**Business impacts of CWE of OWASP top 10**

1. **Broken Access Control :-**

**CWE 287 - Improper Authentication**

Improper authentication vulnerabilities occur when authentication mechanisms are not properly implemented, allowing attackers to bypass authentication.

**Business Impact**

CWE-287, "Improper Authentication," poses both technical and business risks. It allows attackers to gain unauthorized access, compromise sensitive data, and escalate privileges within applications. This can result in financial losses, reputation damage, legal actions, operational disruptions, and customer churn. Technical consequences include data exposure, session hijacking, and vulnerability exploitation. These technical impacts translate into real-world business implications such as financial setbacks, loss of trust, regulatory penalties, operational downtime, and intellectual property theft. Addressing this vulnerability is essential to prevent these multifaceted risks.

1. **Cryptographic Failures :-**

**CWE 327 - Use of broken or risky cryptographic algorithm**

This CWE focuses on the use of cryptographic algorithms that are known to be vulnerable, deprecated, or insufficiently secure. Implementing weak or broken algorithms can lead to unauthorized access, data breaches, and exploitation of encrypted data.

**Business Impact**

CWE-327, "Use of a Broken or Risky Cryptographic Algorithm," has significant technical and business impact. Using vulnerable cryptographic algorithms can lead to unauthorized access, data breaches, and compromised confidentiality. Attackers can exploit weaknesses in these algorithms to decrypt sensitive information, undermining data security. This can result in financial losses due to breach aftermath costs, legal liabilities, and reputational damage. Additionally, regulatory penalties and customer trust erosion are likely, impacting long-term business viability. Addressing this vulnerability is crucial to prevent these far-reaching consequences.

1. **Injections :-**

**CWE 89 - SQL Injection**

This is one of the most well-known injection vulnerabilities. It occurs when an application doesn't properly validate or sanitize user input, allowing attackers to insert malicious SQL queries into input fields. Successful SQL injection attacks can lead to unauthorized access, data manipulation, and potentially full control of the database.

**Business Impact**

CWE-89, "SQL Injection," carries substantial technical and business impact. By exploiting inadequate input validation, attackers can manipulate SQL queries, potentially gaining unauthorized access to databases, extracting sensitive information, or even modifying data. This can result in financial losses due to data breaches, legal liabilities, and reputational harm. Operational disruptions, compromised customer trust, and regulatory penalties are likely, underscoring the need for robust input validation measures to prevent these far-reaching consequences.

1. **Insecure Design :-**

**CWE 352 - Cross Site Request Forgery(CSRF)**

CSRF vulnerabilities often stem from insecure design choices, particularly related to how the application handles state-changing requests. Poorly designed authentication and session management mechanisms can allow attackers to trick users into performing unintended actions without their consent.

**Business Impact**

CWE-352, "Cross-Site Request Forgery (CSRF)," presents notable technical and business impact. By exploiting poor design of authentication and session management, attackers can manipulate user actions without consent, potentially leading to unauthorized transactions, data manipulation, and account compromise. This can result in financial losses, legal liabilities, and customer trust erosion. Operational disruptions, regulatory penalties, and reputational damage are likely, underscoring the need for robust session handling mechanisms to prevent these adverse consequences.

1. **Security Misconfiguration :-**

**CWE 290 - Authentication Bypass by Spoofing**

This CWE involves misconfigurations that allow attackers to impersonate legitimate users or systems. Poorly configured authentication checks can enable attackers to bypass security controls.

**Business Impact**

CWE-290, "Authentication Bypass by Spoofing," has significant technical and business impact. Exploiting misconfigurations that allow attackers to impersonate legitimate users or systems can result in unauthorized access, data breaches, and manipulation of sensitive information. This can lead to financial losses due to breach aftermath costs, legal liabilities, and reputational damage. Additionally, operational disruptions, regulatory penalties, and erosion of customer trust are likely, underscoring the need for robust authentication mechanisms to prevent these wide-ranging consequences.