Task 3:

1. CWE: CWE-284 - Improper Access Control

OWASP CATEGORY: A01 2021 Broken Access Control

DESCRIPTION: The software does not properly restrict access to resources based on the identity of the user, allowing unauthorized users to access restricted functionality.

BUSINESS IMPACT: Insufficient access control can lead to unauthorized access to sensitive data, unauthorized modifications, and privilege escalation. These vulnerabilities can enable attackers to compromise critical systems, steal confidential information, and manipulate functionality, ultimately damaging the organization's reputation and causing financial losses. If not solved, unauthorized users might gain access to sensitive data or perform actions they're not allowed to. The security officer can implement proper access controls, role-based permissions, and input validation to mitigate this risk. Failure to do so could lead to data breaches, unauthorized actions, and regulatory non-compliance.

2. CWE: CWE-310 - Cryptographic Issues

OWASP CATEGORY: A02 2021 Cryptographic Failures

DESCRIPTION: The software uses weak or insecure cryptographic algorithms, improperly manages cryptographic keys, or has other vulnerabilities related to cryptography that can lead to data exposure or system compromise.

BUSINESS IMPACT: Cryptographic failures can result in the exposure of sensitive data, undermining data privacy and potentially leading to regulatory non-compliance. Attackers can exploit cryptographic weaknesses to decrypt sensitive information, impersonate legitimate users, and perform unauthorized actions, causing severe financial and legal consequences. To address this, the cybersecurity officer should ensure the use of strong encryption methods, key management practices, and regular cryptography audits. If not addressed, weak cryptography can lead to data breaches, unauthorized data access, and loss of trust from customers or partners.

3. CWE: CWE-89 - SQL Injection

OWASP CATEGORY: A03 2021 Injection

DESCRIPTION: The software allows malicious input to be included in SQL queries, enabling attackers to manipulate the query's logic and potentially access or modify data stored in the database.

BUSINESS IMPACT: SQL injection can lead to unauthorized data access, unauthorized data modification, and even complete data loss. Attackers can exploit this vulnerability to steal sensitive information, modify or delete critical data, disrupt business operations, and compromise the confidentiality and integrity of data, impacting the organization's credibility and trustworthiness. Solving this issue involves input validation, using prepared statements, and using parameterized queries. If unaddressed, injection vulnerabilities can lead to data breaches, unauthorized access, and potential system compromise.

4. CWE: CWE-799 - Improper Control of Interaction Frequency

OWASP CATEGORY: A04 2021 Insecure Design

DESCRIPTION: The software does not properly control the frequency or rate of interactions with a resource, leading to vulnerabilities that attackers can exploit to disrupt or compromise the system.

BUSINESS IMPACT: Insecure design can result in denial-of-service (DoS) attacks, system instability, and unavailability of services. Attackers can exploit these vulnerabilities to overload systems, interrupt critical services, and degrade user experience, leading to operational disruptions, loss of customer trust, and potential financial losses. To mitigate, cybersecurity officers can promote threat modeling, secure design patterns, and reference architectures. If not solved, design flaws can result in insecure software, increased vulnerabilities, and potential exploits.

5. CWE: CWE-16 - Configuration

OWASP CATEGORY: A05 2021 Security Misconfiguration

DESCRIPTION: The software's configuration settings are insecure or incomplete, allowing attackers to exploit weaknesses in the system's configuration and gain unauthorized access or control.

BUSINESS IMPACT: Security misconfigurations can lead to unauthorized data access, exposure of sensitive information, and unauthorized system manipulation. Attackers can leverage these misconfigurations to breach data privacy, modify system behavior, and compromise the confidentiality and integrity of information, resulting in legal liabilities, reputational damage, and financial penalties. To address this, security officers must follow best practices, use secure default settings, and regularly audit configurations. If not addressed, misconfigurations can lead to data leaks, compliance violations, and reputational damage.