

# INCIDENTE SQL INJECTION

## Introduccion

Se encontró una vulnerabilidad en sql injection y se consiguió explotar en la web con DVWA

## Descripción de incidente

En la web fue encontrada una vulnerabilidad en el apartado de sql injection, la vulnerabilidad de permite al atacante inyectar código malicioso en la web que le permite tener acceso a la base de datos poniendo en compromiso la integridad y la confidencialidad de los datos

## Metodo usado para SQL injection

Para demostrar la vulnerabilidad solo hay que replicar el metodo usado.

En el user ID se escribió: 1' OR '1'='1

Al utilizar este método la pagina devolvió las credenciales almacenadas en la base de datos

## Impacto del incidente

Esta vulnerabilidad le permitió al atacante acceder a la información confidencial de la base de datos pudiendo así logearse con las credenciales que no son suyas poniendo así en riesgo la confidencialidad y la integridad de los datos de las cuentas de otros usuarios

## Recomendaciones

Para solucionar la vulnerabilidad deberían configurar la web para que lo que escriba un usuario externo no se comunique directamente con la base de datos. Aparte se recomendaría hacer auditorias periódicas para descartar posibles vulnerabilidades que vayan surgiendo en la empresa

## Conclusion

Se ha descubierto una vulnerabilidad importante que pone en riesgo la seguridad de la empresa pero que tiene una solución relativamente sencilla y económica