## **Vulnerability Analysis and Assessment**

## **Part 1: Executive Summary**

1. **Overview**

Cybersecurity protects digital systems, networks, and data from unauthorized access, attacks, damage, or theft. In an increasingly digital and interconnected world, cybersecurity plays a critical role in ensuring the confidentiality, integrity, and availability of information and systems. It encompasses a wide range of technologies, processes, and practices designed to safeguard digital assets and mitigate the risks posed by cyber threats.

The OWASP Top 10 list aims to highlight the ten most critical and prevalent security risks in web applications and software systems. This list serves as a valuable resource for developers, security professionals, and organizations to prioritize their efforts and focus on addressing the most significant security vulnerabilities that could potentially be exploited by attackers. By raising awareness about these common risks, the OWASP Top 10 aims to guide the implementation of effective security measures, best practices, and mitigation strategies to build more secure and resilient applications.

Common Weakness Enumeration (CWE) is a community-developed list of common software security weaknesses or vulnerabilities. It provides a standardized way to categorize and describe common security issues that can arise in software systems, applications, and code. Each weakness in the CWE list is assigned a unique identifier and includes a detailed description of the vulnerability, its potential impact, and guidance on preventing or mitigating it. CWE helps developers, security professionals, and organizations identify, understand, and address security weaknesses in their software, leading to more secure and robust applications.

In this project we are going to identify the CWE references for each OWASP top 10 vulnerabilities. For each vulnerability

1. **List of Vulnerable Parameter, Location discovered**

|  |  |  |
| --- | --- | --- |
| **S. No.** | **Name of The Vulnerability** | **References-CWE** |
| A01 | Broken Access Control | CWE-200: Exposure of Sensitive Information to an Unauthorized Actor |
| A02 | Cryptographic Failures | CWE-325: Missing Cryptographic Step |
| A03 | Injection | CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') |
| A04 | Insecure Design | CWE-257: Storing Passwords in a Recoverable Format |
| A05 | Security Misconfiguration | CWE-11: ASP.NET Misconfiguration: Creating Debug Binary |
| A06 | Vulnerable and Outdated Components | CWE-1104: Use of Unmaintained Third Party Components |
| A07 | [Identification and Authentication Failures](https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/) | CWE-290: Authentication Bypass by Spoofing |
| A08 | Software and Data Integrity Failures | CWE-494: Download of Code Without Integrity Check |
| A09 | Security Logging and Monitoring Failures | CWE-532: Insertion of Sensitive Information into Log File |
| A10 | Server-Side Request Forgery | CWE-918: Server-Side Request Forgery (SSRF) |

1. **Vulnerability Details – CWE**

**1 . Vulnerability Name**: Exposure of Sensitive Information to an Unauthorized Actor

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

**OWASP Category**: A01:2021 – Broken Access Control

**Description**: The product reveals confidential data to an entity that lacks explicit authorization to access such information.

**Business Impact**: The exposure of sensitive information to an unauthorized actor can have severe business consequences, including potential legal liabilities, loss of customer trust, financial penalties, and a negative impact on the company's brand reputation. This breach could also disrupt normal operations, require costly mitigation efforts, and necessitate implementing stricter security measures to prevent future incidents.

**2 . Vulnerability Name**: Missing Cryptographic Step

**CWE** : CWE-325: Missing Cryptographic Step

**OWASP Category**: A02:2021 –Cryptographic Failures

**Description**: The product does not implement a required step in a cryptographic algorithm, resulting in weaker encryption than advertised by the algorithm.

**Business Impact**: A missing cryptographic step in a process or system can result in compromised data integrity and confidentiality. This vulnerability might lead to unauthorized access, data manipulation, and breaches, potentially causing substantial financial losses, legal liabilities, damaged customer trust, and harm to the company's reputation. Rapid remediation and security enhancement measures would be imperative to address such a critical lapse.

**3 . Vulnerability Name**: Improper Neutralization of Special Elements used in a Command

**CWE** : CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

**OWASP Category**: A03:2021 –Injection

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

**Business Impact**: Failing to properly neutralize special elements within a command can have serious business ramifications. This vulnerability may allow attackers to execute malicious commands, potentially leading to unauthorized data exposure, system disruption, and even complete compromise. As a result, sensitive information might be stolen, operations could be severely impacted, customer trust could erode, and the company could face financial losses, legal actions, and reputational damage. Swift corrective actions and reinforced security protocols would be essential to mitigate this risk effectively.

**4 . Vulnerability Name**: Storing Passwords in a Recoverable Format

**CWE** : CWE-257: Storing Passwords in a Recoverable Format

**OWASP Category**: A04:2021 – Insecure Design

**Description**: The storage of passwords in a recoverable format makes them subject to password reuse attacks by malicious users. In fact, it should be noted that recoverable encrypted passwords provide no significant benefit over plaintext passwords since they are subject not only to reuse by malicious attackers but also by malicious insiders. If a system administrator can recover a password directly, or use a brute force search on the available information, the administrator can use the password on other accounts.

**Business Impact**: Storing passwords in a recoverable format poses significant business risks. If such a vulnerability is exploited, it could lead to unauthorized access, data breaches, and compromised user accounts. This breach of security might result in legal consequences, loss of customer trust, financial penalties, and reputational harm for the company. Ensuring passwords are securely hashed and encrypted is crucial to prevent these potential consequences and maintain a strong security posture.

**5 . Vulnerability Name**: ASP.NET Misconfiguration: Creating Debug Binary

**CWE** : CWE-11: ASP.NET Misconfiguration: Creating Debug Binary

**OWASP Category**: A05:2021 – Security Misconfiguration

**Description**: Debugging messages help attackers learn about the system and plan a form of attack.

**Business Impact**: This oversight may expose sensitive source code and internal system details, making it easier for attackers to identify vulnerabilities and potentially leading to unauthorized system access and data breaches. The resulting consequences could include intellectual property theft, customer data exposure, operational disruptions, legal liabilities, financial losses, and damage to the company's reputation. It is vital to ensure proper configuration and deployment practices to mitigate these risks effectively.

**6. Vulnerability Name**: Use of Unmaintained Third Party Components

**CWE** : CWE-1104: Use of Unmaintained Third Party Components

**OWASP Category**: A06:2021 – Vulnerable and Outdated Components

**Description**: The product relies on third-party components that are not actively supported or maintained by the original developer or a trusted proxy for the original developer.

**Business Impact**: These components may contain vulnerabilities that can be exploited by attackers, potentially leading to security breaches, data compromises, and system failures. Such incidents could result in financial losses, regulatory non-compliance, legal actions, erosion of customer trust, and damage to the company's reputation. Regularly updating and monitoring third-party components is crucial to minimize these risks and maintain a robust security posture.

**7. Vulnerability Name**: Authentication Bypass by Spoofing

**CWE** : CWE-290: Authentication Bypass by Spoofing

**OWASP Category**: A07:2021 – [Identification and Authentication Failures](https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/)

**Description**: This attack-focused weakness is caused by incorrectly implemented authentication schemes that are subject to spoofing attacks.

**Business Impact**: Attackers exploiting this vulnerability can gain unauthorized access to systems, applications, or data by disguising their identity. This could lead to data breaches, compromised user accounts, unauthorized transactions, and even system manipulation or disruption. The resulting impact might include financial losses, regulatory penalties, legal liabilities, customer distrust, and damage to the company's reputation. Implementing strong authentication mechanisms and continuous monitoring are essential to prevent and mitigate the risks associated with authentication spoofing.

**8. Vulnerability Name**: Download of Code Without Integrity Check

**CWE** : CWE-494: Download of Code Without Integrity Check

**OWASP Category**: A08:2021 – Software and Data Integrity Failures

**Description**: The product downloads source code or an executable from a remote location and executes the code without sufficiently verifying the origin and integrity of the code.

**Business Impact**: This vulnerability exposes systems to the risk of malicious code injection, which can lead to unauthorized access, data breaches, system instability, and compromised functionalities. These outcomes could result in financial losses, regulatory violations, legal liabilities, reputational damage, and erosion of customer trust. Ensuring robust code validation and integrity checks before downloading is crucial to mitigate potential risks and uphold a strong security posture.

**9. Vulnerability Name**: Insertion of Sensitive Information into Log File

**CWE** : CWE-532: Insertion of Sensitive Information into Log File

**OWASP Category**: A09:2021 – Security Logging and Monitoring Failures

**Description**: Information written to log files can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information.

**Business Impact**: This lapse could expose confidential data, such as user credentials or proprietary details, potentially leading to unauthorized access, data breaches, and regulatory non-compliance. These consequences might result in financial losses, legal liabilities, tarnished reputation, and erosion of customer trust. Implementing proper log management practices, including sanitization of sensitive information, is crucial to mitigate these risks and maintain data security and compliance.

**10. Vulnerability Name**: Server-Side Request Forgery (SSRF)

**CWE** : CWE-918: Server-Side Request Forgery (SSRF)

**OWASP Category**: A10:2021 – Server-Side Request Forgery

**Description**: The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.

**Business Impact**: Attackers exploiting SSRF can manipulate a server into making unauthorized requests to other internal resources or external services, potentially leading to data breaches, unauthorized access, and even remote code execution. This could result in compromised systems, customer data exposure, financial losses, regulatory penalties, legal actions, and damage to the company's reputation. Implementing robust input validation, network segmentation, and security controls is critical to preventing and mitigating the risks associated with SSRF vulnerabilities.