Reporte de Vulnerabilidad: SQL Injection

Nombre de la vulnerabilidad:

SQL Injection (Inyección SQL)

ID de prueba:

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

Descripción del problema:

Se ha detectado una vulnerabilidad de tipo **inyección SQL** en el sistema. Esta falla ocurre cuando los datos ingresados por el usuario (como el "ID") no se validan correctamente y se usan directamente en una consulta a la base de datos.

En esta prueba, se utilizó el siguiente valor como ID:

```
bash
CopiarEditar
1' OR '1'='1
```

Este valor **modifica la consulta SQL** original, haciendo que se devuelvan **todos los registros de la base de datos**, en lugar de solo uno.

Resultados obtenidos:

La siguiente información fue revelada, lo cual **no debería ser accesible solo con un ID**:

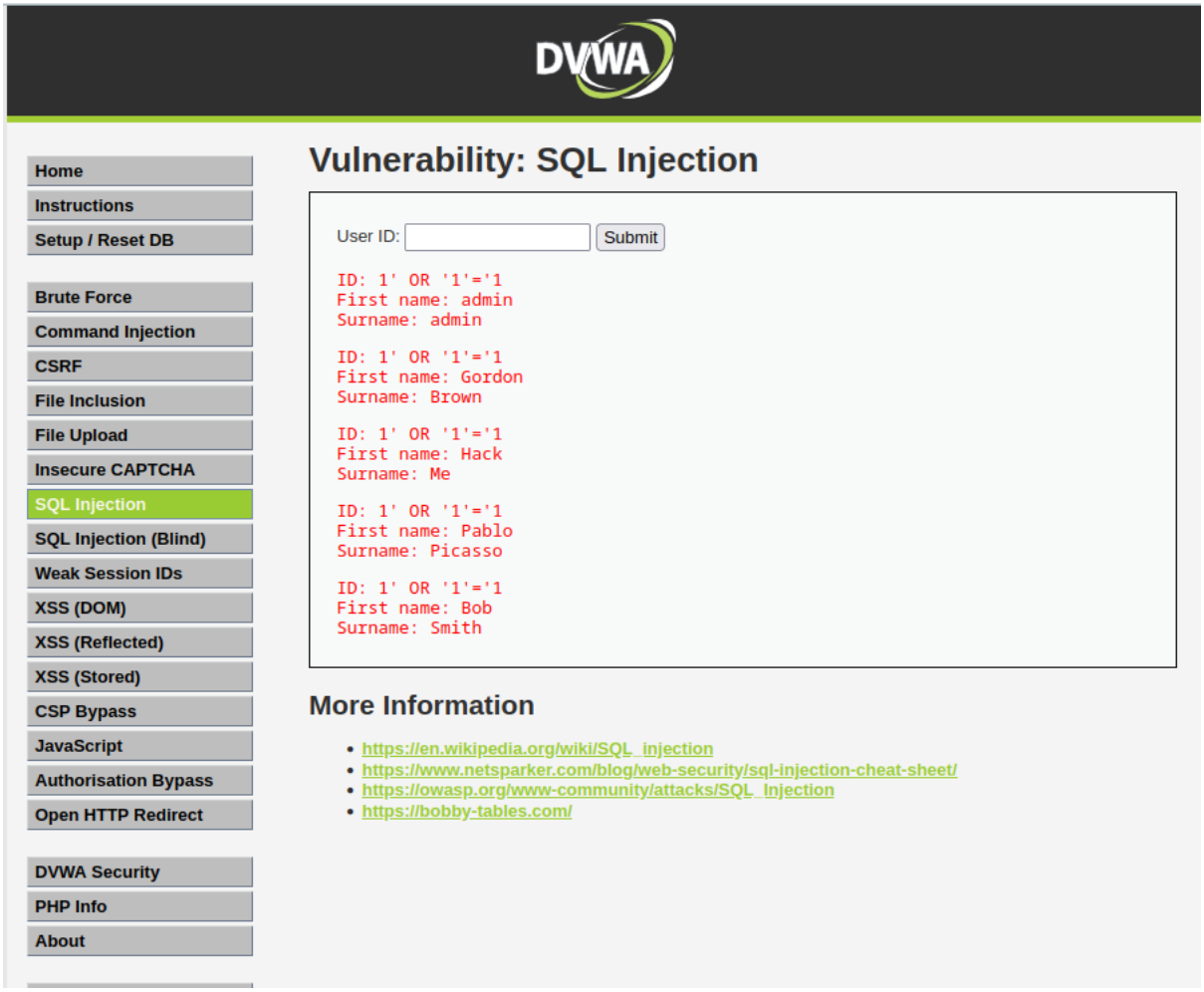
ID ingresado	Nombre	Apellido
1' OR '1'='1	admin	admin
1' OR '1'='1	Gordon	Brown
1' OR '1'='1	Hack	Me
1' OR '1'='1	Pablo	Picasso

1' OR '1'='1 Bob Smith

Esto indica que la aplicación está ejecutando el siguiente tipo de consulta insegura:

```
sql
CopiarEditar
SELECT * FROM users WHERE id = '1' OR '1'='1';
```

La condición `'1'='1'` **siempre es verdadera**, por lo tanto se devuelven **todos los usuarios**.



Riesgos:

- Acceso no autorizado a datos personales.
- Robo o manipulación de datos.
- Posible compromiso total de la base de datos.

- Incumplimiento de leyes de protección de datos (como GDPR o Ley Federal de Protección de Datos Personales en México).

Recomendaciones:

1. **Usar consultas preparadas (prepared statements)** en lugar de concatenar texto directamente en SQL.
2. **Validar y sanitizar todas las entradas del usuario.**
3. **Limitar los permisos del usuario de base de datos** utilizado por la aplicación.
4. **Implementar un firewall de aplicaciones web (WAF).**
5. **Realizar pruebas de seguridad regularmente** (pentesting y análisis estático).

Conclusión:

Esta prueba demuestra que el sistema es **vulnerable a inyecciones SQL**. Urge tomar medidas correctivas para proteger los datos y evitar posibles ataques.