



Nombre Taller: lab 11

## Inyección de Segunda Orden

### Detalles Prácticos:

Descripción: Explotar una vulnerabilidad de tipo SQL Injection segunda orden

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 tipo **SQL injection de segundo orden**, en el cual el payload no se ejecuta el el momento de la inyección, sino que queda almacenado en la bbdd y se evalúa en una acción posterior(como el login)

#### 1. Análisis inicial de la aplicación

La aplicación tiene dos formularios:

- Sign Up: registra un nuevo usuario
  - Login: iniciar sesión con un usuario ya registrado
- Ambos envían datos mediante método POST

#### 2. Pimera prueba de login

Se intenta acceder con un payload clásico

username: ' OR 1=1-- -	password: (daigual)
------------------------	---------------------



## 5. Conclusión

Este laboratorio demuestra cómo un imput malicioso, si no se sanitiza ni calida al ser almacenado, puede aprovecharse en otra etapa del flujo de la app, permitiendo evadir controles o manipular datos

## 6. Medidas de Mitigación recomendadas

Uso de prepared statements o sentencias parametrizadas
Validación y escape de datos antes de almacenarlos
Principio de menor privilegio en consultas a la bbdd
Nunca reutilizar directamente valores almacenados sin volver a validarlos
Configurar mensajes de error genéricos