INFORME TÉCNICO: INYECCIÓN SQL EN DVWA

Fecha del incidente: 16 de julio de 2025

Autor del informe: Jorge Teran

Herramienta utilizada: Damn Vulnerable Web Application (DVWA)

Introducción

Este informe documenta una vulnerabilidad de inyección SQL identificada durante una práctica de laboratorio en la aplicación Damn Vulnerable Web Application (**DVWA**), ejecutada en un entorno controlado. El objetivo del ejercicio fue comprender cómo funcionan los ataques de inyección SQL y evaluar su impacto dentro de un sistema web inseguro.

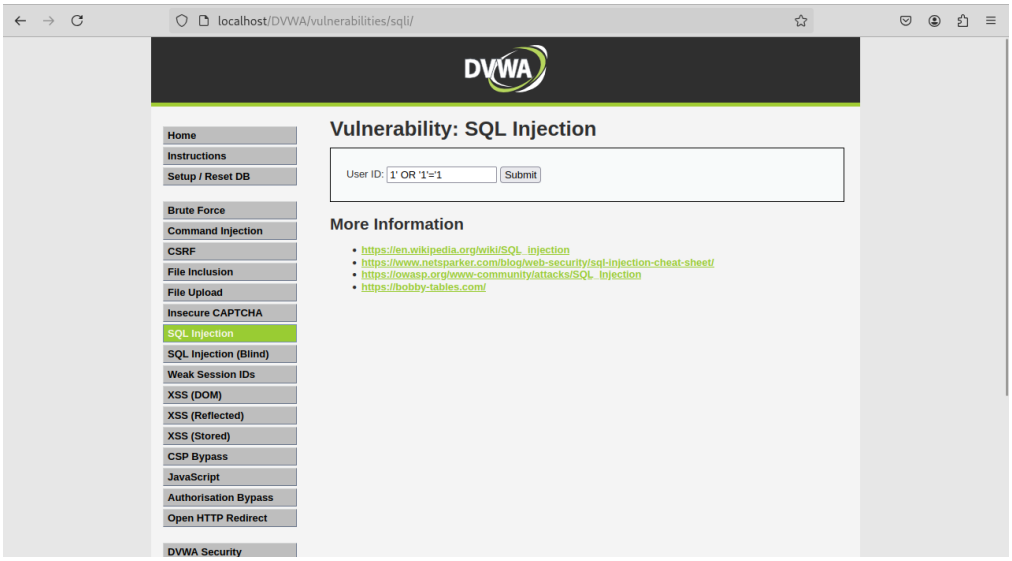
Descripción Del Incidente

Durante la prueba, se detectó que la aplicación DVWA, configurada intencionalmente en nivel de seguridad “**bajo**”, es vulnerable a ataques de inyección SQL. El incidente simula una situación real en la que una mala implementación de las consultas a base de datos puede ser explotada por un atacante para obtener acceso no autorizado, visualizar información sensible o incluso comprometer todo el sistema.

Proceso de reproducción

Configuración previa:

1. Se ingresó a la plataforma **DVWA**.
2. Utilizando: Usuario: admin / Contraseña: password
3. En la pestaña “**DVWA Security**”, se cambió el nivel de seguridad de “Impossible” a "low".
4. Se accedió a la sección de "SQL Injection".
5. En el campo “User ID” se ingresó el siguiente comando:



6. Al hacer clic en "Submit", el sistema permitió el acceso sin validar credenciales.

Resultado

- Se obtuvo acceso al panel interno de **DVWA** como si se tratara de un usuario autenticado.
- No se realizaron validaciones en el back-end (parte del sitio web o aplicación que no es visible para el usuario), lo cual confirma la vulnerabilidad.

Impacto del incidente

- Compromiso de autenticación: se logró eludir completamente el control de acceso.
- Riesgo de filtración de datos: un atacante con conocimientos básicos podría usar técnicas similares para acceder, modificar o eliminar información.
- Escalamiento de privilegios: en una aplicación real, esta falla podría dar acceso a paneles administrativos o comandos del sistema.

Recomendaciones

- Nunca confiar en la entrada del cliente, especialmente en formularios críticos como login.
- Monitorear y registrar intentos fallidos de acceso: para detectar patrones de ataque.
- Realizar pruebas de penetración regularmente: incluso en entornos de desarrollo y pruebas.

Conclusión

El ejercicio permitió demostrar cómo una vulnerabilidad básica de inyección SQL puede ser explotada fácilmente en sistemas mal configurados o sin prácticas de seguridad adecuadas.