Informe de Gestión de Incidentes conforme a la ISO 27001

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

1. Introducción

Este informe detalla la identificación y explotación de una vulnerabilidad de SQL Injection detectada en la aplicación Damn Vulnerable Web Application (DVWA). La prueba se realizó en un entorno controlado con el propósito de demostrar una vulnerabilidad común y su posible impacto en la seguridad de la aplicación.

2. Descripción del Incidente

Durante la evaluación de seguridad realizada sobre DVWA, se detectó una vulnerabilidad de inyección SQL en el módulo denominado "SQL Injection". Esta vulnerabilidad permite que un atacante inyecte consultas SQL maliciosas a través de los campos de entrada del sitio web, comprometiendo la integridad y confidencialidad de los datos almacenados en la base de datos.

3. Método de Inyección SQL Utilizado

Para replicar y demostrar la vulnerabilidad, se utilizó la siguiente carga útil (payload) en el campo "User ID":

‘ UNION SELECT username, password FROM users WHERE id = 1 #

Este payload modifica la consulta SQL original para devolver los nombres de usuario y contraseñas almacenados en la tabla users, específicamente para el usuario con id = 1. La ejecución exitosa de esta inyección permite obtener credenciales sin autorización.

4. Impacto del Incidente

La explotación de esta vulnerabilidad podría permitir a un atacante:

- Acceder y extraer información confidencial de la base de datos, incluyendo credenciales de usuarios.
- Modificar, eliminar o comprometer datos sensibles almacenados en la aplicación.
- Esto representa un riesgo significativo para la confidencialidad, integridad y disponibilidad de los datos y servicios proporcionados por DVWA.

5. Recomendaciones

En base a los hallazgos, se sugieren las siguientes medidas correctivas y preventivas:

- Validación de Entradas: Implementar validaciones estrictas para todos los datos proporcionados por el usuario, usando consultas parametrizadas para prevenir inyección SQL.

- Pruebas de Penetración: Realizar auditorías de seguridad regulares, incluyendo pruebas de penetración, para identificar y mitigar vulnerabilidades antes de que puedan ser explotadas.

- Capacitación y Concientización: Formar al personal técnico y no técnico en buenas prácticas de desarrollo seguro y aumentar la conciencia sobre los riesgos de vulnerabilidades de seguridad.

6. Conclusiones

La detección y explotación exitosa de la vulnerabilidad de inyección SQL en la aplicación DVWA , pone de manifiesto la necesidad crítica de implementar fuertes medidas de seguridad durante el proceso de desarrollo y mantenimiento de aplicaciones web.

La inyección SQL sigue siendo una de las amenazas más comunes y peligrosas ya que permite a los atacantes comprometer la confidencialidad, integridad y disponibilidad de la información almacenada en las bases de datos.

Se recomienda adoptar un enfoque integral de seguridad mas allá de medidas reactivas, que van desde la validación estricta hasta monitorización y capacitación del personal.

Recomendación de herramientas para mejorar estos procesos:

- WAF: Firewall de primera línea defensiva.

- ORM: Frameworks para abstraer acceso a bases de datos.

- Análisis de seguridad de código: detección de vulnerabilidades tempranas.

- Gestión de estas vulnerabilidades y pruebas de penetración: auditorías identificativas.

- Capacitación continua: formación constante.

  En resumen, hablaríamos de un computo entre buenas prácticas de desarrollo, herramientas tecnológicas y concienciación del personal.