Título del Reporte

Vulnerabilidad de Inyección SQL en DVWA

Introducción

Este informe detalla la identificación y explotación de una vulnerabilidad de inyección SQL en la aplicación Damn Vulnerable Web Application (DVWA). La prueba se realizó en un entorno controlado con el objetivo de demostrar una vulnerabilidad común y su impacto en la seguridad de las aplicaciones web.

Descripción del Incidente

Durante la evaluación de seguridad de DVWA, se descubrió una vulnerabilidad de inyección SQL en el módulo "SQL Injection". Esta vulnerabilidad permite a un atacante inyectar consultas SQL maliciosas a través de los campos de entrada de la aplicación web, comprometiendo la integridad y confidencialidad de los datos almacenados en la base de datos.

Proceso de Reproducción

Para replicar y demostrar la vulnerabilidad, se utilizó la siguiente carga SQL en el campo "User ID":

1' OR '1'='1

Esta carga explota la vulnerabilidad al modificar la consulta SQL original de manera que devuelva todos los registros de la base de datos en lugar de uno solo. Como resultado, la aplicación muestra información confidencial de múltiples usuarios, incluyendo nombres y apellidos.

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 usuario.
- Modificar, eliminar o comprometer datos sensibles almacenados en la aplicación.
- Obtener control sobre la base de datos e incluso sobre la aplicación si se encadenan otras vulnerabilidades.

Este incidente representa un riesgo significativo para la confidencialidad, integridad y disponibilidad de los datos y servicios proporcionados por DVWA.

Recomendaciones

Con base en los hallazgos de esta evaluación de seguridad, se recomiendan las siguientes medidas correctivas y preventivas:

1. **Validación de Entrada:** Implementar validaciones estrictas para todos los datos ingresados por el usuario y utilizar consultas parametrizadas para prevenir la inyección SQL.
2. **Uso de ORM y Prepared Statements:** Implementar Object-Relational Mapping (ORM) o declaraciones preparadas en la aplicación para evitar la manipulación directa de consultas SQL.
3. **Pruebas de Penetración:** Realizar auditorías de seguridad periódicas, incluyendo pruebas de penetración, para identificar y mitigar vulnerabilidades antes de que sean explotadas por atacantes.
4. **Educación y Concienciación:** Capacitar al personal técnico y no técnico en prácticas de desarrollo seguro y concienciar sobre los riesgos asociados con las vulnerabilidades de seguridad.
5. **Uso de Web Application Firewalls (WAF):** Implementar un firewall de aplicaciones web para detectar y bloquear patrones de ataque de inyección SQL en tiempo real.

Conclusión

La identificación y explotación de la vulnerabilidad de inyección SQL en DVWA destaca la importancia de la seguridad proactiva en el desarrollo y mantenimiento de aplicaciones web. La implementación de controles de seguridad robustos y el seguimiento de las mejores prácticas de ciberseguridad son esenciales para proteger los activos críticos y garantizar la continuidad del negocio.