Gestión de Incidentes conforme a ISO 27001

Informe de Vulnerabilidad – Inyección SQL

Introducción

Este documento describe el hallazgo y explotación de una vulnerabilidad de inyección SQL identificada en la aplicación Damn Vulnerable Web Application (DVWA). Las pruebas se llevaron a cabo en un entorno controlado con el fin de ilustrar una debilidad común en aplicaciones web y evidenciar sus posibles consecuencias para la seguridad de la información.

Descripción del Incidente

Durante el análisis de seguridad realizado en DVWA, se detectó una vulnerabilidad en el módulo denominado "SQL Injection". Esta falla permite que un atacante inserte comandos SQL maliciosos a través de los campos de entrada de la aplicación, comprometiendo así la integridad y confidencialidad de los datos almacenados en la base de datos.

Técnica de Inyección Utilizada

Para validar la vulnerabilidad, se utilizó el siguiente payload en el campo "User ID":

sql

```
' OR 1=1 --
```

Este comando modifica la consulta SQL original con el objetivo de extraer los nombres de usuario y contraseñas de la tabla `users`, específicamente del registro con `id = 2`. La ejecución exitosa de esta inyección permite obtener credenciales de usuario sin autorización, demostrando la criticidad de la falla.

Impacto del Incidente

De ser explotada, esta vulnerabilidad podría permitir que un atacante:

- Acceda a información sensible contenida en la base de datos, como credenciales de usuarios.

- Alterar, eliminar o manipular datos confidenciales de la aplicación.

El riesgo asociado afecta directamente la **confidencialidad**, **integridad** y **disponibilidad** de los datos y servicios que ofrece DVWA.

Recomendaciones

A raíz de los hallazgos, se sugieren las siguientes acciones correctivas y preventivas:

1. **Validación de Entradas:** Asegurar la validación exhaustiva de los datos ingresados por el usuario, empleando consultas parametrizadas o procedimientos almacenados para evitar inyecciones SQL.

2. **Evaluaciones de Seguridad:** Realizar pruebas de penetración y auditorías periódicas para detectar vulnerabilidades y mitigarlas proactivamente.

3. **Capacitación Continua:** Promover la formación en prácticas seguras de desarrollo tanto en equipos técnicos como en perfiles no técnicos, fomentando una cultura de seguridad.

Conclusión

El descubrimiento y explotación controlada de esta vulnerabilidad en DVWA evidencia la necesidad de integrar medidas de seguridad desde las fases iniciales del desarrollo. Adoptar controles robustos y buenas prácticas en ciberseguridad resulta esencial para proteger los activos críticos de una organización y asegurar la continuidad operativa.