**HACKING WORDPRESS WITH WPSCAN**

WordPress is a free open source content management system. Thousands of Web sites run WordPress, and it is considered the top blogging platform in the world. According to [*Usage Statistics and Market Share of Content*](http://w3techs.com/technologies/overview/content_management/all/)[*Management Systems for Websites* (](http://w3techs.com/technologies/overview/content_management/all/)W3Techs. January 2015. Retrieved January 2015), 23% of the world’s top

10 million Web sites use WordPress.

So…let’s hack WordPress!

We are going to use WPScan to test our WordPress installation. This is a security scanner that attempts to find known security weaknesses within WordPress installations. The application is provided for free on the wpscan.org site, and the intended audience is security professionals or WordPress administrators. WPScan is used to determine the security posture of WordPress installations.

The main features of WPScan include:

o Username enumeration (from the author)

o Multi-threaded, weak password cracking

o Version enumeration (from the generator meta tag)

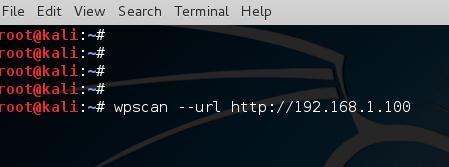
o Vulnerability enumeration, which is based on the installed version

o Plugin enumeration using the To-Do plugin

o It also includes a variety of other security checks

The syntax to get started with WPScan is:

*wpscan –-url wordpress\_url*

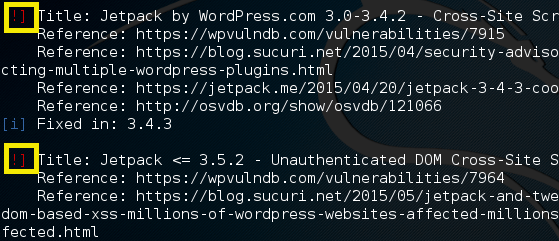


Note: The first time you run it, you may find that you need to update the database.



You should be able to quickly determine the WordPress version, which plugins are installed, and what theme is active when you open the scanner.

The first thing we will do is look for lines beginning with a red plus (+). These are the known WordPress vulnerabilities.



If the correct vulnerability exists, you can enumerate a user list from WordPress with the following command:

*wpscan –-url wordpress\_url –-enumerate u*



I ran the command, and you can see WPScan discovered usernames on this system:



Once user names have been collected, you then can attempt to brute force crack the associated passwords. In order to so, you will need a password list. Kali has a number of different wordlists at this location:

You can also download our custom word list from here: **/usr/share/wordlists WARNING: DO A SAVE AS OR YOUR BROWSER MAY CRASH** <http://www.drchaos.com/public_files/chaos-dictionary.lst.txt>

If you prefer, you can also use this link to get a tool to create your own word lists:

[**Dr. Chaos – Creating Custom Worldlists and Dictionary Files**](http://www.drchaos.com/creating-custom-dictionary-files-using-cewl/)

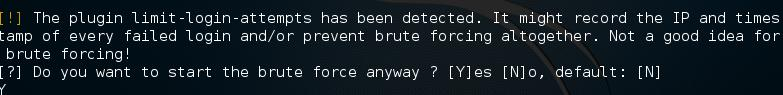
To brute force crack passwords associated with usernames, use the following command:

*wpscan –-url [wordpress\_url] –-word list [path\_to\_world list] –-username [username to bruteforce]*

*–threads [number of threads]*



Some installations of WordPress will make it very difficult to brute force the password.



If this happens, we might need to rethink our approach.

The result? If you are lucky, you can see WPScan was able to crack the password with the results below.



Please note that not all versions of WordPress are vulnerable, and many hosted service providers are now providing automatic patching and upgrading. However, WPScan is a great way of testing your own environment and ensuring it is safe.