Nombre Taller:Lab 0x05

APIs 0x01: Broken Function-Level Authorization (BFLA)

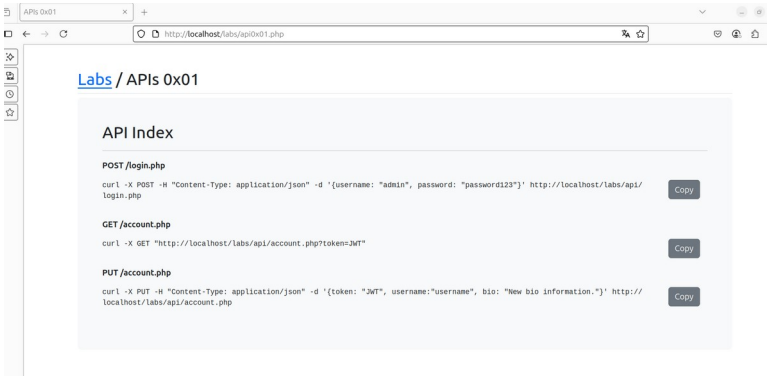
Detalles Prácticos:

Descripción:Este labortorio demuestra una vulnerabilidad típica en APIs: **la falta de validación del usuario autenticado al ejecutar funciones sensibles,** como actualizar datos de otros usuarios. En este caso, la API permite modificar la biografía de cualquier cuenta usando un token JWT válido, incluso si no corresponde con el usuario afectado.
Nivel(Básico/Intermedio o avanzado)
Instructores:Rieradipe

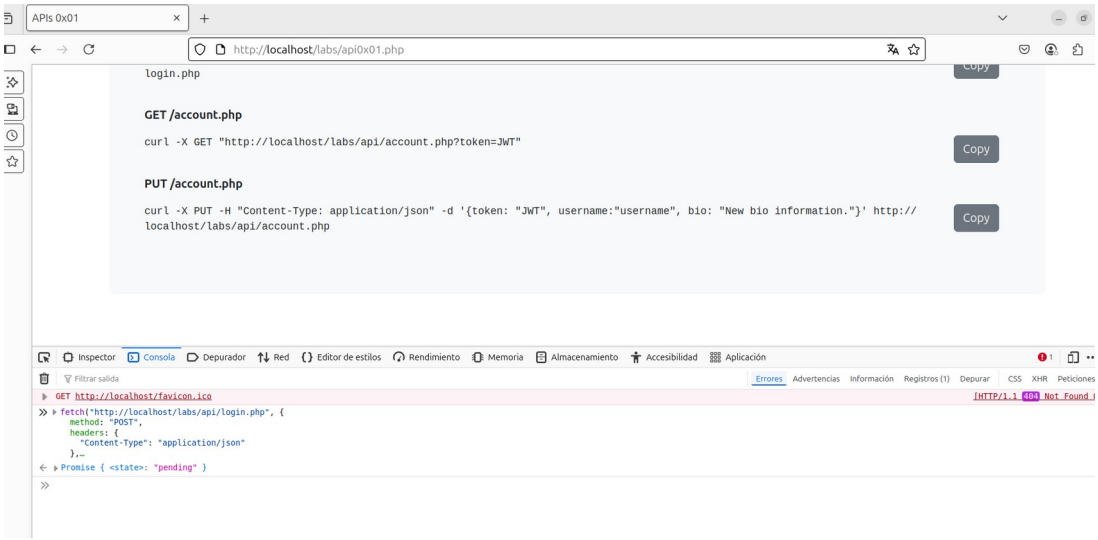
Tabla de contenidos:

Metodología:
Para detectar y explotar la vulnerabilidad de **Broken Function-Level Authorization**, se siguió el siguiente enfoque:

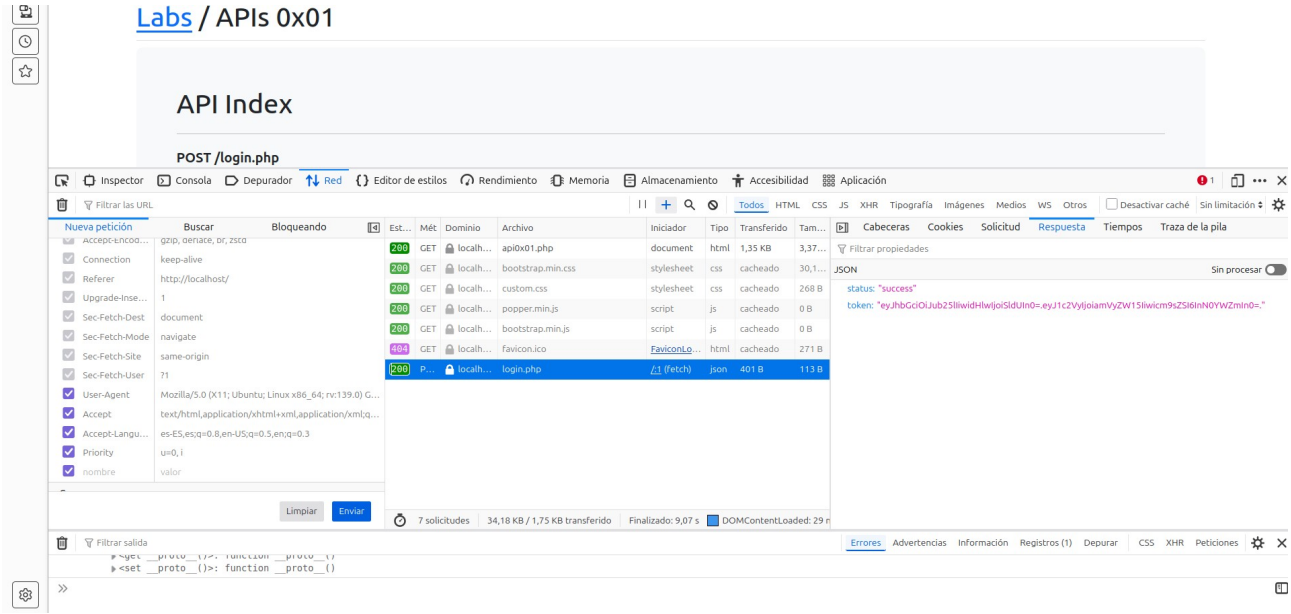
- Inspección de la documentación de la API
  Se analizaron los endpoint disponibles en la interfaz del lab (POST/login.php, GET/account.php, PUT/account.php) para entender cómo se gestionan la autenticación y la modificación de datos



- Obtención de un token JWT válido
  Se ejecutó una petición manual desde la consola del navegador utilizando las credenciales proporcionadas (jeremy:cheesecake).



- Se observó la respuesta en la pestaña RED, verificando que se devolvía un token, sin firma y manipulable



- Análisis del comportamiento de los endpoints protegidos
  Se utilizó el token obtenido para acceder al endpoint GET/account.php y confirmar que devuelve información asociada al usuario autenticado

Explotación del fallo:
Desde la consola del navegador se realizó una petición PUT a account.php utilizando el token de jeremy, pero modificando los datos de jessamy, lo cual no debería estar permitido.

- Ataque: ejecución de función con privilegios indebidos

  Se envió una petición PUT modificando el campo username con valor distinto al del usuario autenticado, lo que permitió modificar la biografía de otro usuario (jessamy). Esta acción confirmó la ausencia de validación de identidad y el fallo de control de acceso funcional