EXPOSICIÓN DE DATOS POR INYECCIÓN SQL EN DVWA

1.INTRODUCCIÓN

en un entorno de práctica de virtualbox se desplegó DVWA sobre debian el objeto fue identificar y demostrar,de forma controlada y educativa,una debilidad de validación de entradas que permite ejecutar inyecciones SQL y acceder a información sin autorizacion El manejo y registro de hallazgo se alinean con buenas practicas de gestión de incidentes

2.DESCRIPCIÓN DEL INCIDENTE

El módulo SQL inyección de DVWA construye consultas concatenando texto ingresado por el usuario. Al no existir validación/parametrización, es posible alterar la lógica de la consulta y recuperar registros de la base de datos la vulnerabilidad quedó evidenciada cuando el sistema devolvió múltiples usuarios tras enviar un valor manipulado en el campus USER ID.

3.PROCESO DE REPRODUCCIÓN

En la misma vm se accede a la interfaz de DVWA desde el navegador e inicia sesión, se crea o restablece la base de datos hasta la confirmación en DVWA security se fija al final del nivel en low. seguidamente se abre el módulo SQL inyección y en el campo user id se introduce una cadena que haga verdadera la condición (1` OR `1`=`1`) y se envía un formulario . como resultado la aplicación devuelve el listado de varios usuarios.

4.IMPACTO DEL INCIDENTE

CONFIDENCIALIDAD-comprometida;es posible leer información de usuarios

INTEGRIDAD existe riesgo de modificación/borrado de datos si el atacante extiende la inyección.

DISPONIBILIDAD-no se afecto en esta prueba peri consultas pesadas/maliciosas podrían degradar el servicio.

SEVERIDAD ESTIMADA-ALTA;exfiltración de datos con payload simple

SUPERFICIE AFECTADA-cualquier punto de la app que forme consultas con entrada sin sanitizar.

5.RECOMENDACIÓN

corrección principal:migrar a consultas preparadas/parametrizadas y validación estricta de entradas(longitud,listas blancas)y escape según el contexto

DEFENSA DE PROFUNDIDAD

revisar credenciales por defecto y fortalecer contraseñas,registro y monitoreo de patrones de inyección,considerar reglas en el WAF para bloquear firmas comunes de SQL
incorporar revisiones de código y pruebas SAST/DAST antes de releases

6.CONCLUSIÓN

La prueba demostró que en el entorno de laboratorio,DVWA permite inyección SQL y exposición de datos por falta de parametrización y validaciones. implementar prepared statements,y validación de entradas y principio de menor privilegio reduce drásticamente el riesgo.con estas medidas y monitoreo continuo, incidentes similares pueden prevenirse en entornos productivos.