Comprehensive Report on SQL Injection Attacks

SQL injection is a code injection technique used to attack data-driven applications by inserting malicious SQL statements into input fields, bypassing security measures.

Types of SQL Injection Attacks:

Severity Scale Ranges from 1 to 5

1 being the lowest, 5 being the most highest

1. **In-band SQL Injection: The most common type where the attacker uses the same communication channel to launch the attack and gather results.**
   Severity: 3
2. **Error-based SQL Injection: Exploits error messages generated from the database to gather information.**
   Severity: 4
3. **Blind SQL Injection: Involves sending SQL queries to the database, determining the validity of the query based on the application's response.**
   Severity: 5
4. **Union-based SQL Injection: Manipulates the result of a UNION SQL operator to gather information from the database.**
   Severity: 2

Prevention:

- **Use parameterized queries or prepared statements.**
- **Validate and sanitize user inputs.**
- **Apply least privilege principles to database accounts.**
- **Regularly update and patch your software.**
- **Implement input validation on both client and server sides.**
- **Use web application firewalls (WAFs) to filter and monitor incoming traffic.**
- **Employ stored procedures or ORM frameworks.**
- **Implement proper error handling to avoid exposing sensitive information.**
- **Use security-focused coding practices and frameworks.**
- **Perform security audits and penetration testing regularly.**