AI FOR CYBERSECURITY

ASSIGNMENT – 1

Name:V.Y.Koushik

Reg.No:21BCE9368

1. CWE: CWE 285- Improper Authorization

OWASP CATEGORY : A01 2021 Broken Access Control

DESCRIPTION: The product does not perform or incorrectly performs anauthorization check when an actor attempts to access a resource or performan action.

BUSINESS IMPACT: Assuming a user with a given identity, authorizationis the process of determining whether that user can access a givenresource, based on the user's privileges and any permissions or otheraccess-control specifications that apply to the resource. When accesscontrol checks are not applied consistently - or not at all - users are able toaccess data or perform actions that they should not be allowed to perform.This can lead to a wide range of problems, including information exposures,denial of service, and arbitrary code execution.

2. CWE: CWE-916: Use of Password Hash With Insufficient Computational Effort

OWASP CATEGORY : A02 2021 Cryptographic Failures.

DESCRIPTION: The product generates a hash for a password, but it uses ascheme that does not provide a sufficient level of computational eort thatwould make password cracking attacks infeasible or expensive.

BUSINESS IMPACT: In this design, authentication involves accepting anincoming password, computing its hash, and comparing it to the storedhash. After an attacker has acquired stored password hashes, they arealways able to brute force hashes o line. As a defender, it is only possibleto slow down offline attacks by selecting hash algorithms that are asresource intensive as possible.

3. CWE: CWE 564: SQL Injection: Hibernate

OWASP CATEGORY : A03 2021 Injection

DESCRIPTION : Using Hibernate to execute a dynamic SQL statement builtwith usercontrolled input can allow an attacker to modify the statement'smeaning or to execute arbitrary SQL commands.

BUSINESS IMPACT: Hackers use SQL injection attacks to access sensitivebusiness or personally identifiable information (PII), which ultimatelyincreases sensitive data exposure. Using SQL injection, attackers canretrieve and alter data, which risks exposing sensitive company data storedon the SQL server. Compromise Users' Privacy: Depending on the datastored on the SQL server, an attack can expose private user data, such ascredit card numbers.

4. CWE: CWE 653: Improper Isolation or Compartmentalization

OWASP CATEGORY : A04 2021 Insecure Design

DESCRIPTION: The product violates well-established principles for securedesign.This can introduce resultant weaknesses or make it easier fordevelopers to introduce related weaknesses during implementation.Because code is centered around design, it can be resource-intensive to fixdesign problems.

BUSINESS IMPACT: Insecure system configuration risks stem from flawsin the security settings, configuration and hardening of the di erentsystems across the pipeline (e.g. SCM, CI, Artifact repository), oftenresulting in "low hanging fruits" for attackers looking to expand theirfoothold in the environment.

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 HTTPSsessions is not set, which could cause the user agent to send those cookiesin plaintext over an HTTP session.

BUSINESS IMPACT: Security misconfigurations allow attackers to gainunauthorized access to networks, systems and data, which in turn cancause significant monetary and reputational damage to your organization.