Reporte de Vulnerabilidad: Inyección SQL en DVWA

Introducción

Este reporte documenta la identificación y explotación de una vulnerabilidad de inyección SQL en la aplicación DVWA (Damn Vulnerable Web Application), la cual se emplea con fines educativos y de prueba en entornos controlados. El objetivo es evidenciar el impacto potencial de una inyección SQL no mitigada y proporcionar recomendaciones para prevenir este tipo de ataques en sistemas reales.

Descripción del Incidente

Durante una sesión de prueba en DVWA, se identificó una vulnerabilidad de tipo **Inyección SQL** (SQL Injection) en un parámetro de entrada que interactúa directamente con una base de datos sin una validación adecuada. Al manipular el valor del parámetro `ID`, se logró acceder a múltiples registros de usuarios, eludiendo los mecanismos normales de autenticación o filtrado de datos.

Proceso de Reproducción

1. **Entorno de prueba**: DVWA en nivel de seguridad "Low".

2. **Paso 1**: Acceder a la funcionalidad de búsqueda de usuarios por ID.

Paso 2: En el campo de entrada correspondiente al `ID`, ingresar la siguiente cadena maliciosa:

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

3.
4. **Paso 3**: Enviar el formulario.

Resultado obtenido:
La aplicación retornó múltiples registros de usuarios, lo que indica que la consulta SQL subyacente fue manipulada con éxito para devolver toda la tabla de usuarios. Los datos expuestos incluyen:

- First name: admin, Surname: admin

- First name: Gordon, Surname: Brown
- First name: Hack, Surname: Me
- First name: Pablo, Surname: Picasso
- First name: Bob, Surname: Smith

Impacto del Incidente

- **Exposición de datos sensibles**: Se obtuvo acceso no autorizado a información de múltiples usuarios.
- **Violación de confidencialidad**: Cualquier atacante puede visualizar datos internos sin autenticación previa.
- **Posible escalamiento de privilegios**: En un entorno real, esta vulnerabilidad podría utilizarse para obtener credenciales administrativas.
- **Riesgo de modificación o destrucción de datos**: En fases más avanzadas, un atacante podría modificar o eliminar información crítica.

Recomendaciones

1. **Validación y saneamiento de entradas**: Utilizar funciones como `mysqli_real_escape_string()` o mecanismos ORM para filtrar las entradas del usuario.
2. **Uso de consultas preparadas (prepared statements)**: Implementar sentencias SQL parametrizadas para prevenir inyecciones.
3. **Configuración del entorno**: Asegurar que el entorno de producción tenga configuraciones más estrictas, a diferencia de entornos de prueba como DVWA.
4. **Monitoreo y registros**: Implementar registros de actividad y sistemas de detección de intrusos (IDS) para alertar sobre intentos de inyección.
5. **Formación continua**: Capacitar al equipo de desarrollo en prácticas seguras de codificación.

Conclusión

La explotación de la vulnerabilidad de inyección SQL en DVWA demuestra cómo una aplicación web sin validación adecuada de entradas puede comprometer la integridad y confidencialidad de su base de datos. Aunque DVWA está diseñado para simular fallos de seguridad, los mismos principios aplican a aplicaciones reales. Implementar las recomendaciones descritas contribuirá significativamente a mitigar riesgos similares en entornos de producción.