

Forum:[Hack Forums](#)

Thread: [False Positives Brute Forcing](#)

SilentNuke - April 27, 2024, 2:40 am

Hello all.

I have set up a few test environments to try a few brute forcing methods on a few different web apps and software, but i am stuck.

Whilst using Hydra on a wordpress setup, i either get a false positive - and its usually on the same password, it doesnt detect the password, or every password is the right password. I have also used a different script which isnt as complicated as Hydra:

<https://github.com/1N3/Wordpress-XMLRPC-Brute-Force-Exploit>

This also flags the same password as correct every time i run it.

Hydra input:

Code hydra -V -l xxx -P /usr/share/wordlists/rockyou.txt [LINK DELETED BY STAFF]

https-post-form

"/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In&redirect_to=https%3A%2F%2Fwebsite.com%2Fwp-admin%2F&testcookie=1:S=Location"

I have tried countless iterations, read many articles and watch many videos on using hydra for wordpress, and none of them seem to do the job. Ive tried using :F=Error: The password you entered for the username xxxxx is incorrect, but displays an error:

Quote:[ERROR] no valid optional parameter type given: F

Any help would be great.

Thank you.

Dolla\$ - April 28, 2024, 9:43 am

There's no way you're going to brute force a new version of WordPress using /wp-login.php, buddy. The website is protected against brute forcing using a CSRF token. To attempt brute forcing, you must utilize xmlrpc.php if it's enabled.

Some documentation, to help you achieve this :

<https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/wordpress>

Also, if you want to test on a more dedicated environnement, you should consider using this :

<https://owasp.org/www-project-juice-shop/>

xx

SilentNuke - April 30, 2024, 4:17 am

(Apr 28, 2024 09:43 AM)Dolla\$ Wrote: [\[CITE\]](#) There's no way you're going to brute force a new version of WordPress using /wp-login.php, buddy. The website is protected against brute forcing using a CSRF token. To attempt brute forcing, you must utilize xmlrpc.php if it's enabled.

Some documentation, to help you achieve this :

<https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/wordpress>

Also, if you want to test on a more dedicated environnement, you should consider using this :

<https://owasp.org/www-project-juice-shop/>

xx

Are you sure? Ive got the usernames as it tells me 'Password for xxx is incorrect', and when using hydra, i see it attempts the login, then redirects back to the login page if it fails - as it does if doing it manually.

Dolla\$ - May 1, 2024, 10:51 am

(Apr 30, 2024 04:17 AM)SilentNuke Wrote: [\[CITE\]](#) Are you sure? Ive got the usernames as it tells me 'Password for xxx is incorrect', and when using hydra, i see it attempts the login, then redirects back to the login page if it fails - as it does if doing it manually.

If you use the last version of Wordpress definitely, yes