ZAP Scanning Report Vancouver

Site: http://192.168.32.101

Generated on Thu, 22 Jun 2023 13:37:24

ZAP Version: 2.12.0

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	5
Informational	4

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	19
Content Security Policy (CSP) Header Not Set	Medium	18
Missing Anti-clickjacking Header	Medium	11
Vulnerable JS Library	Medium	1
Cookie No HttpOnly Flag	Low	7
Cookie without SameSite Attribute	Low	7
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	36
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	53
X-Content-Type-Options Header Missing	Low	37
Charset Mismatch	Informational	3
Cookie Poisoning	Informational	3
Information Disclosure - Suspicious Comments	Informational	8
User Controllable HTML Element Attribute (Potential XSS)	Informational	14

Alert Detail

Medium	Absence of Anti-CSRF Tokens
	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

Description	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://192.168.32.101/backup_wordpress/
Method	GET
Attack	
Evidence	<form role="search" method="get" class="search-form" action="/backup_wordpress/">
URL	http://192.168.32.101/backup_wordpress/?author=1
Method	GET
Attack	
Evidence	<form role="search" method="get" class="search-form" action="/backup_wordpress/">
URL	http://192.168.32.101/backup_wordpress/?author=2
Method	GET
Attack	
Evidence	<form role="search" method="get" class="search-form" action="/backup_wordpress/">
URL	http://192.168.32.101/backup_wordpress/?cat=1
Method	GET
Attack	
Evidence	<form role="search" method="get" class="search-form" action="/backup_wordpress/">
URL	http://192.168.32.101/backup_wordpress/?m=201803
Method	GET
Attack	
Evidence	<form role="search" method="get" class="search-form" action="/backup_wordpress/">
URL	http://192.168.32.101/backup_wordpress/?p=1
Method	GET
Attack	
Evidence	<form action="/backup_wordpress/wp-comments-post.php" method="post" id="commentform" class="comment-form" novalidate>
URL	http://192.168.32.101/backup_wordpress/?p=1
Method	GET
Attack	
Evidence	<form role="search" method="get" class="search-form" action="/backup_wordpress/">
URL	http://192.168.32.101/backup_wordpress/?p=1&replytocom=1
Method	GET

Attack	
Evidence	<form action="/backup_wordpress/wp-comments-post.php" method="post" id="commentform" class="comment-form" novalidate>
URL	http://192.168.32.101/backup_wordpress/?p=1&replytocom=1
Method	GET
Attack	
Evidence	<form role="search" method="get" class="search-form" action="/backup_wordpress/">
URL	http://192.168.32.101/backup_wordpress/?p=2
Method	GET
Attack	
Evidence	<form role="search" method="get" class="search-form" action="/backup_wordpress/">
URL	http://192.168.32.101/backup_wordpress/?p=2
Method	GET
Attack	
Evidence	<form role="search" method="get" class="search-form" action="/backup_wordpress/">
URL	http://192.168.32.101/backup_wordpress/?p=5
Method	GET
Attack	
Evidence	<form action="/backup_wordpress/wp-comments-post.php" method="post" id="commentform" class="comment-form" novalidate>
URL	http://192.168.32.101/backup_wordpress/?p=5
Method	GET
Attack	
Evidence	<form role="search" method="get" class="search-form" action="/backup_wordpress/">
URL	http://192.168.32.101/backup_wordpress/?page_id=2
Method	GET
Attack	
Evidence	<form role="search" method="get" class="search-form" action="/backup_wordpress/">
URL	http://192.168.32.101/backup_wordpress/?s
Method	GET
Attack	
Evidence	<form role="search" method="get" class="search-form" action="/backup_wordpress/">
URL	http://192.168.32.101/backup_wordpress/wp-login.php
Method	GET
Attack	
Evidence	<form name="loginform" id="loginform" action="/backup_wordpress/wp-login.php" method="post">
URL	http://192.168.32.101/backup_wordpress/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	<form name="lostpasswordform" id="lostpasswordform" action="/backup_wordpress/wp-login.php?action=lostpassword" method="post">
URL	http://192.168.32.101/backup_wordpress/wp-login.php

Method	POST
Attack	
Evidence	<form name="loginform" id="loginform" action="/backup_wordpress/wp-login.php" method="post">
URL	http://192.168.32.101/backup_wordpress/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	<form name="lostpasswordform" id="lostpasswordform" action="/backup_wordpress/wp-login.php?action=lostpassword" method="post">
Instances	19
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 http://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://192.168.32.101
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?author=1
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?author=2
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?cat=1
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?m=201803
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?p=1
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?p=1&replytocom=1
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?p=2
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?p=5
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?page_id=2

Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?s
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-login.php
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/sitemap.xml
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-comments-post.php
Method	POST
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-login.php
Method	POST
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	
Instances	18
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://192.168.32.101
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?author=1
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?author=2
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?cat=1
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?m=201803
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?p=1
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?p=1&replytocom=1
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?p=5
Method	GET
Attack	
Evidence	

URL	http://192.168.32.101/backup_wordpress/?page_id=2
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?s
Method	GET
Attack	
Evidence	
Instances	11
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
WASC Id	15
Plugin Id	10020

Medium	**Vulnerable JS Library**
Description	The identified library jquery, version 1.12.3 is vulnerable.
URL	http://192.168.32.101/backup_wordpress/wp-includes/js/jquery/jquery.js?ver=1.12.3
Method	GET
Attack	
Evidence	/*! jQuery v1.12.3
Instances	1
Solution	Please upgrade to the latest version of jquery.
Reference	https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://bugs.jquery.com/ticket/11974 https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://github.com/jquery/jquery.com/issues/162
CWE Id	829
WASC Id	
Plugin Id	10003

Low	**Cookie No HttpOnly Flag**
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	http://192.168.32.101/backup_wordpress/wp-login.php
Method	GET

Attack	
Evidence	Set-Cookie: wordpress_test_cookie
URL	http://192.168.32.101/backup_wordpress/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
URL	http://192.168.32.101/backup_wordpress/wp-comments-post.php
Method	POST
Attack	
Evidence	Set-Cookie: comment_author_af3fdc36e2f7c2fe3d3d367f5803f739
URL	http://192.168.32.101/backup_wordpress/wp-comments-post.php
Method	POST
Attack	
Evidence	Set-Cookie: comment_author_email_af3fdc36e2f7c2fe3d3d367f5803f739
URL	http://192.168.32.101/backup_wordpress/wp-comments-post.php
Method	POST
Attack	
Evidence	Set-Cookie: comment_author_url_af3fdc36e2f7c2fe3d3d367f5803f739
URL	http://192.168.32.101/backup_wordpress/wp-login.php
Method	POST
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
URL	http://192.168.32.101/backup_wordpress/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Instances	7
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

Low	**Cookie without SameSite Attribute**
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	http://192.168.32.101/backup_wordpress/wp-login.php
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
URL	http://192.168.32.101/backup_wordpress/wp-login.php?action=lostpassword
Method	GET

Attack	
Evidence	Set-Cookie: wordpress_test_cookie
URL	http://192.168.32.101/backup_wordpress/wp-comments-post.php
Method	POST
Attack	
Evidence	Set-Cookie: comment_author_af3fdc36e2f7c2fe3d3d367f5803f739
URL	http://192.168.32.101/backup_wordpress/wp-comments-post.php
Method	POST
Attack	
Evidence	Set-Cookie: comment_author_email_af3fdc36e2f7c2fe3d3d367f5803f739
URL	http://192.168.32.101/backup_wordpress/wp-comments-post.php
Method	POST
Attack	
Evidence	Set-Cookie: comment_author_url_af3fdc36e2f7c2fe3d3d367f5803f739
URL	http://192.168.32.101/backup_wordpress/wp-login.php
Method	POST
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
URL	http://192.168.32.101/backup_wordpress/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Instances	7
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

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://192.168.32.101/backup_wordpress/
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?author=1
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?author=1&feed=rss2

Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?author=2
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?author=2&feed=rss2
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?cat=1
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?cat=1&feed=rss2
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?feed=comments-rss2
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?feed=rss2
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?feed=rss2&p=1
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?feed=rss2&p=5
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?feed=rss2&page_id=2
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?feed=rss2&s
Method	GET

Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?format=xml&rest_route=%2Foembed%2F1.0%2Fembed&url=%2Fbackup_wordpress%2F%3Fp%3D1
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?format=xml&rest_route=%2Foembed%2F1.0%2Fembed&url=%2Fbackup_wordpress%2F%3Fp%3D5
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?format=xml&rest_route=%2Foembed%2F1.0%2Fembed&url=%2Fbackup_wordpress%2F%3Fpage_id%3D2
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?m=201803
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?p=1
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?p=1&replytocom=1
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?p=2
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?p=5
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?page_id=2
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?rest_route=%2Foembed%2F1.0%2Fembed&url=%2Fbackup_wordpress%2F%3Fp%3D1

Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?rest_route=%2Foembed%2F1.0%2Fembed&url=%2Fbackup_wordpress%2F%3Fp%3D5
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?rest_route=%2Foembed%2F1.0%2Fembed&url=%2Fbackup_wordpress%2F%3Fpage_id%3D2
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?rest_route=/
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/?s
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/wp-admin/
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/wp-admin/load-styles.php?c=0&dir=ltr&load%5B%5D=dashicons,buttons,forms,l10n,login&ver=4.5
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/wp-login.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/xmlrpc.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26

URL	http://192.168.32.101/backup_wordpress/xmlrpc.php?rsd
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/wp-comments-post.php
Method	POST
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/wp-login.php
Method	POST
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
URL	http://192.168.32.101/backup_wordpress/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	X-Powered-By: PHP/5.3.10-1ubuntu3.26
Instances	36
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	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	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://192.168.32.101
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?author=1
Method	GET

Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?author=1&feed=rss2
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?author=2
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?author=2&feed=rss2
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?cat=1
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?cat=1&feed=rss2
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?feed=comments-rss2
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?feed=rss2
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?feed=rss2&p=1
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?feed=rss2&p=5
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?feed=rss2&page_id=2
Method	GET
Attack	

Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?feed=rss2&s
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?format=xml&rest_route=%2Foembed%2F1.0%2Fembed&url=%2Fbackup_wordpress%2F%3Fp%3D1
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?format=xml&rest_route=%2Foembed%2F1.0%2Fembed&url=%2Fbackup_wordpress%2F%3Fp%3D5
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?format=xml&rest_route=%2Foembed%2F1.0%2Fembed&url=%2Fbackup_wordpress%2F%3Fpage_id%3D2
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?m=201803
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?p=1
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?p=1&replytocom=1
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?p=2
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?p=5
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?page_id=2
Method	GET

Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?rest_route=%2Foembed%2F1.0%2Fembed&url=%2Fbackup_wordpress%2F%3Fp%3D1
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?rest_route=%2Foembed%2F1.0%2Fembed&url=%2Fbackup_wordpress%2F%3Fp%3D5
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?rest_route=%2Foembed%2F1.0%2Fembed&url=%2Fbackup_wordpress%2F%3Fpage_id%3D2
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?rest_route=/
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/?s
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/wp-admin/
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/wp-admin/load-styles.php?c=0&dir=ltr&load%5B%5D=dashicons,buttons,forms,l10n,login&ver=4.5
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/wp-content/themes/twentysixteen/css/ie.css?ver=20160412
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/wp-content/themes/twentysixteen/css/ie7.css?ver=20160412
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)

URL	http://192.168.32.101/backup_wordpress/wp-content/themes/twentysixteen/css/ie8.css?ver=20160412
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/wp-content/themes/twentysixteen/genericons/genericons.css?ver=3.4.1
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/wp-content/themes/twentysixteen/js/functions.js?ver=20160412
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/wp-content/themes/twentysixteen/js/html5.js?ver=3.7.3
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/wp-content/themes/twentysixteen/js/skip-link-focus-fix.js?ver=20160412
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/wp-content/themes/twentysixteen/style.css?ver=4.5
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/wp-includes/js/comment-reply.min.js?ver=4.5
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.0
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/wp-includes/js/jquery/jquery.js?ver=1.12.3
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/wp-includes/js/wp-embed.min.js?ver=4.5

Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/wp-includes/wlwmanifest.xml
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/wp-login.php
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/xmlrpc.php
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/xmlrpc.php?rsd
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/robots.txt
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/sitemap.xml
Method	GET
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/wp-comments-post.php
Method	POST
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/wp-login.php
Method	POST
Attack	
Evidence	Apache/2.2.22 (Ubuntu)
URL	http://192.168.32.101/backup_wordpress/wp-login.php?action=lostpassword
Method	POST

Attack	
Evidence	Apache/2.2.22 (Ubuntu)
Instances	53
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://192.168.32.101
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?author=1
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?author=1&feed=rss2
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?author=2
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?author=2&feed=rss2
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?cat=1

Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?cat=1&feed=rss2
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?feed=comments-rss2
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?feed=rss2
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?feed=rss2&s
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?m=201803
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?p=1
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?p=1&replytocom=1
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?p=5
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?page_id=2
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?s
Method	GET

Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-admin/load-styles.php?c=0&dir=ltr&load%5B%5D=dashicons,buttons,forms,l10n,login&ver=4.5
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-content/themes/twentysixteen/css/ie.css?ver=20160412
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-content/themes/twentysixteen/css/ie7.css?ver=20160412
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-content/themes/twentysixteen/css/ie8.css?ver=20160412
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-content/themes/twentysixteen/genericons/genericons.css?ver=3.4.1
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-content/themes/twentysixteen/js/functions.js?ver=20160412
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-content/themes/twentysixteen/js/html5.js?ver=3.7.3
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-content/themes/twentysixteen/js/skip-link-focus-fix.js?ver=20160412
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-content/themes/twentysixteen/style.css?ver=4.5
Method	GET

Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-includes/js/comment-reply.min.js?ver=4.5
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.0
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-includes/js/jquery/jquery.js?ver=1.12.3
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-includes/js/wp-embed.min.js?ver=4.5
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-includes/wlwmanifest.xml
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-login.php
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/xmlrpc.php?rsd
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/robots.txt
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-login.php
Method	POST

Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	
Instances	37
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	**Charset Mismatch**
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://192.168.32.101/backup_wordpress/?format=xml&rest_route=%2Foembed%2F1.0%2Fembed&url=%2Fbackup_wordpress%2F%3Fp%3D1
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?format=xml&rest_route=%2Foembed%2F1.0%2Fembed&url=%2Fbackup_wordpress%2F%3Fp%3D5
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?format=xml&rest_route=%2Foembed%2F1.0%2Fembed&url=%2Fbackup_wordpress%2F%3Fpage_id%3D2
Method	GET
Attack	
Evidence	
Instances	3
Solution	Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.
Reference	http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection
CWE Id	436
WASC Id	15

Plugin Id	90011

Informational	Cookie Poisoning
Description	This check looks at user-supplied input in query string parameters and POST data to identify where cookie parameters might be controlled. This is called a cookie poisoning attack, and becomes exploitable when an attacker can manipulate the cookie in various ways. In some cases this will not be exploitable, however, allowing URL parameters to set cookie values is generally considered a bug.
URL	http://192.168.32.101/backup_wordpress/wp-comments-post.php
Method	POST
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-comments-post.php
Method	POST
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-comments-post.php
Method	POST
Attack	
Evidence	
Instances	3
Solution	Do not allow user input to control cookie names and values. If some query string parameters must be set in cookie values, be sure to filter out semicolon's that can serve as name/value pair delimiters.
Reference	http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-cookie
CWE Id	20
WASC Id	20
Plugin Id	10029

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://192.168.32.101/backup_wordpress/wp-content/themes/twentysixteen/js/html5.js?ver=3.7.3
Method	GET
Attack	
Evidence	select
URL	http://192.168.32.101/backup_wordpress/wp-content/themes/twentysixteen/js/skip-link-focus-fix.js?ver=20160412
Method	GET
Attack	
Evidence	admin
URL	http://192.168.32.101/backup_wordpress/wp-content/themes/twentysixteen/js/skip-link-focus-fix.js?ver=20160412
Method	GET
Attack	
Evidence	select

URL	http://192.168.32.101/backup_wordpress/wp-includes/js/jquery/jquery.js?ver=1.12.3
Method	GET
Attack	
Evidence	db
URL	http://192.168.32.101/backup_wordpress/wp-includes/js/jquery/jquery.js?ver=1.12.3
Method	GET
Attack	
Evidence	select
URL	http://192.168.32.101/backup_wordpress/wp-login.php
Method	GET
Attack	
Evidence	select
URL	http://192.168.32.101/backup_wordpress/wp-login.php
Method	POST
Attack	
Evidence	select
URL	http://192.168.32.101/backup_wordpress/wp-comments-post.php
Method	POST
Attack	
Evidence	bug
Instances	8
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	**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://192.168.32.101/backup_wordpress/?author=1
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?cat=1
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?p=1
Method	GET

Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/?p=1&replytocom=1
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-login.php
Method	POST
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-login.php
Method	POST
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-login.php
Method	POST
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-login.php
Method	POST
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-login.php?action=lostpassword
Method	POST
Attack	

Evidence	
URL	http://192.168.32.101/backup_wordpress/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	
Instances	14
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute
CWE Id	20
WASC Id	20
Plugin Id	10031