ISO 27001 Compliant Incident Management Report -SQL Injection Vulnerability.

Introducción

En este informe se detalla la identificación y explotación de una vulnerabilidad de inyección SQL usando DVWA (Web Damn Vulnerable Web Application).

Esta prueba se ha llevado a cabo en un entorno controlado (máquina virtual Debian), La evaluación se realiza en base a la ISO 27001, con el objetivo de demostrar una vulnerabilidad común y su impacto potencial en la seguridad de aplicación.

Proceso de Reproducción

Se instaló DVWA en el entorno de prueba, siguiendo la guía de instalación, para analizar una vulnerabilidad de SQL Injection. Esta vulnerabilidad permite a un atacante inyectar consultas SQL maliciosas a través de los campos de entrada de detaps de la aplicación web, comprometido así la integridad y confidencialidad de los datos almacenados en la base de datos, es una vulnerabilidad de gravedad alta.

Se configuró el nivel de seguridad como bajo "low".

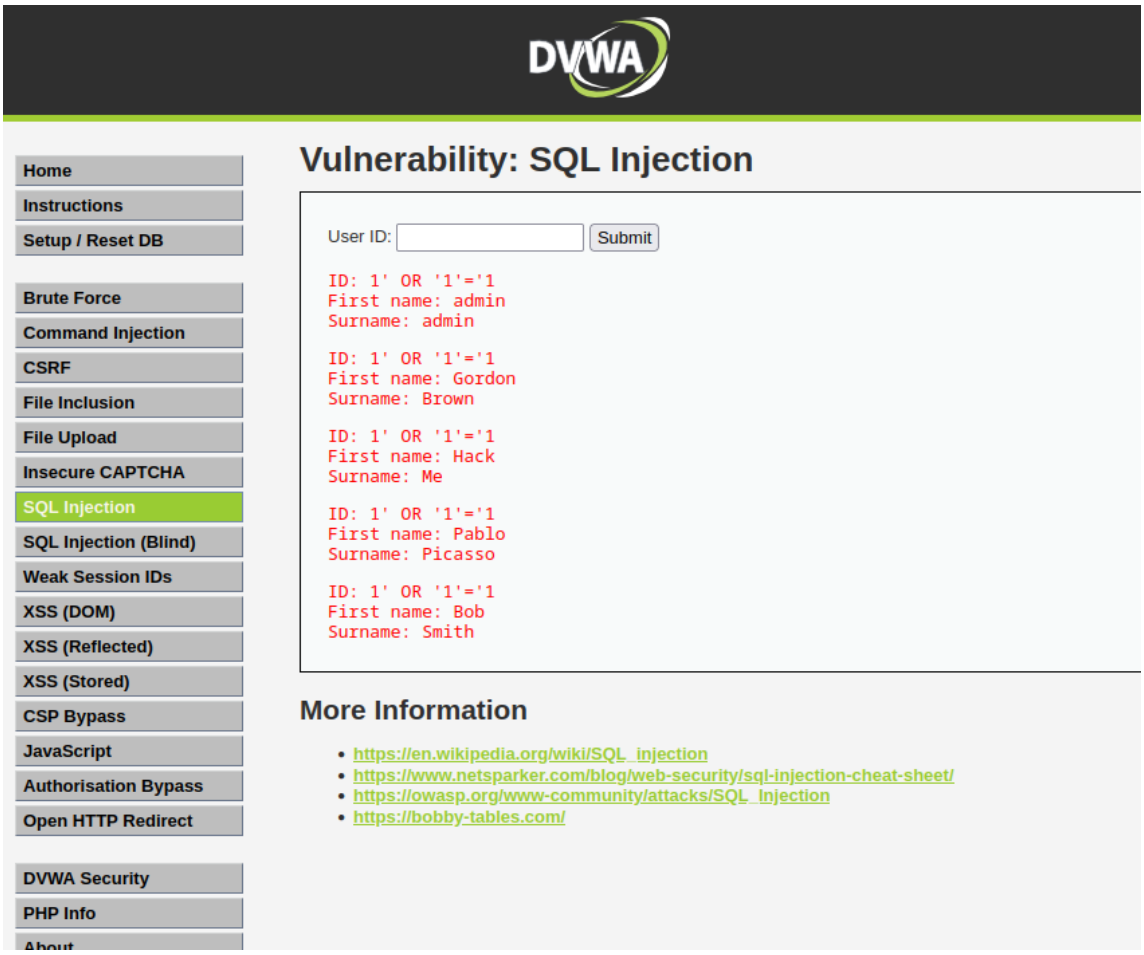
Método de inyección SQL utilizado

El modulo de autenticación de usuarios permite ejecución de consultas SQL maliciosas.

Para replicar y demostrar la vulnerabilidad, se utilizo el siguiente payload SQL en el campo de user ID:

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

Al pulsar "Submit" la aplicación respondió con una lista de usuarios que se encuentra dentro de la base de datos, lo que nos confirma que la inyección SQL ha funcionado y que se ha producido un acceso no autorizado a información confidencial.



Impacto del Incidente

La explotación de esta vulnerabilidad permite a un atacante:

- Acceder y extraer información confidencial de la base de datos, en este caso credenciales de usuarios.
- Al tener estos datos, podríamos modificar, eliminar o comprometer datos sensibles almacenados en la aplicación.

Esto representa un riesgo significativo para la confidencialidad, integridad y disponibilidad de los datos y servicios proporcionados por DVWA.

Las consecuencias podrían incluir:

- **Confidencialidad**: Compromiso de datos personales y confidenciales almacenados en la base de datos. Se han expuesto nombres y apellidos.
- **Integridad**: Manipulación de información crítica, permitiendo la modificación o eliminación de datos.
- **Disponibilidad**: se podría utilizar la información para afectar a la disponibilidad del servicio.

La explotación de la inyección SQL revela una falta de controles lo que representa un riesgo de seguridad alto.

Recomendaciones

En base a la ISO 27001, se recomiendan los suguientes controles para mitigar el riesgo de un ataque SQL inyection:

1. Validación de Entradas: Implementar estrictas validaciones de entrada para todos los datos recibidos de los usuarios, utilizando parámetros seguros en las consultas SQL para prevenir inyecciones SQL, uso de comandos maliciosos o caracteres especiales.
2. Controles de acceso: limitar los usuarios con privilegios de acceso a datos sensibles. Restringir el acceso a la base de datos exclusivamente a usuarios con credenciales y permisos.
3. Pruebas de penetración: Realizar auditorías regulares de seguridad, incluyendo pruebas de penetración, para identificar y mitigar vulnerabilidades de seguridad antes de que sean explotadas por atancantes.
4. Realizar evaluaciones periodicas, de manera que podamos realizar un monitoreo continuo, pudiendo detectar cambios o intrusiones.
5. Actualizaciones periódicas: que mantengan el sistema seguro.
6. Protocolos y políticas de seguridad: Su implementación proporcionará un marco de actuación y organización que permitirá realizar todas las tareas anteriores.
7. Educación y Concienciación: Capacitar al personal técnico y no tencnico en prácticas seguras de desarrollo de aplicaciones y concienciar sobre los riesgos asociados con las vulenrabilidades de seguridad.

Conclusión

La identificación y explotacion exitosa de la vulnerabilidad de inyección SQL en DVWA demuestra la importancia de implementar controles de seguridad.
La vulnerabilidad SQL inyection es una de las más comunes y de mayor riesgo para la seguridad de las aplicaciones web.

Las medidas recomendadas permiten adoptar controles y prácticas que mejoraran la seguridad y reducirán la probabilidad de que estos ataques tengan éxito, y por lo tanto de que comprometan los datos e información almacenada.