AI FOR CYBER SECURITY WITH IBM QRADAR

Name: J. Manasa

TASK-3: Vulnerabilities of first 5 OWASP categories

1. CWE: CWE-377- Insecure Temporary File
OWASP CATEGORY: A01 2021-Broken Access Control
DESCRIPTION: Creating and using insecure temporary files can leave application and system data vulnerable to attack.

BUSINESS IMPACT: If temporary files containing sensitive information (such as login credentials, financial data, or personal information) are accessible by unauthorized individuals, it can lead to data breaches, unauthorized access, identity theft, financial loss, and damage to an organization's reputation. Attackers could exploit these insecure files to gain insights into the system's operation or extract sensitive data, leading to legal and financial consequences for the organization. Proper handling and secure management of temporary files are essential to prevent this type of vulnerability.

2. CWE: CWE-322: Key Exchange without Entity Authentication
OWASP CATEGORY: A02 2021-Cryptographic Failures
DESCRIPTION: The product performs a key exchange with an actor without verifying the identity of that actor.

BUSINESS IMPACT: Without proper entity authentication during key exchange, malicious actors can impersonate legitimate parties and gain unauthorized access to encrypted communication or sensitive data. This could result in data breaches, unauthorized information disclosure, compromised system integrity, and loss of trust among users or clients. Proper entity authentication in key exchange protocols is crucial for maintaining the confidentiality and integrity of communication, as well as safeguarding critical business information.

3. CWE: CWE-116: Improper Encoding or Escaping of Output
OWASP CATEGORY: A03 2021-Injection
DESCRIPTION: The product prepares a structured message for communication with another component, but encoding or escaping of the data is either missing or done incorrectly. As a result, the intended structure of the message is not preserved.

BUSINESS IMPACT: If output data is not properly encoded or escaped, attackers can inject malicious code (such as scripts or SQL queries) into the output, leading to cross-site scripting (XSS) attacks, SQL injection attacks, and other forms of data manipulation. This can result in unauthorized access, data theft, defacement of websites, disruption of services, and damage to the organization's reputation. Addressing this weakness is crucial to ensuring the security of applications and protecting sensitive user data from exploitation.

4. CWE: CWE-525: Use of Web Browser Cache Containing Sensitive Information
OWASP CATEGORY: A04 2021 -Insecure Design
DESCRIPTION: The web application does not use an appropriate caching policy that specifies the extent to which each web page and associated form fields should be cached.

BUSINESS IMPACT: If sensitive information, such as login credentials, personal data, or financial details, is cached in a web browser and not properly managed, unauthorized users could gain access to this data by compromising the browser cache. This can lead to identity theft, unauthorized account access, financial fraud, and a breach of privacy for users. The organization's reputation may suffer, and legal and regulatory consequences could arise due to the mishandling of sensitive data. Proper cache management and secure handling of sensitive information are essential to mitigate this risk.

5. CWE: CWE-260: Password in Configuration File
OWASP CATEGORY: A05 2021 -Insecure Design
DESCRIPTION: The product stores a password in a configuration file that might be accessible to actors who do not know the password.

BUSINESS IMPACT: Storing passwords in plain text configuration files can lead to unauthorized access, data breaches, and compromised systems. Attackers who gain access to these files can use the exposed credentials to infiltrate systems, steal sensitive data, manipulate settings, and potentially gain control over critical resources. This can result in financial loss, reputational damage, legal consequences, and the loss of trust from customers and stakeholders. Proper encryption and secure handling of credentials are crucial to prevent the exploitation of this weakness and to ensure the security of sensitive information.