ZAP Scanning Report

Site: http://192.168.123.30

Generated on Tue, 7 May 2024 13:47:33

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	3
Low	6
Informational	6

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	49
Content Security Policy (CSP) Header Not Set	Medium	40
Missing Anti-clickjacking Header	Medium	17
Cookie No HttpOnly Flag	Low	34
Cookie without SameSite Attribute	Low	34
Private IP Disclosure	Low	6
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	135
Timestamp Disclosure - Unix	Low	1
X-Content-Type-Options Header Missing	Low	110
Charset Mismatch	Informational	4
Cookie Poisoning	Informational	12
Information Disclosure - Suspicious Comments	Informational	68
Modern Web Application	Informational	12
Session Management Response Identified	Informational	46
User Controllable HTML Element Attribute (Potential XSS)	Informational	121

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

Description	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://192.168.123.30/2022/10/27/hello-world/
Method	GET
Attack	
Evidence	<form action="http://192.168.123.30/wp-comments-post.php" method="post" id=" commentform" class="comment-form" novalidate>
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: "author" "comment_parent" "comment_post_ID" "email" "submit" "url" "wp-comment-cookies-consent"].
URL	http://192.168.123.30/2022/10/27/hello-world/?replytocom=1
Method	GET
Attack	
Evidence	<form action="http://192.168.123.30/wp-comments-post.php" method="post" id=" commentform" class="comment-form" novalidate>
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: "author" "comment_parent" "comment_post_ID" "email" "submit" "url" "wp-comment-cookies-consent"].
URL	http://192.168.123.30/2022/10/27/hello-world/?replytocom=2
Method	GET
Attack	
Evidence	<form action="http://192.168.123.30/wp-comments-post.php" method="post" id=" commentform" class="comment-form" novalidate>
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: "author" "comment_parent" "comment_post_ID" "email" "submit" "url" "wp-comment-cookies-consent"].
URL	http://192.168.123.30/2022/10/27/hello-world/?replytocom=3
Method	GET
Attack	
Evidence	<form action="http://192.168.123.30/wp-comments-post.php" method="post" id=" commentform" class="comment-form" novalidate>

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: "author" "comment_parent" "comment_post_ID" "email" "submit" "url" "wp-comment-cookies-consent"].
URL	http://192.168.123.30/2024/05/07/contact-us/
Method	GET
Attack	
Evidence	<form action="http://192.168.123.30/wp-comments-post.php" method="post" id="commentform" class="comment-form" novalidate>
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: "author" "comment_parent" "comment_post_ID" "email" "submit" "url" "wp-comment-cookies-consent"].
URL	http://192.168.123.30/wp-login.php
Method	GET
Attack	
Evidence	<form name="loginform" id="loginform" action="http://192.168.123.30/wp-login.php" 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] was found in the following HTML form: [Form 1: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	http://192.168.123.30/wp-login.php
Method	GET
Attack	
Evidence	<form id="language-switcher" action="" method="get">
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 2: ""].
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	<form name="lostpasswordform" id="lostpasswordform" action="http://192.168.123.30/wp-login.php?action=lostpassword" 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] was found in the following HTML form: [Form 1: "redirect_to" "user_login" "wp-submit"].
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "action"].
URL	http://192.168.123.30/wp-login.php?action=lostpassword&wp_lang=en_GB

Method	GET
Attack	
Evidence	<form name="lostpasswordform" id="lostpasswordform" action="http://192.168.123.30/wp-login.php?action=lostpassword" 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] was found in the following HTML form: [Form 1: "redirect_to" "user_login" "wp-submit"].
URL	http://192.168.123.30/wp-login.php?action=lostpassword&wp_lang=en_GB
Method	GET
Attack	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "action"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
Attack	
Evidence	<form name="loginform" id="loginform" action="http://192.168.123.30/wp-login.php" 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] was found in the following HTML form: [Form 1: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
Attack	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "redirect_to"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	<form name="loginform" id="loginform" action="http://192.168.123.30/wp-login.php" 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] was found in the following HTML form: [Form 1: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	<form id="language-switcher" action="" method="get">

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 2: "redirect_to"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F
Method	GET
Attack	
Evidence	<form name="loginform" id="loginform" action="http://192.168.123.30/wp-login.php" 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] was found in the following HTML form: [Form 1: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F
Method	GET
Attack	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "redirect_to"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F%3Freplytocom%3D1
Method	GET
Attack	
Evidence	<form name="loginform" id="loginform" action="http://192.168.123.30/wp-login.php" 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] was found in the following HTML form: [Form 1: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F%3Freplytocom%3D1
Method	GET
Attack	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "redirect_to"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	<form name="loginform" id="loginform" action="http://192.168.123.30/wp-login.php" method="post">
Other	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

Info	HTML form: [Form 1: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "redirect_to"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F
Method	GET
Attack	
Evidence	<form name="loginform" id="loginform" action="http://192.168.123.30/wp-login.php" 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] was found in the following HTML form: [Form 1: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F
Method	GET
Attack	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "redirect_to"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	<form name="loginform" id="loginform" action="http://192.168.123.30/wp-login.php" 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] was found in the following HTML form: [Form 1: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "redirect_to"].
	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%

URL	2Fabout-us%2F
Method	GET
Attack	
Evidence	<form name="loginform" id="loginform" action="http://192.168.123.30/wp-login.php" 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] was found in the following HTML form: [Form 1: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F
Method	GET
Attack	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "redirect_to"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	<form name="loginform" id="loginform" action="http://192.168.123.30/wp-login.php" 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] was found in the following HTML form: [Form 1: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "redirect_to"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F
Method	GET
Attack	
Evidence	<form name="loginform" id="loginform" action="http://192.168.123.30/wp-login.php" 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] was found in the following HTML form: [Form 1: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F

Method	GET
Attack	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "redirect_to"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	<form name="loginform" id="loginform" action="http://192.168.123.30/wp-login.php" 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] was found in the following HTML form: [Form 1: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "redirect_to"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F
Method	GET
Attack	
Evidence	<form name="loginform" id="loginform" action="http://192.168.123.30/wp-login.php" 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] was found in the following HTML form: [Form 1: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F
Method	GET
Attack	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "redirect_to"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB
Method	GET
Attack	

Evidence	<form name="loginform" id="loginform" action="http://192.168.123.30/wp-login.php" 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] was found in the following HTML form: [Form 1: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "redirect_to"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F
Method	GET
Attack	
Evidence	<form name="loginform" id="loginform" action="http://192.168.123.30/wp-login.php" 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] was found in the following HTML form: [Form 1: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F
Method	GET
Attack	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "redirect_to"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	<form name="loginform" id="loginform" action="http://192.168.123.30/wp-login.php" 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] was found in the following HTML form: [Form 1: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	<form id="language-switcher" action="" method="get">

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 2: "redirect_to"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fdestinations%2F
Method	GET
Attack	
Evidence	<form name="loginform" id="loginform" action="http://192.168.123.30/wp-login.php" 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] was found in the following HTML form: [Form 1: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fdestinations%2F
Method	GET
Attack	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "redirect_to"].
URL	http://192.168.123.30/wp-login.php?wp_lang=en_GB
Method	GET
Attack	
Evidence	<form name="loginform" id="loginform" action="http://192.168.123.30/wp-login.php" 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] was found in the following HTML form: [Form 1: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	http://192.168.123.30/wp-login.php?wp_lang=en_GB
Method	GET
Attack	
Evidence	<form id="language-switcher" action="" method="get">
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 2: ""].
URL	http://192.168.123.30/wp-login.php
Method	POST
Attack	
Evidence	<form name="loginform" id="loginform" action="http://192.168.123.30/wp-login.php" 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] was found in the following HTML form: [Form 1: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].

URL	http://192.168.123.30/wp-login.php
Method	POST
Attack	
Evidence	<form id="language-switcher" action="" method="get">
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 2: ""].
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	<form name="lostpasswordform" id="lostpasswordform" action="http://192.168.123.30/wp-login.php?action=lostpassword" 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] was found in the following HTML form: [Form 1: "redirect_to" "user_login" "wp-submit"].
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "action"].
Instances	49
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://192.168.123.30/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/2022/10/27/hello-world/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/2022/10/27/hello-world/?replytocom=1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/2022/10/27/hello-world/?replytocom=2
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/2022/10/27/hello-world/?replytocom=3
Method	GET
Attack	
Evidence	
Other	

Info	
URL	http://192.168.123.30/2022/10/27/hello-world/embed/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/2024/05/07/contact-us/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/2024/05/07/contact-us/embed/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/about-us/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/about-us/embed/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/author/alex/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/author/student/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/category/uncategorised/

Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/destinations
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/destinations/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/destinations/embed/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-admin/admin-ajax.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php?action=lostpassword&wp_lang=en_GB
Method	GET

Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F%3Freplytocom%3D1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB

Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	
Other	

Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fdestinations%2F
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php?wp_lang=en_GB
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-comments-post.php
Method	POST
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php
Method	POST
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	
Other	

Info	
Instances	40
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 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	**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://192.168.123.30/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/2022/10/27/hello-world/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/2022/10/27/hello-world/?replytocom=1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/2022/10/27/hello-world/?replytocom=2
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/2022/10/27/hello-world/?replytocom=3
Method	GET
Attack	
Evidence	

Other Info	
URL	http://192.168.123.30/2022/10/27/hello-world/embed/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/2024/05/07/contact-us/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/2024/05/07/contact-us/embed/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/about-us/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/about-us/embed/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/author/alex/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/author/student/
Method	GET
Attack	
Evidence	
Other Info	

URL	http://192.168.123.30/category/uncategorised/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/destinations
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/destinations/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/destinations/embed/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.123.30/wp-comments-post.php
Method	POST
Attack	
Evidence	
Other Info	
Instances	17
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

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://192.168.123.30/wp-login.php
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?action=lostpassword&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?action=lostpassword&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wp_lang
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
Attack	

Evidence	Set-Cookie: wp_lang
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F%3Freplytocom%3D1
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wp_lang
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB

Method	GET
Attack	
Evidence	Set-Cookie: wp_lang
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wp_lang
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wp_lang
Other Info	

URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wp_lang
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wp_lang
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fdestinations%2F
Method	GET
Attack	

Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wp_lang
Other Info	
URL	http://192.168.123.30/wp-comments-post.php
Method	POST
Attack	
Evidence	Set-Cookie: comment_author_a8c90a9396755f00f92986b973e8b1c9
Other Info	
URL	http://192.168.123.30/wp-comments-post.php
Method	POST
Attack	
Evidence	Set-Cookie: comment_author_email_a8c90a9396755f00f92986b973e8b1c9
Other Info	
URL	http://192.168.123.30/wp-comments-post.php
Method	POST
Attack	
Evidence	Set-Cookie: comment_author_url_a8c90a9396755f00f92986b973e8b1c9
Other Info	
URL	http://192.168.123.30/wp-login.php
Method	POST
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other	

Info	
Instances	34
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://192.168.123.30/wp-login.php
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?action=lostpassword&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?action=lostpassword&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wp_lang
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET

Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wp_lang
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F%3Freplytocom%3D1
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wp_lang
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%

URL	2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wp_lang
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wp_lang
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie

Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wp_lang
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wp_lang
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB
Method	GET

Attack	
Evidence	Set-Cookie: wp_lang
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fdestinations%2F
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?wp_lang=en_GB
Method	GET
Attack	
Evidence	Set-Cookie: wp_lang
Other Info	
URL	http://192.168.123.30/wp-comments-post.php
Method	POST
Attack	
Evidence	Set-Cookie: comment_author_a8c90a9396755f00f92986b973e8b1c9
Other Info	
URL	http://192.168.123.30/wp-comments-post.php
Method	POST
Attack	
Evidence	Set-Cookie: comment_author_email_a8c90a9396755f00f92986b973e8b1c9
Other Info	
URL	http://192.168.123.30/wp-comments-post.php
Method	POST
Attack	
Evidence	Set-Cookie: comment_author_url_a8c90a9396755f00f92986b973e8b1c9
Other Info	
URL	http://192.168.123.30/wp-login.php
Method	POST
Attack	

Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	Set-Cookie: wordpress_test_cookie
Other Info	
Instances	34
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	**Private IP Disclosure**
Description	A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.
URL	http://192.168.123.30/2022/10/27/hello-world/feed/
Method	GET
Attack	
Evidence	192.168.123.65
Other Info	192.168.123.65
URL	http://192.168.123.30/author/student/feed/
Method	GET
Attack	
Evidence	192.168.123.65
Other Info	192.168.123.65
URL	http://192.168.123.30/category/uncategorised/feed/
Method	GET
Attack	
Evidence	192.168.123.65
Other Info	192.168.123.65
URL	http://192.168.123.30/comments/feed/
Method	GET
Attack	
Evidence	192.168.123.65
Other Info	192.168.123.65
URL	http://192.168.123.30/feed/

Method	GET
Attack	
Evidence	192.168.123.65
Other Info	192.168.123.65
URL	http://192.168.123.30/wp-json/wp/v2/posts/1
Method	GET
Attack	
Evidence	192.168.123.65
Other Info	192.168.123.65
Instances	6
Solution	Remove the private IP address from the HTTP response body. For comments, use JSP/ASP /PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.
Reference	https://tools.ietf.org/html/rfc1918
CWE Id	200
WASC Id	13
Plugin Id	2

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://192.168.123.30/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/2022/10/27/hello-world/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/2022/10/27/hello-world/?replytocom=1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/2022/10/27/hello-world/?replytocom=2
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)

Other Info	
URL	http://192.168.123.30/2022/10/27/hello-world/?replytocom=3
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/2022/10/27/hello-world/embed/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/2022/10/27/hello-world/feed/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/2024/05/07/contact-us/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/2024/05/07/contact-us/embed/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/2024/05/07/contact-us/feed/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/?p=1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	

URL	http://192.168.123.30/?p=20
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/?p=37
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/?p=39
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/about-us/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/about-us/embed/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/author/alex/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/author/alex/feed/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/author/student/
Method	GET

Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/author/student/feed/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/category/uncategorised/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/category/uncategorised/feed/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/comments/feed/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/destinations
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/destinations/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/destinations/embed/
Method	GET
Attack	

Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/favicon.ico
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/feed/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/robots.txt
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/sitemap.xml
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-admin/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-admin/admin-ajax.php
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-admin/css/forms.min.css?ver=6.1.1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other	

Info	
URL	http://192.168.123.30/wp-admin/css/l10n.min.css?ver=6.1.1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-admin/css/login.min.css?ver=6.1.1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-admin/js/password-strength-meter.min.js?ver=6.1.1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-admin/js/user-profile.min.js?ver=6.1.1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/themes/archeo-wpcom/assets/fonts/Chivo-Bold.woff2
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/themes/archeo-wpcom/assets/fonts/Chivo-Regular.woff2
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/themes/archeo-wpcom/assets/fonts/Chivo-Thin.woff2
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/themes/archeo-wpcom/assets/images/palais-du-cirque.jpg

Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/themes/archeo-wpcom/style.css?ver=1.0.21
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/uploads/2024/05/cfd33950780ffb3baab671c30e82882c53f77227_s2_n3_y2-207x300.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/uploads/2024/05/cfd33950780ffb3baab671c30e82882c53f77227_s2_n3_y2.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/uploads/2024/05/Colosseum_-_Rome_-_Italy_16800139540-1024x546.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/uploads/2024/05/Colosseum_-_Rome_-_Italy_16800139540-1536x818.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/uploads/2024/05/Colosseum_-_Rome_-_Italy_16800139540-2048x1091.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	

URL	http://192.168.123.30/wp-content/uploads/2024/05/Colosseum_-_Rome_-_Italy_16800139540-300x160.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/uploads/2024/05/Colosseum_-_Rome_-_Italy_16800139540-768x409.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/uploads/2024/05/grandcanyon-1024x400.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/uploads/2024/05/grandcanyon-1536x600.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/uploads/2024/05/grandcanyon-300x117.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/uploads/2024/05/grandcanyon-768x300.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/uploads/2024/05/grandcanyon.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
	http://192.168.123.30/wp-content/uploads/2024/05/great-wall-china-tourists-GWOC0417-

URL	10bddbf0783644c386178f62117b2132-1024x640.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/uploads/2024/05/great-wall-china-tourists-GWOC0417-10bddbf0783644c386178f62117b2132-300x188.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/uploads/2024/05/great-wall-china-tourists-GWOC0417-10bddbf0783644c386178f62117b2132-768x480.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/uploads/2024/05/great-wall-china-tourists-GWOC0417-10bddbf0783644c386178f62117b2132.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/uploads/2024/05/statueofliberty_marleywhite_ade589d3-cd9a-bb18-49e62d2eff2efad5-1024x683.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/uploads/2024/05/statueofliberty_marleywhite_ade589d3-cd9a-bb18-49e62d2eff2efad5-1536x1024.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/uploads/2024/05/statueofliberty_marleywhite_ade589d3-cd9a-bb18-49e62d2eff2efad5-2048x1365.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)

Other Info	
URL	http://192.168.123.30/wp-content/uploads/2024/05/statueofliberty_marleywhite_ade589d3-cd9a-bb18-49e62d2eff2efad5-300x200.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-content/uploads/2024/05/statueofliberty_marleywhite_ade589d3-cd9a-bb18-49e62d2eff2efad5-768x512.jpg
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/blocks/cover/style.min.css?ver=6.1.1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/blocks/gallery/style.min.css?ver=6.1.1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/blocks/heading/style.min.css?ver=6.1.1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/blocks/navigation/style.min.css?ver=6.1.1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/blocks/navigation/view-modal.min.js?ver=45f05135277abf0b0408
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)

Other Info	
URL	http://192.168.123.30/wp-includes/blocks/navigation/view.min.js?ver=c24330f635f5cb9d5e0e
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/blocks/paragraph/style.min.css?ver=6.1.1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/css/buttons.min.css?ver=6.1.1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/css/dashicons.min.css?ver=6.1.1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/css/wp-embed-template-ie.min.css?ver=6.1.1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/images/w-logo-blue-white-bg.png
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/images/w-logo-blue.png
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	

URL	http://192.168.123.30/wp-includes/js/comment-reply.min.js?ver=6.1.1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/js/dist/hooks.min.js?ver=4169d3cf8e8d95a3d6d5
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/js/dist/i18n.min.js?ver=9e794f35a71bb98672ae
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/js/dist/vendor/regenerator-runtime.min.js?ver=0.13.9
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/js/jquery/jquery.min.js?ver=3.6.1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/js/underscore.min.js?ver=1.13.4

Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/js/wp-emoji-release.min.js?ver=6.1.1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/js/wp-util.min.js?ver=6.1.1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/js/zxcvbn-async.min.js?ver=1.0
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-includes/wlwmanifest.xml
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-json/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-json/oembed/1.0/embed?format=xml&url=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-json/oembed/1.0/embed?format=xml&url=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F
Method	GET

Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-json/oembed/1.0/embed?format=xml&url=http%3A%2F%2F192.168.123.30%2Fabout-us%2F
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-json/oembed/1.0/embed?format=xml&url=http%3A%2F%2F192.168.123.30%2Fdestinations%2F
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-json/oembed/1.0/embed?url=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-json/oembed/1.0/embed?url=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-json/oembed/1.0/embed?url=http%3A%2F%2F192.168.123.30%2Fabout-us%2F
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-json/oembed/1.0/embed?url=http%3A%2F%2F192.168.123.30%2Fdestinations%2F
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	

URL	http://192.168.123.30/wp-json/wp/v2/categories/1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-json/wp/v2/pages/20
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-json/wp/v2/pages/37
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-json/wp/v2/posts/1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-json/wp/v2/posts/39
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-json/wp/v2/users/1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-json/wp/v2/users/2
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php
Method	GET

Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php?action=lostpassword&wp_lang=en_GB
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F%3Freplytocom%3D1
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB

Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	

URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fdestinations%2F
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php?wp_lang=en_GB
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-sitemap-index.xsl
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)

Other Info	
URL	http://192.168.123.30/wp-sitemap-posts-page-1.xml
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-sitemap-posts-post-1.xml
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-sitemap-taxonomies-category-1.xml
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-sitemap-users-1.xml
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-sitemap.xml
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-sitemap.xsl
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/xmlrpc.php
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	

URL	http://192.168.123.30/xmlrpc.php?rsd
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-comments-post.php
Method	POST
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php
Method	POST
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Other Info	
Instances	135
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	200
WASC Id	13
Plugin Id	10036

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server - Unix
URL	http://192.168.123.30/destinations/embed/
Method	GET
Attack	
Evidence	1722420953
Other Info	1722420953, which evaluates to: 2024-07-31 11:15:53
Instances	1
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	200
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://192.168.123.30/
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://192.168.123.30/2022/10/27/hello-world/
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://192.168.123.30/2022/10/27/hello-world/?replytocom=1
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://192.168.123.30/2022/10/27/hello-world/?replytocom=2
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://192.168.123.30/2022/10/27/hello-world/?replytocom=3
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://192.168.123.30/2022/10/27/hello-world/embed/
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://192.168.123.30/2022/10/27/hello-world/feed/
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://192.168.123.30/2024/05/07/contact-us/
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://192.168.123.30/2024/05/07/contact-us/embed/
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://192.168.123.30/2024/05/07/contact-us/feed/
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://192.168.123.30/about-us/
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://192.168.123.30/about-us/embed/
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://192.168.123.30/author/alex/
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://192.168.123.30/author/alex/feed/
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://192.168.123.30/author/student/
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://192.168.123.30/author/student/feed/
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://192.168.123.30/category/uncategorised/
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://192.168.123.30/category/uncategorised/feed/
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://192.168.123.30/comments/feed/
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://192.168.123.30/destinations
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://192.168.123.30/destinations/
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://192.168.123.30/destinations/embed/
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://192.168.123.30/feed/
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://192.168.123.30/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.
URL	http://192.168.123.30/wp-admin/css/forms.min.css?ver=6.1.1
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://192.168.123.30/wp-admin/css/l10n.min.css?ver=6.1.1
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://192.168.123.30/wp-admin/css/login.min.css?ver=6.1.1
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://192.168.123.30/wp-admin/js/password-strength-meter.min.js?ver=6.1.1
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://192.168.123.30/wp-admin/js/user-profile.min.js?ver=6.1.1
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://192.168.123.30/wp-content/themes/archeo-wpcom/assets/fonts/Chivo-Bold.woff2

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://192.168.123.30/wp-content/themes/archeo-wpcom/assets/fonts/Chivo-Regular.woff2
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://192.168.123.30/wp-content/themes/archeo-wpcom/assets/fonts/Chivo-Thin.woff2
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://192.168.123.30/wp-content/themes/archeo-wpcom/assets/images/palais-du-cirque.jpg
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://192.168.123.30/wp-content/themes/archeo-wpcom/style.css?ver=1.0.21
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://192.168.123.30/wp-content/uploads/2024/05/cfd33950780ffb3baab671c30e82882c53f77227_s2_n3_y2-207x300.jpg
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.
	http://192.168.123.30/wp-content/uploads/2024/05

URL	/cfd33950780ffb3baab671c30e82882c53f77227_s2_n3_y2.jpg
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://192.168.123.30/wp-content/uploads/2024/05/Colosseum_-_Rome_-_Italy_16800139540-1024x546.jpg
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://192.168.123.30/wp-content/uploads/2024/05/Colosseum_-_Rome_-_Italy_16800139540-1536x818.jpg
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://192.168.123.30/wp-content/uploads/2024/05/Colosseum_-_Rome_-_Italy_16800139540-2048x1091.jpg
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://192.168.123.30/wp-content/uploads/2024/05/Colosseum_-_Rome_-_Italy_16800139540-300x160.jpg
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://192.168.123.30/wp-content/uploads/2024/05/Colosseum_-_Rome_-_Italy_16800139540-768x409.jpg
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	http://192.168.123.30/wp-content/uploads/2024/05/grandcanyon-1024x400.jpg
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://192.168.123.30/wp-content/uploads/2024/05/grandcanyon-1536x600.jpg
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://192.168.123.30/wp-content/uploads/2024/05/grandcanyon-300x117.jpg
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://192.168.123.30/wp-content/uploads/2024/05/grandcanyon-768x300.jpg
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://192.168.123.30/wp-content/uploads/2024/05/grandcanyon.jpg
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://192.168.123.30/wp-content/uploads/2024/05/great-wall-china-tourists-GWOC0417-10bddbf0783644c386178f62117b2132-1024x640.jpg
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	http://192.168.123.30/wp-content/uploads/2024/05/great-wall-china-tourists-GWOC0417-10bddbf0783644c386178f62117b2132-300x188.jpg
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://192.168.123.30/wp-content/uploads/2024/05/great-wall-china-tourists-GWOC0417-10bddbf0783644c386178f62117b2132-768x480.jpg
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://192.168.123.30/wp-content/uploads/2024/05/great-wall-china-tourists-GWOC0417-10bddbf0783644c386178f62117b2132.jpg
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://192.168.123.30/wp-content/uploads/2024/05/statueofliberty_marleywhite_ade589d3-cd9a-bb18-49e62d2eff2efad5-1024x683.jpg
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://192.168.123.30/wp-content/uploads/2024/05/statueofliberty_marleywhite_ade589d3-cd9a-bb18-49e62d2eff2efad5-1536x1024.jpg
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://192.168.123.30/wp-content/uploads/2024/05/statueofliberty_marleywhite_ade589d3-cd9a-bb18-49e62d2eff2efad5-2048x1365.jpg
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://192.168.123.30/wp-content/uploads/2024/05/statueofliberty_marleywhite_ade589d3-cd9a-bb18-49e62d2eff2efad5-300x200.jpg
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://192.168.123.30/wp-content/uploads/2024/05/statueofliberty_marleywhite_ade589d3-cd9a-bb18-49e62d2eff2efad5-768x512.jpg
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://192.168.123.30/wp-includes/blocks/cover/style.min.css?ver=6.1.1
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://192.168.123.30/wp-includes/blocks/gallery/style.min.css?ver=6.1.1
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://192.168.123.30/wp-includes/blocks/heading/style.min.css?ver=6.1.1
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://192.168.123.30/wp-includes/blocks/navigation/style.min.css?ver=6.1.1

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://192.168.123.30/wp-includes/blocks/navigation/view-modal.min.js?ver=45f05135277abf0b0408
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://192.168.123.30/wp-includes/blocks/navigation/view.min.js?ver=c24330f635f5cb9d5e0e
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://192.168.123.30/wp-includes/blocks/paragraph/style.min.css?ver=6.1.1
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://192.168.123.30/wp-includes/css/buttons.min.css?ver=6.1.1
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://192.168.123.30/wp-includes/css/dashicons.min.css?ver=6.1.1
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://192.168.123.30/wp-includes/css/wp-embed-template-ie.min.css?ver=6.1.1
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://192.168.123.30/wp-includes/images/w-logo-blue-white-bg.png
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://192.168.123.30/wp-includes/images/w-logo-blue.png
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://192.168.123.30/wp-includes/js/comment-reply.min.js?ver=6.1.1
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://192.168.123.30/wp-includes/js/dist/hooks.min.js?ver=4169d3cf8e8d95a3d6d5
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://192.168.123.30/wp-includes/js/dist/i18n.min.js?ver=9e794f35a71bb98672ae
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://192.168.123.30/wp-includes/js/dist/vendor/regenerator-runtime.min.js?ver=0.13.9

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://192.168.123.30/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0
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://192.168.123.30/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2
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://192.168.123.30/wp-includes/js/jquery/jquery.min.js?ver=3.6.1
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://192.168.123.30/wp-includes/js/underscore.min.js?ver=1.13.4
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://192.168.123.30/wp-includes/js/wp-emoji-release.min.js?ver=6.1.1
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://192.168.123.30/wp-includes/js/wp-util.min.js?ver=6.1.1

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://192.168.123.30/wp-includes/js/zxcvbn-async.min.js?ver=1.0
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://192.168.123.30/wp-includes/wlwmanifest.xml
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://192.168.123.30/wp-login.php
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://192.168.123.30/wp-login.php?action=lostpassword
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://192.168.123.30/wp-login.php?action=lostpassword&wp_lang=en_GB
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F%3Freplytocom%3D1
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fdestinations%2F
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://192.168.123.30/wp-login.php?wp_lang=en_GB
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://192.168.123.30/wp-sitemap-index.xsl
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://192.168.123.30/wp-sitemap-posts-page-1.xml
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://192.168.123.30/wp-sitemap-posts-post-1.xml
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://192.168.123.30/wp-sitemap-taxonomies-category-1.xml
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://192.168.123.30/wp-sitemap-users-1.xml
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://192.168.123.30/wp-sitemap.xml
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://192.168.123.30/wp-sitemap.xsl
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://192.168.123.30/xmlrpc.php?rsd
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://192.168.123.30/wp-comments-post.php
Method	POST
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://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php?action=lostpassword
Method	POST
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	110
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	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://192.168.123.30/wp-json/oembed/1.0/embed?format=xml&url=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F
Method	GET
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	http://192.168.123.30/wp-json/oembed/1.0/embed?format=xml&url=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F
Method	GET
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	http://192.168.123.30/wp-json/oembed/1.0/embed?format=xml&url=http%3A%2F%2F192.168.123.30%2Fabout-us%2F
Method	GET
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	http://192.168.123.30/wp-json/oembed/1.0/embed?format=xml&url=http%3A%2F%2F192.168.123.30%2Fdestinations%2F
Method	GET
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
Instances	4
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/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://192.168.123.30/wp-login.php?action=lostpassword&wp_lang=en_GB
Method	GET
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: http://192.168.123.30/wp-login.php?action=lostpassword&wp_lang=en_GB User-input was found in the following cookie: wp_lang=en_GB; path=/ The user input was: wp_lang=en_GB
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB User-input was found in the following cookie: wp_lang=en_GB; path=/ The user input was: wp_lang=en_GB
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB User-input was found in the following cookie: wp_lang=en_GB; path=/ The user input was: wp_lang=en_GB
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB User-input was found in the following cookie: wp_lang=en_GB; path=/ The user input was: wp_lang=en_GB
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB User-

	input was found in the following cookie: wp_lang=en_GB; path=/ The user input was: wp_lang=en_GB
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB User-input was found in the following cookie: wp_lang=en_GB; path=/ The user input was: wp_lang=en_GB
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB User-input was found in the following cookie: wp_lang=en_GB; path=/ The user input was: wp_lang=en_GB
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB User-input was found in the following cookie: wp_lang=en_GB; path=/ The user input was: wp_lang=en_GB
URL	http://192.168.123.30/wp-login.php?wp_lang=en_GB
Method	GET
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: http://192.168.123.30/wp-login.php?wp_lang=en_GB User-input was found in the following cookie: wp_lang=en_GB; path=/ The user input was: wp_lang=en_GB
URL	http://192.168.123.30/wp-comments-post.php
Method	POST
Attack	
Evidence	
Other	An attacker may be able to poison cookie values through POST parameters. To test if this is a more serious issue, you should try resending that request as a GET, with the POST parameter included as a query string parameter. For example: https://nottrusted.com/page?value=maliciousInput. This was identified at: http://192.168.123.30/wp-comments-post.php

Info	User-input was found in the following cookie: comment_author_a8c90a9396755f00f92986b973e8b1c9=ZAP; expires=Sat, 19-Apr-2025 17:40:57 GMT; Max-Age=30000000; path=/ The user input was: author=ZAP
URL	http://192.168.123.30/wp-comments-post.php
Method	POST
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through POST parameters. To test if this is a more serious issue, you should try resending that request as a GET, with the POST parameter included as a query string parameter. For example: https://nottrusted.com/page?value=maliciousInput. This was identified at: http://192.168.123.30/wp-comments-post.php User-input was found in the following cookie: comment_author_email_a8c90a9396755f00f92986b973e8b1c9=zaproxy@example.com; expires=Sat, 19-Apr-2025 17:40:57 GMT; Max-Age=30000000; path=/ The user input was: email=zaproxy@example.com
URL	http://192.168.123.30/wp-comments-post.php
Method	POST
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through POST parameters. To test if this is a more serious issue, you should try resending that request as a GET, with the POST parameter included as a query string parameter. For example: https://nottrusted.com/page?value=maliciousInput. This was identified at: http://192.168.123.30/wp-comments-post.php User-input was found in the following cookie: comment_author_url_a8c90a9396755f00f92986b973e8b1c9=https://zap.example.com; expires=Sat, 19-Apr-2025 17:40:57 GMT; Max-Age=30000000; path=/ The user input was: url=https://zap.example.com
Instances	12
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	https://en.wikipedia.org/wiki/HTTP_cookie https://cwe.mitre.org/data/definitions/565.html
CWE Id	565
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://192.168.123.30/2022/10/27/hello-world/embed/
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script> /*! This file is auto-generated */ !function(c,u){"use strict";var r,t,e,a=u.querySelector&&c.addEventListener,f=!1;fun", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/2024/05/07/contact-us/embed/
Method	GET
Attack	

Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script> /*! This file is auto-generated */ !function(c,u){"use strict";var r,t,e,a=u.querySelector&&c.addEventListener,f=!1;fun", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/about-us/embed/
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script> /*! This file is auto-generated */ !function(c,u){"use strict";var r,t,e,a=u.querySelector&&c.addEventListener,f=!1;fun", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/destinations/embed/
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script> /*! This file is auto-generated */ !function(c,u){"use strict";var r,t,e,a=u.querySelector&&c.addEventListener,f=!1;fun", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-admin/js/user-profile.min.js?ver=6.1.1
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "!function(o){var e,a,t,n,i,r,d,p,l,c,u=!1,h=wp.i18n.__;function f(){"function"!=typeof zxcvbn?setTimeout(f,50):(!a.val()||c.hasC", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-includes/blocks/navigation/view-modal.min.js?ver=45f05135277abf0b0408
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "!function(){"use strict";function e(e,t){for(var o=0;o<t.length;o++){var n=t[o];n.enumerable=n.enumerable||!1,n.configurable=!0,", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: ""undefined"==typeof jQuery.migrateMute&&(jQuery.migrateMute=!0),function(t){"use strict";"function"==typeof define&&define.amd?d", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-includes/js/jquery/jquery.min.js?ver=3.6.1
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.
URL	http://192.168.123.30/wp-includes/js/underscore.min.js?ver=1.13.4
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "!function(n,r){var t,e;"object"==typeof exports&&"undefined"!=typeof module?module.exports=r():"function"==typeof define&&define", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-includes/js/wp-emoji-release.min.js?ver=6.1.1
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "var twemoji=function(){"use strict";var f={base:"https://twemoji.maxcdn.com/v/14.0.2/",ext:".png",size:"72x72",className:"emoji"", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-includes/js/wp-util.min.js?ver=6.1.1
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "window.wp=window.wp||{},function(s){var t="undefined"==typeof _wpUtilSettings?{}:_wpUtilSettings;wp.template=_.memoize(function(", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script id='password-strength-meter-js-translations'> (function(domain, translations) { var localeData = translations.locale", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> function wp_attempt_focus() {setTimeout(function() {try {d = document.getElementById("user_", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php
Method	GET
Attack	
Evidence	user
Other	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script id='user-profile-js-extra'> var userProfileL10n = {"user_id":"0","nonce":"

Info	5508ef3dac"}; </script>", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script id='password-strength-meter-js-translations'> (function(domain, translations) { var localeData = translations.locale", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> function wp_attempt_focus() {setTimeout(function() {try {d = document.getElementById("user_", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script id='user-profile-js-extra'> var userProfileL10n = {"user_id":"0","nonce":" 5508ef3dac"}; </script>", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script id='password-strength-meter-js-translations'> (function(domain, translations) { var localeData = translations.locale", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> function wp_attempt_focus() {setTimeout(function() {try {d = document.getElementById("user_", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script id='user-profile-js-extra'> var userProfileL10n = {"user_id":"0","nonce":" 5508ef3dac"}; </script>", see evidence field for the suspicious comment/snippet.

URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script id='password-strength-meter-js-translations'> (function(domain, translations) { var localeData = translations.locale", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> function wp_attempt_focus() {setTimeout(function() {try {d = document.getElementById("user_", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script id='user-profile-js-extra'> var userProfileL10n = {"user_id":"0","nonce":"5508ef3dac"}; </script>", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F%3Freplytocom%3D1
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script id='password-strength-meter-js-translations'> (function(domain, translations) { var localeData = translations.locale", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F%3Freplytocom%3D1
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> function wp_attempt_focus() {setTimeout(function() {try {d = document.getElementById("user_", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F%3Freplytocom%3D1
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script id='user-profile-js-extra'> var userProfileL10n = {"user_id":"0","nonce":"5508ef3dac"}; </script>", see evidence field for the suspicious comment/snippet.

URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script id='password-strength-meter-js-translations'> (function(domain, translations) { var localeData = translations.locale", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> function wp_attempt_focus() {setTimeout(function() {try {d = document.getElementById("user_", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script id='user-profile-js-extra'> var userProfileL10n = {"user_id":"0","nonce":"5508ef3dac"}; </script>", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script id='password-strength-meter-js-translations'> (function(domain, translations) { var localeData = translations.locale", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> function wp_attempt_focus() {setTimeout(function() {try {d = document.getElementById("user_", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script id='user-profile-js-extra'> var userProfileL10n = {"user_id":"0","nonce":"5508ef3dac"}; </script>", see evidence field for the suspicious comment/snippet.

URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script id='password-strength-meter-js-translations'> (function(domain, translations) { var localeData = translations.locale", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> function wp_attempt_focus() {setTimeout(function() {try {d = document.getElementById("user_", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script id='user-profile-js-extra'> var userProfileL10n = {"user_id":"0","nonce":"5508ef3dac"}; </script>", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script id='password-strength-meter-js-translations'> (function(domain, translations) { var localeData = translations.locale", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> function wp_attempt_focus() {setTimeout(function() {try {d = document.getElementById("user_", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script id='user-profile-js-extra'> var userProfileL10n = {"user_id":"0","nonce":"5508ef3dac"}; </script>", see evidence field for the suspicious comment/snippet.

URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script id='password-strength-meter-js-translations'> (function(domain, translations) { var localeData = translations.locale", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> function wp_attempt_focus() {setTimeout(function() {try {d = document.getElementById("user_", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script id='user-profile-js-extra'> var userProfileL10n = {"user_id":"0","nonce":"5508ef3dac"}; </script>", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script id='password-strength-meter-js-translations'> (function(domain, translations) { var localeData = translations.locale", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> function wp_attempt_focus() {setTimeout(function() {try {d = document.getElementById("user_", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F
Method	GET
Attack	
Evidence	user
Other	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script id='user-profile-js-extra'> var userProfileL10n = {"user_id":"0","nonce":"

Info	5508ef3dac"}; </script>", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script id='password-strength-meter-js-translations'> (function(domain, translations) { var localeData = translations.locale", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> function wp_attempt_focus() {setTimeout(function() {try {d = document.getElementById("user_", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script id='user-profile-js-extra'> var userProfileL10n = {"user_id":"0","nonce":"5508ef3dac"}; </script>", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script id='password-strength-meter-js-translations'> (function(domain, translations) { var localeData = translations.locale", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> function wp_attempt_focus() {setTimeout(function() {try {d = document.getElementById("user_", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F
Method	GET
Attack	
Evidence	user
Other	The following pattern was used: \bUSER\b and was detected in the element starting with:

Info	"<script id='user-profile-js-extra'> var userProfileL10n = {"user_id":"0","nonce":"5508ef3dac"}; </script>", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script id='password-strength-meter-js-translations'> (function(domain, translations) { var localeData = translations.locale", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> function wp_attempt_focus() {setTimeout(function() {try {d = document.getElementById("user_", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script id='user-profile-js-extra'> var userProfileL10n = {"user_id":"0","nonce":"5508ef3dac"}; </script>", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script id='password-strength-meter-js-translations'> (function(domain, translations) { var localeData = translations.locale", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> function wp_attempt_focus() {setTimeout(function() {try {d = document.getElementById("user_", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F
Method	GET
Attack	
Evidence	user

Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script id='user-profile-js-extra'> var userProfileL10n = {"user_id":"0","nonce":" 5508ef3dac"}; </script>", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script id='password-strength-meter-js-translations'> (function(domain, translations) { var localeData = translations.locale", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> function wp_attempt_focus() {setTimeout(function() {try {d = document.getElementById("user_", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script id='user-profile-js-extra'> var userProfileL10n = {"user_id":"0","nonce":" 5508ef3dac"}; </script>", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fdestinations%2F
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script id='password-strength-meter-js-translations'> (function(domain, translations) { var localeData = translations.locale", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fdestinations%2F
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> function wp_attempt_focus() {setTimeout(function() {try {d = document.getElementById("user_", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fdestinations%2F
Method	GET
Attack	
Evidence	user

Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script id='user-profile-js-extra'> var userProfileL10n = {"user_id":"0","nonce":"5508ef3dac"}; </script>", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?wp_lang=en_GB
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script id='password-strength-meter-js-translations'> (function(domain, translations) { var localeData = translations.locale", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?wp_lang=en_GB
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> function wp_attempt_focus() {setTimeout(function() {try {d = document.getElementById("user_", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php?wp_lang=en_GB
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script id='user-profile-js-extra'> var userProfileL10n = {"user_id":"0","nonce":"5508ef3dac"}; </script>", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php
Method	POST
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script id='password-strength-meter-js-translations'> (function(domain, translations) { var localeData = translations.locale", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php
Method	POST
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> function wp_attempt_focus() {setTimeout(function() {try {d = document.getElementById("user_", see evidence field for the suspicious comment/snippet.
URL	http://192.168.123.30/wp-login.php
Method	POST
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script id='user-profile-js-extra'> var userProfileL10n = {"user_id":"0","nonce":"5508ef3dac"}; </script>", see evidence field for the suspicious comment/snippet.
Instances	68

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://192.168.123.30/
Method	GET
Attack	
Evidence	<a href="http://192.168.123.30" target="_self" rel="home" aria-current="page">Holiday Destinations</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://192.168.123.30/2022/10/27/hello-world/
Method	GET
Attack	
Evidence	<a href="http://192.168.123.30" target="_self" rel="home">Holiday Destinations</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://192.168.123.30/2022/10/27/hello-world/?replytocom=1
Method	GET
Attack	
Evidence	<a href="http://192.168.123.30" target="_self" rel="home">Holiday Destinations</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://192.168.123.30/2022/10/27/hello-world/?replytocom=2
Method	GET
Attack	
Evidence	<a href="http://192.168.123.30" target="_self" rel="home">Holiday Destinations</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://192.168.123.30/2022/10/27/hello-world/?replytocom=3
Method	GET
Attack	
Evidence	<a href="http://192.168.123.30" target="_self" rel="home">Holiday Destinations</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://192.168.123.30/2024/05/07/contact-us/
Method	GET
Attack	
Evidence	<a href="http://192.168.123.30" target="_self" rel="home">Holiday Destinations</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://192.168.123.30/about-us/
Method	GET
Attack	
Evidence	<a href="http://192.168.123.30" target="_self" rel="home">Holiday Destinations</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://192.168.123.30/author/alex/
Method	GET
Attack	
Evidence	<a href="http://192.168.123.30" target="_self" rel="home">Holiday Destinations</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://192.168.123.30/author/student/
Method	GET
Attack	
Evidence	<a href="http://192.168.123.30" target="_self" rel="home">Holiday Destinations</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://192.168.123.30/category/uncategorised/
Method	GET
Attack	
Evidence	<a href="http://192.168.123.30" target="_self" rel="home">Holiday Destinations</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://192.168.123.30/destinations
Method	GET
Attack	
Evidence	<a href="http://192.168.123.30" target="_self" rel="home">Holiday Destinations</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://192.168.123.30/destinations/
Method	GET
Attack	
Evidence	<a href="http://192.168.123.30" target="_self" rel="home">Holiday Destinations</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	12
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	Session Management Response Identified
Description	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	http://192.168.123.30/wp-login.php
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-login.php?action=lostpassword&wp_lang=en_GB
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F%3Freplytocom%3D1

Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie

URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fdestinations%2F
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-login.php?wp_lang=en_GB
Method	GET
Attack	
Evidence	WP%20Cookie%20check

Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-comments-post.php
Method	POST
Attack	
Evidence	https%3A%2F%2Fzap.example.com
Other Info	cookie:comment_author_url_a8c90a9396755f00f92986b973e8b1c9 cookie: comment_author_email_a8c90a9396755f00f92986b973e8b1c9
URL	http://192.168.123.30/wp-login.php
Method	POST
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	POST
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/2022/10/27/hello-world/embed
Method	GET
Attack	
Evidence	zaproxy%40example.com
Other Info	cookie:comment_author_email_a8c90a9396755f00f92986b973e8b1c9
URL	http://192.168.123.30/2022/10/27/hello-world/embed
Method	GET
Attack	
Evidence	https%3A%2F%2Fzap.example.com
Other Info	cookie:comment_author_url_a8c90a9396755f00f92986b973e8b1c9
URL	http://192.168.123.30/2022/10/27/hello-world/embed
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/2024/05/07/contact-us/embed
Method	GET
Attack	
Evidence	zaproxy%40example.com
Other Info	cookie:comment_author_email_a8c90a9396755f00f92986b973e8b1c9

URL	http://192.168.123.30/2024/05/07/contact-us/embed
Method	GET
Attack	
Evidence	https%3A%2F%2Fzap.example.com
Other Info	cookie:comment_author_url_a8c90a9396755f00f92986b973e8b1c9
URL	http://192.168.123.30/2024/05/07/contact-us/embed
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/?p=1
Method	GET
Attack	
Evidence	zaproxy%40example.com
Other Info	cookie:comment_author_email_a8c90a9396755f00f92986b973e8b1c9
URL	http://192.168.123.30/?p=1
Method	GET
Attack	
Evidence	https%3A%2F%2Fzap.example.com
Other Info	cookie:comment_author_url_a8c90a9396755f00f92986b973e8b1c9
URL	http://192.168.123.30/author/alex/feed
Method	GET
Attack	
Evidence	zaproxy%40example.com
Other Info	cookie:comment_author_email_a8c90a9396755f00f92986b973e8b1c9
URL	http://192.168.123.30/author/alex/feed
Method	GET
Attack	
Evidence	https%3A%2F%2Fzap.example.com
Other Info	cookie:comment_author_url_a8c90a9396755f00f92986b973e8b1c9
URL	http://192.168.123.30/author/alex/feed
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-admin/js
Method	GET

Attack	
Evidence	zaproxy%40example.com
Other Info	cookie:comment_author_email_a8c90a9396755f00f92986b973e8b1c9
URL	http://192.168.123.30/wp-admin/js
Method	GET
Attack	
Evidence	https%3A%2F%2Fzap.example.com
Other Info	cookie:comment_author_url_a8c90a9396755f00f92986b973e8b1c9
URL	http://192.168.123.30/wp-admin/js
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-admin/js/user-profile.min.js?ver=6.1.1
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-includes/blocks/heading/style.min.css?ver=6.1.1
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-includes/images
Method	GET
Attack	
Evidence	zaproxy%40example.com
Other Info	cookie:comment_author_email_a8c90a9396755f00f92986b973e8b1c9
URL	http://192.168.123.30/wp-includes/images
Method	GET
Attack	
Evidence	https%3A%2F%2Fzap.example.com
Other Info	cookie:comment_author_url_a8c90a9396755f00f92986b973e8b1c9
URL	http://192.168.123.30/wp-includes/images
Method	GET
Attack	

Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-json/wp/v2/categories/1
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	http://192.168.123.30/wp-json/wp/v2/users/1
Method	GET
Attack	
Evidence	zaproxy%40example.com
Other Info	cookie:comment_author_email_a8c90a9396755f00f92986b973e8b1c9
URL	http://192.168.123.30/wp-json/wp/v2/users/1
Method	GET
Attack	
Evidence	https%3A%2F%2Fzap.example.com
Other Info	cookie:comment_author_url_a8c90a9396755f00f92986b973e8b1c9
URL	http://192.168.123.30/wp-json/wp/v2/users/1
Method	GET
Attack	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
Instances	46
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/session-mgmt-id
CWE Id	
WASC Id	
Plugin Id	10112

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://192.168.123.30/2022/10/27/hello-world/?replytocom=1
Method	GET
Attack	
Evidence	
Other	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://192.168.123.30/2022/10/27/hello-world/?replytocom=1 appears to include user input in: a(n) [meta] tag [content]

Info	attribute The user input found was: replytocom=1 The user-controlled value was: width=device-width, initial-scale=1
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	GET
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://192.168.123.30/wp-login.php?action=lostpassword appears to include user input in: a(n) [form] tag [id] attribute The user input found was: action=lostpassword The user-controlled value was: lostpasswordform
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	GET
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://192.168.123.30/wp-login.php?action=lostpassword appears to include user input in: a(n) [form] tag [name] attribute The user input found was: action=lostpassword The user-controlled value was: lostpasswordform
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	GET
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://192.168.123.30/wp-login.php?action=lostpassword appears to include user input in: a(n) [input] tag [value] attribute The user input found was: action=lostpassword The user-controlled value was: lostpassword
URL	http://192.168.123.30/wp-login.php?action=lostpassword&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?action=lostpassword&wp_lang=en_GB appears to include user input in: a(n) [form] tag [id] attribute The user input found was: action=lostpassword The user-controlled value was: lostpasswordform
URL	http://192.168.123.30/wp-login.php?action=lostpassword&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?action=lostpassword&wp_lang=en_GB appears to include user input in: a(n) [form] tag [name] attribute The user input found was: action=lostpassword The user-controlled value was: lostpasswordform
URL	http://192.168.123.30/wp-login.php?action=lostpassword&wp_lang=en_GB
Method	GET
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if

Other Info	XSS might be possible. The page at the following URL: http://192.168.123.30/wp-login.php?action=lostpassword&wp_lang=en_GB appears to include user input in: a(n) [input] tag [value] attribute The user input found was: action=lostpassword The user-controlled value was: lostpassword
URL	http://192.168.123.30/wp-login.php?action=lostpassword&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?action=lostpassword&wp_lang=en_GB appears to include user input in: a(n) [option] tag [value] attribute The user input found was: wp_lang=en_GB The user-controlled value was: en_gb
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-login.php?action=lostpassword
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F appears to include user input in: a(n) [form] tag [action] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-login.php
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F

Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-admin/css/forms.min.css?ver=6.1.1
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-admin/css/l10n.min.css?ver=6.1.1
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-admin/css/login.min.css?ver=6.1.1
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/css/buttons.min.css?ver=6.1.1
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/css/dashicons.min.css?ver=6.1.1
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if

Other Info	XSS might be possible. The page at the following URL: http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-admin/js/password-strength-meter.min.js?ver=6.1.1
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-admin/js/user-profile.min.js?ver=6.1.1
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/dist/hooks.min.js?ver=4169d3cf8e8d95a3d6d5
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/dist/i18n.min.js?ver=9e794f35a71bb98672ae
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/dist/vendor/regenerator-runtime.min.js?ver=0.13.9
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The

	user-controlled value was: http://192.168.123.30/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/jquery/jquery.min.js?ver=3.6.1
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/underscore.min.js?ver=1.13.4
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/wp-util.min.js?ver=6.1.1
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/zxcvbn-async.min.js?ver=1.0

URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-login.php?action=lostpassword
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [form] tag [action] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-login.php
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-admin/css/forms.min.css?ver=6.1.1

URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-admin/css/l10n.min.css?ver=6.1.1
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-admin/css/login.min.css?ver=6.1.1
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/css/buttons.min.css?ver=6.1.1
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/css/dashicons.min.css?ver=6.1.1
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.

	168.123.30/ The user-controlled value was: http://192.168.123.30/wp-admin/js/password-strength-meter.min.js?ver=6.1.1
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-admin/js/user-profile.min.js?ver=6.1.1
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/dist/hooks.min.js?ver=4169d3cf8e8d95a3d6d5
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/dist/i18n.min.js?ver=9e794f35a71bb98672ae
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/dist/vendor/regenerator-runtime.min.js?ver=0.13.9
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if

Other Info	XSS might be possible. The page at the following URL: http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/jquery/jquery.min.js?ver=3.6.1
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/underscore.min.js?ver=1.13.4
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/wp-util.min.js?ver=6.1.1
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/zxcvbn-async.min.js?ver=1.0
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F&wp_lang=en_GB appears to include user input in: a(n) [option] tag [value] attribute The user input found was: wp_lang=en_GB The user-controlled value was: en_gb
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/2022/10/27/hello-world/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/2022/10/27/hello-world/ The user-controlled value was: http://192.168.123.30/2022/10/27/hello-world/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F%3Freplytocom%3D1
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F%3Freplytocom%3D1 appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/2022/10/27/hello-world/?replytocom=1 The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F%3Freplytocom%3D1
Method	GET

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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F%3Freplytocom%3D1 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/2022/10/27/hello-world/?replytocom=1 The user-controlled value was: http://192.168.123.30/2022/10/27/hello-world/?replytocom=1
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/2022/10/27/hello-world/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/2022/10/27/hello-world/ The user-controlled value was: http://192.168.123.30/2022/10/27/hello-world/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2022%2F10%2F27%2Fhello-world%2F&wp_lang=en_GB appears to include user input in: a(n) [option] tag [value] attribute The user input found was: wp_lang=en_GB The user-controlled value was: en_gb
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/2024/05/07/contact-us/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F

Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/2024/05/07/contact-us/ The user-controlled value was: http://192.168.123.30/2024/05/07/contact-us/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/2024/05/07/contact-us/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/2024/05/07/contact-us/ The user-controlled value was: http://192.168.123.30/2024/05/07/contact-us/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2F2024%2F05%2F07%2Fcontact-us%2F&wp_lang=en_GB appears to include user input in: a(n) [option] tag [value] attribute The user input found was: wp_lang=en_GB The user-controlled value was: en_gb
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/about-us/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F

Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/about-us/ The user-controlled value was: http://192.168.123.30/about-us/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/about-us/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/about-us/ The user-controlled value was: http://192.168.123.30/about-us/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fabout-us%2F&wp_lang=en_GB appears to include user input in: a(n) [option] tag [value] attribute The user input found was: wp_lang=en_GB The user-controlled value was: en_gb
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/author/alex/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F

Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/author/alex/ The user-controlled value was: http://192.168.123.30/author/alex/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/author/alex/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/author/alex/ The user-controlled value was: http://192.168.123.30/author/alex/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Falex%2F&wp_lang=en_GB appears to include user input in: a(n) [option] tag [value] attribute The user input found was: wp_lang=en_GB The user-controlled value was: en_gb
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/author/student/ The user-controlled value was: http://192.168.123.30/
	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%

URL	2Fauthor%2Fstudent%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/author/student/ The user-controlled value was: http://192.168.123.30/author/student/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/author/student/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/author/student/ The user-controlled value was: http://192.168.123.30/author/student/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fauthor%2Fstudent%2F&wp_lang=en_GB appears to include user input in: a(n) [option] tag [value] attribute The user input found was: wp_lang=en_GB The user-controlled value was: en_gb
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/category/uncategorised/ The user-controlled value was: http://192.168.123.30/

URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/category/uncategorised/ The user-controlled value was: http://192.168.123.30/category/uncategorised/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/category/uncategorised/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/category/uncategorised/ The user-controlled value was: http://192.168.123.30/category/uncategorised/
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fcategory%2Funcategorised%2F&wp_lang=en_GB appears to include user input in: a(n) [option] tag [value] attribute The user input found was: wp_lang=en_GB The user-controlled value was: en_gb
URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fdestinations%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fdestinations%2F appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/destinations/ The user-controlled value was: http://192.168.123.30/

URL	http://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fdestinations%2F
Method	GET
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://192.168.123.30/wp-login.php?redirect_to=http%3A%2F%2F192.168.123.30%2Fdestinations%2F appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/destinations/ The user-controlled value was: http://192.168.123.30/destinations/
URL	http://192.168.123.30/wp-login.php?wp_lang=en_GB
Method	GET
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://192.168.123.30/wp-login.php?wp_lang=en_GB appears to include user input in: a(n) [option] tag [value] attribute The user input found was: wp_lang=en_GB The user-controlled value was: en_gb
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-login.php?action=lostpassword
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/2022/10/27/hello-world/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if

Other Info	XSS might be possible. The page at the following URL: http://192.168.123.30/wp-login.php appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/about-us/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/author/alex/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/author/student/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/category/uncategorised/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [form] tag [action] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-login.php
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/
URL	http://192.168.123.30/wp-login.php
Method	POST

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://192.168.123.30/wp-login.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/2022/10/27/hello-world/ The user-controlled value was: http://192.168.123.30/2022/10/27/hello-world/
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/about-us/ The user-controlled value was: http://192.168.123.30/about-us/
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/author/alex/ The user-controlled value was: http://192.168.123.30/author/alex/
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/author/student/ The user-controlled value was: http://192.168.123.30/author/student/
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=http://192.168.123.30/category/uncategorised/ The user-controlled value was: http://192.168.123.30/category/uncategorised/
URL	http://192.168.123.30/wp-login.php
Method	POST
Attack	
Evidence	
Other	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://192.168.123.30/wp-login.php appears to include user input in: a(n) [link] tag [href] attribute The user input found was:

Info	redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-admin/css/forms.min.css?ver=6.1.1
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-admin/css/l10n.min.css?ver=6.1.1
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-admin/css/login.min.css?ver=6.1.1
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/css/buttons.min.css?ver=6.1.1
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/css/dashicons.min.css?ver=6.1.1
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-admin/js/password-strength-meter.min.js?ver=6.1.1
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-admin/js/user-profile.min.js?ver=6.1.1
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/dist/hooks.min.js?ver=4169d3cf8e8d95a3d6d5
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/dist/i18n.min.js?ver=9e794f35a71bb98672ae
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/dist/vendor/regenerator-runtime.min.js?ver=0.13.9
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.3.2

URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/jquery/jquery.min.js?ver=3.6.1
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/underscore.min.js?ver=1.13.4
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/wp-util.min.js?ver=6.1.1
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=http://192.168.123.30/ The user-controlled value was: http://192.168.123.30/wp-includes/js/zxcvbn-async.min.js?ver=1.0
URL	http://192.168.123.30/wp-login.php
Method	POST
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://192.168.123.30/wp-login.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: rememberme=forever The user-controlled value was: forever
URL	http://192.168.123.30/wp-login.php
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if

Other Info	XSS might be possible. The page at the following URL: http://192.168.123.30/wp-login.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: wp-submit=Log In The user-controlled value was: log in
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	POST
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://192.168.123.30/wp-login.php?action=lostpassword appears to include user input in: a(n) [form] tag [id] attribute The user input found was: action=lostpassword The user-controlled value was: lostpasswordform
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	POST
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://192.168.123.30/wp-login.php?action=lostpassword appears to include user input in: a(n) [form] tag [name] attribute The user input found was: action=lostpassword The user-controlled value was: lostpasswordform
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	POST
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://192.168.123.30/wp-login.php?action=lostpassword appears to include user input in: a(n) [input] tag [value] attribute The user input found was: action=lostpassword The user-controlled value was: lostpassword
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	POST
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://192.168.123.30/wp-login.php?action=lostpassword appears to include user input in: a(n) [input] tag [value] attribute The user input found was: user_login=ZAP The user-controlled value was: zap
URL	http://192.168.123.30/wp-login.php?action=lostpassword
Method	POST
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://192.168.123.30/wp-login.php?action=lostpassword appears to include user input in: a(n) [input] tag [value] attribute The user input found was: wp-submit=Get New Password The user-controlled value was: get new password
Instances	121
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