Project 7 - WordPress Pentesting

Time spent: **2** hours spent in total

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

Pentesting Report

1. (Required) Upload same origin method execution CVE:2016-4566
  - [ ] Summary: I read the links to find the code and then changed it to localhost which is the victim ur. When the user clicks on the malicious button, the popup shows up.

2. (Required) Unauthenticated stored cross-site-scripting (xss) CVE:36844
  - [ ] Summary:
I created a new file and tested its size. I changed the file to make it larger, above 64Kb
After I uploaded the code to the comment, the popup appeared
  - [ ] GIF Walkthrough: the comment and the
  - [ ] Steps to recreate:
  - [ ] Affected source code:
    - [Link 1](https://core.trac.wordpress.org/browser/tags/version/src/source_file.php)
3. (Required) Vulnerability Name or ID: Large file
  - [ ] Summary:
   I upload a media file to WordPress that has an exploit by using the max size.
Find an image to upload that is above 2MB, and in the name of the file add following code

<img src=x onerror=alert(1)>.png