Vulnerabilidad de SQL Injection: Ejemplo de ataque utilizando la cadena `1' OR '1'='1`

En este reporte, se analizará una vulnerabilidad de inyección SQL (SQL Injection) encontrada en una aplicación que permite la manipulación no autorizada de consultas SQL. Se investigará cómo el uso de la cadena maliciosa `1' OR '1'='1` afecta la seguridad de la base de datos y la integridad del sistema, permitiendo potenciales ataques que comprometen la confidencialidad, integridad y disponibilidad de los datos.

Descripción del Incidente:
Se detectó una vulnerabilidad de SQL Injection en una aplicación web que permite al atacante modificar las consultas SQL enviadas al servidor de bases de datos. El incidente se identifica cuando, al introducir la cadena `1' OR '1'='1` en un campo de entrada de la aplicación, la consulta SQL se altera de tal manera que devuelve todos los registros de la base de datos, en lugar de los que cumplen con un criterio específico.

Este tipo de ataque aprovecha la falta de sanitización adecuada de los datos de entrada en la aplicación y puede llevar a la exposición de datos confidenciales, ejecución de operaciones no autorizadas y potencial control total sobre la base de datos.

Proceso de Reproducción:

1. Acceder a la aplicación web afectada e identificar un formulario vulnerable (por ejemplo, un formulario de inicio de sesión).

   En el campo de nombre de usuario o contraseña, introducir la siguiente cadena maliciosa:
   bash

   Copiar código
   ```
   1' OR '1'='1
   ```

2.

   Al enviar el formulario, el servidor construye la siguiente consulta SQL (suponiendo que la consulta original sea similar a):
   sql

Copiar código

```
SELECT * FROM usuarios WHERE usuario = '1' OR '1'='1' AND
contraseña = '...'
```

3. Dado que la condición `OR '1'='1'` siempre es verdadera, la consulta devuelve todos los registros de la tabla `usuarios`, permitiendo el acceso no autorizado al sistema.

Impacto del Incidente:
El impacto de esta vulnerabilidad es alto, ya que puede llevar a las siguientes consecuencias:

- **Acceso no autorizado a datos sensibles:** Un atacante puede obtener información confidencial como nombres de usuario, contraseñas (en texto claro si no están cifradas), correos electrónicos y otros datos críticos.
- **Compromiso total del sistema:** Dependiendo de los permisos del usuario de la base de datos, el atacante podría realizar modificaciones, eliminar registros o incluso tomar control completo del servidor.
- **Daño reputacional y financiero:** La exposición de información confidencial puede derivar en violaciones legales, pérdida de confianza de los clientes y sanciones regulatorias.

Conclusión:

La vulnerabilidad de SQL Injection detectada mediante la cadena `1' OR '1'='1` es un riesgo serio para la seguridad de las aplicaciones web. Los desarrolladores deben asegurarse de implementar las prácticas de programación segura mencionadas anteriormente, además de realizar auditorías regulares de seguridad. La protección contra este tipo de ataques es crucial para mantener la integridad y confidencialidad de los datos en aplicaciones y sistemas empresariales.