ISO 27001 Informe de gestión de incidentes conforme - Vulnerabilidad SQL Injection

INTRODUCCIÓN

En este informe vamos a explicar la vulnerabilidad de inyección SQL, encontrada con DVWA.
La prueba que se muestra a continuación se lleva a cabo en un entorno controlado con el objetivo de demostrar esta vilnerabilidad, como se lleva a cabo y sus consecuencias.

DESCRIPCIÓN DEL INCIDENTE

A partir de la auditoría realizada con DVWA, se descubre una vulnerabilidad de inyección SQL con el módulo SQL inyecction.

Estas vulnerabilidades, permiten a un atacante lanzar consultas SQL a través de los campos de entrada (Usuario, contraseña, búsqueda…) Comprometiendo la confidencialidad e integridad de los datos almacenados en la BD.

Método de Inyección utilizado

Para replicar la vulnerabilidad se utilizó la siguiente consulta en el campo “User ID”:

sql:

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

Esta Modificación en la consulta, nos permite cargarla como parte de la misma si el campo está concatenado

Ej: SELECT * FROM usuarios WHERE usuario='$usuario' AND password='$password';

Se convierte en

SELECT * FROM usuarios WHERE usuario=’ OR ‘1’=’1' AND password=' OR '1'='1';

Esta consulta nos arrojará todos los datos de la tabla, aprovechándose de la vulnerabilidad de modificar consultas en sql de forma que nos devuelva los datos del cliente almacenados en la tabla (Nombre y Apellido), pero podría ser también utilizada para obtener contraseñas, o cualquier otro dato almacenado con un campo de entrada que le haga referencia.

Esto se debe a que la consulta pasa de ser un campo / valor que coincida (==) a ser una condición verdadea (1 es igual a 1, por lo que es TRUE), lo que nos arrojará todos los resultados.

Impacto del incidente

Al tener este fallo en nuestro sitio, abrimos la puerta a que un atacante con conocimientos mínimos pueda:

- Obtener información sensible como Nombres y contraseñas
- Modificar o comprometer la integridad de la BBDD
- Obtener datos de consultas de otros usuarios

Esto representa una gran amenaza para los tres pilares fundamentales de la seguridad, y es un error fácilmente explotable, y que puede tener mas impactos que no contemplamos directamente.

Recomendaciones

Tras analizar los resultados de la auditoria, recomendamos que se apliquen las siguientes medidas:

- Escaneo de entradas;
  - Implementar validaciones estrictas para todos los datos dados por el usuarios
- Parametrizar las Consultas a la BD
  - Una forma de cubrir la base de datos de este tipo de ataques es parametrizando todas las consultas, lo que nos asegura que el usuario no puede inyectar consultas
    - Ejemplo: mysql_real_escape_string https://www.php.net/manual/en/function.mysql-real-escape-string.php
- Educación y concienciación: Capacitar a todo el personal en practicas seguras sobre desarrollo y los riegos de las malas practicas.
  - Educar al personal técnico en técnicas de desarrollo seguro y buenas practicas.

Conclusiones

La explotación de esta vulnerabilidad, incluso en dvwa, nos muestra lo importante que es seguir buenas practicas en la creación y mantenimiento de aplicaciones web, así como el alcance que puede tener no seguirlas.
Establecer Controles de seguridad y límites a lo que un usuario puede llegar a hacer es fundamental, así como seguir las practicas de seguridad que se mencionan en las recomendaciones para que la empresa pueda seguir funcionando sin perder dinero, tiempo o reputación.