Informe de Vulnerabilidad:

Inyección SQL en DVWA

Este informe detalla la identificación y explotación de una vulnerabilidad de **inyección SQL** en la aplicación web **Damn Vulnerable Web Application (DVWA)** en **http://localhost/DVWA**. Se describe el proceso de reproducción del ataque, su impacto potencial y recomendaciones para mitigar el riesgo.

Descripción del Incidente

Se ha detectado una vulnerabilidad de **inyección SQL** en el formulario de autenticación de DVWA. Esta vulnerabilidad permite a un atacante acceder a la base de datos sin necesidad de conocer credenciales válidas, lo que podría comprometer la seguridad de la aplicación.

Proceso de Reproducción

- Entorno de Pruebas

- **Aplicación:** DVWA (Damn Vulnerable Web Application)
- **URL afectada:** `http://localhost/DVWA/login.php`
- **Tipo de inyección:** SQL Injection Clásico

- Pasos para Explotar la Vulnerabilidad

1. Acceder a la página de inicio de sesión: `http://localhost/DVWA/login.php`
2. Ingresar la siguiente cadena en el campo de usuario:
   ' OR '1'='1
3. Ingresar cualquier valor o dejar en blanco el campo de contraseña.
4. Presionar el botón de inicio de sesión.
5. Resultado: Se obtiene acceso sin necesidad de credenciales válidas.

Impacto del Incidente

El aprovechamiento de esta vulnerabilidad permite a un atacante:

- Autenticarse sin conocer credenciales válidas.
- Acceder a datos sensibles almacenados en la base de datos.
- Modificar o eliminar registros.
- Escalar privilegios y comprometer el sistema.

Recomendaciones

Para mitigar esta vulnerabilidad, se recomienda implementar las siguientes medidas:

- Uso de consultas preparadas para evitar la manipulación de las consultas SQL.
- Validación y saneamiento de entrada del usuario, asegurando que solo se ingresen datos esperados.
- Uso de mecanismos de control de acceso para restringir privilegios.
- Implementación de un Web Application Firewall (WAF) para detectar y bloquear ataques SQLi.
- Auditoría de seguridad periódica para identificar vulnerabilidades en la aplicación.

Conclusión

Se ha demostrado la existencia de una vulnerabilidad de **inyección SQL** en **DVWA**. Esta falla permite a atacantes comprometer la seguridad del sistema y acceder a información crítica. Se recomienda aplicar las medidas sugeridas para mitigar este riesgo y mejorar la seguridad de la aplicación.

autor : Omar Siccha

Marzo 2025, Barcelona