ASSIGNMENT_1

TOP_5_OWASP_VULNERABILITIES

1. Broken Access Control:

“CWE 377 - Insecure Temporary File”

Creating and using insecure temporary files can leave application and system data vulnerable to attack.

“Business Impact”

If temporary files containing sensitive information (such as login credentials, financial data, or personal information) are accessible by unauthorized individuals, it can lead to data breaches, unauthorized access, identity theft, financial loss, and damage to an organization's reputation. Attackers could exploit these insecure files to gain insights into the system's operation or extract sensitive data, leading to legal and financial consequences for the organization. Proper handling and secure management of temporary files are essential to prevent this type of vulnerability.

2. Cryptographic Failures:

“CWE 327 - Use of broken or risky cryptographic algorithm”

This CWE focuses on the use of cryptographic algorithms that are known to be vulnerable, deprecated, or insufficiently secure. Implementing weak or broken algorithms can lead to unauthorized access, data breaches, and exploitation of encrypted data.

“Business Impact”

It has significant technical and business impact. Using vulnerable cryptographic algorithms can lead to unauthorized access, data breaches, and compromised confidentiality. Attackers can exploit weaknesses in these algorithms to decrypt sensitive information, undermining data security. This can result in financial losses due to breach aftermath costs, legal liabilities, and reputational damage. Additionally, regulatory penalties and customer trust erosion are likely, impacting long-term business viability. Addressing this vulnerability is crucial to prevent these far-reaching consequences.

3. Injections:

“CWE 116 - Improper Encoding or Escaping of Output”

The product prepares a structured message for communication with another component, but encoding or escaping of the data is either missing or done incorrectly. As a result, the intended structure of the message is not preserved.

“Business Impact”

If output data is not properly encoded or escaped, attackers can inject malicious code (such as scripts or SQL queries) into the output, leading to cross-site scripting (XSS) attacks, SQL injection attacks, and other forms of data manipulation. This can result in unauthorized access, data theft, defacement of websites, disruption of services, and damage to the organization's reputation. Addressing this weakness is crucial to ensuring the security of applications and protecting sensitive user data from exploitation.

4. Insecure Design:

“CWE 657 - Violation of Secure Design Principles”

The product violates well-established principles for secure design.

“Business Impact”

This vulnerability emerges when software systems are developed without following established security best practices and design principles. As a result, applications become susceptible to various attacks and breaches. Exploiting this flaw can lead to unauthorized access, data breaches, system compromise, and operational disruptions. The business impact encompasses financial losses, regulatory penalties, legal actions, reputational damage, erosion of customer trust, and increased security-related development costs. Addressing this issue necessitates reevaluating and retrofitting the software's design, diverting resources from innovation and development efforts, potentially delaying project timelines and undermining competitiveness.

5. Security Misconfiguration:

“CWE 11 - ASP.NET Misconfiguration: Creating Debug Binary”

The product transmits sensitive or security critical data in cleartext in a communication channel that can be sniffed by unauthorized actors.

“Business Impact”

Security Misconfiguration can harm businesses by exposing confidential data during transmission, leading to data breaches, compromised customer trust, regulatory violations, and potential legal consequences.