Assignment - 1:

S.no	Name of Vulnerability	CWE Reference
1.	Broken Access Control	CWE 284- Improper Access Control
2.	Cryptographic Failures	CWE 327- Use of a broken or risky cryptographic algorithm
3.	Injection	CWE 91: XML Injection (aka Blind XPath Injection)
4.	Insecure Design	CWE 657 – Violation of Secure Design Principles
5.	Security Misconfiguration	CWE 732- Incorrect permission Assignment for critical resource

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 Scenarios the permissions and resources for any services are given access to the authorized users only. If improper access control exists, unauthorized users may gain access to sensitive or confidential information that they should not have access to. This could result in the exposure of sensitive customer data, proprietary business information, financial records, or any other confidential data that the organization handles. This unauthorized access or data exposure can have a several consequences for business including, reputation damage, Legal and regulatory consequences, financial loss, competitive disadvantage, operational disreputation, customer impact.

2. **CWE: CWE 327- Use of a broken or risky cryptographic algorithm**

   OWASP Category: A02 2021 Cryptographic Failure.

   Description: The product uses a risky or broken cryptographic algorithm or protocol.

   Business Impact: Using a non-standard or well-known insecure algorithm is dangerous because a determined adversary may be able to break the algorithm and compromise whatever data has been protected. When an organisation uses cryptographic algorithms that are broken or known to be risky, it opens the door to potential security breaches and data loss. Here is how this vulnerability can impact a business-like data exposure, loss of trust, competitive disadvantage etc.

3. CWE: CWE 91: XML Injection (aka Blind XPath Injection)

OWASP A03 2021 Injection

Description: The product does not properly neutralize special elements that are used in XML, allowing attackers to modify the syntax, content, or commands of the XML before it is processed by an end system.

Business Impact: Hackers uses XML injection, within XML, special elements could include reserved words or characters like “<", ">", """, and "&", which could then be used to add new data or modify XML syntax. So when an XML injection vulnerability exists in an application, it can have significant repercussions for a business including Data Manipulation, Un authorized Access, Application Disruption, Financial Loss etc.

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

OWASP Category: A04 2021 – Insecure Design

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

Business Impact: If a company or organisation violates the design principles this will results in a weakness or make it easier for the developers to introduce related weaknesses during implementation. Because the entire security and core part is centred around the design architecture of that application. If a hacker breaches its deign it can be resource intensive to fix design problems. When an application or system violates secure design principles, it can have several adverse effects on a business-like Security vulnerability, Data breaches, Reputation Damage, regulatory nan compliance, Increased development and maintenance costs, loss of competitive advantages. Etc.

5. CWE: CWE 732- Incorrect permission Assignment for critical resource

OWASP Category: A05 2021- Security Misconfigurations

Description: The product specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors.

Business Impact: When a resource is given a permission setting that provides access to a wider range of actors than required, it could lead to the exposure of sensitive information, or the modification of that resource by unintended parties. This is especially dangerous when the resource is related to program configuration, execution, or sensitive user data. For example, consider a misconfigured storage account for the cloud that can be read or written by a public or anonymous user.