**BUSINESS IMPACT ANALYSIS**

The SQL injection attack consists of the insertion or “injection” of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands.

**Threat Modelling**

* SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.
* SQL Injection is very common with PHP and ASP applications due to the prevalence of older functional interfaces. Due to the nature of programmatic interfaces available, J2EE and ASP.NET applications are less likely to have easily exploited SQL injections.
* The severity of SQL Injection attacks is limited by the attacker’s skill and imagination, and to a lesser extent, defense in depth countermeasures, such as low privilege connections to the database server and so on. In general, consider SQL Injection a high impact severity.

**Understanding the potential consequences of SQL injection vulnerability on a business**

SQL injection vulnerabilities can have significant business impacts on organizations, including financial losses, damage to reputation, legal consequences, and operational disruptions. Let's conduct a thorough analysis of these potential impacts:

**Financial Losses**:

Unauthorized access to sensitive data: SQL injection can allow attackers to retrieve, modify, or delete data stored in databases. If attackers gain access to valuable or confidential information such as customer data, financial records, or intellectual property, it can lead to financial losses through fraud, identity theft, or competitive disadvantages.

Loss of revenue and business opportunities: Exploitation of SQL injection vulnerabilities can result in service disruptions, leading to lost sales, customers, and business opportunities.

Cost of incident response: Organizations may need to invest in forensic investigations, security assessments, and remediation efforts to mitigate the impact of a SQL injection attack. These costs can be significant, depending on the severity and scope of the incident.

Damage to Reputation: Customer trust and brand reputation: If a SQL injection vulnerability is exploited, customer data may be compromised, eroding trust in the organization's ability to protect sensitive information. News of a data breach can spread quickly, damaging the organization's reputation and leading to customer churn.

Compliance and regulatory issues: Many industries have legal requirements and regulations regarding the protection of customer data. A SQL injection attack resulting in data breaches can lead to non-compliance penalties, fines, and legal actions.

**Legal Consequences**:

Legal liabilities: Organizations may face legal consequences, including lawsuits from affected customers or stakeholders, for failing to protect their data adequately. This can result in significant financial penalties and legal fees.

Regulatory fines: Government agencies, such as data protection authorities, may impose fines for data breaches caused by SQL injection vulnerabilities, particularly if non-compliance with applicable regulations is established.

**Operational Disruptions:**

Downtime and service disruptions**:** Successful exploitation of SQL injection vulnerabilities can lead to system downtime or reduced availability of critical applications or services. This can impact business operations, productivity, and customer satisfaction.

Recovery and remediation costs: Resolving a SQL injection attack requires investigation, vulnerability patching, data recovery, and infrastructure reconfiguration. These activities can be time-consuming, disrupt normal operations, and incur additional costs.