FUNDACIÓN UNIVERSITARIA SAN MATEO INGENIERÍA DE SISTEMAS

SÉPTIMO SEMESTRE GRUPO 02N30



VIGILADA MINEDUCACIÓN

MODELOS DE CALIDAD DE SOFTWARE ABRIL 2025

BRANDON YESID REYES PARDO

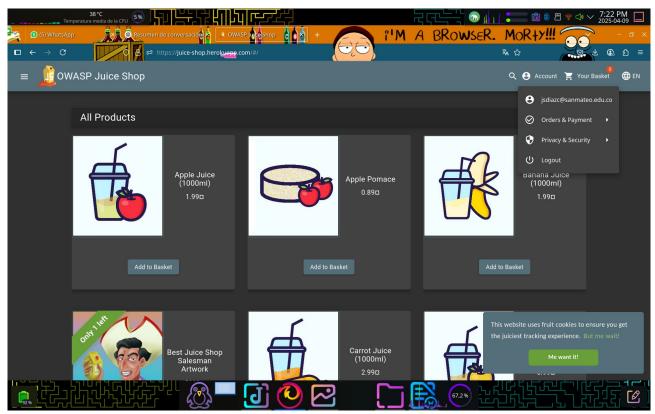
JUAN SEBASTIAN DIAZ CHAPARRO

HAROLD YESID SALCEDO ANGARITA

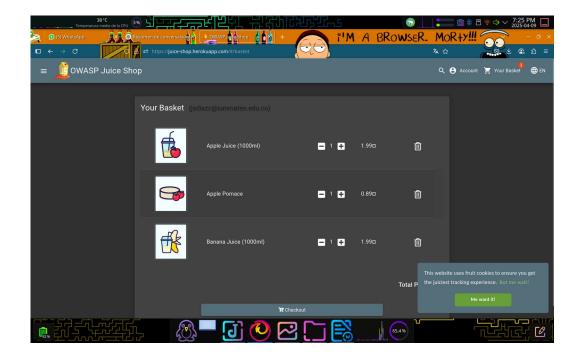
TALLER

PARTE 6

1. https://juice-shop.herokuapp.com crear cuenta iniciar sesión

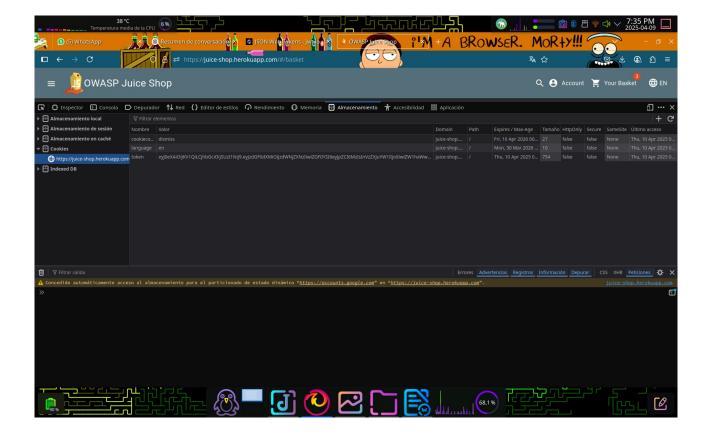


2. Acceder a secciones privadas Your Basket Order history

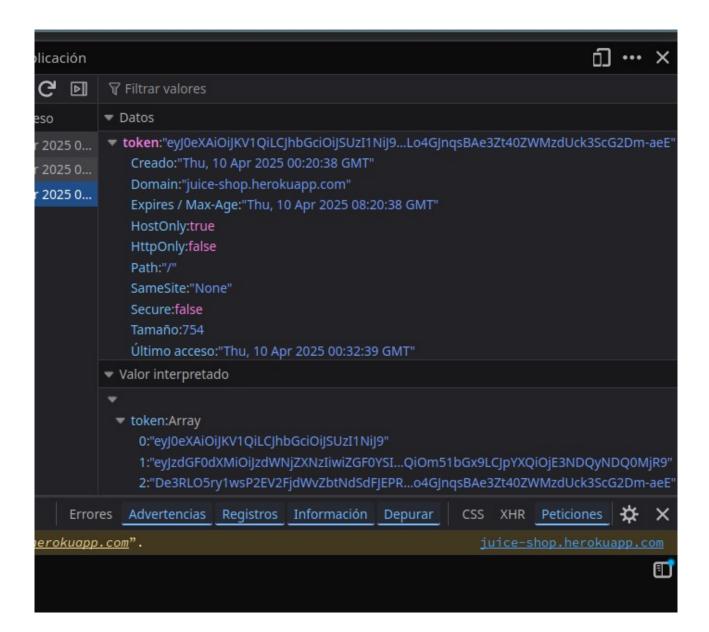


3. Abrir DevTools (herramientas de desarrollador)

- F12 o clic derecho → "Inspeccionar"
- Ir a la pestaña Application
- En el menú izquierdo, entrar a Cookies y seleccionar https://juice-shop.herokuapp.com
- Revisar cookies activas



Buscar si hay una cookie con el nombre token (muy común para JWTs)



4. Analizar el token con JWT

Ir a https://jwt.io

Copiar el valor del token desde las cookies

Analizar el JWT



eyJ0eXAi0iJKV1QiLCJhbGci0iJSUzI1NiJ9.ey JzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZ CI6MzIsInVzZXJuYW1lIjoiIiwiZW1haWwi0iJq c2RpYXpjQHNhbm1hdGVvLmVkdS5jbyIsInBhc3N 3b3JkIjoiYTIxODc1ZGY0ZmJ1NjQ2YzY00DEzMG ${\tt QyY2IzN2EzYjAiLCJyb2x1IjoiY3VzdG9tZXIiL}$ CJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb2dpbklw IjoiMC4wLjAuMCIsInByb2ZpbGVJbWFnZSI6Ii9 hc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2 RlZmF1bHQuc3ZnIiwidG90cFN1Y3J1dCI6IiIsI $\verb|mlzQWN0aXZ1Ijp0cnV1LCJjcmVhdGVkQXQi0iIy| \\$ MDI1LTA0LTEwIDAwOjIwOjIzLjQ1NSArMDA6MDA iLCJ1cGRhdGVkQXQi0iIyMDI1LTA0LTEwIDAw0j ${\tt IwOjIzLjQ1NSArMDA6MDAiLCJkZWxldGVkQXQiO}$ m51bGx9LCJpYXQi0jE3NDQyNDQ0MjR9.De3RL05 ry1wsP2EV2FjdWvZbtNdSdFJEPRb4gdwKe6-VoCm19T5KMq5u9idEdpP1vJMgQhHBysFea30dHT IYxFyRC7ueryBzNFPniyP0TQtyV6m4FtqhXqgfq 9pHsL6a4vBLJ4_RLo4GJnqsBAe3Zt40ZWMzdUck 3ScG2Dm-aeE

```
HEADER: ALGORITHM & TOKEN TYPE
       "typ": "JWT",
"alg": "RS256"
PAYLOAD: DATA
        "status": "success".
            "username": "",
"email": "jsdiazc@sanmateo.edu.co",
"password": "a21875df4fbe646c648130d2cb37a3b0",
   password: azib/SdTaTpeb4bcb4b130d2cD3/aSb0,
"role": "usutomer",
"deluxeToken": "",
"lastLoginIp": "0.0.0.0",
"profileImage": "/assets/public/images/uploads/
default.svg",
"totpSecret": "",
             TisActive: true,
"oreatedAt": "2025-04-10 00:20:23.455 +00:00",
"updatedAt": "2025-04-10 00:20:23.455 +00:00",
"deletedAt": null
          "iat": 1744244424
```









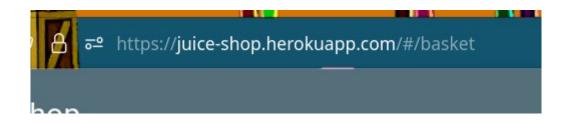








```
PAYLOAD: DATA
   "status": "success",
   "data": {
     "id": 32.
     "username": "",
     "email": "jsdiazc@sanmateo.edu.co",
      "password": "a21875df4fbe646c648130d2cb37a3b0",
      "role": "customer",
      "deluxeToken": "",
      "lastLoginIp": "0.0.0.0",
      "profileImage": "/assets/public/images/uploads/
 default.svg",
     "totpSecret": "",
     "isActive": true,
      "createdAt": "2025-04-10 00:20:23.455 +00:00",
      "updatedAt": "2025-04-10 00:20:23.455 +00:00",
      "deletedAt": null
    "iat": 1744244424
VERIFY SIGNATURE
```

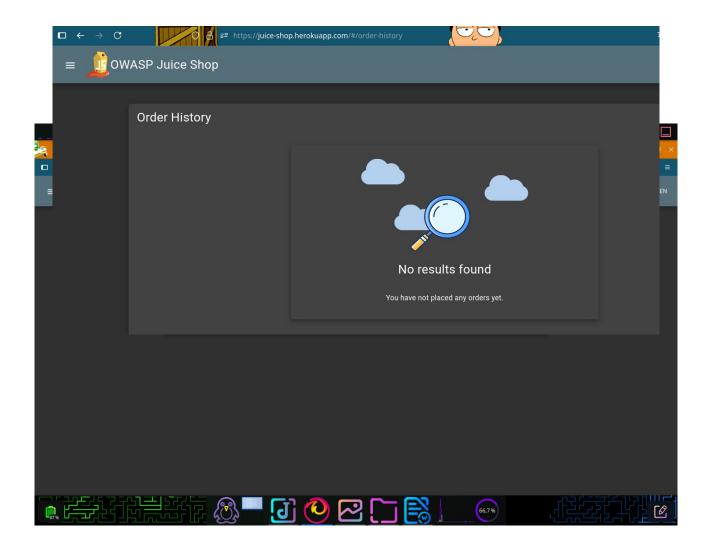


5. Cerrar sesión.

Escribir en el navegador:

https://juice-shop.herokuapp.com/#/basket

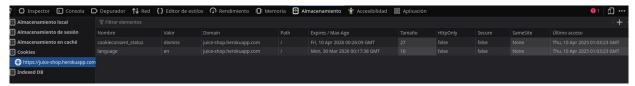
https://juice-shop.herokuapp.com/#/order-history



6. Se Puedo ingresar ?:

No, después de cerrar sesión ya no se puede acceder a las secciones privadas como el carrito

• Las cookies están protegidas:



Sí, están protegidas. Al cerrar sesión, la cookie con el token de sesión fue eliminada automáticamente, lo cual indica que el sistema maneja bien la limpieza de sesión.

• Puedo manipular el token

No, ya no es posible porque el token desapareció al cerrar sesión. Esto indica que no quedó ninguna sesión activa reutilizable o manipulable.

• El sistema Valida la sesión:

Sí, el sistema valida correctamente la sesión. Si no hay token válido en las cookies, **bloquea el acceso a las rutas privadas**.

- Se puedo acceder al recurso privado
- No, los recursos privados como el carrito o el historial de compras ya no son accesibles al intentar escribir directamente la URL.
- Que mejoras sugiere:
- Aunque el sistema funciona correctamente, se pueden sugerir las siguientes mejoras:
- 1. **Agregar la bandera HttpOnly y Secure a las cookies del token**, si no estaban presentes antes de cerrar sesión, para mayor seguridad.
- 2. **Manejar redirecciones automáticas**: actualmente, si intentas acceder directamente al /basket sin estar logueado, simplemente no carga. Lo ideal sería que redirija al login automáticamente.
- 3. **Mostrar mensajes claros al usuario**, por ejemplo: "No tienes sesión activa" en vez de simplemente ocultar el contenido.