Stuti Maitra Sarkar
21BCI0126

Top 5 OWASP Common Weakness Enumeration (CWE) vulnerabilities:

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

Description:

Cross-site Scripting (XSS) occurs when a web application includes untrusted data in a web page that is then rendered in a user's browser. This allows an attacker to inject malicious scripts into web pages viewed by other users.

Business Impact:

- Loss of Trust: XSS attacks can steal sensitive data, such as login credentials or personal information. This can lead to a loss of customer trust and a damaged reputation.

- Regulatory Violations: Data breaches resulting from XSS can lead to legal and regulatory consequences, including fines and legal actions.

- Financial Loss: Remediation and recovery from an XSS attack can be costly, including legal expenses and customer compensation.

- Disruption: Exploiting XSS can disrupt business operations, impact customer services, and result in downtime.

2. CWE-89: SQL Injection

Description:

SQL Injection is a type of vulnerability that allows an attacker to manipulate SQL queries. By injecting malicious SQL statements, an attacker can access, modify, or delete data in a database.

Business Impact:

- Data Breaches: SQL Injection can result in unauthorized access to, modification, or deletion of sensitive data. This can lead to data breaches, which can be highly damaging to an organization.

- Reputation Damage: A data breach due to SQL Injection can severely harm an organization's reputation, leading to a loss of customer trust.

- Financial Loss: Legal and regulatory costs, as well as compensation for affected individuals, can result in substantial financial losses.

Stuti Maitra Sarkar
21BCI0126
Task 1

- Operational Disruption: Remediation efforts, including system downtime for patching and forensics, can disrupt normal business operations.

3. CWE-78: Improper Neutralization of Special Elements Used in an OS Command ('OS Command Injection')

Description:

OS Command Injection occurs when an application incorporates untrusted data into system-level commands. An attacker can then manipulate the input to execute malicious commands on the host operating system.

Business Impact:

- System Compromise: Successful OS Command Injections can compromise the security and integrity of the host system. This can lead to unauthorized access, data breaches, and data loss.

- Legal and Compliance Issues: Organizations may face legal and regulatory challenges if a breach results from OS Command Injection.

- Downtime and Recovery Costs: Mitigating OS Command Injection vulnerabilities can result in system downtime and recovery costs.

- Reputation Damage: The compromise of a system's security can harm an organization's reputation.

4. CWE-311: Hard-Coded Password

Description:

Hard-coded passwords refer to credentials that are embedded directly in an application's source code. These are often overlooked and easily discoverable by attackers.

Business Impact:

- Unauthorized Access: Hard-coded passwords can provide unauthorized access to critical systems, potentially leading to data breaches and other malicious activities.

- Compliance Violations: Many compliance standards require secure storage and handling of passwords. Hard-coding them can lead to compliance violations and associated penalties.

- Financial Loss: Addressing hard-coded password vulnerabilities can be expensive, including the costs of code review, updates, and auditing.

Stuti Maitra Sarkar
21BCI0126
Task 1

- Reputation Damage: Security lapses like hard-coded passwords can damage an organization's reputation, particularly when data breaches occur.

5. CWE-306: Missing Authentication for Critical Function

Description:

Missing Authentication for Critical Function refers to scenarios where an application fails to require proper authentication before allowing access to sensitive functions or data.

Business Impact:

- Unauthorized Access: This vulnerability can lead to unauthorized access to critical functions, allowing attackers to manipulate or steal sensitive data.

- Regulatory Violations: Many regulations mandate proper authentication for sensitive functions. Non-compliance can result in legal and regulatory consequences.

- Operational Disruption: Remediation efforts, such as introducing proper authentication mechanisms, can disrupt normal business operations.

- Reputation Damage: Security lapses leading to unauthorized access can harm an organization's reputation and customer trust.

These are just a few examples of OWASP CWEs and their potential business impacts. Addressing these vulnerabilities is critical to maintaining the security, integrity, and reputation of an organization. Proper security practices, such as regular vulnerability assessments, penetration testing, and secure coding, are essential to mitigating these risks and ensuring the protection of both data and business interests.