Assignment #1

NAME- LOVE YADAV   REG - 21BCB0120

List of Vulnerable Parameter, location discovered

S.No	Name of the Vulnerability	Reference CWE
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-564: SQL Injection: Hibernate**
4	Insecure Design	**CWE-657: Violation of Secure Design Principles**

5	Security Misconfiguration	**CWE 614-Sensitive Cookie in HTTPS Session Without 'Secure' Attribute**

1. CWE: CWE-284: Improper Access Control

Description

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

BUSINESS IMPACT:

Improper Access Control is a significant security vulnerability that can have profound business impacts. It occurs when an application or system fails to enforce appropriate access controls, allowing unauthorized users to access sensitive resources or perform actions they shouldn't have permission to do. The business impact includes data breaches, financial losses, regulatory non-compliance, reputation damage, intellectual property theft, operational disruption, legal consequences, resource misuse, loss of business opportunities, long-term impact, intellectual property theft, and privacy violations. To mitigate the business impact of Improper Access Control, organizations should implement robust access controls, conduct regular security assessments, provide security training for developers, and follow secure coding practices. Security audits, penetration testing, and ongoing monitoring are essential to identify and rectify access control weaknesses before they are exploited.

2. CWE:CWE-327: Use of a Broken or Risky Cryptographic Algorithm

Description

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

BUSINESS IMPACT:

CWE-327 refers to the use of vulnerable, weak, or compromised cryptographic algorithms, which can have significant business impacts. These vulnerabilities can lead to data breaches, loss of confidentiality, regulatory non-compliance, privacy violations, financial losses, reputation damage, intellectual property theft, operational disruptions, long-term consequences, technical debt, and customer and partner confidence loss. To mitigate these risks, organizations should use strong, well-vetted cryptographic algorithms, stay informed about the latest vulnerabilities, and regularly update their encryption practices. Regular security assessments, including penetration testing, can help identify and rectify cryptographic weaknesses before they are exploited by malicious actors. By implementing security standards and conducting regular assessments, organizations can protect sensitive information and avoid long-term consequences.

3 CWE .CWE-564: SQL Injection: Hibernate

Description

Using Hibernate to execute a dynamic SQL statement built with user-controlled input can allow an attacker to modify the statement's meaning or to execute arbitrary SQL commands.

Hackers use SQL injection attacks to access sensitive business or personally identifiable information (PII), which ultimately increases sensitive data exposure. Using SQL injection, attackers can retrieve and alter data, which risks exposing sensitive company data stored on the SQL server. Compromise Users' Privacy: Depending on the data stored on the SQL server, an attack can expose private user data, such as credit card numbers.

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

Description

The product violates well-established principles for secure design

BUSINESS IMPACT:

CWE-657 refers to security vulnerabilities in software or systems that arise when developers fail to adhere to established security principles. This can have significant business impacts, including increased vulnerabilities, data breaches, regulatory non-compliance, reputational damage, financial losses, long-term impact, increased development costs, delayed time-to-market, intellectual property theft, lack of competitive advantage, operational disruptions, and legal consequences. To mitigate the business impact of CWE-657, organizations should prioritize secure design principles from the outset of software development, conduct security reviews, and adhere to best practices. Regular security assessments, threat modeling, and employee training are essential to identify and address design-related security weaknesses before they are exploited.

5.CWE: CWE 614-Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

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:

Security misconfigurations allow attackers to gain unauthorized access to networks, systems and data, which in turn can cause significant monetary and reputational damage to your organization.