

Intro

Today, the most important tool for scanning *WordPress* instances and performing security tests on web applications that implement this technology is **WPScan**.

WPScan is a tool that allows us to *fully automate* all the processes we saw in the manual enumeration section. We can enumerate **users**, **directories**, as well as **the WordPress version** running on a web application, **plugins and themen** and their versions—all of this, I repeat, *completely automatically*.

We can also perform a brute-force attack on an exposed WordPress login to gain access to said panel, something we'll cover in another section.

Also, with this tool, we can enumerate system sections, among other things.

This tool comes installed by default 🐉 in Kali and will be used from the terminal.

Without further ado, let's learn how to use WPScan.

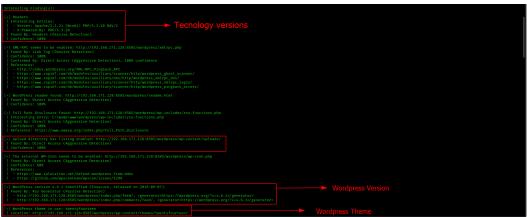
wc WPScan in action

To use a generic scan using WPScan we just have to run the next command

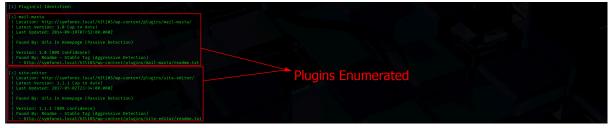
wpscan --url http://Target.WebSite/

With the result:

Manchine #1



Maniche #2



As we can see, we have enumerated a lot of interesting information like the *WordPress* version, directory listing, and even **plugins** and **theme** versions. With this information, we can investigate if those versions have **some of those software have a public exploit**, maybe *on internet* or using tools like **Searchsploit** (see the article **Searchsploit**), and **go to the phase of exploitation**. All this information enumerated *completely automatically*.

It's important to mention that we used two different machines in this case. We weren't able to list any plugins on the first one, but we'll see other alternatives in other sections, both in terms of techniques and tools, to obtain this information.

But with WPScan we can go beyond. If we add the flag **-e** we can enumerate all that information and also **the users of** that *WordPress* whit the command:

wpscan --url http://TargetWebSite/ -e

Manichine #1

And look, we have enumerated all the **users** that exist on the *WordPress* instance, completely automatically.

Conclusions

And there are some things we can do automatically with **WPscan**. We can do *more* things with this powerful tool, but in this section I want us to focus on *enumeration* and how we can do it completely automated. In future sections, we'll look at how we can do other cool things like **brute-force attacks**.