Título del Reporte Reporte de Incidente: Inyección SQL en DVWA (Laboratorio)

Introducción Este reporte describe un incidente de seguridad simulado en la aplicación Damn Vulnerable Web Application (DVWA), instalada en una máquina virtual para fines educativos. El objetivo del ejercicio es identificar y explotar una vulnerabilidad de inyección SQL y analizar su impacto en un entorno controlado.

Descripción del Incidente Durante las pruebas sobre el módulo “SQL Injection” de DVWA se detectó que el parámetro de entrada “User ID” no valida correctamente los datos introducidos por el usuario. Esto permite inyectar código SQL dentro de la consulta ejecutada en la base de datos y obtener más información de la prevista, lo que representa una vulnerabilidad crítica en una aplicación real.

Proceso de Reproducción 1. Acceder a http://127.0.0.1/dvwa/ e iniciar sesión con: usuario admin, contraseña password. 2. En la pestaña “DVWA Security”, establecer el nivel de seguridad en “Low”. 3. Ir al módulo “SQL Injection”. Primero probar con un ID legítimo (por ejemplo 1) y comprobar que se muestra un solo usuario. 4. Introducir el payload 1' OR '1'='1 en el campo “User ID” y enviar la petición. 5. Observar que la aplicación devuelve información de varios usuarios, confirmando la inyección SQL.

Impacto del Incidente Si esta vulnerabilidad existiera en un entorno de producción, un atacante podría acceder a información sensible almacenada en la base de datos (usuarios, correos, contraseñas cifradas, etc.). Además, podría modificar o eliminar datos, afectar el funcionamiento normal de la aplicación y generar consecuencias legales y de reputación para la organización.

Recomendaciones - Utilizar consultas preparadas y parámetros en lugar de concatenar directamente la entrada del usuario en las sentencias SQL. - Implementar validación y filtrado de datos del lado del servidor, verificando tipos de datos (por ejemplo, que el ID sea numérico). - Aplicar el principio de mínimo privilegio en las cuentas de la base de datos. - Manejar los errores de forma segura, evitando mostrar mensajes internos de la base de datos al usuario final. - Realizar revisiones de código y pruebas de seguridad periódicas para detectar este tipo de vulnerabilidades.

Conclusión El ejercicio demostró que el módulo “SQL Injection” de DVWA es vulnerable a inyección SQL cuando la aplicación no valida ni parametriza correctamente las entradas del usuario. Aunque se trata de un entorno de laboratorio, el incidente ilustra claramente los riesgos que este tipo de fallo supondría en una aplicación real. La adopción de las recomendaciones indicadas es esencial para reducir la superficie de ataque y mejorar la seguridad de las aplicaciones web.