**Reporte de Incidente de Seguridad**

Vulnerabilidad de Inyección SQL

## Descripción del Incidente

Durante la evaluación de seguridad de la aplicación Damn Vulnerable Web Application (DVWA), se identificó una vulnerabilidad de **inyección SQL** en el módulo "SQL Injection". Esta vulnerabilidad permite a un atacante inyectar consultas SQL maliciosas a través del campo de entrada "User ID", comprometiendo la integridad y confidencialidad de la base de datos.

## Método de Explotación

Se utilizó ' OR '1'='1 para demostrar la vulnerabilidad. Este ataque permitió el acceso a múltiples registros de la base de datos, exponiendo información como nombres de usuario y apellidos.

## Impacto del Incidente

Acceder y extraer información confidencial de la base de datos, incluidos credenciales de usuario.

Este incidente representa una amenaza significativa a la confidencialidad, integridad y disponibilidad de los datos almacenados en el sistema.

## Medidas Correctivas y Preventivas

1. Aplicar validaciones estrictas en todos los campos de entrada y usar consultas preparadas para evitar la manipulación de SQL.
2. Realizar auditorías de seguridad periódicas para identificar y corregir vulnerabilidades antes de que sean explotadas.
3. Entrenar al personal de desarrollo en prácticas seguras de codificación y concienciar sobre los riesgos de seguridad.
4. Adoptar estándares de seguridad como OWASP Top 10 y asegurar el cumplimiento de normativas de protección de datos.

## Conclusión

El hallazgo de esta vulnerabilidad resaltan la importancia de adoptar un enfoque proactivo en la seguridad de las aplicaciones web. La implementación de medidas de seguridad adecuadas es esencial para proteger los activos críticos y garantizar la continuidad del negocio.