

Reporte de incidencia de seguridad de acuerdo con la norma ISO 27001

Introducción

en este documento se aborda los detalles sobre la falla de seguridad en correlación de un SQL inyection, está presente falla afecto la integridad y la confidencialidad de la plataforma Danm Vulnerable Web Application (DVWA).

Descripción del incidente

Durante las pruebas de efectuadas, revelo una falla de seguridad de tipo SQL inyection. Esta falla da cabida para recibir ataques maliciosos que pueden dejar expuesta información de sensible, tanto de la plataforma como los usuarios en sí.

Identificación de la vulnerabilidad

La vulnerabilidad se está asociada directamente con la estructura del código, donde la variable de consulta de datos corre expedita.

De esta línea de código se genera el problema

```
SELECT first_name, last_name FROM users WHERE user_id = '$id';
```

El valor de **\$id** se inserta directamente en SQL sin validación

Impacto del incidente

Acceso y extracción de información confidencial, evadiendo lo que conforma el protocolo de CIA.

Recomendaciones

Validación de entradas: estructurar la captación de datos con el fin de ofrecer rigidez

Pruebas periódicas de penetración: programar auditorias para comprobar y actualizar los pasos de seguridad

