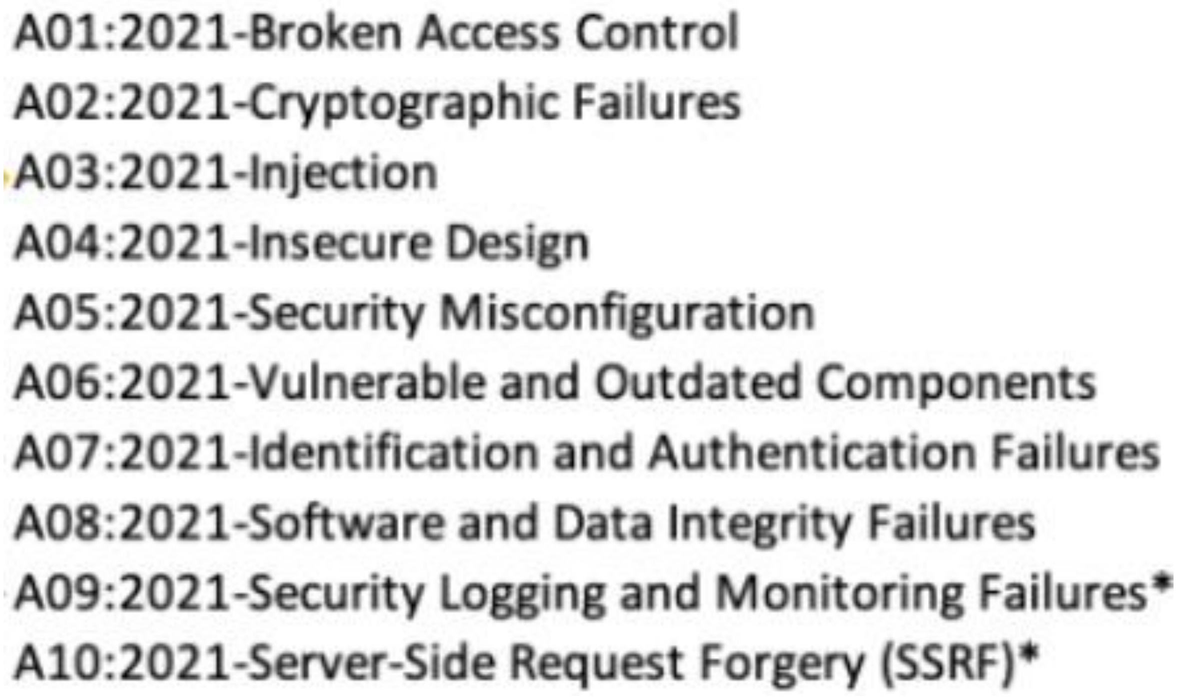
Hrishik Manoj
21BCE8607
VIT AP
CSE : CYBERSECURITY

ASSIGNMENT-1

Work: Study the top 10 OWASP and make a report with business impactfor the first 5



A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
A10:2021-Server-Side Request Forgery (SSRF)*

1. BROKEN ACCESS CONTROL

CWE-284: Improper Access Control

DESCRIPTION:

CWE-284, "Improper Access Control," is a software flaw resulting from inadequate access restrictions, enabling unauthorized access to sensitive data or functions. Exploitable by attackers to bypass security measures, it poses serious risks to system integrity. Implementing strong access controls, including authentication and authorization, is essential for mitigation.

BUSINESS IMPACT:

CWE-284, "Improper Access Control," can have severe business impacts. Exploitation can lead to unauthorized access, data breaches, and system compromise. This may result in loss of sensitive information, reputation damage, legal liabilities, and financial losses due to regulatory fines, customer attrition, and operational disruptions. Mitigation efforts are essential to safeguard business assets and maintain trust.

2.CRYPTOGRAPHIC FAILURES

CWE-331: Insufficient Entropy

DESCRIPTION:

CWE-331, "Insufficient Entropy," refers to vulnerabilities due to inadequate randomness in data generation, such as cryptographic keys. Attackers exploit this weakness to predict values, compromising cryptographic operations' security. Robust entropy sources are crucial to prevent this and ensure the effectiveness of cryptographic protections.

BUSINESS IMPACT:

CWE-331, "Insufficient Entropy," can harm businesses by weakening encryption. This makes it easier for attackers to guess sensitive information like passwords or access encrypted data. Such breaches can lead to data leaks, financial losses, and damage to a company's reputation, potentially scaring away customers and partners.

3. 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, "Code Injection," can seriously hurt businesses. It lets attackers sneak harmful code into software, causing unauthorized access and data breaches. This can cost money, harm the company's name, and disrupt operations. To prevent this, strong security measures and careful code checking are a must.

4.INSECURE DESIGN

CWE-657: Violation of Secure Design Principles

DESCRIPTION:

CWE-657, "Violation of Secure Design Principles," means making software without following safety rules. This lets bad actors attack the software easily. By sticking to these rules, we build software that can better defend against threats and avoid getting hacked.

BUSINESS IMPACT:

CWE-657, "Violation of Secure Design Principles," negatively affects businesses by producing vulnerable software. Attackers exploit these weaknesses, leading to data breaches, financial losses, and reputational damage. Incorporating secure design practices helps prevent these consequences, ensuring software is resilient against threats and safeguarding the business's assets and reputation.

5. SECURITY MISCONFIGURATION

CWE-15

Hrishik Manoj
21BCE8607
VIT AP
CSE : CYBERSECURITY

DESCRIPTION

CWE-15, "Security Misconfiguration," points to vulnerabilities that occur due to incorrect configuration settings. These settings might grant unauthorized access, expose sensitive information, or weaken security measures. Attackers can exploit these misconfigurations to gain access to systems and data.

BUSINESS IMPACT:

Security misconfigurations can have significant business impacts. They expose organizations to data breaches, financial losses, and reputation damage. Attackers can exploit these vulnerabilities to steal sensitive information, disrupt services, or even take control of systems. Addressing security misconfigurations is essential to prevent these negative consequences and maintain a strong security posture.