Ben Farrell

CSCI 480 Cybersecurity

4/15/18

**Week 7 Assignment** – Wordpress vulnerability testing in Kali linux environment

**Time spent:**

About 17 hours in total

**Pentest results:**

**1.** Legacy Theme Preview Cross-Site Scripting

- Vulnerability types: XSS Vulnerability

- Tested in version: 4.2.3

- Fixed in version: 4.2.4

- Affected source code: Theme

- <https://blog.sucuri.net/2015/08/persistent-xss-vulnerability-in-wordpress-explained.html>

**2.** User List Table Cross-Site Scripting

- Vulnerability types: XSS Vulnerability

- Tested in version: 4.3

- Fixed in version: 4.3.1

- Affected source code: Users

- https://github.com/WordPress/WordPress/commit/f91a5fd10ea7245e5b41e288624819a37adf290a

**3.** SSRF Bypass using Octal & Hexedecimal IP addresses

- Vulnerability types: SSRF Vulnerability

- Tested in version: 4.4.2

- Fixed in version: 4.5

- Affected source code: IP Address

- <https://github.com/WordPress/WordPress/commit/af9f0520875eda686fd13a427fd3914d7aded049>

**3.** Unauthorized Category Removal from Post

- Vulnerability types: XSS Vulnerability

- Tested in version: 2.5.0-4.5.0

- Fixed in version: 4.5

- Affected source code: Posts

- https://github.com/WordPress/WordPress/commit/6d05c7521baa980c4efec411feca5e7fab6f307c

**Resources used:**

-Kali Linux

-Oracle VMBox

-Powershell

-Licecap

-Vagrant

-WPScan

-Wordpress

-Notepad

-Word

-Github

**Recap:**

This was a long and tedious task for me. I was dealing with a lot of version matching issues, having to uninstall and start from scratch a few times. It eventually all came together, which was almost a blessing in disguise because I learned how to do it pretty well with how many times I had to redo it all.