1. Título del Incidente

Explotación de Vulnerabilidad de Inyección SQL en DVWA – 14/07/2025

2. Resumen Ejecutivo

El 14 de julio de 2025 se realizó la explotación exitosa de una vulnerabilidad de inyección SQL en la aplicación Damn Vulnerable Web Application (DVWA), instalada en una máquina virtual Debian 12 configurada sobre VirtualBox.
La prueba demostró la obtención no autorizada de múltiples registros de usuarios mediante la manipulación de consultas SQL, validando así la existencia de la debilidad en la validación de entradas.
El propósito es fortalecer la capacidad de respuesta ante incidentes, conforme a los lineamientos de la ISO/IEC 27001.

3. Línea de Tiempo

Fecha y Hora	Descripción
14/07/2025 10:00	Inicio de máquina virtual Debian 12 con DVWA
14/07/2025 10:10	Acceso al módulo de SQL Injection
14/07/2025 10:15	Ejecución de payload 1' OR '1'='1
14/07/2025 10:16	Extracción de registros de usuarios
14/07/2025 10:20	Toma de captura de pantalla de la explotación
14/07/2025 10:45	Elaboración y cierre del reporte

4. Descripción Técnica:

Vulnerabilidad identificada: Inyección SQL (SQLi).

Aplicación afectada: DVWA versión última estable.

Entorno: Máquina virtual Debian 12 sobre VirtualBox.

Base de datos: MySQL/MariaDB.

Vector de ataque: Campo User ID en módulo SQL Injection.

Payload utilizado:

1' OR '1'='1

Resultado: Se logró la consulta de toda la tabla de usuarios sin necesidad de credenciales válidas.

5. Impacto:

Se obtuvo acceso a información sensible simulada: nombres y apellidos de usuarios.

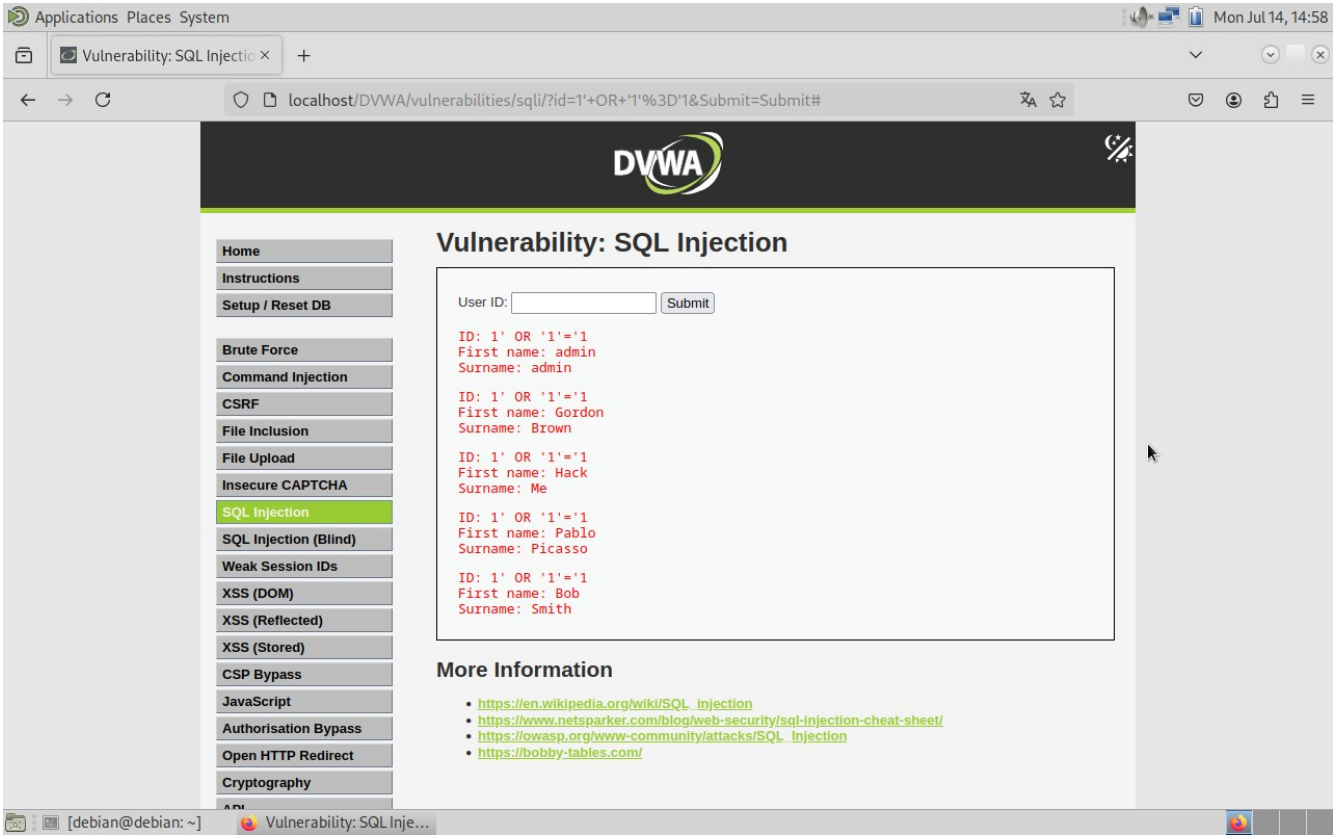
La explotación permitió omitir controles de autenticación.

El escenario es aislado y controlado, sin afectación real a producción.

Se confirma la criticidad alta de este vector en entornos reales.

6. Evidencias

Captura de pantalla de la explotación exitosa:



Descripción:

Se observa la respuesta del servidor tras enviar el payload 1' OR '1'='1, devolviendo múltiples registros de usuarios: admin admin, Gordon Brown, Hack Me, Pablo Picasso, Bob Smith.

Ubicación del archivo: Screenshot at 2025-07-14 14-58-25.png

7. Acciones Tomadas

Confirmación de la vulnerabilidad y ejecución controlada del ataque.

Registro de logs y evidencia gráfica.

Restablecimiento de la base de datos DVWA a su estado inicial mediante Setup / Reset DB.

8. Causa Raíz

El módulo vulnerable no aplica saneamiento de entradas (falta de prepared statements) y concatena la entrada del usuario directamente en la consulta SQL, lo que permite modificar su lógica.

9. Lecciones Aprendidas

La validación de entradas es una de las barreras más críticas para evitar inyecciones SQL.

La ejecución de pruebas en entornos virtualizados garantiza seguridad y reversibilidad.

La documentación precisa de incidentes fortalece la gestión de vulnerabilidades y facilita auditorías.

10. Recomendaciones:

Utilizar consultas parametrizadas/preparadas en desarrollo web.

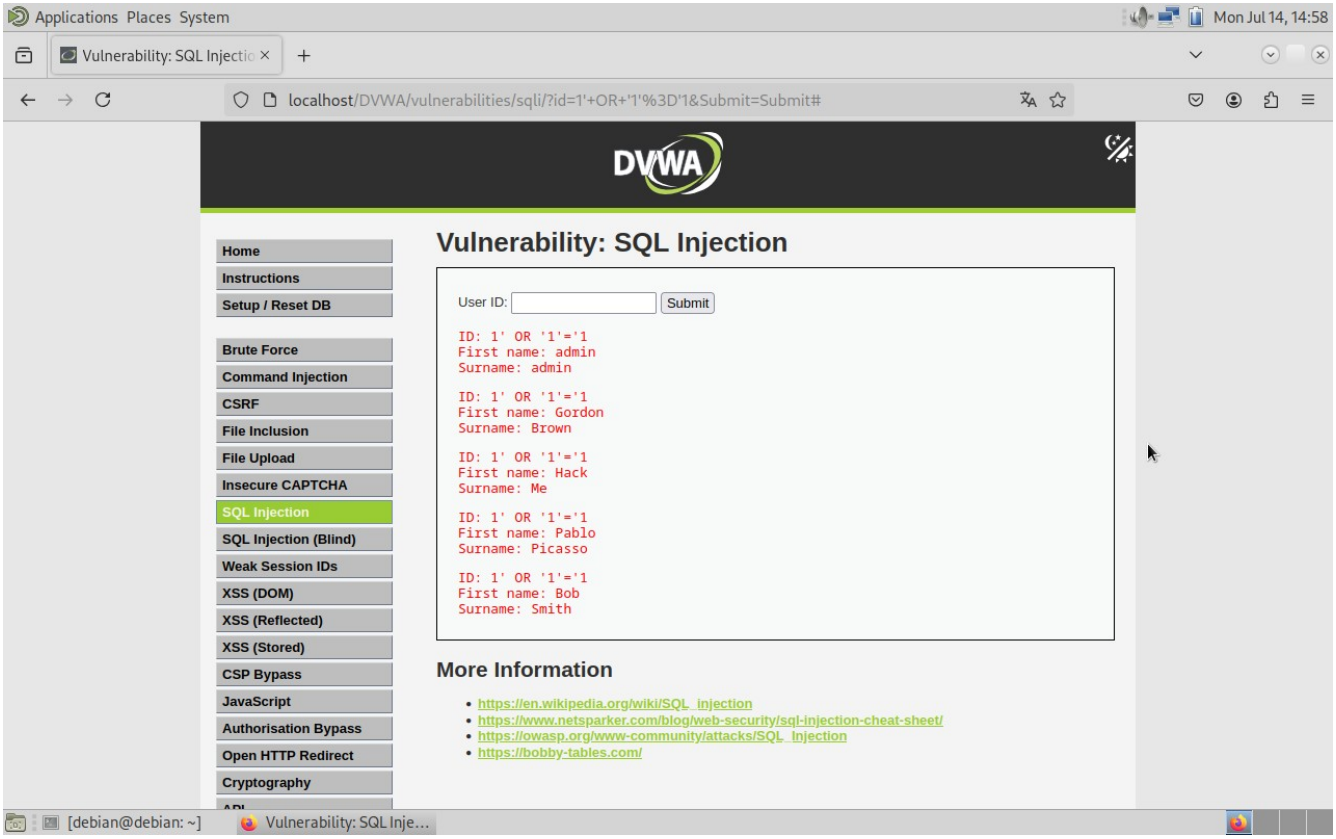
Implementar filtros de validación y sanitización robustos.

Revisar periódicamente la configuración de la base de datos y los permisos de usuario.

Incluir pruebas de penetración regulares.

11. Anexos

Captura de pantalla:



Logs de prueba: Consultas ejecutadas y respuestas de MySQL.

✅ Información de Redacción

Fecha del informe: 14/07/2025

Autor: Carlos Navarro Sanchez

Propósito: Ejercicio de prácticas controladas de seguridad ofensiva y respuesta a incidentes bajo la norma ISO/IEC 27001.