Niraianbu porchezhian
21BCE0965
Task 3

Task-3

TOP 5 OWASP CWE DESCRIPTION WITH BUSINESS IMPACT

1. CWE-20: Improper Input Validation

Description:

CWE-20, known as "Improper Input Validation," occurs when an application fails to properly validate user-supplied input. This weakness can lead to various security issues, including SQL injection, cross-site scripting (XSS), and remote code execution.

Business Impact:

For businesses, CWE-20 poses significant risks. An attacker can exploit this weakness to steal sensitive customer data, manipulate application functionality, and even take control of the application. This can result in data breaches, loss of customer trust, financial penalties, and damage to the brand's reputation.

2. CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Description:

CWE-79, or "Cross-Site Scripting (XSS)," occurs when an application includes untrusted data in a web page without proper validation or escaping. Attackers can then inject malicious scripts into the web pages viewed by other users, compromising their accounts and data.

Business Impact:

XSS vulnerabilities can lead to severe business consequences. Exploited XSS flaws can allow attackers to steal sensitive user information, such as login credentials and financial data. Additionally, they can deface websites, distribute malware, and tarnish a company's image. Customers may lose trust in the organization's online services.

3. CWE-306: Missing Authentication for Critical Function

Description:

CWE-306, "Missing Authentication for Critical Function," occurs when an application fails to require authentication for critical operations or functionalities. This oversight enables unauthorized users to access sensitive functions, posing significant security risks.

Business Impact:

The business impact of CWE-306 can be devastating. Unauthorized access to critical functions can result in data breaches, financial losses, and legal consequences. Customers' confidential information may be exposed, leading to a loss of trust and reputation damage.

4. CWE-89: SQL Injection

Description:

CWE-89, known as "SQL Injection," arises when an application accepts untrusted data and directly incorporates it into SQL queries without proper validation. Attackers can exploit this weakness to manipulate the database, extract sensitive data, or even delete records.

Business Impact:

SQL Injection can have severe business ramifications. An attacker with successful SQL injection can access, modify, or delete critical data, leading to data breaches, financial losses, and potential legal actions. Additionally, it can harm the organization's reputation and customer trust.

5. CWE-312: Cleartext Storage of Sensitive Information

Description:

CWE-312, "Cleartext Storage of Sensitive Information," occurs when an application stores sensitive data, such as passwords or encryption keys, in an insecure manner, such as in plaintext. This makes it easier for attackers to obtain this information.

Business Impact:

Storing sensitive data in cleartext can result in data exposure and breaches. Attackers can exploit this weakness to gain unauthorized access to sensitive accounts or information, leading to financial losses, regulatory penalties, and damage to the company's reputation.