Informe completo sobre ataques de inyección SQL
La inyección SQL es una técnica de inyección de código utilizada para atacar aplicaciones basadas en d
declaraciones SQL maliciosas en campos de entrada, eludiendo las medidas de seguridad.
Tipos de ataques de inyección SQL:
La escala de gravedad va del 1 al 5
1 es el más bajo, 5 es el más alto
1. Inyección SQL en banda: el tipo más común donde los atacantes usan lo mismo
canales de comunicación para lanzar ataques y recaudar ingresos.
Gravedad: 3
2. Inyección de SQL basada en errores: aprovecha los mensajes de error generados desde la base de d
recopilar información.
Gravedad: 4
3. Inyección SQL ciega: Implica enviar consultas SQL a la base de datos, especificando
Validez de la consulta basada en la respuesta de la aplicación.
Gravedad: 5
4. Inyección de SQL basada en unión: manipule el resultado del operador UNION SQL para recopilar
información de la base de datos.
Gravedad: 2
Prevención:
Utilice consultas parametrizadas o declaraciones preparadas.
Validar y desinfectar la entrada del usuario.
Utilice el principio de privilegio mínimo en las cuentas de bases de datos.
Actualice y aplique parches a su software con regularidad.
Implementar la validación de entradas tanto en el lado del cliente como en el del servidor.
Utilice un firewall de aplicaciones web (WAF) para filtrar y monitorear el tráfico entrante.
Utilice procedimientos almacenados o un marco ORM.
Implemente un manejo adecuado de errores para evitar la exposición de información confidencial.
Utilice marcos y prácticas de codificación centrados en la seguridad.
Realice auditorías de seguridad y pruebas de penetración con regularidad.