Assignment 1

- **Hardik Kankane (21BCE10413)**

Overview:

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 collaborative online community focused on advancing web application security. It offers a wide range of freely accessible resources, including articles, methodologies, documentation, tools, and technologies. Guided by The OWASP Foundation, a non-profit organization, this community unites global experts and volunteers in the pursuit of enhancing web application security.

A notable contribution from OWASP is the OWASP Top 10 - 2023. This publication stems from extensive research, synthesizing data from over 40 partner organizations. It provides a concise guide outlining the most prevalent and critical security vulnerabilities facing web applications today. This resource empowers developers, security professionals, and organizations to prioritize their security efforts effectively, strengthening their defenses against evolving threats. The OWASP Top 10 serves as a valuable roadmap for securing digital assets and protecting user data in an increasingly complex digital landscape.

OWASP TOP 10 – 2023

These are the OWASP top 10 vulnerabilities 2023 that every web and application developers should look out before proceeding with the development.

1. **Broken Access Control**
2. **Cryptographic Failures**
3. **Injection**
4. **Insecure Design**
5. **Security Misconfiguration**
6. **Vulnerable and Outdated Components**
7. **Identification and Authentication Failures**
8. **Software and Data Integrity Failures**
9. **Security Logging and Monitoring**
10. **Server-Side Request Forgery**

Vulnerabilities

1. **Broken Access Control**

    - **CWE**: CWE-285
    - **OWASP Category**: Access Control
    - **Description**: Broken Access Control occurs when a web application fails to enforce proper access controls, allowing users to perform actions or access resources they should not be able to. This can range from viewing sensitive information to manipulating critical settings.
    - **Business Impact**: If exploited, Broken Access Control can lead to unauthorized access, exposing confidential data or functionalities. This may result in financial loss, regulatory penalties, and severe reputational damage, eroding trust in the application or service.
2. **Injection**
    - **CWE**: CWE-89
    - **OWASP Category**: Injection
    - **Description**: Injection vulnerabilities involve attackers injecting malicious code (such as SQL, XML, or OS commands) into an application's input fields. This can lead to unauthorized execution of commands or manipulation of the application's behavior.
    - **Business Impact**: Successful exploitation of Injection vulnerabilities can lead to data breaches, unauthorized access, and potential manipulation or corruption of critical information. The consequences may include financial losses, legal penalties, and damage to an organization's reputation.
3. **Security Misconfiguration**
    - **CWE**: CWE-209
    - **OWASP Category**: Security Misconfiguration
    - **Description**: Security Misconfiguration arises when security settings, like permissions, authentication, or encryption, are not correctly implemented. This can leave sensitive resources exposed and provide an entry point for attackers.
    - **Business Impact**: Security Misconfigurations can lead to data breaches, unauthorized actions, reputational damage, and regulatory fines. Additionally, rectifying these misconfigurations can be resource-intensive, incurring further costs.
4. **Vulnerable and Outdated Components**
    - **CWE**: CWE-937
    - **OWASP Category**: Components with Known Vulnerabilities
    - **Description**: This vulnerability occurs when a web application uses outdated or known-to-be-vulnerable components, like libraries or frameworks. Attackers exploit these vulnerabilities to gain unauthorized access or compromise the system.
    - **Business Impact**: The use of vulnerable and outdated components can result in data breaches, legal liabilities, and reputational damage. It may also necessitate significant resources for patching and updating, potentially causing operational disruptions.
5. **Cryptographic Failures**
    - **CWE**: CWE-310
    - **OWASP Category**: Cryptographic Failures

- **Description**: Cryptographic Failures refer to instances where encryption and hashing techniques are not implemented or configured correctly. This can lead to weaker encryption, making it easier for attackers to bypass security measures or gain unauthorized access.
- **Business Impact**: Cryptographic Failures can compromise data confidentiality, potentially leading to financial losses, regulatory fines, and damage to the organization's reputation. Additionally, sensitive information may be exposed to unauthorized parties, which can have severe legal and compliance implications.