Informe de gestión de incidentes conforme a la norma ISO 27001: Vulnerabilidad de inyección SQL

Introducción

El presente documento detalla la explotación de una vulnerabilidad de Inyección SQL detectada en el entorno de pruebas DVWA. Este incidente se categoriza como un fallo crítico en la validación de entradas de datos, afectando la confidencialidad e integridad de la base de una base de datos.

Descripción del Incidente:

La aplicación DVWA sufrió un acceso no autorizado a su base de datos a través del campo de búsqueda de usuarios. Un atacante externo aprovechó el formulario de "User ID" para introducir código malicioso en lugar de un número de identificación común.

Proceso de Reproducción:

1. Ingresar a la aplicación DVWA e iniciar sesión.
2. Navegar al menú lateral izquierdo y seleccionar la opción **"SQL Injection"**.
3. Ubicar el cuadro de texto etiquetado como **"User ID"**.
4. Escribir exactamente la siguiente cadena: `1' OR '1'='1`.
5. Hacer clic en el botón **"Submit"**.
6. Observar que la pantalla despliega la lista completa de usuarios de la base de datos en lugar de uno solo.

Impacto del incidente:

El impacto de un ataque de Inyección SQL es uno de los más graves en seguridad de la información, ya que afecta directamente al activo más valioso de una organización, los datos. El atacante puede tener acceso a información confidencial, tal como: Nombres, Apellidos, correos, Números telefónicos, información bancaria, información médica, etc.

Recomendaciones:

1. **Filtrar las entradas:** La aplicación debe revisar lo que el usuario escribe y prohibir el uso de símbolos raros (como comillas) que puedan confundir al sistema.

2. **Preparar las consultas:** Usar un método donde la base de datos reciba los datos por separado de las órdenes, para que nunca confunda un comentario del usuario con una instrucción.

3. **Limitar permisos:** Configurar la base de datos para que la aplicación solo pueda ver lo mínimo necesario y no toda la información.

4. **Revisión técnica:** Examinar el código de la página frecuentemente para encontrar estos errores antes de que alguien más los use para atacar.

Conclusión:

Se comprobó que la aplicación es vulnerable porque permite que cualquier persona manipule la base de datos simplemente escribiendo un código en el formulario de usuario. El incidente demostró que la seguridad actual es insuficiente, ya que se pudo extraer información privada de todos los usuarios de manera muy fácil y rápida.

Es urgente aplicar mejores filtros mas seguros. Si no, cualquier atacante podría robar, cambiar o borrar toda la información importante del sistema. Para cumplir con las normas de seguridad ISO 27001, este error debe corregirse de inmediato para proteger la confianza de los usuarios y la integridad de los datos.