OWSAP TOP 5 VULNERABILITY

1:-BROKEN ACCESS CONTROL

**CWE-285: Improper Authorization**

**Description:-** The product does not perform or incorrectly performs an authorization check when an actor attempts to access a resource or perform an action.

BUSINESS IMPACT:- CWE-285, "Improper Authorization," is a software vulnerability that occurs when systems or applications fail to properly control user access. The business impact of this vulnerability includes:

* Data Breaches: Unauthorized access can lead to data breaches, exposing sensitive information and resulting in financial and reputational damage.
* Financial Loss: Attackers can perform unauthorized actions, causing financial losses for organizations and customers.
* Reputation Damage: Incidents can harm an organization's reputation, leading to customer distrust and loss of business.
* Legal Consequences: Non-compliance with regulations can result in fines and lawsuits.
* Operational Disruption: Unauthorized access can disrupt operations, causing downtime.
* Intellectual Property Theft: Access to proprietary information can lead to intellectual property theft.
* Loss of Competitive Advantage: Competitors may gain insights into business processes.
* Regulatory Non-Compliance: Failing to protect data can lead to regulatory penalties.
* Customer Impact: Customers may suffer identity theft and financial losses.
* Operational Costs: Responding to incidents incurs operational expenses.
* In essence, improper authorization can have severe financial, reputational, and operational consequences, emphasizing the need for strong access controls and security practices.

2:-CRYPTOGRAPHIC FAILURES

**CWE-327: Use of a Broken or Risky Cryptographic Algorithm**

**DESCRIPTION:-** The product uses a broken or risky cryptographic algorithm or protocol.

BUSINESS IMPACT:- CWE-327, "Use of a Broken or Risky Cryptographic Algorithm," refers to vulnerabilities that occur when weak or deprecated cryptographic algorithms are used for protecting sensitive data. The business impact of this vulnerability includes:

* Data Exposure: Weak encryption can lead to data exposure, compromising sensitive information.
* Loss of Trust: Customers may lose trust in the organization due to inadequate data protection.
* Legal Consequences: Non-compliance with data protection laws can result in legal penalties and lawsuits.
* Financial Loss: Data breaches can lead to financial losses, including regulatory fines and remediation costs.
* Reputation Damage: A security incident can harm the organization's reputation, affecting customer relationships and future business.
* Competitive Disadvantage: Security weaknesses can lead to a loss of competitive advantage in the market.
* Operational Disruption: Security incidents can disrupt normal business operations and lead to downtime.

In summary, the business impact of CWE-327 involves data exposure, legal issues, financial losses, reputational damage, and operational disruption, underscoring the importance of using strong cryptographic algorithms to protect sensitive data.

INJECTION:-

**CWE-94: Improper Control of Generation of Code ('Code Injection')**

**DESCRIPTION:-** The product constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment.

BUSINESS IMPACT:- CWE-94, "Improper Control of Generation of Code ('Code Injection')," can have severe business impacts, including data breaches, financial losses, reputational damage, legal consequences, operational disruption, and potential regulatory penalties. This vulnerability allows attackers to execute malicious code within an application, compromising security and integrity.

INSECURE DESIGN:-

|  |  |
| --- | --- |
|  |  |
| **CWE-657: Violation of Secure Design Principles**  **DESCRIPTION:-** The product violates well-established principles for secure design.  BUSINESS IMPACT:- CWE-657, "Violation of Secure Design Principles," can result in significant business impacts, such as security breaches, data loss, reputation damage, legal consequences, operational disruption, competitive disadvantages, and increased long-term costs. |

Security Misconfiguration

**CWE CATEGORY: OWASP Top Ten 2013 Category A5 - Security Misconfiguration**

**DESCRIPTION:-** Weaknesses in this category are related to the A5 category in the OWASP Top Ten 2013.

BUSINESS IMPACT:- Security misconfigurations categorized under OWASP Top Ten 2013 Category A5 can lead to significant business impacts. These include data exposure, reputation damage, operational disruptions, financial losses, regulatory non-compliance, competitive disadvantages, and long-term costs.