ASSIGNMENT 1

Overview of the assignment:

To write the business impact for top 5 out of top 10 OWASP vulnerabilities with a CWE for each of the vulnerabilities.

OWASP

The Open Web Application Security Project (OWASP) is a nonprofit organization dedicated to improving the security of web applications and software. It provides resources, tools, and guidelines to help developers, security professionals, and organizations enhance the security of their web applications. OWASP's mission is to make web application security visible and ensure that security is a top priority during application development, deployment, and maintenance.

The organization releases a list of the top 10 most critical web application security risks, known as the "OWASP Top Ten." These vulnerabilities pose significant threats to web applications and are crucial to address to protect against cyberattacks and data breaches. The OWASP Top Ten list serves as a widely recognized reference for organizations seeking to prioritize their security efforts.

OWASP Top 10 -2021

- 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- A06:2021-Vulnerable and Outdated Components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

Business Impact of Top 5 of 10 OWASP-2021

1) Broken Access Control (CWE-285):

Business Impact: Broken access control vulnerabilities can result in unauthorized access to sensitive functionality or data within an application. This can lead to data breaches, unauthorized modifications, and disclosure of private information. The business consequences include financial losses due to legal fines, loss of reputation, and the compromise of intellectual property or customer data.

2) Cryptographic Failures (CWE-310):

Business Impact: Cryptographic failures can result in the compromise of encrypted data, leaving sensitive information exposed. This may lead to regulatory non-compliance, data breaches, and potential damage to an organization's reputation. Inadequate encryption can also result in financial losses and legal liabilities.

3) Injection (CWE-89):

Business Impact: Injection vulnerabilities, such as SQL injection, can lead to unauthorized access, data tampering, or data theft. This can result in compromised confidentiality, integrity,

and availability of data. The business impacts include financial losses, legal consequences, and reputational damage.

4) Insecure Design (CWE-749):

Business Impact: Insecure design can lead to fundamental flaws in an application's architecture, allowing attackers to exploit vulnerabilities. Such flaws can result in data breaches, system failures, and potential financial losses. Inadequate security at the design stage can also delay time-to-market and damage customer trust.

5) Security Misconfiguration (CWE-732):

Business Impact: Security misconfigurations can expose critical application components and sensitive data. Attackers may exploit these misconfigurations to gain unauthorized access or disrupt services, potentially leading to data breaches, operational downtime, legal liabilities, and loss of customer trust.