Reporte de Incidente de Seguridad - DVWA

Título del Reporte

Explotación de Vulnerabilidad por Inyección SQL en la Aplicación DVWA (Damn Vulnerable Web Application)

Introducción

Este informe documenta la explotación de una vulnerabilidad de inyección SQL (SQL Injection) en la plataforma de pruebas DVWA. El objetivo de la actividad fue demostrar el riesgo de este tipo de vulnerabilidades en aplicaciones web mediante la simulación de un ataque controlado.

Descripción del Incidente

Durante una sesión de pruebas de penetración en un entorno controlado, se identificó una vulnerabilidad de inyección SQL en el módulo "SQL Injection" de DVWA. Esta vulnerabilidad permite a un atacante manipular las consultas SQL realizadas al servidor, accediendo a datos confidenciales sin autorización.

Proceso de Reproducción

1. Se accedió a la URL: http://localhost/DVWA
2. Se inició sesión con las credenciales predeterminadas:
   - Usuario: admin
   - Contraseña: password
3. Se navegó a la sección DVWA Security y se estableció el nivel de seguridad en Low.
4. Se accedió al módulo SQL Injection.
5. En el campo "User ID", se ingresó el siguiente payload de prueba:

   1' OR '1'='1

6. Se presionó el botón Submit.
7. La aplicación devolvió un listado completo de usuarios almacenados en la base de datos, demostrando la vulnerabilidad.

Impacto del Incidente

La vulnerabilidad permite a un atacante acceder a información sensible directamente desde la base de datos, como nombres de usuarios y otros posibles datos personales. En un entorno real, esto podría comprometer la confidencialidad de los usuarios, facilitar accesos no autorizados y abrir la puerta a ataques mayores como extracción

masiva de datos, acceso privilegiado o incluso borrado de información.

Recomendaciones

- Implementar consultas preparadas (prepared statements) para prevenir inyecciones SQL.
- Validar y sanitizar todos los datos ingresados por el usuario.
- Aumentar el nivel de seguridad de la aplicación a "Medium" o "High" como mínimo.
- Aplicar controles de acceso adecuados para limitar la exposición de datos.
- Auditar regularmente el código y los accesos a base de datos.

Conclusión

El ejercicio realizado permitió evidenciar de forma práctica la gravedad de una vulnerabilidad por inyección SQL en una aplicación web. Este tipo de fallos son fácilmente explotables si no se aplican buenas prácticas de desarrollo seguro. Es crucial que los desarrolladores y administradores de sistemas integren mecanismos de defensa en profundidad para mitigar este tipo de amenazas.