Nombre Taller: Lab 10

Laboratorio SQL Injection 0x03 - [Challenge]

Detalles Prácticos:

Descripción:Explotar una vulnerabilidad SQL
Nivel(Básico/Intermedio o avanzado)
Instructores:Rieradipe

Tabla de contenidos:

Introducción	Contexto del taller
	Objetivos generales y específicos
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

Objetivo:

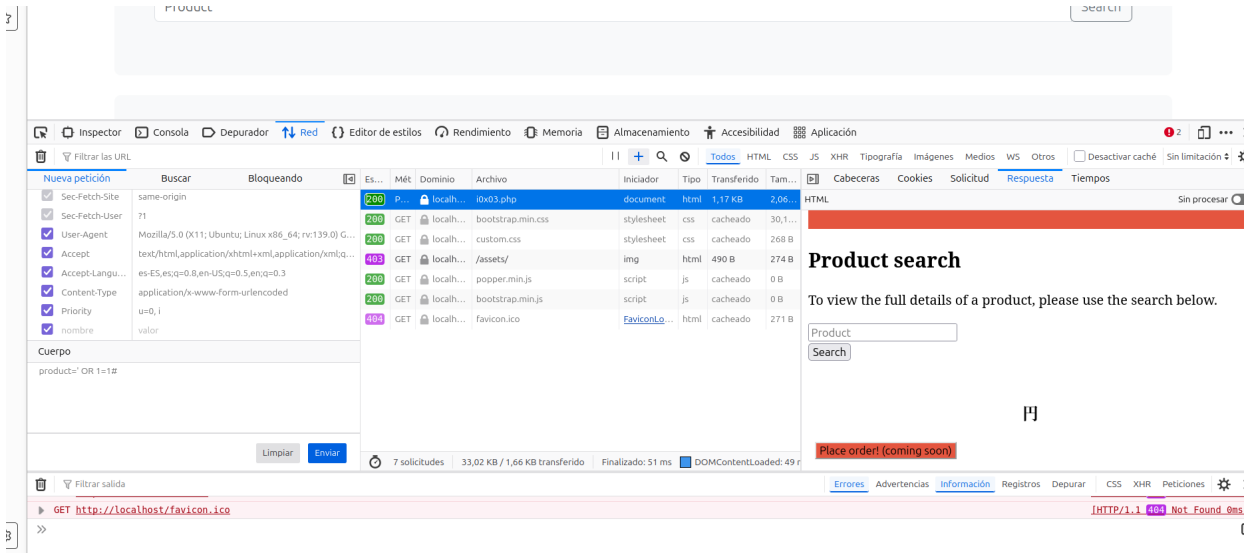
Explotar una vulnerabilidad de inyección SQL para extraer información sensible de la bbdd.
Ejemplo: nombres de usuario, contraseñas.
Esto lo hacemos mediante técnicas manuales(UNION SELECT) y análisis con herramientas como DEVTOOLS

Metodologá utilizada:

1. **Verificación de la vulnerabilidad**
   Usamos un payload clásico de autenticación para comprobar si hay SQLi

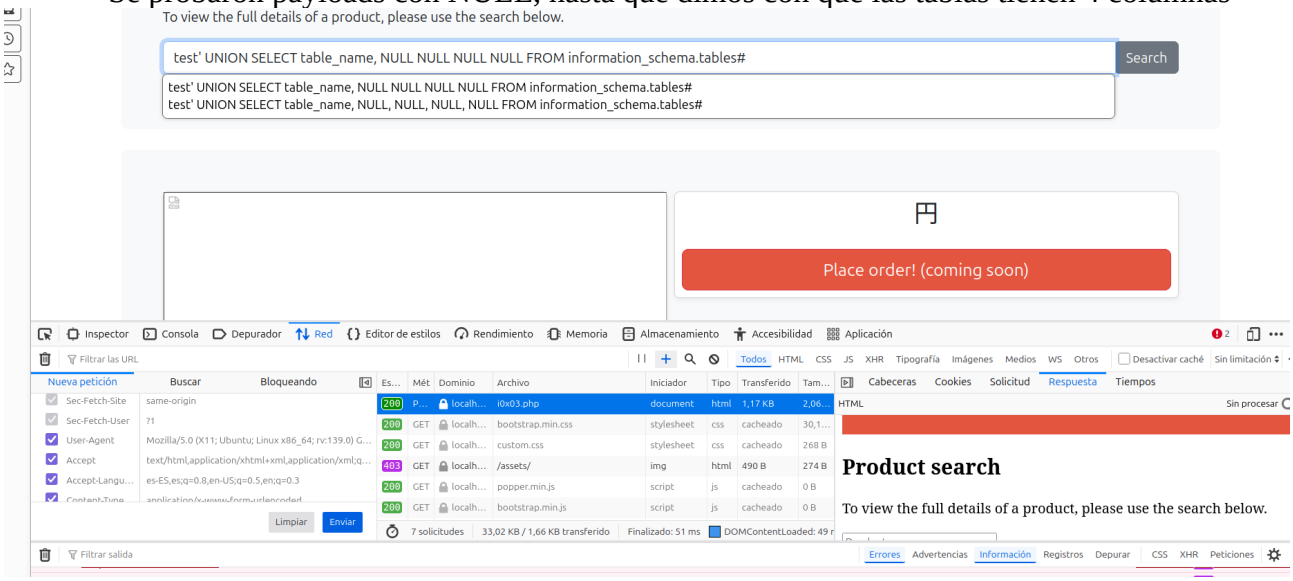
```
' OR 1=1#
```

La aplicación responde con un cambio en la vista,confirmando la presencia de SQLi

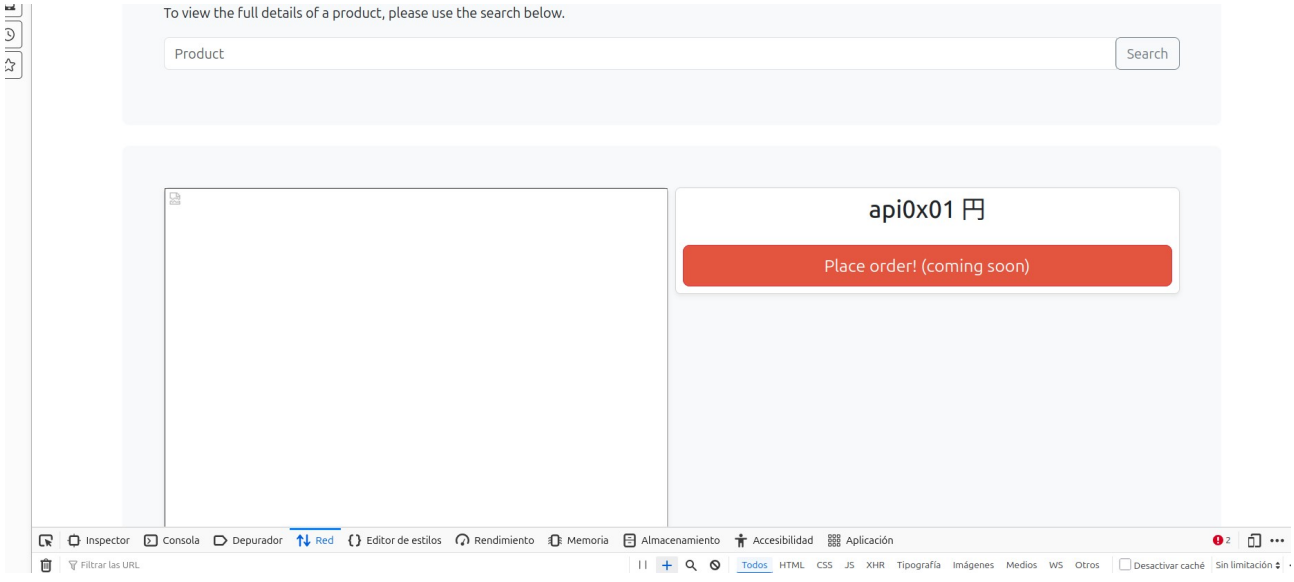


2. Determinación del número de columnas

Se probarón payloads con NULL, hasta que dimos con que las tablas tienen 4 columnas



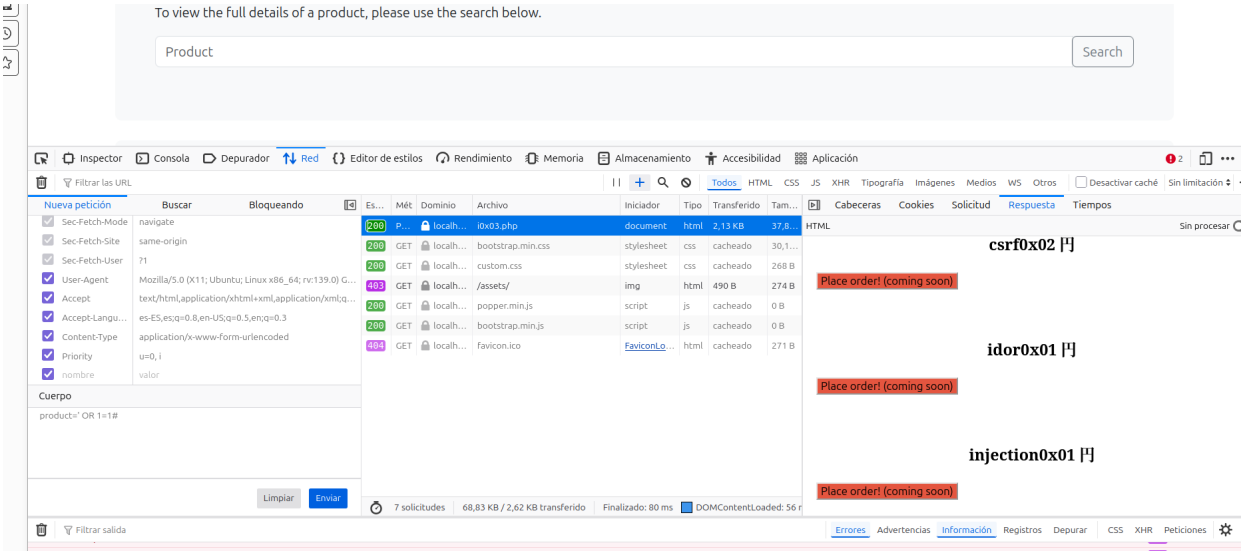
3. Enumeración de columnas



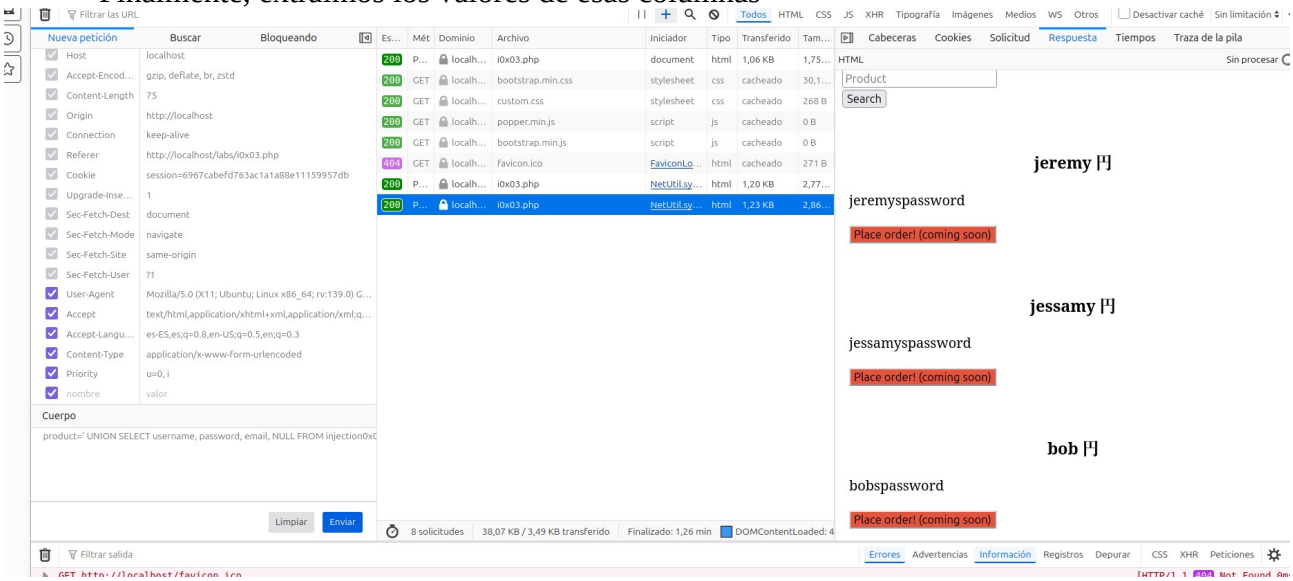
4. **Enumeración de tablas**
   Utilizamos el payload:

' UNION SELECT table_name, NULL, NULL, NULL FROM information_schema.tables#

Resultado en pantalla; se identifican tablas como injection0x01, idor0x01...



5. **Extracción de datos**
   Finalmente, extraimos los valores de esas columnas



Lección clave:

El uso de UNION SELECT permite concatenar resultados visibles en la interfaz, si el número de columnas es correcto. Toda la explotación se realizó desde DevTools, sin herramientas externas

<u>Recomendaciones de mitigación:</u>

Implementar **prepared statements** que separan los datos del código SQL, impidiendo que los datos se interpreten como instrucciones SQL