Forum:Hack Forums

Thread: hydra http-post-form bruteforce attack

foreign84 - *July 15, 2017, 3:51 am*
hi

how can I attack to a wordpress site with using hydra http-post-form bruteforce attack ?

Mr. Robot - *July 15, 2017, 3:53 am*
If you are just attacking a wordpress site you shouldn't need to use hydra, there is a metasploit module for it.

Link the site you are trying to attack.
Make sure you have also done both a spider of the site using something like ZAP as well as running wpscan

foreign84 - *July 15, 2017, 3:58 am*
(Jul 15, 2017 03:53 AM)Mr. Robot Wrote: *[CITE]* If you are just attacking a wordpress site you shouldn't need to use hydra, there is a metasploit module for it.

Link the site you are trying to attack.
Make sure you have also done both a spider of the site using something like ZAP as well as running wpscan
yea I know wpscan script. But I want to use hydra, Is it possible ? or how can I do that for any target web page ?

Mr. Robot - *July 15, 2017, 4:00 am*
(Jul 15, 2017 03:58 AM)foreign84 Wrote: *[CITE]* yea I know wpscan script. But I want to use hydra, Is it possible ? or how can I do that for any target web page ?
What? Please post the site you are trying to attack. If you merely want to attack it you don't need to reinvent the wheel for a wordlist attack.

AS far as using hydra is concerned, read the --help and you wont have any issues. It's self explanatory.

When using wpscan please use --enumerate -u to get a list of valid usernames for the site, then use a password list against those.

Example:

Code wpscan -u www.jaimedicalsystems.com --enumerate u

To run a dictionary attack against those users you would then do the following

Code wpscan --url www.jaimedicalsystems.com --wordlist rockyou.txt --username rdevlin --threads 4
Obviously replacing the website with the target, wordlist with your password file, username (rdevlin)

to one you enumerate and then threads.

foreign84 - *July 15, 2017, 4:09 am*

thanks but I know how using wpscan.

target.com/wp.login.php
username:admin

hydra target.com -l admin -P /root/Desktop/password.txt http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In:Error" -vV

result: hydra is finding too much true login result for that attack

Mr. Robot - *July 15, 2017, 4:22 am*

(Jul 15, 2017 04:09 AM)foreign84 Wrote: *[CITE]* thanks but I know how using wpscan.

target.com/wp.login.php
username:admin

hydra target.com -l admin -P /root/Desktop/password.txt http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log In:Error" -vV

result: hydra is finding too much true login result for that attack
I see a few things that might be an issue, why not try the method I posted above. You will get better results.