Information Security Project Proposal

Authors: Andriy Polulyakh and Valentina Prighel

**Main Objective**: Creation of an automated penetration testing platform for a specific target CMS.

**Target**: Wordpress CMS

Vulnerabilities to test:  
  
XSS: <https://www.exploitalert.com/view-details.html?id=32881>

SQL Injection: <https://www.exploitalert.com/view-details.html?id=32093>

SQL Injection: <https://www.exploitalert.com/view-details.html?id=32094>

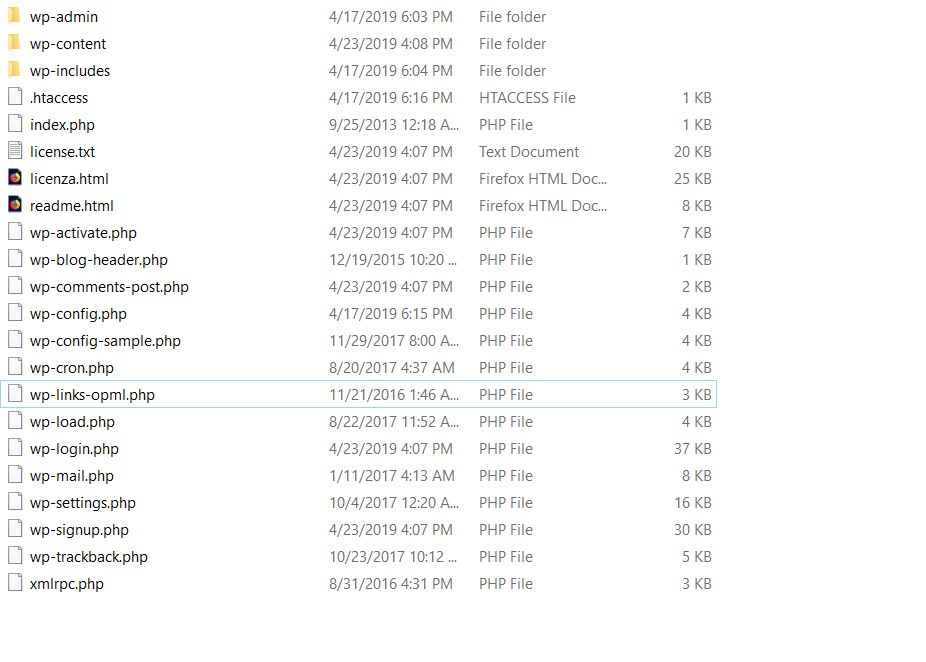
Remote Code upload and execution: <https://www.exploitalert.com/view-details.html?id=32184>

Arbitrary file download on different themes, by following this example vulnerability:

<https://www.exploitalert.com/view-details.html?id=32768>

(The idea is to test some general cases , for example theme\_name/download.php?file=//../../wpconfig.php) and also to test the vulnerability on some already known themes that suffer this problem.

To gain information about the system, we are going to interface our penetration testing application with WPScan.



Since WordPress uses the same basic architecture in all the builds we have the possibility and the advantage to have a really well-defined idea of how the target platform looks like. Moreover we have access to some plugins that we are going to test, therefore we could access the code directly and better understand the vulnerabilities.