Nombre Taller: Lab 0x05

IDOR con enumeración de cuentas administrativas

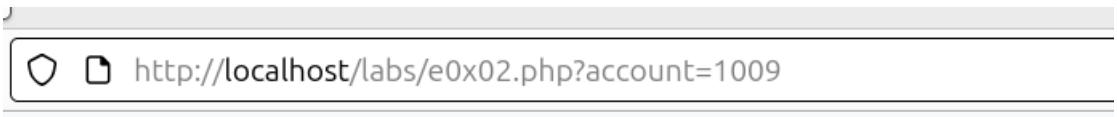
Detalles Prácticos:

Descripción: Este laboratorio se centra en identificar y explotar una vulnerabilidad de tipo **IDOR** (insecure direct object reference) mediante la manipulación directa de parámetros en la URL.
Nivel(Básico/Intermedio o avanzado)
Instructores:Rieradipe

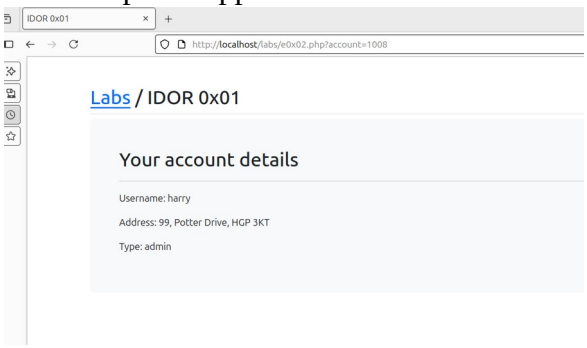
Tabla de contenidos:

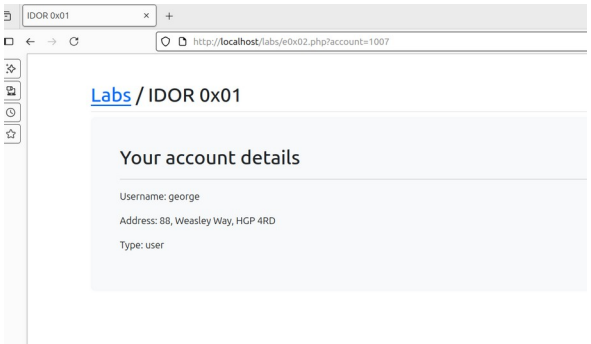
Introducción:
Se analiza un caso donde la aplicación permite acceder a los datos sensibles de otras cuentas, simplemente modificando el valor del parámetro account en la URL. La falta de verificación en el servidor permite al atacante acceder a información de otros usuarios, incluyendo cuentas con privilegios administrativos, sin necesidad de autentificación adicional

Metodología:
- Enumeración manual

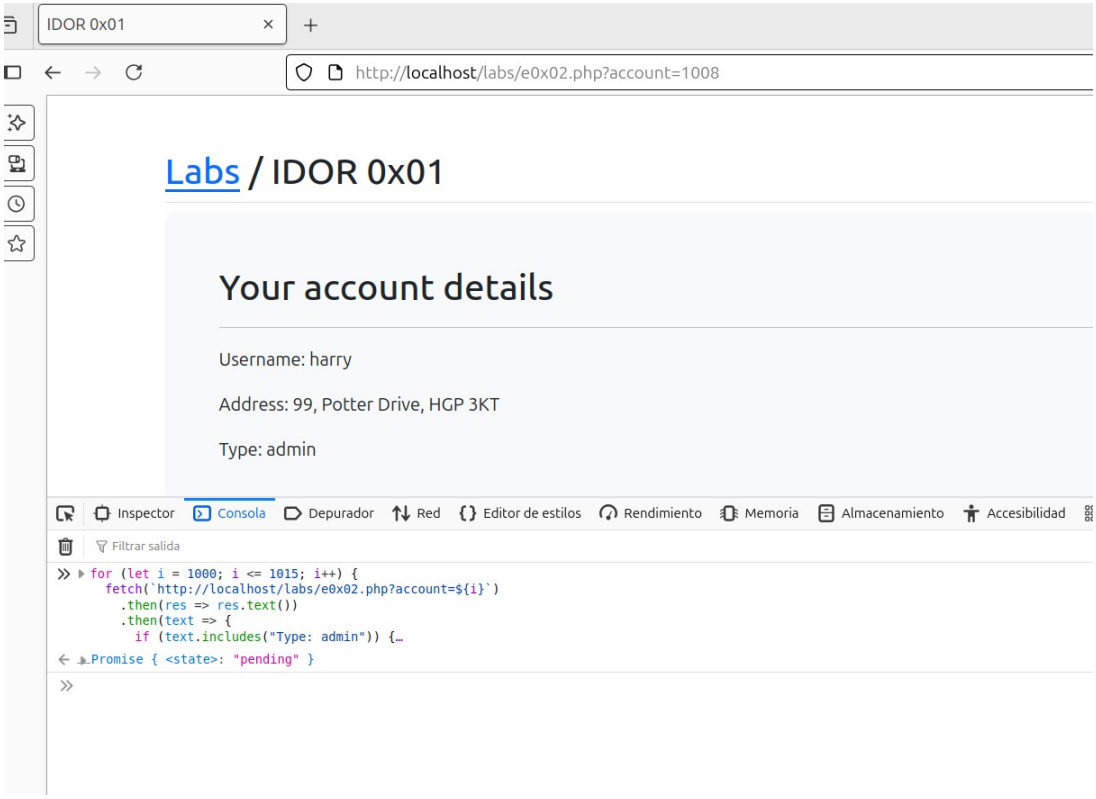


Se probaron manualmente distinatas combinaciones de ID(1000 a 1010), observando el contenido devuelto por la app en cada caso.

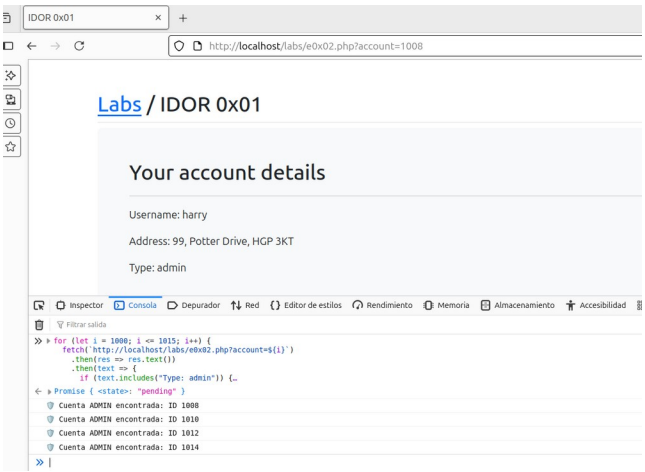




- <u>Enumeración automatizada desde consola del navegador</u>
  Se ha utilizdado el siguiente script de JS en consola:



Y nos arroja resultados positivos, encuentra varios admin en este pequeño script condicional(for if)



Recomendaciones:

El backend **debe** validar que el usuario autenticado solo puede acceder a su propia información. No debe confiar en valores enviados por el cliente(como este caso un ID en la URL) para aplicar reglas de acceso.