter	
Attack	
Evidence	<a href='#' onClick="window.open('./comment.php?aid=1','comment','width=500,height=400')">comment on this artist</a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/artists.php?artist=3
Node Name	http://testphp.vulnweb.com/artists.php (artist)
Method	GET
Parameter	
Attack	
Evidence	<a href='#' onClick="window.open('./comment.php?aid=3','comment','width=500,height=400')">comment on this artist</a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Node Name	http://testphp.vulnweb.com/listproducts.php (cat)
Method	GET
Parameter	
Attack	
Evidence	<a href='#' onClick="window.open('./comment.php?pid=1','comment','width=500,height=400')">comment on this picture</a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
Instances	Systemic
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://example.com
Node Name	https://example.com
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://example.com/
Node Name	https://example.com/
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
URL	https://firefox.settings.services.mozilla.com/v1/
Node Name	https://firefox.settings.services.mozilla.com/v1/
Method	GET
Parameter	cache-control
Attack	
Evidence	max-age=3600
Other Info	
Instances	3
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://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4
Node Name	https://firefox-settings-attachments.cdn.mozilla.net/bundles/startup.json.mozlz4
Method	GET
Parameter	
Attack	
Evidence	HIT
Other Info	
URL	https://firefox.settings.services.mozilla.com/v1/
Node Name	https://firefox.settings.services.mozilla.com/v1/
Method	GET
Parameter	
Attack	
Evidence	HIT
Other Info	
URL	https://content-signature-2.cdn.mozilla.net/g/chains/202402/remote-settings.content-signature.mozilla.org-2026-03-08-09-54-23.chain
Node Name	https://content-signature-2.cdn.mozilla.net/g/chains/202402/remote-settings.content-signature.mozilla.org-2026-03-08-09-54-23.chain
Method	GET
Parameter	
Attack	
Evidence	Age: 3054
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://example.com
Node Name	https://example.com
Method	GET
Parameter	
Attack	
Evidence	Age: 3214
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://example.com/
Node Name	https://example.com/

Method	GET
Parameter	
Attack	
Evidence	Age: 3219
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://example.com/
Node Name	https://example.com/
Method	GET
Parameter	
Attack	
Evidence	Age: 3225
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://example.com/robots.txt
Node Name	https://example.com/robots.txt
Method	GET
Parameter	
Attack	
Evidence	Age: 216
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://example.com/sitemap.xml
Node Name	https://example.com/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	Age: 216
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

Informational	User Controllable HTML Element Attribute (Potential XSS)
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	http://testphp.vulnweb.com/guestbook.php
Node Name	http://testphp.vulnweb.com/guestbook.php ()(name,submit,text)
Method	POST
Parameter	submit
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://testphp.vulnweb.com/guestbook.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: submit=add message The user-controlled value was: add message
URL	http://testphp.vulnweb.com/search.php?test=query
Node Name	http://testphp.vulnweb.com/search.php (test)(goButton,searchFor)
Method	POST
Parameter	goButton
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://testphp.vulnweb.com/search.php?test=query appears to include user input in: a(n) [input] tag [name] attribute The user input found was: goButton=go The user-controlled value was: gobutton
Instances	2
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
CWE Id	20
WASC Id	20
Plugin Id	10031

Sequence Details

With the associated active scan results.