AICS-TASK : 3

TITTLE : Top 5 OWASP CWE description with Business Impact

Name : Rohitha Koganti

The Open Web Application Security Project (OWASP) provides a list of the most critical web application security risks, known as the OWASP Top Ten. Each risk is associated with specific Common Weakness Enumeration (CWE) identifiers. Below are the top 5 OWASP CWE descriptions along with their business impact:

1. Injection (CWE-89):

Description: Injection vulnerabilities occur when untrusted data is sent to an interpreter as part of a command or query. This can lead to an attacker injecting malicious code into the application, potentially gaining unauthorized access to data or manipulating it.

Business Impact: Injection attacks can result in data breaches, data loss, unauthorized access, and system downtime. These incidents can lead to legal repercussions, loss of customer trust, and financial damage.

2. Broken Authentication (CWE-287):

Description: Broken authentication vulnerabilities occur when the application fails to properly authenticate and manage user sessions, allowing attackers to bypass authentication and gain unauthorized access to user accounts and sensitive data.

Business Impact: Unauthorized access to user accounts can lead to data breaches, identity theft, fraud, and damage to a company's reputation. Legal and regulatory compliance issues may also arise.

3. Sensitive Data Exposure (CWE-200):

Description: Sensitive data exposure vulnerabilities involve the exposure of sensitive information such as passwords, credit card numbers, or personal identification data due to inadequate data protection mechanisms.

Business Impact: The exposure of sensitive data can result in legal penalties, fines, and severe damage to an organization's reputation. It can also lead to identity theft, financial

fraud, and loss of customer trust.

4. Security Misconfiguration (CWE-732):

Description: Security misconfigurations occur when an application, server, or database is not configured securely, leaving vulnerabilities that can be exploited by attackers.

Business Impact: Misconfigurations can lead to unauthorized access, data breaches, service disruptions, and compliance violations. They can also be exploited to gain control over systems or applications, causing financial and reputational damage.

5. Cross-Site Scripting (XSS) (CWE-79):

Description: Cross-Site Scripting vulnerabilities occur when an application includes untrusted data in a web page that is subsequently executed by a user's browser. This can allow attackers to inject malicious scripts into web pages viewed by other users.

Business Impact: XSS attacks can result in the theft of user data, session hijacking, and the spread of malware. They can also lead to reputational damage and loss of customer trust if users believe the website is not secure.

Addressing these top OWASP CWE vulnerabilities is crucial for businesses to protect their applications and data, maintain compliance with regulations, and safeguard their reputation and financial well-being. Implementing secure coding practices, conducting regular security assessments, and staying informed about emerging threats are essential steps in mitigating these risks.