Informe de Gestión de Incidentes conforme a la norma ISO 27001 - Vulnerabilidad de Inyección SQL

Introducción

Este informe detalla la identificación y explotación de una vulnerabilidad de inyección SQL en la aplicación web DVWA. La prueba se realizó en un entorno controlado para demostrar una vulnerabilidad común y su posible impacto en la seguridad de la aplicación.

Descripción del incidente

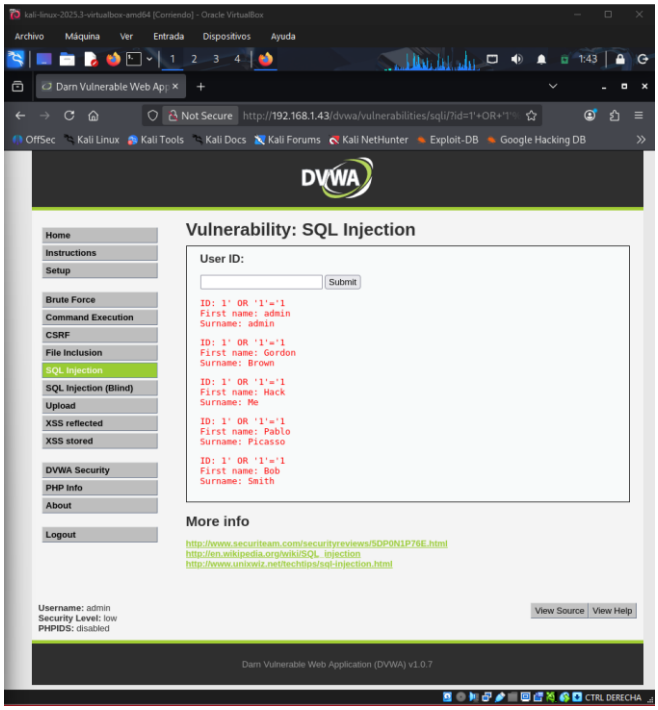
Durante la evaluación de seguridad, se descubrió una vulnerabilidad de inyección SQL en el módulo "Inyección SQL". Esta vulnerabilidad permite a un atacante inyectar consultas SQL maliciosas a través de los campos de entrada de la aplicación web, comprometiendo así la integridad y confidencialidad de los datos almacenados en la base de datos.

Método de inyección SQL utilizado

Para replicar y demostrar la vulnerabilidad, se utilizó la siguiente carga útil SQL en el campo "ID de usuario":

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

Esta carga útil aprovecha la vulnerabilidad para modificar la consulta SQL original de forma que devuelva los nombres de usuario y las contraseñas almacenados en la tabla users. Al ejecutar correctamente esta inyección SQL se obtienen las credenciales de los usuarios de la tabla.



Impacto del incidente

La explotación de esta vulnerabilidad podría permitir a un atacante:

- Acceder y extraer información confidencial de la base de datos, incluidas las credenciales de usuario.
- Modificar, eliminar o comprometer datos confidenciales almacenados en la aplicación.

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

Recomendaciones

Con base en los hallazgos de esta evaluación de seguridad, se recomiendan las siguientes medidas correctivas y preventivas:

1. Implementar validaciones de entrada estrictas para todos los datos proporcionados por el usuario, utilizando parámetros seguros en las consultas SQL para evitar la inyección de SQL.
2. Realizar auditorías de seguridad periódicas, incluyendo pruebas de penetración, para identificar y mitigar las vulnerabilidades de seguridad antes de que sean explotadas por atacantes.
3. Capacitar al personal técnico y no técnico en prácticas seguras de desarrollo de aplicaciones y concientizar sobre los riesgos asociados a las vulnerabilidades de seguridad.
4. Cifrar las credenciales de los usuarios en la base de datos, con el objetivo de que si en algún momento se ve expuesta, no sea posible para los usuarios conocer las mismas.

Conclusiones

La identificación y explotación exitosa de la vulnerabilidad de inyección de SQL en DVWA subraya la importancia de la seguridad proactiva en el desarrollo y mantenimiento de aplicaciones web.

Implementar controles de seguridad robustos y seguir las mejores prácticas de ciberseguridad es esencial para proteger los activos críticos y garantizar la continuidad del negocio.