**TASK-3**

**OWASP TOP 10 CWE DETAILS AND BUSINESS IMPACT**

**1)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:**Access control involves the use of several protection mechanisms such as:Authentication (proving the identity of an actor),Authorization (ensuring that a given actor can access a resource), and Accountability (tracking of activities that were performed).If suppose a unauthorized actor came to see the resources if any of the above mechanism is not applied or otherwise fails ,then they are giving chance to the attackers.This can leads to compromise the security of the product by gaining privileges, reading sensitive information, executing commands, evading detection.

**2)CWE-261: Weak Encoding for Password**

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

**Description:**Obscuring a password with a trivial encoding does not protect the password.

**Business Impact:** Basically passwords are some of the most commonly used authentication mechanisms. To authenticate to a system/application, a user provides a password, which is compared to a value stored on the server. If the two values match, then the user is granted access. Otherwise, access is denied.Password encoding can go wrong in some ways like when the passwords are stored in plain text,using simple encoding algorithms like Base64 which is reversible that means we can decode the original value and use of weak hash algorithms that can be exploited by brute force attacks .This can lead to sensitive data exposure or system compromise.

**3)CWE-20: Improper Input Validation**

**OWASP Category:** A03:2021-Injection

**Description:**The product receives input or data, but it does not validate or incorrectly validates that the input has the properties that are required to process the data safely and correctly.

**Business Impact:** The failure to properly validate or sanitize input data from untrusted sources before using it in a software system leads to parts of the system receiving unintended input, which may result in altered control flow, arbitrary control of a resource, or arbitrary code execution. This can lead to a range of security vulnerabilities which include security breaches, unauthorized access, disruptions to application functionality, privacy violations by exposing user information, legal and regulatory penalties due to mishandling of data, reputational damage, and resource consumption through attacks like Denial of Service (DoS) .

**4)CWE-602: Client-Side Enforcement of Server-Side Security**

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

**Description:**The product is composed of a server that relies on the client to implement a mechanism that is intended to protect the server.

**Business Impact:**When the server relies on protection mechanisms placed on the client side, an attacker can modify the client-side behavior to bypass the protection mechanisms resulting in potentially unexpected interactions between the client and server**.** When critical security decisions are made on the client side, data integrity can be compromised. If a messaging app relies solely on the client to determine message recipients, attackers can manipulate the client to send messages to unintended recipients, causing miscommunication or privacy breaches.This can lead to loss of data integrity,data breaches and reduced security control.

**5)CWE-547: Use of Hard-coded, Security-relevant Constants**

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

**Description:**The product uses hard-coded constants instead of symbolic names for security-critical values, which increases the likelihood of mistakes during code maintenance or security policy change.

**Business Impact:**Relying on hard-coded values for security has some limitations on flexibility, complicating updates, increasing vulnerability to attacks, and potentially exposing sensitive data. .