TASK 3:

Saloni Ghule

CWE 284 for Broken Access Control:

Description:

The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

Business impact:

Broken access control (CWE 284) can cause unauthorized data leaks, regulatory fines, financial fraud, disrupted operations, and harm to reputation, leading to financial losses, legal trouble, and customer distrust.

CWE 310 for Cryptographic failures:

Description:

Weaknesses in this category are related to the use of cryptography.

Business Impact:

These issues involve weaknesses in how information is encrypted and protected. If not addressed, they can lead to data breaches, unauthorized access, and loss of sensitive information. This can result in damaged customer trust, legal repercussions, financial losses, and harm to the company's reputation. Therefore, it's crucial for businesses to prioritize strong encryption practices to mitigate these risks and safeguard their operations and customer data.

CWE-89 for Injection:

Description:

CWE-89 is the specific Common Weakness Enumeration (CWE) identifier for "SQL Injection," which is a type of security vulnerability that occurs when an attacker is able to manipulate or inject malicious SQL code into a web application's input fields or parameters.

Business impact:

It allows hackers to sneak malicious code into a website's input fields, leading to unauthorized access of sensitive data like customer information or financial records. This breach of security can harm customer trust, result in legal penalties, cause financial losses, and damage the company's reputation. It's essential for businesses to prevent SQL Injection to safeguard their data and maintain a secure online environment.

CWE for 676 Insecure Design :

Description:

This category encompasses various weaknesses related to the design of software applications that can lead to security vulnerabilities.

Business Impact:

Insecure Application Design, can have significant business impacts. If not addressed, it can lead to security vulnerabilities that attackers exploit to gain unauthorized access, steal sensitive data, or disrupt services. This can result in breaches, financial losses, legal consequences, damage to customer trust, and harm to the company's reputation. Fixing these design flaws early is crucial to prevent these risks and ensure the security of the business's applications and systems.

CWE for 494 Security Misconfiguration:

Description:

CWE-494 is a Common Weakness Enumeration (CWE) identifier that refers to the "Download of Code Without Integrity Check" vulnerability. This weakness occurs when software or data is downloaded from a remote source without verifying its integrity. In other words, the downloaded code or data has not been checked for tampering or unauthorized modifications, allowing potentially malicious content to be executed on the system.

Business impact:

If exploited, malicious code could be introduced into the system during downloads, leading to unauthorized access, data breaches, and potential disruptions. This can result in compromised customer data, financial losses, legal repercussions, and damage to the company's reputation. Implementing integrity checks helps prevent these risks and ensures the security and reliability of the software or system.