Informe de Gestión de Incidentes según ISO 27001 – Vulnerabilidad de Inyección SQL

Introducción

Este informe documenta la identificación y explotación exitosa de una vulnerabilidad de inyección SQL en la aplicación web Damn Vulnerable Web Application (DVWA). La prueba se realizó en un entorno virtual controlado utilizando una máquina virtual Debian en VirtualBox. Este ejercicio demuestra una vulnerabilidad crítica en aplicaciones web y resalta la importancia de aplicar buenas prácticas de seguridad en el desarrollo de software.

Descripción del Incidente

Durante la evaluación del módulo de "SQL Injection" de DVWA (con el nivel de seguridad configurado en "low"), se descubrió una vulnerabilidad de inyección SQL en el campo de entrada del ID de usuario. Esta vulnerabilidad permite a un atacante manipular la consulta SQL ejecutada por la aplicación web y obtener información no autorizada de la base de datos.

Método de Inyección SQL Utilizado

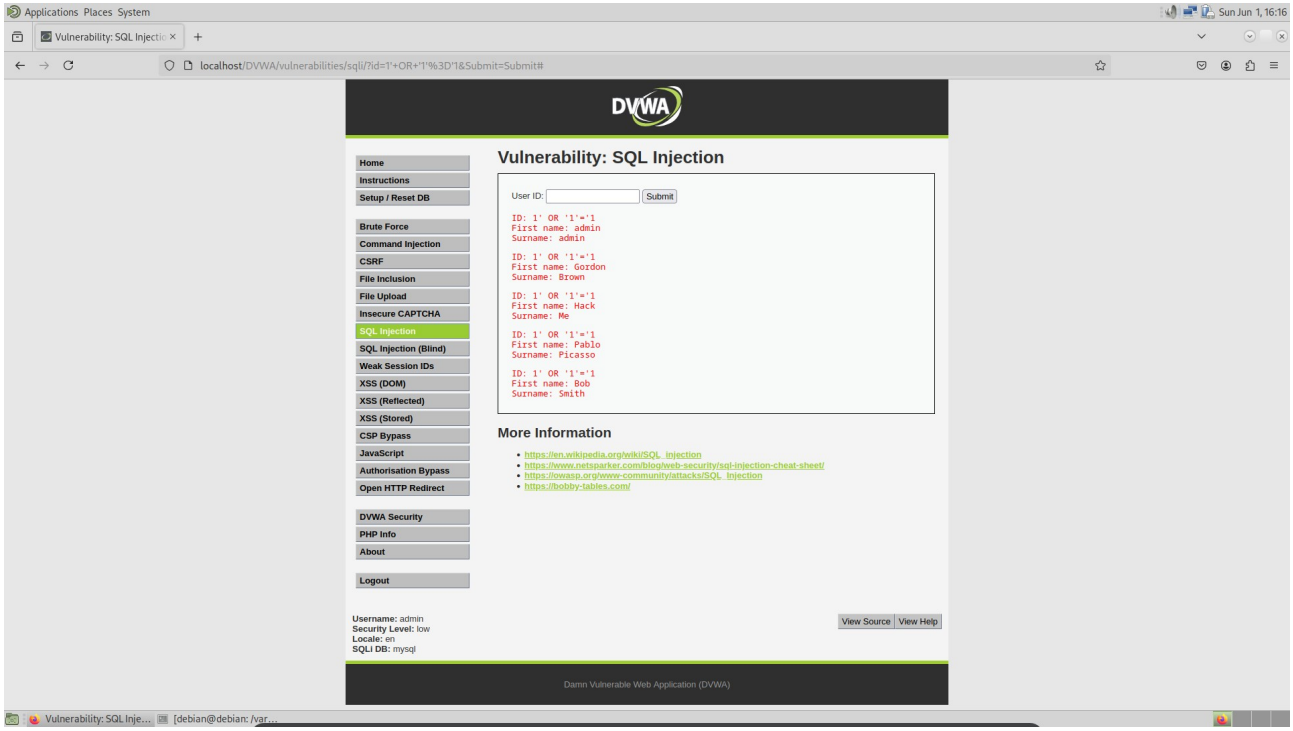
El payload utilizado para explotar la vulnerabilidad fue:

1' OR '1'='1

Al ser enviado a través del campo de ID de usuario, la consulta se modifica para que siempre sea verdadera, lo que provoca que la aplicación devuelva todos los registros de usuarios en lugar de uno solo.

Resultados Observados

Tras ejecutar correctamente el payload, la aplicación respondió con los siguientes registros:



Esto confirma que la aplicación es vulnerable y expone datos de todos los usuarios sin autorización adecuada.

Impacto del Incidente

La explotación de esta vulnerabilidad puede provocar:

Exposición de Datos: Un atacante puede acceder a nombres de usuario, contraseñas y otros datos sensibles.

Riesgos para la Integridad: Actores maliciosos podrían modificar o eliminar registros de la base de datos.

Violación de la Confidencialidad: Los datos de los usuarios son divulgados sin autorización.

Esto compromete los tres pilares fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad (CIA).

Recomendaciones

Para prevenir esta vulnerabilidad y mitigar futuros riesgos, se recomiendan las siguientes acciones:

Validación de Entradas: Utilizar sentencias preparadas o consultas parametrizadas para sanear la entrada de datos del usuario.

Fortalecimiento de Seguridad: Elevar el nivel de seguridad de DVWA y aplicar el principio de mínimo privilegio al usuario de la base de datos.

Pruebas de Penetración: Realizar pruebas periódicas de seguridad utilizando herramientas automatizadas y análisis manual.

Capacitación del Personal: Formar a los desarrolladores en prácticas de codificación segura y en las vulnerabilidades más comunes según OWASP Top 10.

Conclusión

La explotación exitosa de la vulnerabilidad de inyección SQL en DVWA demuestra los riesgos que implica una gestión inadecuada de entradas del usuario. Cumplir con la norma ISO 27001 e implementar controles de seguridad robustos es fundamental para proteger la información sensible y garantizar la continuidad del negocio.