Introducción

Durante una práctica en el entorno DVWA (Damn Vulnerable Web Application), llevé a cabo una prueba de seguridad enfocada en identificar y explotar una vulnerabilidad de tipo inyección SQL.

Esta actividad fue realizada en un entorno controlado, con fines formativos y de aprendizaje en ciberseguridad ofensiva.

Descripción del Incidente

Analizando el módulo “SQL Injection” de DVWA, detecté que el campo 'User ID' no cuenta con validación adecuada. Esto me permitió modificar la consulta SQL original y acceder a datos sensibles almacenados en la base de datos, sin necesidad de autenticación previa.

Proceso de Reproducción

1. Accedí a DVWA en http://localhost/dvwa.
2. Inicié sesión con las credenciales por defecto:
    a. Usuario: admin
    b. Contraseña: password
3. Ajusté el nivel de seguridad a Low en el panel de configuración.
4. Ingresé al módulo SQL Injection.
5. En el campo “User ID” introduje el siguiente payload: **1' OR '1'='1**
6. Al hacer clic en Submit, la aplicación mostró todos los registros de usuarios, lo que confirmó la vulnerabilidad.

Impacto del Incidente

A partir de esta inyección, pude acceder a información sin autorización. En un entorno real, un atacante podría:

- Obtener datos confidenciales.
- Saltarse el control de autenticación.
- Manipular o extraer información de la base de datos.

- Comprometer sistemas dependientes.

La vulnerabilidad representa un riesgo alto, según el ranking OWASP.

Recomendaciones

- Validar entradas con consultas preparadas.
- Aplicar el principio de mínimo privilegio en cuentas de base de datos.
- Realizar auditorías de seguridad periódicas.
- Formar al personal técnico en desarrollo seguro.

Conclusión

Esta práctica me permitió comprobar cómo una falla básica como la inyección SQL puede tener un gran impacto si no se gestiona adecuadamente. Reforzar la seguridad desde el desarrollo es clave para prevenir este tipo de riesgos.