Título del reporte:

Reporte del Incidente de Inyección SQL en Máquina DVWA

Introducción:

El propósito de este reporte es documentar el incidente de inyección SQL detectado en una máquina DVWA, describiendo los detalles del ataque, el proceso de reproducción, el impacto generado, y las recomendaciones para prevenir futuros incidentes.

Descripción del incidente:

Fecha del incidente: 20 de febrero de 2025

A las 17:30, se detectó un ataque de inyección SQL en una máquina DVWA que estaba siendo utilizada como servidor de base de datos. El atacante logró inyectar código SQL malicioso en un campo de entrada no seguro, lo que le permitió obtener acceso no autorizado a datos sensibles almacenados en la base de datos.

Proceso de reproducción:

1. Acceder al formulario de login en la aplicación web

2. En el campo de nombre de usuario, ingresar el siguiente payload malicioso: 1' OR '1' = '1

3. Enviar el formulario.

4. Observar que el atacante ha obtenido acceso no autorizado al sistema.

Impacto del incidente:

- Acceso no autorizado a datos sensibles.

- Riesgo de manipulación y exfiltración de datos.

- Potencial daño a la reputación de la organización.

- Posibles sanciones legales por incumplimiento de regulaciones de protección de datos.

Recomendaciones:

1. Validación de entradas: Implementar una validación estricta de todas las entradas de usuario para asegurarse de que solo se acepten datos válidos.

2. Parcheo y actualización: Asegurarse de que el servidor Debian y todas las aplicaciones estén actualizadas con los últimos parches de seguridad.

3. Monitoreo y auditoría: Implementar un sistema de monitoreo y auditoría para detectar actividades sospechosas y responder rápidamente a posibles ataques.

4. Educación : Capacitar al personal en prácticas de seguridad para que reconozcan y eviten vulnerabilidades comunes.

Conclusión:

El incidente de inyección SQL en DVWA destaca la importancia de implementar medidas de seguridad adecuadas para proteger los sistemas y los datos sensibles.