**Overview**

Table

|  |  |  |
| --- | --- | --- |
| **S.No** | **Vulnerability Name** | **CWE** |
| A01 | Broken Access Control | CWE-284: Improper Access Control |
| A02 | Cryptographic Failures | CWE CATEGORY:310 Cryptographic Issues |
| A03 | Injection | CWE-94: Improper Control of Generation of Code ('Code Injection') |
| A04 | Insecure Design | CWE-657: Violation of Secure Design Principles |
| A05 | Security Misconfiguration | CWE CATEGORY: 16 Configuration |
| A06 | Vulnerable and Outdated Compnents | CWE-1395: Dependency on Vulnerable Third-Party Component |
| A07 | Identification and Authentication Failures | CWE-287: Improper Authentication |
| A08 | Software and Data Integrity Failures | CWE CATEGORY: 1214 Data Integrity Issues |
| A09 | Security Logging and Monitoring Failures | CWE-778: Insufficient Logging |
| A10 | Server-Side Request Forgery | CWE-918: Server-Side Request Forgery (SSRF) |

**Report**

1. 1.1 Vulnerability Name: Cross-Site Scripting(stored)

**CWE – CWE 284**

**OWASP Category:** Broken Access Control

**Description**

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

**Business Impact**

In scenarios where protective mechanisms are absent or ineffective, malicious actors can exploit vulnerabilities to compromise product security, potentially gaining unauthorized privileges, extracting sensitive data, executing arbitrary commands, or bypassing detection measures. These security breaches primarily stem from two distinguishable behaviors—specification and enforcement issues—in the access control framework. Specification-related weaknesses arise from inaccuracies in defining access control requirements, while enforcement-related weaknesses result from errors within the mechanisms responsible for upholding the specified access controls.

**Regenerate**

1. **2.1** Vulnerability Name: CWE CATEGORY:310 Cryptographic Issues

**CWE – CWE 310**

**OWASP Category:** Cryptographic Failures

**Description**

Weaknesses in this category are related to the design and implementation of data confidentiality and integrity. The weaknesses in this category could lead to a degradation of the quality data if they are not addressed.

**Business Impact**

The weaknesses in this category could lead to a degradation of the quality data if they are not addressed. Such weaknesses can undermine the confidentiality, integrity, and authenticity of sensitive data and communications within an organization's operations. Malicious actors exploiting cryptographic vulnerabilities could potentially gain unauthorized access to sensitive information, compromise the privacy of customers or users, and lead to data breaches with severe legal, financial, and reputational consequences. Additionally, these vulnerabilities might enable attackers to manipulate transactional or operational data, causing disruptions in business processes and financial losses.

1. **3.1** Vulnerability Name: CWE-94: Improper Control of Generation of Code ('Code Injection')

**CWE – CWE 94**

**OWASP Category: 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 behaviour of the intended code segment.

**Business Impact**

When a product permits user input to include code syntax, there's a potential for attackers to construct code that manipulates the product's intended control flow. This manipulation could ultimately result in the execution of arbitrary code. Injection issues span a broad range of problems, each requiring unique mitigation approaches. Therefore, the most efficient approach to addressing these vulnerabilities is to highlight the specific characteristics that categorize them as injection weaknesses.

1. **4.1** Vulnerability Name: CWE-657: Violation of Secure Design Principles

**CWE – CWE 657**

**OWASP Category: Insecure Design**

**Description**

The product violates well-established principles for secure design.

**Business Impact**

Violating secure design principles can result in serious business consequences. Such vulnerabilities compromise system integrity, opening the door to unauthorized data access, functional disruptions, and manipulation by malicious actors. This can lead to legal penalties, reputation damage, and financial losses due to breach investigations, system downtime, and resource redirection. By prioritizing secure design, businesses can mitigate these risks, fostering resilient systems that protect sensitive data and support uninterrupted operations.

1. **5.1** Vulnerability Name: CWE CATEGORY: 16 Configuration

**CWE – CWE 16**

**OWASP Category:** Security Misconfiguration

**Description**

Weaknesses in this category are typically introduced during the configuration of the software.

**Business Impact**

This entry is a Category, but various sources map to it anyway, despite CWE guidance that Categories should not be mapped. In this case, there are no clear CWE Weaknesses that can be utilized. "Inappropriate Configuration" sounds more like a Weakness in CWE's style, but it still does not indicate actual behavior of the product. Further research is still required, however, as a "configuration weakness" might be Primary to many other CWEs, i.e., it might be better described in terms of chaining relationships.

1. **6.1** Vulnerability Name: CWE-1395: Dependency on Vulnerable Third-Party Component

**CWE – CWE 1395**

**OWASP Category:** Vulnerable and Outdated Compnents

**Description**

The product has a dependency on a third-party component that contains one or more known vulnerabilities.

**Business Impact**

Dependency on vulnerable third-party components carries significant business risks. Such dependencies create openings for security breaches and operational disturbances. Exploiting component vulnerabilities could grant unauthorized data access, disrupt systems, and trigger broader attacks. This may result in substantial financial losses due to fines, investigations, and legal actions, alongside reputation damage and customer trust erosion. Mitigating these impacts requires vigilant monitoring and management of third-party dependencies to ensure a secure and uninterrupted business environment.

1. **7.1** Vulnerability Name: CWE-287: Improper Authentication

**CWE – CWE 287**

**OWASP Category:** Identification and Authentication Failures

**Description**

When an actor claims to have a given identity, the product does not prove or insufficiently proves that the claim is correct.

**Business Impact**

Inadequate authentication mechanisms can allow unauthorized access to sensitive systems, applications, and data. This poses a serious risk of data breaches, where attackers could potentially steal or manipulate valuable information, compromising customer privacy and business integrity. Such breaches can lead to regulatory penalties, legal liabilities, and reputational damage. Moreover, unauthorized access can disrupt critical operations, resulting in downtime and financial losses. To mitigate these risks, robust authentication processes are essential to ensure only authorized individuals can access resources, protecting both the organization and its stakeholders.

1. **8.1** Vulnerability Name: CWE CATEGORY: 1214 Data Integrity Issues

**CWE – CWE 1214**

**OWASP Category:** Software and Data Integrity Failures

**Description**

Weaknesses in this category are related to a software system's data integrity components. Frequently these deal with the ability to ensure the integrity of data, such as messages, resource files, deployment files, and configuration files. The weaknesses in this category could lead to a degradation of data integrity quality if they are not addressed.

**Business Impact**

Data integrity issues have far-reaching business impacts. When data accuracy is compromised, it can trigger decision-making errors, disrupt operations, and disappoint customers. In regulated industries, integrity breaches lead to fines and legal consequences. Trust in the organization is eroded, affecting its reputation. Fixing such problems demands resources and time, sidetracking essential tasks. To counter these effects, strong data validation and access controls are essential to ensure operational smoothness and credibility.

1. **9.1** Vulnerability Name: CWE-778: Insufficient Logging

**CWE – CWE 778**

**OWASP Category:** CWE-778: Insufficient Logging

**Description**

When a security-critical event occurs, the product either does not record the event or omits important details about the event when logging it.

**Business Impact**

Insufficient logging has significant business implications. It delays the detection of security issues, making it harder to respond to unauthorized access, breaches, and malicious actions. This can lead to regulatory fines, prolonged damage containment, and compromised compliance. The absence of comprehensive logs also hampers post-incident analysis, hindering the organization's ability to learn and improve. To address this, strong logging practices are essential for effective threat detection, incident response, and maintaining security.

1. **10.1** Vulnerability Name: CWE-918: Server-Side Request Forgery (SSRF)

**CWE – CWE 918**

**OWASP Category:** Server-Side Request Forgery

**Description**

Server-side request forgery or SSRF leverages the ability of a web application to perform unauthorized requests to internal or external systems. If the web application contains functionality that sends requests to other servers and the attacker can interfere with it, it is possible to turn your web server into a proxy.

**Business Impact**

Server-Side Request Forgery (SSRF) vulnerability has significant business consequences. It enables attackers to access internal resources, potentially causing data exposure, remote code execution, and service disruptions. Breaches lead to compromised information, legal issues, and regulatory fines, especially in finance and healthcare. The attacks can cascade into more breaches, prolonging downtime, financial losses, and reputation harm. Mitigation involves strong input validation, network safeguards, and vigilant monitoring to prevent SSRF and its wide-ranging impacts.