Informe de Gestión de Incidentes conforme a ISO 27 001 Vulnerabilidad de Inyección SQL

Introducción

Este informe detalla la identificación, explotación y mitigación de una vulnerabilidad crítica de inyección SQL en la aplicación web Damn Vulnerable Web Application (DVWA). La evaluación se realizó en un entorno controlado para demostrar cómo las inyecciones SQL pueden comprometer la seguridad de las aplicaciones web, y cómo abordar tales vulnerabilidades conforme a las mejores prácticas de ciberseguridad.

Descripción del Incidente

Durante una prueba de penetración en DVWA, se descubrió una vulnerabilidad de inyección SQL en el módulo "SQL Injection". Esta vulnerabilidad permite a un atacante insertar consultas SQL maliciosas a través de campos de entrada, afectando tanto la confidencialidad como la integridad de los datos en la base de datos subyacente.

Método de Inyección SQL Utilizado

La vulnerabilidad fue explotada mediante la inserción del siguiente payload SQL en el campo "User ID":
1' OR '1'='1

Consulta original:
SELECT * FROM users WHERE user_id = '<input>'
Consulta manipulada:
SELECT * FROM users WHERE user_id = '1' OR '1'='1';

Este payload modifica la consulta SQL de tal forma que siempre se evalúa como verdadera, permitiendo al atacante el acceso no autorizado a la base de datos y la consulta de datos sensibles sin necesidad de autenticación.

Impacto del Incidente

La explotación exitosa de esta vulnerabilidad permite a los atacantes realizar diversas acciones no autorizadas, tales como:

- Acceso no autorizado a la base de datos.
- Extracción de información sensible, como credenciales de usuario o datos personales.
- Modificación o eliminación de datos críticos, comprometiendo la integridad de los sistemas.
- Destrucción de la disponibilidad de los servicios mediante la manipulación de consultas SQL.

Recomendaciones

Para mitigar esta vulnerabilidad y prevenir futuros incidentes, se proponen las siguientes acciones correctivas:

- **1 Validación de Entrada**
  - Asegurarse de que todas las entradas proporcionadas por los usuarios sean validadas antes de ser procesadas.
  - Utilizar consultas preparadas y parámetros vinculados para evitar la manipulación de consultas SQL.

- **2 Pruebas de Penetración Regulares**
  - Realizar auditorías de seguridad periódicas para detectar vulnerabilidades y aplicar medidas correctivas antes de que los atacantes las exploten.

- **3 Educación y Concienciación**
  - Capacitar al personal en las mejores prácticas de desarrollo seguro y sensibilizarlos sobre los riesgos relacionados con las inyecciones SQL.

Conclusión

Este incidente resalta la gravedad de las vulnerabilidades de inyección SQL, que pueden comprometer la seguridad de una aplicación web de forma significativa. En el caso de DVWA, un simple payload permitió acceso no autorizado a la base de datos, poniendo en riesgo la confidencialidad, integridad y disponibilidad de los datos.

Prevenir estas amenazas requiere validar estrictamente las entradas, usar consultas preparadas y realizar auditorías periódicas. Además, capacitar al personal en buenas prácticas de seguridad es esencial para fortalecer la protección y reducir riesgos.