Task – 3

AI for Cyber Security

OWASP Top 5

1. **OWASP CATEGORY: A01 2021 Broken Access Control**
   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," represents a significant threat to businesses. This vulnerability arises when systems fail to enforce proper restrictions on user access to resources. Exploiting this flaw can lead to unauthorized data exposure, alterations, or even complete system compromise. Business consequences include breaches of sensitive information, loss of intellectual property, regulatory penalties, legal actions, erosion of customer trust, and reputational damage. Additionally, addressing this issue demands substantial investments in code review, security architecture, and access management solutions, diverting resources from core business activities and hindering innovation while striving to ensure robust access controls.

2. **OWASP CATEGORY: A02 2021 Cryptographic Failures**
   CWE-259: Use of Hard-coded Password

Description:

The product contains a hard-coded password, which it uses for its own inbound authentication or for outbound communication to external components.

Business Impact:

"Use of Hard-coded Password," poses a substantial business risk by embedding passwords directly into code or configuration files. This practice can lead to unauthorized access, data breaches, and compromised systems. If exploited, attackers can gain control over critical assets, manipulate sensitive data, disrupt operations, and compromise customer trust.

Business impact includes financial losses due to data loss or theft, regulatory fines for non-compliance, legal liabilities, reputational damage, and operational downtime. Mitigation efforts require resources for code review, password management, and system updates, impacting development timelines and diverting focus from innovation to security remediation.

3. OWASP CATEGORY: A03 2021 Injection
CWE-94: Improper Control of Generation of Code ('Code 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:

"Improper Control of Generation of Code ('Code Injection')," poses a grave risk to businesses. It occurs when software systems allow untrusted data to influence code execution, enabling attackers to inject malicious code. Exploiting this vulnerability can lead to unauthorized access, data breaches, system compromise, and unauthorized actions. The business impact includes financial losses due to data theft, operational disruption, regulatory fines, legal liabilities, damaged reputation, and erosion of customer trust. Mitigation requires rigorous code review, input validation, and secure coding practices, diverting resources from development and innovation toward addressing security vulnerabilities, slowing down progress and potentially affecting time-to-market goals.

4. OWASP CATEGORY: A04 2021 Insecure Design
CWE-657: Violation of Secure Design Principles

Description:

The product violates well-established principles for secure design.

Business Impact:

"Violation of Secure Design Principles," presents a critical risk to businesses. This vulnerability emerges when software systems are developed without following established security best practices and design principles. As a result, applications become susceptible to various attacks and breaches. Exploiting this flaw can lead to unauthorized access, data breaches, system compromise, and operational disruptions. The business impact encompasses financial losses, regulatory penalties, legal actions, reputational damage, erosion of customer trust, and increased security-related development costs. Addressing this issue necessitates reevaluating and retrofitting the software's design, diverting resources from innovation and development efforts, potentially delaying project timelines and undermining competitiveness.

5. OWASP CATEGORY: A05 2021 Security Misconfiguration

CWE-11: ASP.NET Misconfiguration: Creating Debug Binary

Description:

Debugging messages help attackers learn about the system and plan a form of attack.

Business Impact:

"ASP.NET Misconfiguration: Creating Debug Binary," poses a significant threat to businesses relying on ASP.NET applications. This vulnerability arises when debug information is left within binary files deployed in production environments. Exploiting this flaw allows attackers to gain insights into the application's inner workings, potentially leading to unauthorized access, data exposure, and system compromise. The business impact includes compromised intellectual property, sensitive data breaches, regulatory non-compliance, legal liabilities, reputational damage, and erosion of customer trust. Mitigation efforts involve ensuring proper configuration, code review, and secure deployment practices, diverting resources from development to rectify security gaps, potentially impeding progress and innovation.