AI FOR CYBERSECURITY
ASSIGNMENT - 01

NAME: Nikhil Sri Harsha

Reg.no:21BCE8711

1. CWE: CWE 285- Improper Authorization

OWASP CATEGORY: A01 2021 Broken Access Control

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

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 not applied consistently – or not at all – users are able to access dataor 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 Insumcient Computational Effort

OWASP CATEGORY: A02 2021 Cryptographic Failures.

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

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

3. CWE: CWE 564: SQL Injection: Hibernate

OWASP CATEGORY: A03 2021 Injection

DESCRIPTION: Using Hibernate to execute a dynamic SQL statement built with user-controlled input can allow an attacker to modify the statement or executearbitrary SQL commands.

BUSINESS IMPACT: 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 653: Improper Isolation or Compartmentalization

OWASP CATEGORY: A04 2021 Insecure Design

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

BUSINESS IMPACT: Insecure system configuration risks stem from flawsin the security settings, configuration, and hardening of the different systems across the pipeline (e.g., SCM, CI, Artifact repository), often resulting in “low-hanging fruits” for attackers looking to expandtheir foothold 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 HTTPS sessions is not set, whichcould 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.