TITULO DEL REPORTE=Inyeccion SQL en DDWA
INTRODUCCION=En el entorno de practica de DVWA se detecto una vulnerabilidad de inyeccion SQL en el modulo”SQL INYECCION”
DESCRIPCION DE INCIDETNE=APLICACION AFECTADAEN “http://localhost/DVWA/. el parametro vulnerado fue:id(campo user ID)CAUSA fuel consulta sin parametrizar que sellara la entrada del usuario
PROCESSO DE REPRODUCCION=INICIAR SERVICIOS=sudo service apache2 start && sudo service mariadb start.2=Abrir http://localhost/DVWA/ y entrar con admin y password 3=ir a vulnerabilidades SQL INYECCION 4=en “User ID “enviar 1´ OR ´1´=´1´ IMPACTO DEL INCIDENTE =exfiltracion de datos de usuarios y bypass de controles;posible modificacion de informacion.Riesgo de alta confidencialidad,medio en integridad,bajo en disponibilidad
RECOMENDACIONES=usar consultas parametrizadas,validar limitar id a numerico,minimos privilegiosen la cuenta de DB y podemos ocultar errores SQL al usuario.