

# ZAP Scanning Report

scansione automatica

**Site:** <http://10.0.2.4>

**Generated on** Sun, 12 May 2024 16:17:13

**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	4
Low	2
Informational	2

## Alerts

Name	Risk Level	Number of Instances
<a href="#">Absence of Anti-CSRF Tokens</a>	Medium	2
<a href="#">Content Security Policy (CSP) Header Not Set</a>	Medium	5
<a href="#">Missing Anti-clickjacking Header</a>	Medium	2
<a href="#">Vulnerable JS Library</a>	Medium	1
<a href="#">Server Leaks Version Information via "Server" HTTP Response Header Field</a>	Low	12
<a href="#">X-Content-Type-Options Header Missing</a>	Low	9
<a href="#">Information Disclosure - Suspicious Comments</a>	Informational	2
<a href="#">Modern Web Application</a>	Informational	2

## Alert Detail

Medium	Absence of Anti-CSRF Tokens
	<p>No Anti-CSRF tokens were found in a HTML submission form.</p> <p>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.</p> <p>CSRF attacks are effective in a number of situations, including:</p> <p>* The victim has an active session on the target site.</p>
Description	

	<p>* The victim is authenticated via HTTP auth on the target site.</p> <p>* The victim is on the same local network as the target site.</p> <p>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.</p>
URL	<a href="http://10.0.2.4">http://10.0.2.4</a>
Method	GET
Attack	
Evidence	<form class="form-inline d-flex">
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] was found in the following HTML form: [Form 1: "inputEmail" ].
URL	<a href="http://10.0.2.4/">http://10.0.2.4/</a>
Method	GET
Attack	
Evidence	<form class="form-inline d-flex">
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] was found in the following HTML form: [Form 1: "inputEmail" ].
Instances	2
Solution	<p>Phase: Architecture and Design</p> <p>Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.</p> <p>For example, use anti-CSRF packages such as the OWASP CSRFGuard.</p> <p>Phase: Implementation</p> <p>Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.</p> <p>Phase: Architecture and Design</p> <p>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).</p> <p>Note that this can be bypassed using XSS.</p> <p>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.</p> <p>Note that this can be bypassed using XSS.</p> <p>Use the ESAPI Session Management control.</p> <p>This control includes a component for CSRF.</p> <p>Do not use the GET method for any request that triggers a state change.</p> <p>Phase: Implementation</p>

	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	<a href="http://projects.webappsec.org/Cross-Site-Request-Forgery">http://projects.webappsec.org/Cross-Site-Request-Forgery</a> <a href="https://cwe.mitre.org/data/definitions/352.html">https://cwe.mitre.org/data/definitions/352.html</a>
CWE Id	<a href="#">352</a>
WASC Id	9
Plugin Id	<a href="#">10202</a>

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	<a href="http://10.0.2.4">http://10.0.2.4</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="http://10.0.2.4/">http://10.0.2.4/</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="http://10.0.2.4/img/image.png">http://10.0.2.4/img/image.png</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="http://10.0.2.4/robots.txt">http://10.0.2.4/robots.txt</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="http://10.0.2.4/sitemap.xml">http://10.0.2.4/sitemap.xml</a>
Method	GET
Attack	
Evidence	
Other Info	

Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	<a href="https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy">https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy</a> <a href="https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html</a> <a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a> <a href="https://w3c.github.io/webappsec-csp/">https://w3c.github.io/webappsec-csp/</a> <a href="https://web.dev/articles/csp">https://web.dev/articles/csp</a> <a href="https://caniuse.com/#feat=contentsecuritypolicy">https://caniuse.com/#feat=contentsecuritypolicy</a> <a href="https://content-security-policy.com/">https://content-security-policy.com/</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10038</a>

<b>Medium</b>	<b>Missing Anti-clickjacking Header</b>
Description	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
URL	<a href="http://10.0.2.4">http://10.0.2.4</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="http://10.0.2.4/">http://10.0.2.4/</a>
Method	GET
Attack	
Evidence	
Other Info	
Instances	2
Solution	<p>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.</p> <p>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.</p>
Reference	<a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options</a>
CWE Id	<a href="#">1021</a>
WASC Id	15
Plugin Id	<a href="#">10020</a>

<b>Medium</b>	<b>Vulnerable JS Library</b>
Description	The identified library jquery, version 3.4.1 is vulnerable.
URL	<a href="http://10.0.2.4/vendor/jquery/jquery.min.js">http://10.0.2.4/vendor/jquery/jquery.min.js</a>
Method	GET
Attack	
Evidence	/*! jQuery v3.4.1

Other Info	CVE-2020-11023 CVE-2020-11022
Instances	1
Solution	Please upgrade to the latest version of jquery.
Reference	<a href="https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/">https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/</a>
CWE Id	<a href="#">829</a>
WASC Id	
Plugin Id	<a href="#">10003</a>

<b>Low</b>	<b>Server Leaks Version Information via "Server" HTTP Response Header Field</b>
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	<a href="http://10.0.2.4">http://10.0.2.4</a>
Method	GET
Attack	
Evidence	Apache/2.4.18 (Ubuntu)
Other Info	
URL	<a href="http://10.0.2.4/">http://10.0.2.4/</a>
Method	GET
Attack	
Evidence	Apache/2.4.18 (Ubuntu)
Other Info	
URL	<a href="http://10.0.2.4/css/grayscale.min.css">http://10.0.2.4/css/grayscale.min.css</a>
Method	GET
Attack	
Evidence	Apache/2.4.18 (Ubuntu)
Other Info	
URL	<a href="http://10.0.2.4/img/image.png">http://10.0.2.4/img/image.png</a>
Method	GET
Attack	
Evidence	Apache/2.4.18 (Ubuntu)
Other Info	
URL	<a href="http://10.0.2.4/js/grayscale.min.js">http://10.0.2.4/js/grayscale.min.js</a>
Method	GET
Attack	
Evidence	Apache/2.4.18 (Ubuntu)
Other Info	
URL	<a href="http://10.0.2.4/robots.txt">http://10.0.2.4/robots.txt</a>
Method	GET

Attack	
Evidence	Apache/2.4.18 (Ubuntu)
Other Info	
URL	<a href="http://10.0.2.4/sitemap.xml">http://10.0.2.4/sitemap.xml</a>
Method	GET
Attack	
Evidence	Apache/2.4.18 (Ubuntu)
Other Info	
URL	<a href="http://10.0.2.4/vendor/bootstrap/css/bootstrap.min.css">http://10.0.2.4/vendor/bootstrap/css/bootstrap.min.css</a>
Method	GET
Attack	
Evidence	Apache/2.4.18 (Ubuntu)
Other Info	
URL	<a href="http://10.0.2.4/vendor/bootstrap/js/bootstrap.bundle.min.js">http://10.0.2.4/vendor/bootstrap/js/bootstrap.bundle.min.js</a>
Method	GET
Attack	
Evidence	Apache/2.4.18 (Ubuntu)
Other Info	
URL	<a href="http://10.0.2.4/vendor/fontawesome-free/css/all.min.css">http://10.0.2.4/vendor/fontawesome-free/css/all.min.css</a>
Method	GET
Attack	
Evidence	Apache/2.4.18 (Ubuntu)
Other Info	
URL	<a href="http://10.0.2.4/vendor/jquery-easing/jquery.easing.min.js">http://10.0.2.4/vendor/jquery-easing/jquery.easing.min.js</a>
Method	GET
Attack	
Evidence	Apache/2.4.18 (Ubuntu)
Other Info	
URL	<a href="http://10.0.2.4/vendor/jquery/jquery.min.js">http://10.0.2.4/vendor/jquery/jquery.min.js</a>
Method	GET
Attack	
Evidence	Apache/2.4.18 (Ubuntu)
Other Info	
Instances	12
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	<a href="https://httpd.apache.org/docs/current/mod/core.html#servertokens">https://httpd.apache.org/docs/current/mod/core.html#servertokens</a> <a href="https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)">https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)</a>

	<a href="https://www.troyhunt.com/shhh-dont-let-your-response-headers/">https://www.troyhunt.com/shhh-dont-let-your-response-headers/</a>
CWE Id	<a href="#">200</a>
WASC Id	13
Plugin Id	<a href="#">10036</a>

<b>Low</b>	<b>X-Content-Type-Options Header Missing</b>
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	<a href="http://10.0.2.4">http://10.0.2.4</a>
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	<a href="http://10.0.2.4/">http://10.0.2.4/</a>
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	<a href="http://10.0.2.4/css/grayscale.min.css">http://10.0.2.4/css/grayscale.min.css</a>
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	<a href="http://10.0.2.4/js/grayscale.min.js">http://10.0.2.4/js/grayscale.min.js</a>
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	<a href="http://10.0.2.4/vendor/bootstrap/css/bootstrap.min.css">http://10.0.2.4/vendor/bootstrap/css/bootstrap.min.css</a>
Method	GET
Attack	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Other Info	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	<a href="http://10.0.2.4/vendor/bootstrap/js/bootstrap.bundle.min.js">http://10.0.2.4/vendor/bootstrap/js/bootstrap.bundle.min.js</a>
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	<a href="http://10.0.2.4/vendor/fontawesome-free/css/all.min.css">http://10.0.2.4/vendor/fontawesome-free/css/all.min.css</a>
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	<a href="http://10.0.2.4/vendor/jquery-easing/jquery.easing.min.js">http://10.0.2.4/vendor/jquery-easing/jquery.easing.min.js</a>
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	<a href="http://10.0.2.4/vendor/jquery/jquery.min.js">http://10.0.2.4/vendor/jquery/jquery.min.js</a>
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	9
Solution	<p>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.</p> <p>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.</p>
Reference	<a href="https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)">https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)</a> <a href="https://owasp.org/www-community/Security-Headers">https://owasp.org/www-community/Security-Headers</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10021</a>

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	<a href="http://10.0.2.4/vendor/bootstrap/js/bootstrap.bundle.min.js">http://10.0.2.4/vendor/bootstrap/js/bootstrap.bundle.min.js</a>
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "!function(t,e){\"object\"==typeof exports&&\"undefined\"!=typeof module?e(exports,require(\"jquery\")):\"function\"==typeof define&&defi", see evidence field for the suspicious comment/snippet.
URL	<a href="http://10.0.2.4/vendor/jquery/jquery.min.js">http://10.0.2.4/vendor/jquery/jquery.min.js</a>
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "!function(e,t){\"use strict\";\"object\"==typeof module&&\"object\"==typeof module.exports?module.exports=e.document?t(e,!0):function(\"", see evidence field for the suspicious comment/snippet.
Instances	2
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	<a href="#">200</a>
WASC Id	13
Plugin Id	<a href="#">10027</a>

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	<a href="http://10.0.2.4">http://10.0.2.4</a>
Method	GET
Attack	
Evidence	<a href="#">That's who we are.</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	<a href="http://10.0.2.4/">http://10.0.2.4/</a>
Method	GET
Attack	
Evidence	<a href="#">That's who we are.</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	2
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	<a href="#">10109</a>

