Practica de Incidencias de SQL Injection Vulnerability

Introducción

Informe de la detección de una vulnerabilidad conocido como Inyección SQL, en las pruebas que se ha realizado con la aplicación Web DVWA en la versión de agosto 2020.

Dicha prueba se ha realizado sobre una maquina virtual Debian versión 12.

Descripción del Incidente.

Durante el desarrollo de la práctica se detectó una vulnerabilidad de inyección SQL, a través de la cual el atacante puede consultar y extraer información de la base de datos, fuera el ámbito y la privacidad para la que ha sido concebida la aplicación, también es posible manipular la información de la misma.

Proceso Reproducción

La prueba se realizó sobre una parte de la aplicación donde existe un formulario de consulta en el cual se pide a través de un campo numérico que representa el identificado del usuario devuelve los datos guardados de ese usuario.

Si en el campo ponemos ‘ cerramos la posible sentencia que va a ser lanzada para encontrar el usuario a través de su identificador, Esta al ser interpretada, se está abriendo la posibilidad de poder lanzar sentencias o condiciones que nos devuelvan más información.

En este caso si ponemos **‘ or ‘1’=’1**, en este caso cerramos la instrucción y añadimos una condición que siempre va a ser true, enlazada por el operador lógico OR.

En este caso la vulnerabilidad radica que la aplicación interpreta el código por lo que se une a la sentencia original, devolviendo un listado de todos los usuarios con todos sus datos.

Impacto del Incidente

Esta vulnerabilidad otorga al usuario que sea capaz de explotarla:

- Acceso a la información confidencial alojada en las tablas implicadas.
- Posibilidad de insertar o modificar datos de dichas tablas.

Recomendaciones

- Satinizar los campos antes de ejecutarlos, sobre todo los campos que interactúen son el usuario
- Generar pruebas antes de ponerlo en producción e introducir datos reales.
- Establecer con el equipo de desarrollo, las pautas y estructuras contempladas en el desarrollo seguro.

Conclusiones.

Realizar pruebas sobre las aplicaciones, utilizando las herramientas disponibles como DVWA, es sumamente importante para mantener una actitud proactiva que garantice dentro de lo posible desarrollos y herramientas empresariales completas y seguras