REPORTE DE INCIDENTE DE SEGURIDAD (ISO 27001) – VULNERABILIDAD DE INYECCIÓN SQL

Introducción:

Este reporte describe el hallazgo de una vulnerabilidad técnica identificada durante una prueba de seguridad en la aplicación **DVWA** en nuestro servidor Debian. El fallo permite la manipulación de consultas a la base de datos a través de campos de entrada no saneados correctamente, lo que compromete totalmente la integridad y la confidencialidad de la información en esa base de datos, mediante una inyección SQL sencilla.

Descripción del Incidente:

Se detectó que en el formulario "User ID" en la pestaña SQL INJECCTION no se está validando correctamente la entrada del usuario antes de procesarla en la base de datos de MariaDB. Esto hace que cualquier atacante pueda insertar comandos SQL para obtener e incluso modificar la información que se encuentra en las tablas, ya que el servidor los ejecuta como si fueran comandos legítimos.

Proceso de Reproducción:

Para reproducir esta vulnerabilidad, se llevan a cabo los siguientes pasos:

1. Se ingresa en la aplicación de DVWA.
2. Se navega al módulo "SQL INJECCTION"
3. Se ingresa el Payload siguiente < ' OR '1'='1 >
4. **Resultado:** La aplicación devolvió la lista completa de usuarios y datos de la base de datos en lugar de un solo usuario ya que se modifica la consulta original mediante el uso del payload.

Impacto del Incidente:

Explotar esta vulnerabilidad le permitirá al atacante afectar los tres puntos de la triada de la ciberseguridad.

- **Confidencialidad**: Crítico. Acceso no autorizado a toda la base de datos de usuarios, lo que divulga toda la información.
- **Integridad**: Alto. Posibilidad de modificar o eliminar registros de la base de datos, más aún cuando la consulta se está ejecutando con un usuario root.
- **Disponibilidad**: Medio. Riesgo de denegación de servicio mediante consultas más pesadas o consultas que indispongan la Base de datos.

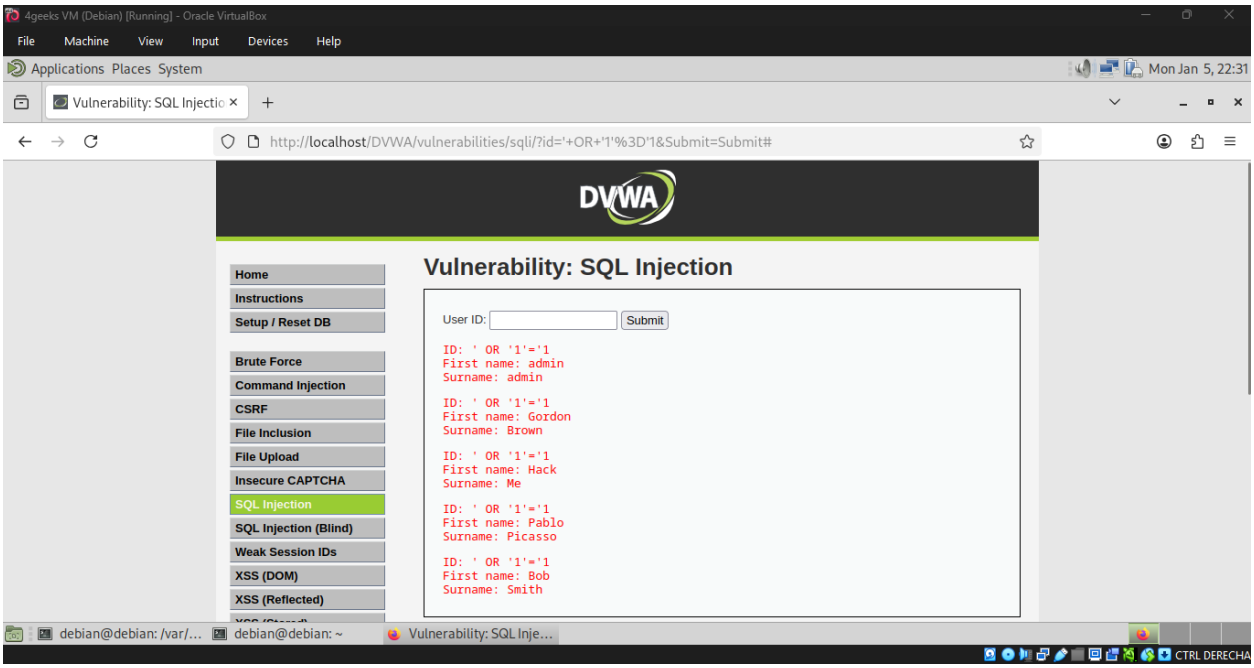
Recomendaciones:

1. **Uso de sentencias preparadas:** Implementar consultas parametrizadas que separen el código SQL del input del usuario, con esto se asegura que los datos que se introduzcan en el form sean tratados como texto únicamente, no como código.
2. **Validación de Entradas:** Aplicar una lista blanca y validación para que el campo ID solo acepte números (propios de un ID en este caso).
3. **Principio del menor privilegio:** Asegurarse que el usuario que se utilice para esta consulta tenga permisos limitados y los mínimos necesarios para su funcionamiento.
4. **Pruebas de penetración:** Llevar a cabo auditorias de seguridad de forma regular, que incluyan pruebas de penetración para identificar y mitigar vulnerabilidades antes de que puedan ser explotadas por un atacante.
5. **Educación y concientización:** Enseñar a los miembros técnicos y no técnicos del equipo acerca de las buenas prácticas de seguridad para el desarrollo de aplicaciones y para crear conciencia acerca de los riesgos asociados a las vulnerabilidades de ciberseguridad.

Conclusión:

Esta vulnerabilidad significa un riesgo crítico para la organización. Es imperativo que se asegure la base de datos y se solucione este posible acceso no autorizado, proteger los datos y cumplir con los estándares de seguridad de la información. Este hallazgo, también resalta la importancia de tener en cuenta la ciberseguridad y las buenas prácticas durante el desarrollo y mantenimiento de las aplicaciones. Es indispensable implementar controles robustos de ciberseguridad para resguardar los recursos de datos críticos y asegurar la continuidad de las operaciones.

Evidencia:


4geeks VM (Debian) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Applications Places System
Mon Jan 5, 22:31
Vulnerability: SQL Injectio
http://localhost/DVWA/vulnerabilities/sqli/?id='+OR+'1'%3D'1&Submit=Submit#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
Vulnerability: SQL Injection
User ID:
Submit
ID: ' OR '1'='1
First name: admin
Surname: admin
ID: ' OR '1'='1
First name: Gordon
Surname: Brown
ID: ' OR '1'='1
First name: Hack
Surname: Me
ID: ' OR '1'='1
First name: Pablo
Surname: Picasso
ID: ' OR '1'='1
First name: Bob
Surname: Smith
debian@debian: /var/...
debian@debian: ~
Vulnerability: SQL Inje...
CTRL DERECHA