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 Worldwide Application Security Project (OWASP) is an online community that produces freely available articles, methodologies, documentation, tools, and technologies in the field of web application security. The OWASP provides free and open resources. It is led by a non-profit group called The OWASP Foundation. The OWASP Top 10 - 2021 is the published result of recent research based on comprehensive data compiled from over 40 partner organizations.

OWASP Top 10 -2021

The OWASP Top 10 is a standard awareness document for developers and web application security that is updated periodically. It represents a broad consensus about the most critical security risks to web applications. Companies should adopt this document and start the process of ensuring that their web applications minimize these risks. Using the OWASP Top 10 is the most effective first step towards changing the software development culture within your organization into one that produces more secure code. This includes:

1. A01:2021-Broken Access Control
2. A02:2021-Cryptographic Failures
3. A03:2021-Injection
4. A04:2021-Insecure Design
5. A05:2021-Security Misconfiguration
6. A06:2021-Vulnerable and Outdated Components
7. A07:2021-Identifcation and Authentication Failures
8. A08:2021-Software and Data Integrity Failures
9. A09:2021-Security Logging and Monitoring Failures
10. A10:2021-Server-Side Request Forgery

1.CWE: CWE 284 - Improper access control

OWASP Category: A01:2021-Broken Access Control

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

BUSINESS IMPACT: In today's competitive landscape, security is a key differentiator for many organizations. Failing to address improper access control issues can put an organization at a disadvantage compared to competitors who prioritize security. This can affect the ability to win contracts, partnerships, and customers.

Improper access control can lead to unauthorized users gaining access to sensitive information and data. This exposure can result in data breaches and leaks, which can damage an organization's reputation and result in legal and regulatory consequences, such as fines for failing to protect customer data.

2.CWE: CWE 310 - Cryptographic issues

OWASP Category: A02:2021-Cryptographic Failures

DESCRIPTION: Weaknesses in this category are related to the design and implementation of data confidentiality and integrity. Frequently these deal with the use of encoding techniques, encryption libraries, and hashing algorithms. The weaknesses in this category could lead to a degradation of the quality data if they are not addressed.

BUSINESS IMPACT: Cryptographic issues can lead to the exposure of sensitive data, such as customer information, payment card details, and intellectual property. When encryption is not properly implemented, attackers may gain access to this information, potentially resulting in data breaches and reputational damage.

Cryptographic vulnerabilities can expose algorithms, keys, or other intellectual property to theft. Competitors or malicious actors could exploit these weaknesses, potentially leading to product or technology theft and harming an organization's competitive advantage.

3.CWE: CWE 89 - Improper Neutralization of Special Elements used in an SQL Command

OWASP Category: A03:2021-Injection

DESCRIPTION: The product constructs all or part of an SQL command using externally influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

BUSINESS IMPACT: SQL Injection can allow attackers to execute arbitrary SQL queries against an application's database. If successful, this can lead to unauthorized access to sensitive data, including customer records, financial information, and intellectual property.

Data breaches resulting from SQL Injection can severely damage an organization's reputation. Customers, partners, and stakeholders may lose trust in the organization's ability to protect their data, potentially leading to customer churn, decreased sales, and difficulties in attracting new clients.

4.CWE: CWE-657: Violation of Secure Design Principles

OWASP Category: A04:2021-Insecure Design

DESCRIPTION: The product violates well-established principles for secure design.

BUSINESS IMPACT: Insecure design can result in vulnerabilities that are easier for attackers to exploit. This can lead to successful attacks, data breaches, and other security incidents that may damage the organization's reputation and finances.

Fixing design flaws and vulnerabilities discovered late in the development process can cause project delays. This may impact the organization's ability to release products or services on schedule, potentially affecting revenue streams.

5.CWE: CWE 16 - Configuration

OWASP Category: A05:2021-Security Misconfiguration

DESCRIPTION: Weaknesses in this category are typically introduced during the software's configuration.

BUSINESS IMPACT: Data breaches and security incidents caused by misconfigurations can severely damage an organization's reputation. Customers, partners, and stakeholders may lose trust in the organization's ability to protect their data, leading to customer churn and lost business opportunities. Misconfigurations can disrupt the normal operation of systems and applications. This can lead to downtime, loss of productivity, and customer frustration. Operational disruptions can result in immediate revenue losses and long-term reputational damage.