A comprehensive report on SQL injection attacks
SQL injection is a code injection technique used to attack SQL-based applications
Malicious SQL statements in input fields, bypassing security measures.
Types of SQL injection attacks:
The severity scale ranges from 1 to 5
1 is the lowest, 5 is the highest
1. In-Domain SQL Injection: The most common type where attackers use the same
Communication channels for launching attacks and collecting revenue.
Intensity: 3
2. Error-based SQL injection: exploits error messages generated from the database to
Data collection.
Intensity: 4
3. Blind SQL Injection: It involves sending and specifying SQL queries to the database
Query validity based on application response.
Intensity: 5
4. Union-based SQL injection: Process the result of the UNION SQL operator to aggregate it
Information from the database.
Intensity: 2
protection:
Use queries with parameters or prepared data.
Validate and sanitize user input.
Use the principle of least privilege in database calculations.
Update and patch your software regularly.
Perform input validation on both the client and server.
Use a Web Application Firewall (WAF) to filter and monitor incoming traffic.
Use stored procedures or ORM framework.
Implement appropriate error handling to prevent disclosure of sensitive information.
Use security-focused coding practices and frameworks.
Conduct security audits and penetration tests regularly.