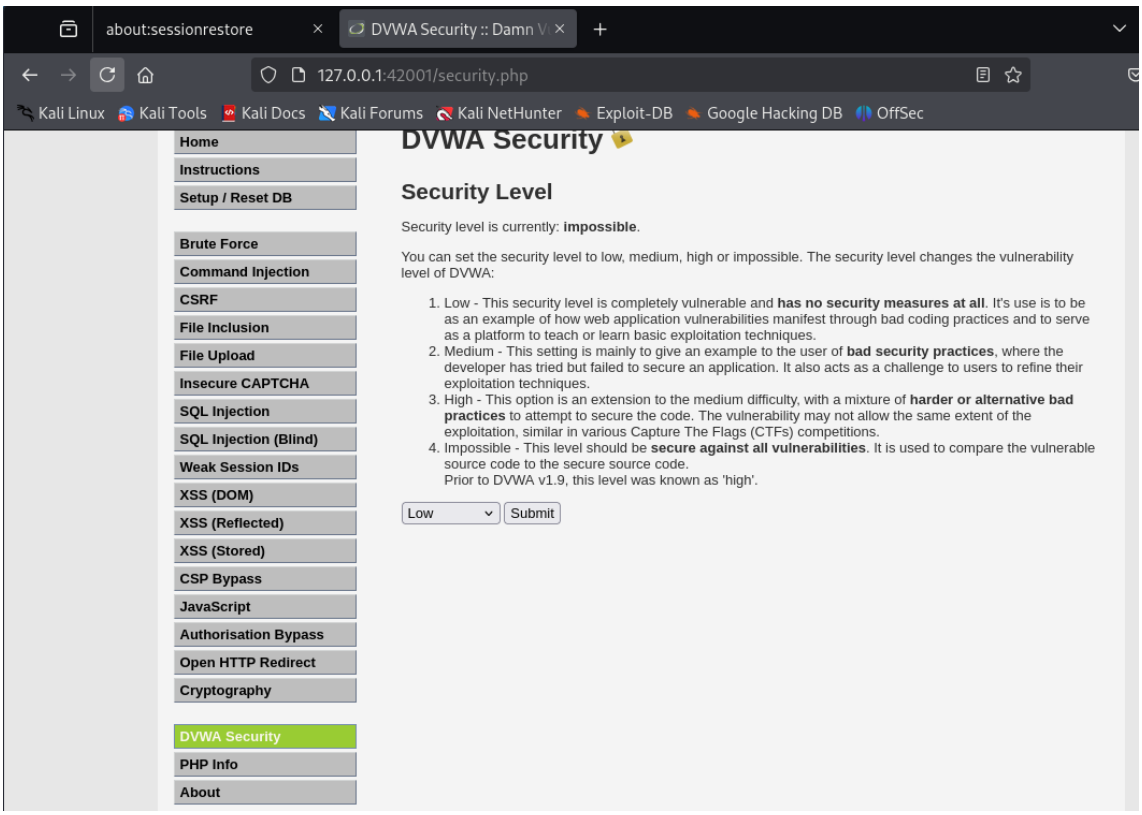
Informe de Gestión de Incidentes – Cumplimiento ISO 27001
Vulnerabilidad por Inyección SQL en DVWA

1. **Introducción**

   Se documenta la detección y explotación controlada de una vulnerabilidad por inyección SQL en el entorno de pruebas de la aplicación *Damn Vulnerable Web Application (DVWA)*, con el objetivo de demostrar el riesgo que representa este tipo de falla común en la seguridad de aplicaciones web.

2. **Bajar el nivel de Seguridad**

   Para la prueba bajamos en la Seguridad el nivel seleccionado a Low.



2. Descripción del Incidente

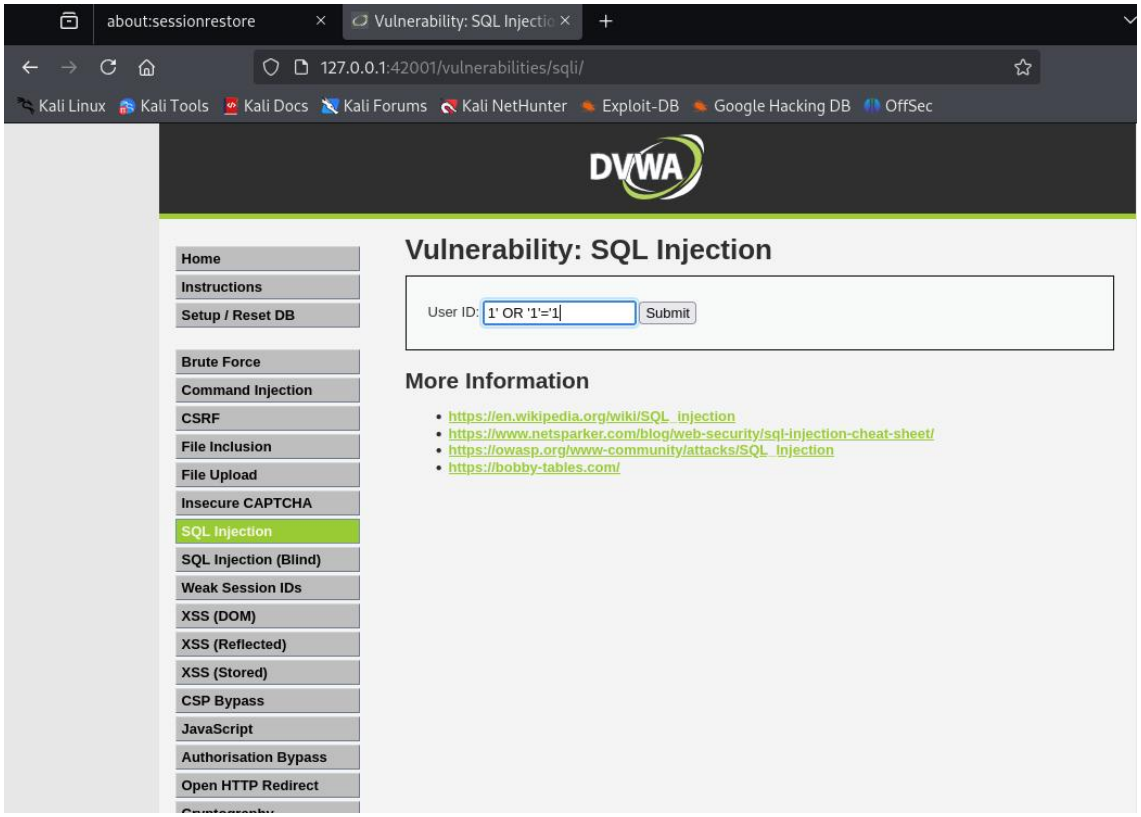
Durante una evaluación de seguridad, se identificó una vulnerabilidad de inyección SQL en el módulo “SQL Injection” de DVWA. La falla permite a un atacante insertar instrucciones SQL maliciosas a través de campos de entrada, comprometiendo así la integridad y confidencialidad de los datos almacenados en la base de datos.

3. Técnica de Inyección SQL Utilizada

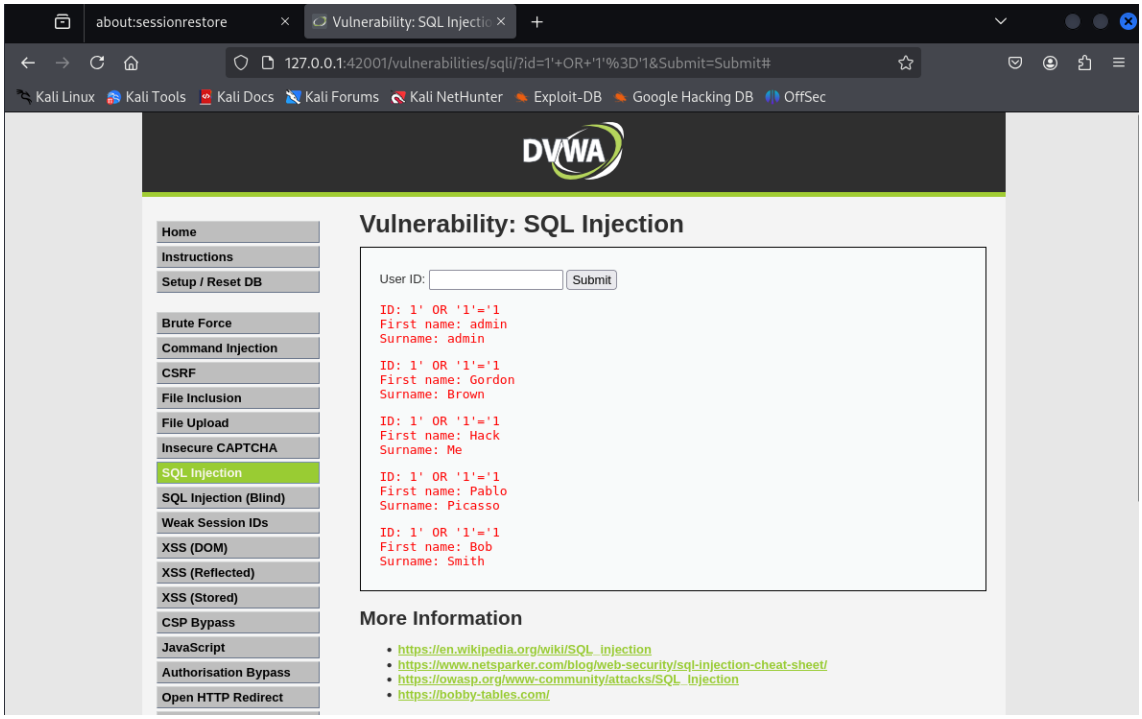
Se utilizó el siguiente payload en el campo "User ID" para explotar la vulnerabilidad:

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

En esta imagen introducimos en la sentencia SQL.



Aquí arroja el resultado con todos los campos de la BD SQL.



Este vector de ataque modifica la consulta SQL original para obtener nombres de usuario y contraseñas del usuario con todos los ID, sin necesidad de autenticación previa.

4. Impacto del Incidente
La explotación de esta vulnerabilidad permite al atacante:

- Acceder a información confidencial (e.g., credenciales de usuarios).
- Alterar, eliminar o comprometer datos sensibles de la aplicación.

Esto afecta directamente a los principios de confidencialidad, integridad y disponibilidad de los activos de información gestionados por la aplicación.

5. Recomendaciones
Se proponen las siguientes medidas correctivas y preventivas:

1. **Validación de Entradas:** Implementar validaciones estrictas y parametrización segura en todas las consultas SQL.
2. **Pruebas de Penetración:** Realizar auditorías periódicas de seguridad para identificar vulnerabilidades antes de su explotación.
3. **Capacitación:** Promover la formación continua en desarrollo seguro y concienciación sobre riesgos de seguridad, tanto en personal técnico como no técnico.

6. Conclusión
La explotación exitosa de esta vulnerabilidad destaca la necesidad de adoptar un enfoque proactivo en ciberseguridad. La implementación de controles robustos y el seguimiento de buenas prácticas son fundamentales para proteger activos críticos y garantizar la continuidad operativa.