Informe de gestión de incidente de seguridad – Explotación de vulnerabilidad de Inyección SQL en DVWA (entorno controlado)

Este informe recoge la identificación, explotación en entorno controlado y análisis de una vulnerabilidad de inyección SQL en la aplicación web Damn Vulnerable Web Application (DVWA).

INTRODUCCIÓN

Durante la evaluación de seguridad de la aplicación DVWA se detectó una vulnerabilidad de tipo inyección SQL en el módulo “SQL Injection”.

Se trata de una vulnerabilidad crítica, ya que permite modificar el comportamiento de las consultas que se envían a la base de datos a través de los datos introducidos por el usuario. Esto ocurre porque no existe una validación adecuada de la información que se introduce en los campos del formulario.

Como consecuencia, un usuario podría acceder a información que no debería estar disponible, como credenciales almacenadas en la base de datos, e incluso llegar a modificar o eliminar registros.

En este caso, el problema se debe a que la aplicación construye la consulta SQL utilizando directamente el valor que introduce el usuario, en lugar de aplicar mecanismos de protección que separen los datos del código.

DESCRIPCIÓN DEL INCIDENTE

Durante la prueba realizada en el módulo “SQL Injection” se comprobó que el campo “User ID” acepta valores manipulados sin aplicar ningún tipo de control.

Al introducir una cadena alterada en dicho campo, la aplicación ejecutó la consulta modificada sin impedir que esa entrada cambiara la lógica del sistema. Esto permitió alterar el funcionamiento normal de la consulta y obtener resultados no previstos.

Este comportamiento demuestra que el sistema no cuenta con medidas adecuadas para evitar que el usuario pueda influir directamente en la consulta que se envía a la base de datos.

PROCESO DE REPRODUCCIÓN

El nivel de seguridad configurado en DVWA para esta prueba fue “low”.
La práctica se realizó en un entorno virtualizado con fines formativos.

Para comprobar la vulnerabilidad, se introdujo en el campo “User ID” la siguiente cadena:

1' OR '1'='1

Tras enviar el formulario, la aplicación mostró varios usuarios en lugar de uno solo. Esto ocurrió porque la condición introducida hizo que la consulta devolviera todos los registros disponibles.

El resultado obtenido confirmó que la aplicación permite modificar la lógica de la consulta mediante valores introducidos por el usuario, lo que evidencia la existencia de la vulnerabilidad.

IMPACTO DEL INCIDENTE

En un entorno real, el impacto de esta vulnerabilidad podría ser muy grave.

Desde el punto de vista técnico, permitiría acceder a información sensible sin autorización, así como modificar o eliminar datos almacenados en la base de datos.

En términos de seguridad de la información, afecta directamente a la confidencialidad y a la integridad, y podría llegar a afectar también a la disponibilidad si se realizaran acciones que interrumpieran el funcionamiento del sistema.

Además, en un contexto organizativo real, una vulnerabilidad de este tipo podría suponer incumplimientos normativos, como el RGPD si se tratara de datos personales, así como sanciones económicas y pérdida de confianza por parte de los usuarios.

También demuestra la necesidad de mejorar los controles de seguridad dentro del Sistema de Gestión de Seguridad de la Información (SGSI).

RECOMENDACIONES

Para evitar que este tipo de vulnerabilidades puedan producirse en un entorno real, se proponen las siguientes medidas:

En primer lugar, es necesario cambiar la forma en que la aplicación realiza las consultas a la base de datos. Los datos introducidos por el usuario no deberían formar parte directa de la consulta, sino gestionarse mediante mecanismos que impidan que puedan alterar su funcionamiento.

También es importante validar correctamente la información que se introduce en los formularios, comprobando que el tipo de dato y el formato sean los adecuados.

Se recomienda igualmente limitar los permisos de acceso a la base de datos, de forma que la cuenta utilizada por la aplicación solo tenga los permisos estrictamente necesarios.

Además, la aplicación no debería mostrar mensajes de error que puedan dar información interna sobre el sistema.

Desde el punto de vista organizativo, dentro del marco del SGSI, se recomienda:

- Incluir criterios de seguridad en el desarrollo de las aplicaciones.
- Realizar pruebas y revisiones de seguridad de forma periódica.
- Tener en cuenta este tipo de riesgos dentro del análisis de riesgos.
- Proporcionar formación básica en seguridad al personal técnico.

La aplicación de estas medidas ayudará a reducir el riesgo y mejorar la seguridad general del sistema.

CONCLUSIÓN

La vulnerabilidad de inyección SQL identificada en DVWA demuestra cómo una falta de validación adecuada de los datos introducidos por el usuario puede comprometer seriamente la seguridad de una aplicación web.

Aunque la prueba se ha realizado en un entorno controlado con fines formativos, en un entorno real podría permitir el acceso no autorizado a información sensible, la modificación de datos e incluso la interrupción del servicio.

Este incidente pone de manifiesto la importancia de integrar la seguridad desde el desarrollo de las aplicaciones y de mantener controles adecuados dentro del Sistema de Gestión de Seguridad de la Información.

En definitiva, detectar y corregir este tipo de vulnerabilidades es fundamental para garantizar la protección de la información y la seguridad del sistema.