Week 7

Kunal Patel

# Project 7 - WordPress Pen testing

Time spent: 4 hours spent in total

- [ ] Summary:

1. Go to a post

Embedded button with malicious link

Click on the button

Got a message that says “alert”

- Vulnerability types: XSS

- Tested in version: 4.5.1

- Fixed in version: 4.2.8

- [ ] Affected source code: http://localhost/?p=4&trashed=1&ids=3



2.

[ ] Summary: 

- Vulnerability types: XSS

- Tested in version: 4.5.1

- Fixed in version: 4.2.8

- [ ] Affected source code:

https://wpvulndb.com/vulnerabilities/8718



3.

[ ] Summary:

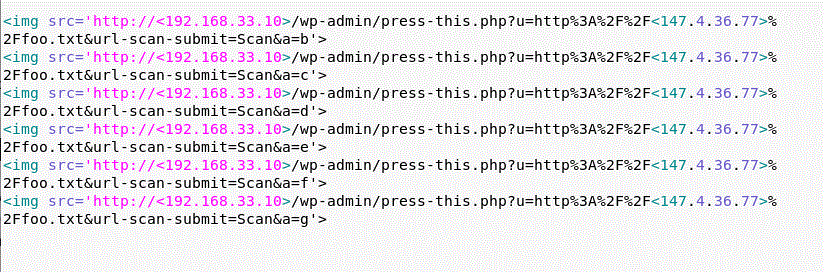
This is a simple javascript injection. Insert the following injection with a string long enough to not be truncated

- Vulnerability types: authentication weakness

- Tested in version: 4.5.3

- Fixed in version: 4.7.3

- [ ] Affected source code: http://localhost/wp-admin/press-this.php?



4.

Authenticated stored cross-site scripting

[ ] Summary:

Steps to recreate: create an image file name with cross-site scripting injected for an which is used as the image title in the attachment pages html, when we upload an image with an injected file name, we can penetrate the site, after waiting for an admin to upload the file - Vulnerability types: Insufficient validation

- Tested in version: 4.5.3

- Fixed in version: 4.6.1

- [ ] Affected source code: https://wordpress.org/news/2015/09/wordpress-4-3-1/

