POSS

Site: http://172.16.2.66

Generated on Tue, 5 Dec 2023 13:56:03

ZAP Version: 2.14.0

Summary of Alerts

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

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	1
Content Security Policy (CSP) Header Not Set	Medium	4
Missing Anti-clickjacking Header	Medium	2
Cross-Domain JavaScript Source File Inclusion	Low	24
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	6
X-Content-Type-Options Header Missing	Low	3
Information Disclosure - Suspicious Comments	Informational	3
Modern Web Application	Informational	3

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://172.16.2.66/sitemap.xml
Method	GET
Attack	
Evidence	<form role="search" method="get" action="http://poss.rom11.ca/" class="wp-block-search__button-outside wp-block-search__text-button wp-block-search" >
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: "wp-block-search__input-2"].
Instances	1
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	http://projects.webappsec.org/Cross-Site-Request-Forgery 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://172.16.2.66
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.66/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.66/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.66/wp-admin/admin-ajax.php
Method	GET
Attack	
Evidence	
Other Info	
Instances	4
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 http://www.w3.org/TR/CSP/ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**Missing Anti-clickjacking Header**
Description	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.

URL	http://172.16.2.66
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.66/
Method	GET
Attack	
Evidence	
Other Info	
Instances	2
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/Headers/X-Frame-Options
CWE Id	[1021](1021)
WASC Id	15
Plugin Id	[10020](10020)

Low	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	http://172.16.2.66
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-content/plugins/woocommerce/assets/js/frontend/add-to-cart.min.js?ver=8.3.1" id="wc-add-to-cart-js" defer data-wp-strategy="defer"></script>
Other Info	
URL	http://172.16.2.66
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-content/plugins/woocommerce/assets/js/frontend/woocommerce.min.js?ver=8.3.1" id="woocommerce-js" defer data-wp-strategy="defer"></script>
Other Info	
URL	http://172.16.2.66
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-content/plugins/woocommerce/assets/js/jquery-blockui/jquery.blockUI.min.js?ver=2.7.0-wc.8.3.1" id="jquery-blockui-js" defer data-wp-strategy="defer"></script>

Other Info	
URL	http://172.16.2.66
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-content/plugins/woocommerce/assets/js/js-cookie/js.cookie.min.js?ver=2.1.4-wc.8.3.1" id="js-cookie-js" defer data-wp-strategy="defer"></script>
Other Info	
URL	http://172.16.2.66
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-includes/blocks/navigation/view.min.js?ver=e3d6f3216904b5b42831" id="wp-block-navigation-view-js" defer data-wp-strategy="defer"></script>
Other Info	
URL	http://172.16.2.66
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-includes/js/dist/interactivity.min.js?ver=6.4.1" id="wp-interactivity-js" defer data-wp-strategy="defer"></script>
Other Info	
URL	http://172.16.2.66
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.4.1" id="jquery-migrate-js"></script>
Other Info	
URL	http://172.16.2.66
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-includes/js/jquery/jquery.min.js?ver=3.7.1" id="jquery-core-js"></script>
Other Info	
URL	http://172.16.2.66/
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-content/plugins/woocommerce/assets/js/frontend/add-to-cart.min.js?ver=8.3.1" id="wc-add-to-cart-js" defer data-wp-strategy="defer"></script>
Other Info	
URL	http://172.16.2.66/
Method	GET

Attack	
Evidence	<script src="http://poss.rom11.ca/wp-content/plugins/woocommerce/assets/js/frontend/woocommerce.min.js?ver=8.3.1" id="woocommerce-js" defer data-wp-strategy="defer"></script>
Other Info	
URL	http://172.16.2.66/
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-content/plugins/woocommerce/assets/js/jquery-blockui/jquery.blockUI.min.js?ver=2.7.0-wc.8.3.1" id="jquery-blockui-js" defer data-wp-strategy="defer"></script>
Other Info	
URL	http://172.16.2.66/
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-content/plugins/woocommerce/assets/js/js-cookie/js.cookie.min.js?ver=2.1.4-wc.8.3.1" id="js-cookie-js" defer data-wp-strategy="defer"></script>
Other Info	
URL	http://172.16.2.66/
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-includes/blocks/navigation/view.min.js?ver=e3d6f3216904b5b42831" id="wp-block-navigation-view-js" defer data-wp-strategy="defer"></script>
Other Info	
URL	http://172.16.2.66/
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-includes/js/dist/interactivity.min.js?ver=6.4.1" id="wp-interactivity-js" defer data-wp-strategy="defer"></script>
Other Info	
URL	http://172.16.2.66/
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.4.1" id="jquery-migrate-js"></script>
Other Info	
URL	http://172.16.2.66/
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-includes/js/jquery/jquery.min.js?ver=3.7.1" id="jquery-core-js"></script>

Other Info	
URL	http://172.16.2.66/sitemap.xml
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-content/plugins/woocommerce/assets/js/frontend/add-to-cart.min.js?ver=8.3.1" id="wc-add-to-cart-js" defer data-wp-strategy="defer"></script>
Other Info	
URL	http://172.16.2.66/sitemap.xml
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-content/plugins/woocommerce/assets/js/frontend/woocommerce.min.js?ver=8.3.1" id="woocommerce-js" defer data-wp-strategy="defer"></script>
Other Info	
URL	http://172.16.2.66/sitemap.xml
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-content/plugins/woocommerce/assets/js/jquery-blockui/jquery.blockUI.min.js?ver=2.7.0-wc.8.3.1" id="jquery-blockui-js" defer data-wp-strategy="defer"></script>
Other Info	
URL	http://172.16.2.66/sitemap.xml
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-content/plugins/woocommerce/assets/js/js-cookie/js.cookie.min.js?ver=2.1.4-wc.8.3.1" id="js-cookie-js" defer data-wp-strategy="defer"></script>
Other Info	
URL	http://172.16.2.66/sitemap.xml
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-includes/blocks/navigation/view.min.js?ver=e3d6f3216904b5b42831" id="wp-block-navigation-view-js" defer data-wp-strategy="defer"></script>
Other Info	
URL	http://172.16.2.66/sitemap.xml
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-includes/js/dist/interactivity.min.js?ver=6.4.1" id="wp-interactivity-js" defer data-wp-strategy="defer"></script>
Other Info	
URL	http://172.16.2.66/sitemap.xml

Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.4.1" id="jquery-migrate-js"></script>
Other Info	
URL	http://172.16.2.66/sitemap.xml
Method	GET
Attack	
Evidence	<script src="http://poss.rom11.ca/wp-includes/js/jquery/jquery.min.js?ver=3.7.1" id="jquery-core-js"></script>
Other Info	
Instances	24
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	[829](829)
WASC Id	15
Plugin Id	[10017](10017)

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://172.16.2.66
Method	GET
Attack	
Evidence	Apache/2.4.41 (Ubuntu)
Other Info	
URL	http://172.16.2.66/
Method	GET
Attack	
Evidence	Apache/2.4.41 (Ubuntu)
Other Info	
URL	http://172.16.2.66/robots.txt
Method	GET
Attack	
Evidence	Apache/2.4.41 (Ubuntu)
Other Info	
URL	http://172.16.2.66/sitemap.xml
Method	GET
Attack	

Evidence	Apache/2.4.41 (Ubuntu)
Other Info	
URL	http://172.16.2.66/wp-admin/
Method	GET
Attack	
Evidence	Apache/2.4.41 (Ubuntu)
Other Info	
URL	http://172.16.2.66/wp-admin/admin-ajax.php
Method	GET
Attack	
Evidence	Apache/2.4.41 (Ubuntu)
Other Info	
Instances	6
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10036

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://172.16.2.66
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	http://172.16.2.66/
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	http://172.16.2.66/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	3
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	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx 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	http://172.16.2.66
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in the element starting with: "<script id="wc-add-to-cart-js-extra"> var wc_add_to_cart_params = {"ajax_url":"\/wp-admin\/admin-ajax.php","wc_ajax_url":"\/?wc-", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.66/
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in the element starting with: "<script id="wc-add-to-cart-js-extra"> var wc_add_to_cart_params = {"ajax_url":"\/wp-admin\/admin-ajax.php","wc_ajax_url":"\/?wc-", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.66/sitemap.xml
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in the element starting with: "<script id="wc-add-to-cart-js-extra"> var wc_add_to_cart_params = {"ajax_url":"\/wp-admin\/admin-ajax.php","wc_ajax_url":"\/?wc-", see evidence field for the suspicious comment/snippet.
Instances	3

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

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://172.16.2.66
Method	GET
Attack	
Evidence	<a href="http://poss.rom11.ca" target="_self" rel="home" aria-current="page">ROM</a>
Other Info	Links have been found with a target of '_self' - this is often used by modern frameworks to force a full page reload.
URL	http://172.16.2.66/
Method	GET
Attack	
Evidence	<a href="http://poss.rom11.ca" target="_self" rel="home" aria-current="page">ROM</a>
Other Info	Links have been found with a target of '_self' - this is often used by modern frameworks to force a full page reload.
URL	http://172.16.2.66/sitemap.xml
Method	GET
Attack	
Evidence	<a href="http://poss.rom11.ca" target="_self" rel="home">ROM</a>
Other Info	Links have been found with a target of '_self' - this is often used by modern frameworks to force a full page reload.
Instances	3
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109