Laurence Bramblett

# Project 7 - WordPress Pentesting

Time spent: \*\*X\*\* hours spent in total

> Objective: Find, analyze, recreate, and document \*\*five vulnerabilities\*\* affecting an old version of WordPress

## Pentesting Report

### 1. (Required) Vulnerability Name or ID

- [ ] Summary: Enumerating Users

- Vulnerability types: Web Application vulnerability

- Tested in version:4.2

- Fixed in version: 4.6

- [ ] GIF Walkthrough:

- [ ] Steps to recreate: Use command wpscan --url http://192.168.33.10/ -e u vt

- [ ] Affected source code:

- [Link 1](https://core.trac.wordpress.org/browser/tags/version/src/source\_file.php)

### 2. (Required) Vulnerability Name or ID User Enumerating “2” CVE 2009-2335

- [ ] Summary: You will receive a “confirmation” if you have chosen a correct username.

- Vulnerability types: Information Exposure

- Tested in version:4.2

- Fixed in version: unknown

- [ ] GIF Walkthrough:

- [ ] Steps to recreate: Enter a username with any password and the ERROR message will tell you if it is a valid username.

- [ ] Affected source code:

- [Link 1](https://core.trac.wordpress.org/browser/tags/version/src/source\_file.php)

### 3. (Required) Vulnerability Name or ID Information Overexposure

- [ ] Summary: You can navigate to /wp-admin/css or /wp-admin/js to view the directory listing

- Vulnerability types: Information Overexposure

- Tested in version: 4.2

- Fixed in version: unknown

- [ ] GIF Walkthrough:

- [ ] Steps to recreate: navigate to /wp-admin/css or /wp-admin/js to view directories.

- [ ] Affected source code:

- [Link 1](https://core.trac.wordpress.org/browser/tags/version/src/source\_file.php)

## Assets

List any additional assets, such as scripts or files

WPScan

## Resources

- [WordPress Source Browser](https://core.trac.wordpress.org/browser/)

- [WordPress Developer Reference](https://developer.wordpress.org/reference/)

GIFs created with ScreenToGif.

## Notes

Describe any challenges encountered while doing the work