

Forum:[Hack Forums](#)

Thread: [How to target a specific site and find vulnerabilities?](#)

Kim Jong-Illest - January 1, 2014, 10:24 am

Hello Folks.

I am looking for a way to target specific sites and find their vulnerabilities. The site I am interested in is ran on Wordpress with no noticeable plugins. I have been researching and looking at SQLi, XSS, etc and I do not know where to begin as most of these simply point you to arbitrary search on google for dorks whilst I am interested in finding a vulnerability on a specific site.

Thank you.

xeonx - January 1, 2014, 10:34 am

You can either do it the manual way, or you can use software for pentesting. There are different tools like that out there, but many of them is quite expensive. Examples can be Netsparker, Nessus and Webcruiser. :)

-Al

Kim Jong-Illest - January 1, 2014, 10:36 am

(Jan 1, 2014 11:34 AM)???- Al Capone -??? Wrote: [\[CITE\]](#) You can either do it the manual way, or you can use software for pentesting. There are different tools like that out there, but many of them is quite expensive. Examples can be Netsparker, Nessus and Webcruiser. :)

-All would prefer to do it the manual way, best way to learn and I find people are far too dependent on tools. I'd rather do it myself and do it the 'honest' way.

Ichi - January 1, 2014, 10:45 am

If your target is running the most updated version of Wordpress with no plugins, then good luck. Don't lose hope though you could always target other sites on the same box and gain access to their website that way. Try running WPScan, it can help enumerate vulnerable plugins and other info that could be used to gain a foothold on your target.

If you're lucky, the site will be using a vulnerable version of Wordpress or running a vulnerable plugin you may have overlooked.

I'm not responsible for what happens, I assume this is a legal pentest

Kim Jong-Illest - January 1, 2014, 10:52 am

(Jan 1, 2014 11:45 AM)Ich Wrote: [\[CITE\]](#) If your target is running the most updated version of Wordpress with no plugins, then good luck. Don't lose hope though you could always target other sites on the same box and gain access to their website that way. Try running WPScan, it can help enumerate vulnerable plugins and other info that could be used to gain a foothold on your target.

If you're lucky, the site will be using a vulnerable version of Wordpress or running a vulnerable plugin you may have overlooked.

*I'm not responsible for what happens, I assume this is a legal pentest*I am not sure as this site is maintained by a 'less than average' administrator.

HaxOr? - *January 1, 2014, 10:56 am*

Is the site on a shared server? If so then this will do:

<https://hackforums.net/showthread.php?tid=2832327>