Informe de Vulnerabilidad de Inyección SQL en DVWA

Introducción:

Informe documentando la vulnerabilidad y explotación de SQLi en DVWA. La vulnerabilidad como tal consiste en insertar código SQL en un sitio web con la intención de acceder a la base de datos y/o manipularlos.

Descripción del Incidente:

En el ejercicio de vulnerabilidad de inyección SQL en la funcionalidad de ingreso de ID de usuario en DVWA podemos inyectar código SQL para asi poder conseguir la base de datos con el nombre de los usuarios.

Proceso de Reproducción:

1. Acceder a la aplicación web en la URL: `http://localhost/DVWA`.
2. Iniciar sesión con las credenciales:
    - Usuario: `admin`
    - Contraseña: `password`
3. Ir a "SQL Injection" en el menú de la aplicación.
4. En el campo "User ID", poner la siguiente sentencia :
   1' OR '1'='1
5. Le damos a "Submit" para que se ejecute.
6. La aplicación devuelve una lista de todos los usuarios almacenados en la base de datos, lo que confirma la vulnerabilidad.

Impacto del Incidente:

- Acceso no autorizado a la base de datos.
- Posible robo de credenciales y datos sensibles.
- Riesgo de alteración o eliminación de datos.
- Posibilidad de escalamiento de privilegios y control total del sistema.

Recomendaciones:

1. Implementar consultas preparadas o declaraciones parametrizadas para evitar inyecciones SQL.
2. Validar todas las entradas de usuario.
3. Restringir los permisos de la base de datos para evitar accesos innecesarios.
4. Mantener el software actualizado con parches de seguridad.

Conclusión:
Se ha identificado y explotado una vulnerabilidad de SQLi en DVWA, permitiendo el acceso

a información no autorizada. Para mitigar este riesgo, se recomienda aplicar medidas de seguridad como el uso de consultas parametrizadas y validación de datos. La implementación de estas prácticas fortalece la seguridad de la aplicación y prevenir futuros ataques.