WEEK 7 LAB ~ WORDPRESS VULNERABILITIES

Vulnerability 1:

User Enumeration, WordPress version 4.2

After attempting multiple logins, we noticed that the first login attempt returns invalid username. Next we tried admin and were prompted with a warning saying “The password you entered for the username Admin is incorrect.” This vulnerability demonstrates that a user can sufficiently determine a correct username and potentially brute force a password.

Vulnerability 2:

XSS, WordPress version 4.2

We found a XSS bug that allows a script to be executed in the comments section of a post. A simple script was inserted and enabled a pop up window to appear.

Vulnerability 3:

XSS WordPress version 4.2

User Enumeration, WordPress 4.2:

The following is a vulnerability that allows anyone the ability to enumerate a list of valid user names on a WordPress site. Although more a design flaw than that of a technical flaw in code, this creates an easier brute force attack for any malicious hacker.

XSS 2, CVE-2017-9061, Test Version: WordPress 4.7.4, patched WordPress 4.7.5:

If a wordpress admin is tricked into attempting to load a bogus media file exceeding maximum allowed file size through upload.php, a carefully crafted file name will allow the execution of cross site scripting. This is due to the lack of file name sanitation.