

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.

 wp-admin	4/17/2019 6:03 PM	File folder	
 wp-content	4/23/2019 4:08 PM	File folder	
 wp-includes	4/17/2019 6:04 PM	File folder	
 .htaccess	4/17/2019 6:16 PM	HTACCESS File	1 KB
 index.php	9/25/2013 12:18 A...	PHP File	1 KB
 license.txt	4/23/2019 4:07 PM	Text Document	20 KB
 licenza.html	4/23/2019 4:07 PM	Firefox HTML Doc...	25 KB
 readme.html	4/23/2019 4:07 PM	Firefox HTML Doc...	8 KB
 wp-activate.php	4/23/2019 4:07 PM	PHP File	7 KB
 wp-blog-header.php	12/19/2015 10:20 ...	PHP File	1 KB
 wp-comments-post.php	4/23/2019 4:07 PM	PHP File	2 KB
 wp-config.php	4/17/2019 6:15 PM	PHP File	4 KB
 wp-config-sample.php	11/29/2017 8:00 A...	PHP File	4 KB
 wp-cron.php	8/20/2017 4:37 AM	PHP File	4 KB
 wp-links-opml.php	11/21/2016 1:46 A...	PHP File	3 KB
 wp-load.php	8/22/2017 11:52 A...	PHP File	4 KB
 wp-login.php	4/23/2019 4:07 PM	PHP File	37 KB
 wp-mail.php	1/11/2017 4:13 AM	PHP File	8 KB
 wp-settings.php	10/4/2017 12:20 A...	PHP File	16 KB
 wp-signup.php	4/23/2019 4:07 PM	PHP File	30 KB
 wp-trackback.php	10/23/2017 10:12 ...	PHP File	5 KB
 xmlrpc.php	8/31/2016 4:31 PM	PHP File	3 KB

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.