Task-3 25-08-23 Friday Sameer Chauhan 21BCE0999

**OWASP-TOP 5 APPLICATION SECURITY RISK**

**1-CWE: 863-Incorrect Authorization**

**OWASP CATEGORY : A01 2021 Broken Access Control**

DESCRIPTION-The product performs an authorization check when an actor attempts to access a resource or perform an action, but it does not correctly perform the check. This allows attackers to bypass intended access restrictions.

BUSINESS IMPACT: Assuming a user with a given identity, authorization is the process of determining whether that user can access a given resource, based on the user's privileges and any permissions or other access-control specifications that apply to the resource.

When access control checks are incorrectly applied, users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information exposures, for example -our college vit is having its website which have attendance portal which can be accessed only by faculty but if there is incorrect authorization student may able to access it illegaly and may update their attendance

## 2. CWE-326 Inadequate Encryption Strength

OWASP CATEGORY : A02 2021 Cryptographic Failures

DESCRIPTION: The product stores or transmits sensitive data using an encryption scheme that is theoretically sound, but is not strong enough for the level of protection required.

BUSINESS IMPACT: IT may have major business impact which can vary from loss of customer trust,to non compliance issues and financial losses for example-a company may have sensitive information of their customers such as adhar number or credit card details but if the encryption strength is not good enough it will be vulnerable to brute force attacks and guesses so data is not safe and may leak .

## 3. CWE-94: Improper Control of Generation of Code ('Code Injection')

OWASP CATEGORY : A03 2021 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 behavior of the intended code segment.

BUSINESS IMPACT: Code injection vulnerabilities can allow attackers to insert their own code into your application. This can lead to unauthorized access to sensitive data, like customer information, financial records, and trade secrets.for example-if I am entering script ‘or 1=1—in the username in amazon which automatically bypass the password so in this way we are able to bypass and enter which may lead to steal of sensitive data hence lead to loss of customer trust of the respective web application

## 4- 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: The business impacts of violating secure design principles (CWE-657) can be substantial, affecting various aspects of an organization's operations, reputation, and security posture.for example-Violating secure design principles can lead to the introduction of security vulnerabilities and weaknesses in software systems, making them more susceptible to exploitation by malicious actors

**5- CWE: CWE 614-Sensitive Cookie in HTTPS Session Without**

**'Secure' Attribute**

OWASP CATEGORY : A05 2021 Security Misconfiguration

DESCRIPTION: The Secure attribute for sensitive cookies in HTTPS

sessions is not set, which could cause the user agent to send those cookies

in plaintext over an HTTP session.

BUSINESS IMPACT:for example you visit a website and it sends you a piece of data known as cookie it stores our information such as login credtionals and preferences .our sensitive information must be sent over secure https connection which means that our data is reached from server to browser securely and not exposed to hackers but a problem can occur here as website fails to add a attribute secure to our cookie without this the browser may sent our cookie over unencrypted https connection thus exposing it to hackers