ASSIGNMENT-1

NAME- SANISETTY HEMA SAGAR
REG-NO-21BCE7769
AWCS

TOP 5 OS VULNELABILITIES

1. INJECTION

CWE-94: IMPROPER CONTROL OF GENERATION OF CODE ('CODE INJECTION')

DISCRIPTION

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

Data Breaches and Unauthorized Access:

Attackers can manipulate code execution to gain unauthorized access to sensitive data, such as customer records, financial information, and intellectual property.

Data breaches can result in legal liabilities, regulatory fines, and loss of customer trust.

Loss of Intellectual Property:

Code Injection can lead to the theft of proprietary algorithms, source code, and other intellectual property, putting a company's competitive advantage at risk.

2.SENSITIVE DATA EXPOSURE

CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Discriprition

The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information.

Business impact

Financial Losses:

Data breaches can lead to direct financial losses through regulatory fines, legal settlements, and reimbursement for affected individuals.

The cost of investigating the breach, notifying customers, and implementing corrective measures can be substantial.

Legal and Regulatory Consequences:

Businesses are often subject to data protection regulations (e.g., GDPR, HIPAA, CCPA), and data exposure can lead to non-compliance and regulatory fines.
Legal actions from affected parties can result in costly lawsuits and damage the company's reputation.

3.BROKEN ACCESS CONTROL
CWE-284: IMPROPER ACCESS CONTROL

DISCRIPTION

The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

BUSINESS IMPACT

Broken access control can lead to unauthorized data breaches, financial losses from fines and legal actions, reputation damage eroding customer trust, regulatory non-compliance, and intellectual property theft. Operational disruptions and legal consequences, along with diminished customer confidence and supply chain risks, contribute to decreased market value and employee morale. The long-term effects include ongoing reputational harm and potential loss of competitive advantage.

4. SECURITY MISCONFIGURATION
CWE: CWE-319: Cleartext Transmission of Sensitive Information

DISCRIPTION

Security misconfiguration is a perilous cybersecurity vulnerability stemming from the improper configuration of software, applications, or systems. This vulnerability arises when security settings are not appropriately defined, leaving digital assets exposed to potential threats. At the heart of the digital battlefield, security misconfiguration opens gateways for attackers to exploit vulnerabilities, potentially leading to unauthorized access, data breaches, and operational disruptions.

BUSINESS IMPACT:

Security Misconfiguration is the fifth-most serious AppSec vulnerability. According to the research, with an average occurrence rate of 4%, over 90% of apps reported misconfiguration. It can hurt organizations by disclosing private information as it is being transmitted, which could result in data breaches, weakened customer confidence, regulatory infractions, and possible legal repercussions. Attackers can access networks, systems, and data without authorization thanks to security configuration errors, which can seriously harm your company's finances and reputation.

5. XML EXTERNAL ENTITIES.
CWE-611: Improper Restriction of XML External Entity Reference

DISCRIPTION

The product processes an XML document that can contain XML entities with URIs that resolve to documents outside of the intended sphere of control, causing the product to embed incorrect documents into its output.

BUSINESS IMPACT

XML External Entity (XXE) attacks can wreak havoc on businesses, leading to unauthorized data exposure, intellectual property theft, and customer records compromise. Financial losses accrue from regulatory fines, litigation, and remediation efforts. Reputation damage and customer distrust ensue, causing potential customer churn and decreased market value. Operational disruptions arise due to breach response and recovery. Compliance violations result from compromised data security. Long-term effects include legal liabilities and impaired brand image.