NAME: MOHAMED NAVEED
REGISTRATION NUMBER: 21BAI1808

The OWASP (Open Web Application Security Project) Top 5 CWE (Common Weakness Enumeration) descriptions with business impact highlight common security weaknesses or vulnerabilities in web applications that can have a significant impact on an organization's business operations, reputation, and security posture. Below are five CWE descriptions with business impact:

1. CWE-22: Improper Limitation of a Pathname to a Restricted Directory ("Directory Traversal"):
   - Description: This weakness occurs when an application allows an attacker to navigate outside of a designated directory, gaining unauthorized access to files and directories on the server.
   - Business Impact: An attacker exploiting this weakness can access sensitive files, potentially compromising confidential data, customer information, or intellectual property. This can lead to legal repercussions, data breaches, and damage to the organization's reputation.

2. CWE-79: Improper Neutralization of Input During Web Page Generation ("Cross-Site Scripting" or "XSS"):
   - Description: XSS vulnerabilities occur when an application fails to properly validate or sanitize user-generated input, allowing malicious scripts to be executed in a user's browser.
   - Business Impact: An attacker can steal user credentials, session cookies, or sensitive information, manipulate web pages, or launch phishing attacks. XSS vulnerabilities can tarnish a company's brand, cause financial losses, and lead to regulatory fines.

3. CWE-89: Improper Neutralization of Special Elements used in an SQL Command ("SQL Injection"):
   - Description: SQL injection occurs when an application fails to validate and sanitize user input, allowing attackers to inject malicious SQL queries into the database.
   - Business Impact: Attackers can gain unauthorized access to, modify, or delete sensitive data in the database, potentially leading to data breaches, financial losses, and legal repercussions. It can also disrupt business operations and damage customer trust.

4. CWE-306: Missing Authentication for Critical Function:
   - Description: This weakness occurs when an application fails to properly authenticate users for critical functions, allowing unauthorized users to perform actions that can have a significant impact on the application or business.
   - Business Impact: Unauthorized users may gain access to critical functionality, potentially disrupting operations, manipulating data, or causing financial harm. The lack of authentication can lead to regulatory compliance issues and reputational damage.

5. CWE-352: Cross-Site Request Forgery (CSRF):
   - Description: CSRF vulnerabilities occur when an attacker tricks a user into making an unintended and unauthorized request to a web application on which the user is authenticated.

NAME: MOHAMED NAVEED
REGISTRATION NUMBER: 21BAI1808

- Business Impact: Attackers can perform actions on behalf of authenticated users without their consent, such as changing settings, initiating financial transactions, or causing data loss. CSRF attacks can lead to financial losses, damage to user trust, and regulatory consequences.

Addressing these CWEs and other security weaknesses through secure development practices, code reviews, and regular security assessments is crucial to mitigating business risks associated with web application vulnerabilities. Proactive security measures can help protect an organization's assets, reputation, and customer trust.