



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	Contexto del taller
	Objetivos generales y específicos. Vulnerabilidad IDOR que permite acceder a datos de otras cuentas (incluso admin) manipulando el parámetro account en la URL.
Materiales Necesarios	Software requeridos
	Recursos Adicionales
Metodología	Desglose paso a paso del proceso
	Practicas recomendadas
Ejercicios Prácticos	Captura de solicitudes
	Análisis y pruebas
Resultados y Evaluación	Resultados esperados de las actividades
	Criterios de evaluación
Conclusión	Resumen de aprendizajes
	Preguntas y próximos pasos

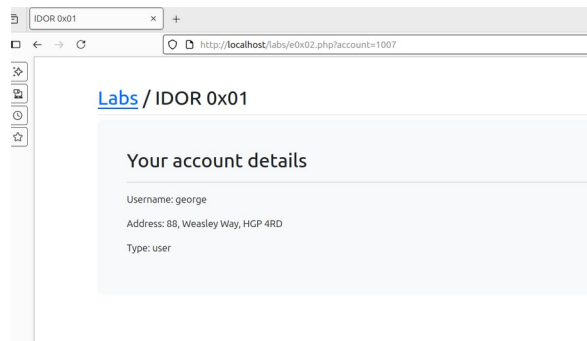
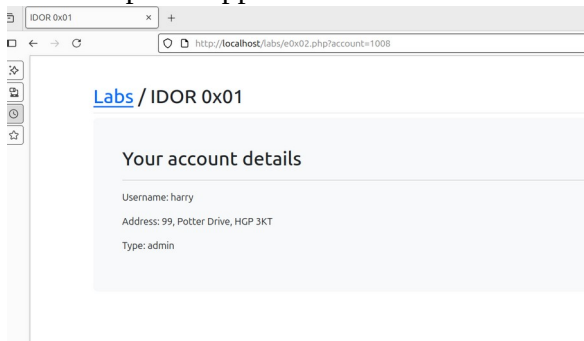
Introducción:

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 autenticación adicional

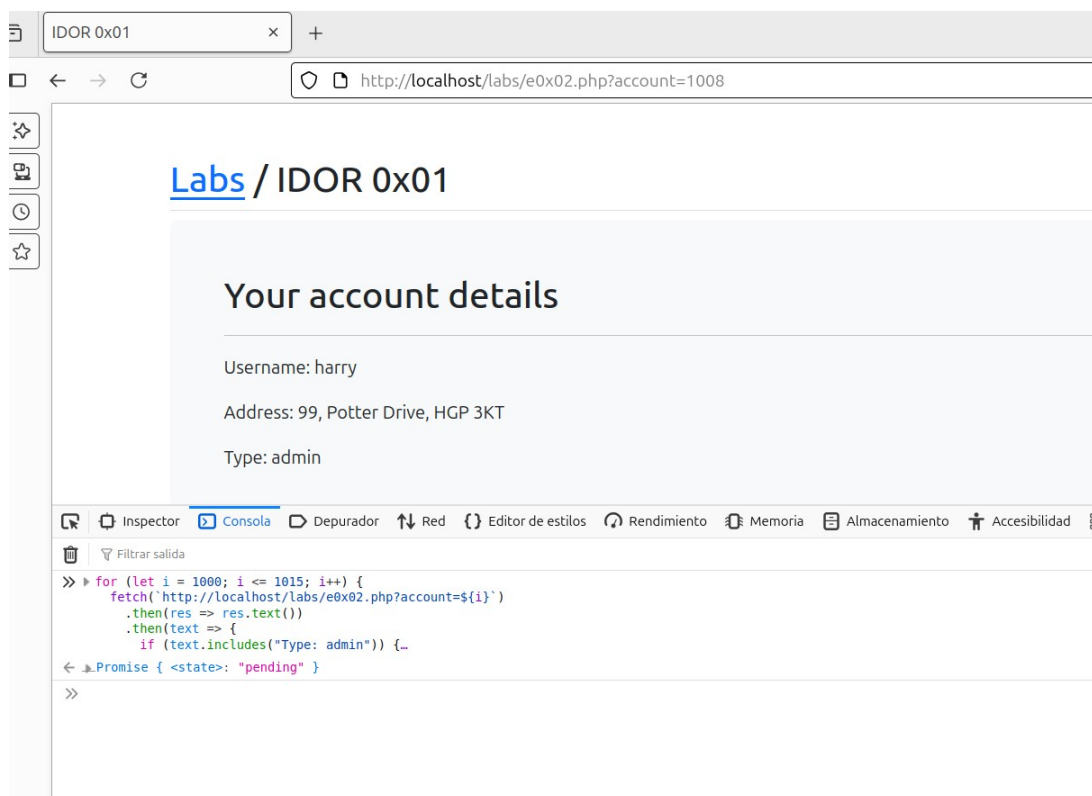
Metodología:

- Enumeración manual

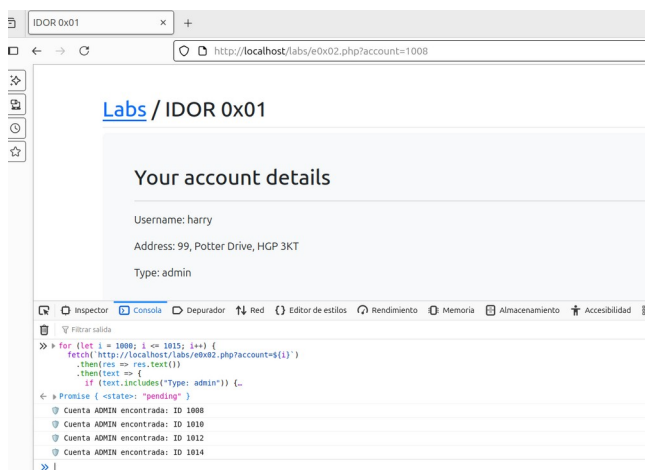
Se probaron manualmente distintas combinaciones de ID(1000 a 1010), observando el contenido devuelto por la app en cada caso.



- Enumeración automatizada desde consola del navegador
Se ha utilizado 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.