Cumplimiento del ISO 27001

Reporte de Inyección SQL

Introducción:

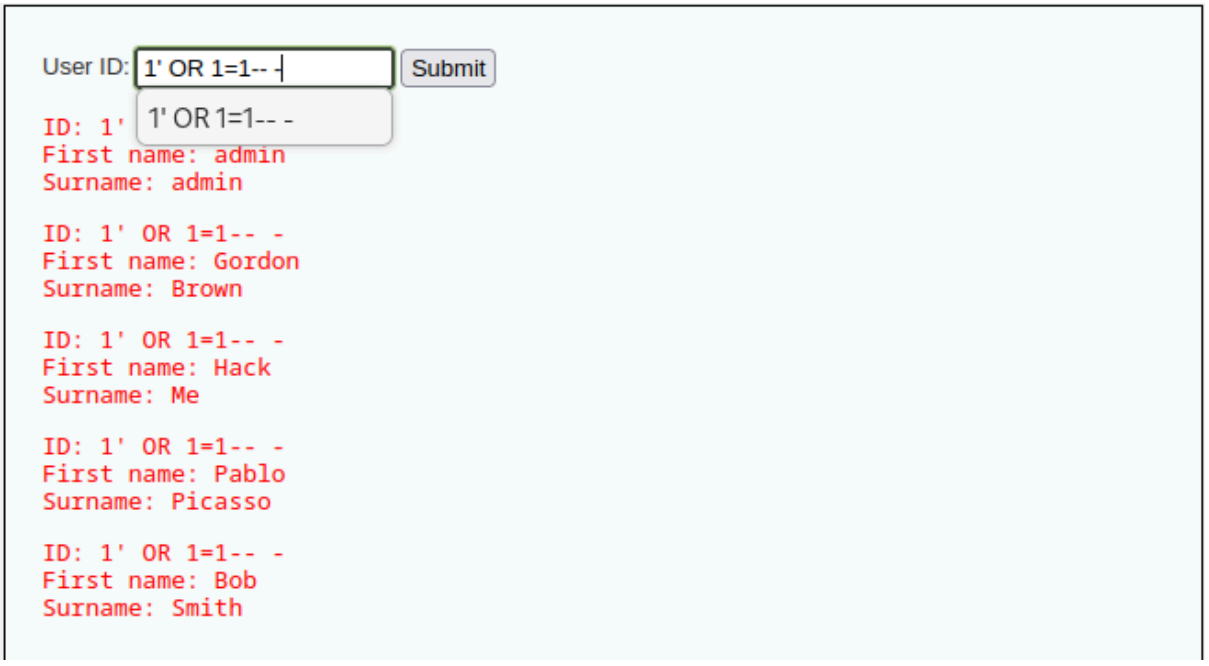
En este reporte podemos ver una inyección SQL la cuál vulnera nuestra Damn Vulnerable Web Application (DVWA).

Descripción del incidente:

En la sesión de seguridad rutinaria, hemos hallado una vulnerabilidad en la web DVWA, el cual es una inyección SQL que compromete a los nombres y apellidos de nuestros usuarios.

Método usado en la inyección SQL:

La inyección de SQL es la siguiente:



Esta inyección nos devuelve todos los usuarios conectados a nuestra red e incluso sus apellidos, pudiendo así saber las credenciales de nuestros clientes y sin tener permisos para obtener esta información tan confidencial.

Recomendaciones:

1. **Validación por lista blanca:** Reducir los permisos (privilegios mínimos) y aceptar solo formatos aceptados.
2. **Habilitar alertas:** Para continuas peticiones que se soliciten en un periodo de tiempo.
3. **Ocultar mensajes de error:** Ocultar los mensajes detallados que no sean solicitados por el propio usuario.
4. **Usar consultas parametrizadas:** Usar parámetros o otro tipo de consultas que no tengan libertad para escribir tantos caracteres.

Conclusión:

La identificación de esta inyección SQL en el DVWA es importante para controlar el acceso y no exponer nuestros datos a otro usuario sin privilegios.

Implementando las recomendaciones, debería de poder arreglar el control de esta inyección.