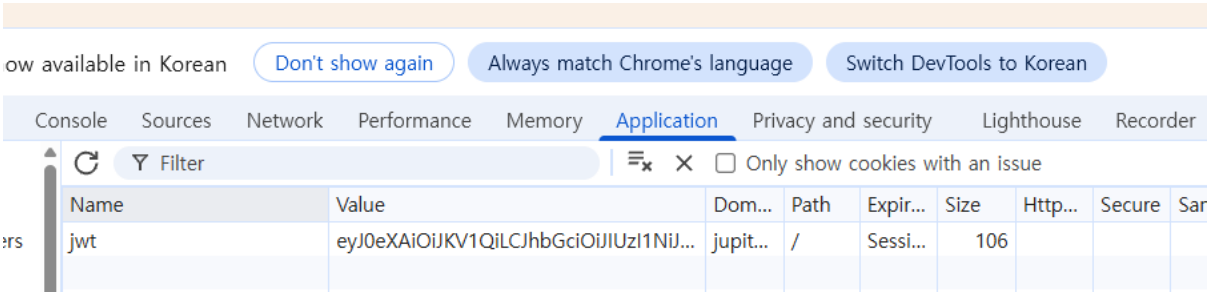
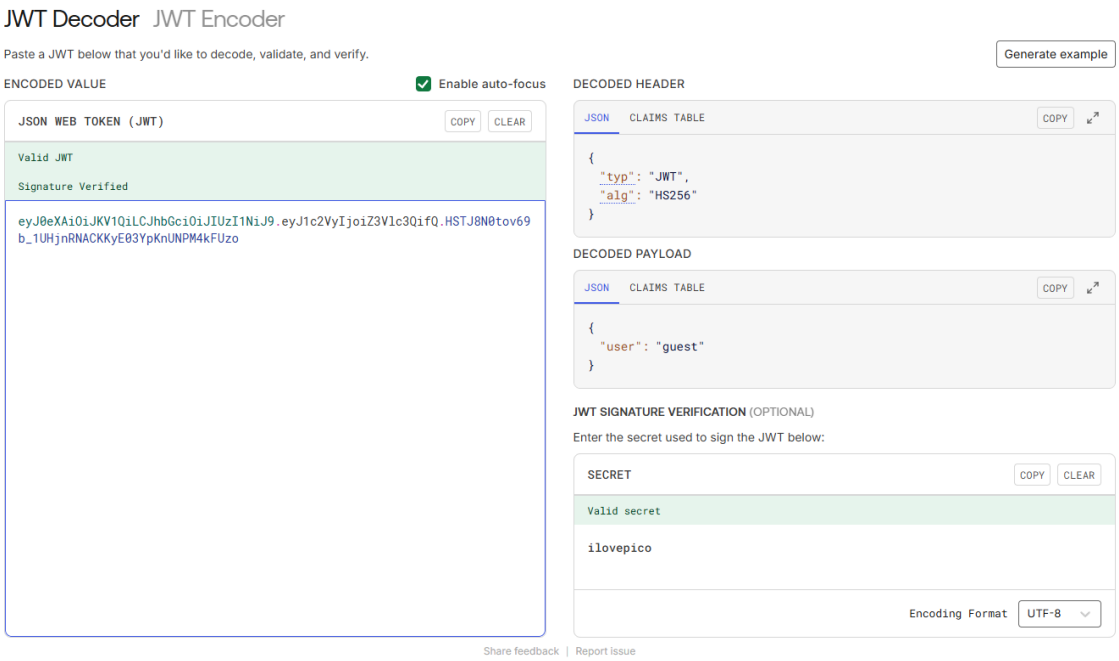
name을 입력하면 로그인이된다.



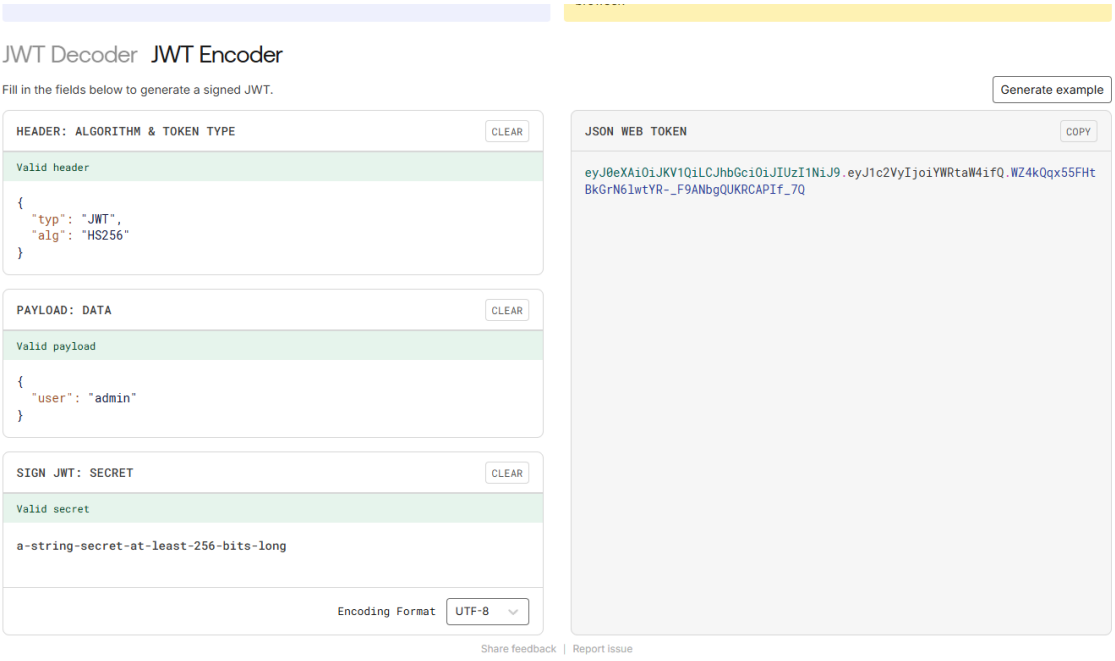
로그인이되면 jwt 쿠키가 생긴다. 해당 값은 jwt 인증 방식을 사용한 base64로 인코딩된 값이다.

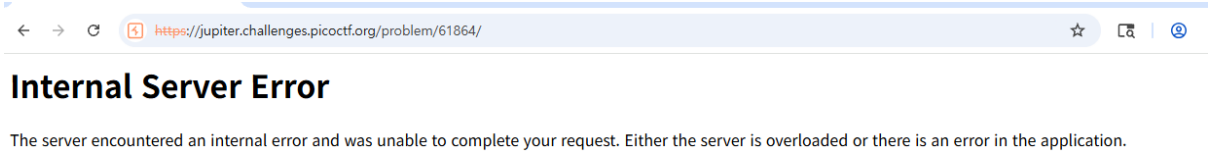


jwt 토큰은 Header.Payloads.Signature 세 부분으로 나뉘어 있다. Header는 JWT 토큰 유형과 Signature 부분에 사용될 서명 알고리즘 종류를 나타내고, Payloads는 서비스에 필요한 데이터들을 설명한다. 마지막으로 Signature는 base64로 인코딩된 Header와 Payloads를 합쳐 서명 알고리즘을 사용하여 서명한다.

jwt.io에서 해당 값을 보면 user 값이 guest인 것을 볼 수 있다.

user을 admin으로 변경하고, 쿠키값을 위조해봤더니 안되었다.





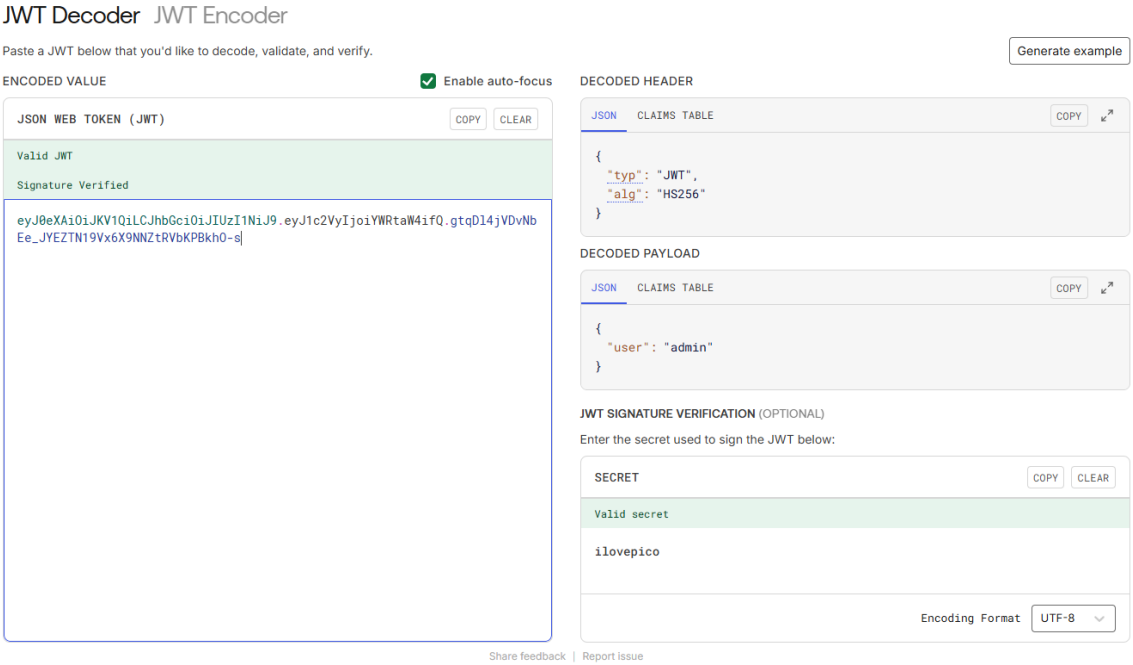
개인키를 알아내야 하는 것 같다.

john the ripper 툴을 사용해 jwt 토큰에서 HMAC 포맷으로 개인키를 알아낼 수 있다고 한다.

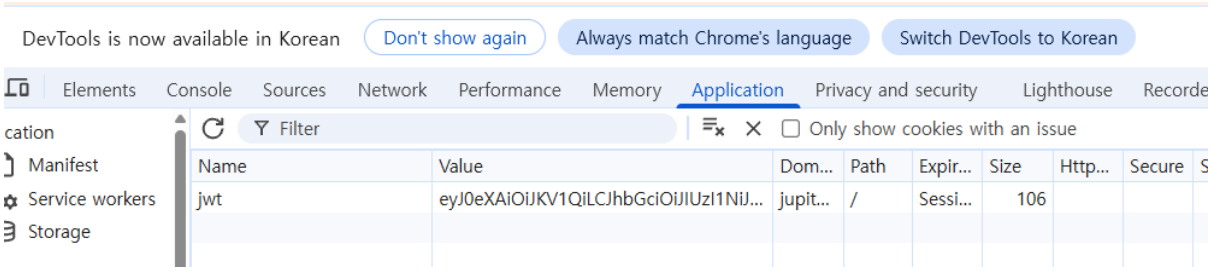
```
</body>
root@hkh:/mnt/c/Users/hkh/Downloads/rockyou.txt# echo 'eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiYWRtaW4ifQ.gtqDl
4jVDvNbEe_JYEZTN19Vx6X9NNZtRVbKPBkhO-s' > crack.txt
```

쿠키 값을 crack.txt에 저장하고, 크랙을 시도하면 ilovepico라는 서명키값이 나온다.

```
root@hkh:/mnt/c/Users/hkh/Downloads/rockyou.txt# john --format=HMAC-SHA256 --wordlist=./rockyou.txt crack.txt | grep pic
o
Using default input encoding: UTF-8
Will run 28 OpenMP threads
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
ilovepico        (?)
1g 0:00:00:03 DONE (2025-10-10 14:44) 0.2646g/s 1956Kp/s 1956Kc/s 1956KC/s inZtinX..ilovemymother89
```



해당 값을 signature 값에 넣으면 값이 생성된다.



해당 값을 쿠키 값에 넣고, 새로고침하면 FLAG가 나온다.

Welcome to JaWT!

JaWT is an online scratchpad, where you can "jot" down whatever you'd like! Consider it a notebook for your thoughts.
JaWT works best in Google Chrome for some reason.

Hello admin!

Here is your JaWT scratchpad!

picoCTF{jawt_was_just_what_you_thought_1ca14548}

Logout

Register with your name!