# Report Draft

## Title: Critical WordPress Exploit Chain

## Executive Summary

This report documents a successful exploitation of a vulnerable WordPress instance hosted on 192.168.18.140. The attack leveraged outdated WordPress core and theme components, culminating in remote code execution via authenticated access and reverse shell deployment. No XSS vulnerabilities were confirmed during testing.

## Findings

|  |  |
| --- | --- |
| Item | Details |
| Host | 192.168.18.140 |
| WordPress Version | 4.3.1 (released 2015-09-15) |
| Theme | TwentyFifteen v1.3 (outdated) |
| Credentials | elliot / ER28-0652 |
| Exploit Chain | Authenticated login → Theme editor RCE → Reverse shell |
| Payload | Bash reverse shell via index.php |
| Shell Access | Achieved via Netcat listener |

## Exploit Log

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Exploit ID | Description | Target IP | Status | Payload |
| 1 | Auth RCE via Theme | 192.168.18.140 | Success | Bash Reverse Shell |

## Evidence

* Login success with “elliot / ER28-0652”
* Reverse shell triggered via index.php
* Netcat listener received shell
* whoami confirmed web server user
* Shell stabilized using python -c 'import pty; pty.spawn("/bin/bash")'

## Remediation

* Immediately update WordPress core to latest version
* Replace outdated themes and plugins
* Disable theme editor in production (define('DISALLOW\_FILE\_EDIT', true);)
* Enforce strong credentials and 2FA
* Restrict access to /wp-login.php and /xmlrpc.php
* Enable Web Application Firewall (WAF)