AI for Cyber Security with IBM Qradar

Name: MAYANDI VARUN

Registration Number: 21BCE9893

Assignment-1

Top 5 OWASP CATEGORY : Vulnerabilities

CWE: CWE-284: Improper Access Control

OWASP CATEGORY: A01 2021 Broken Access Control

Description:

The product does not restrict or incorrectly restricts access to a resource from an unauthorized actor.

Business Impact:

Improper access control can have serious business impacts. It can lead to unauthorized access to sensitive data, data breaches, loss of intellectual property, legal and regulatory penalties, damaged reputation, customer distrust, and financial losses due to lawsuits, remediation costs, and operational disruptions, causing financial losses and legal consequences. Moreover, customer trust can erode, affecting reputation and future business.

CWE-326: Inadequate Encryption Strength

OWASP CATEGORY: A02 2021 Cryptographic Failures

Description:

The product stores or transmits sensitive data using an encryption scheme that is theoretically sound, but is not strong enough for the level of protection required.

Business Impact:

Using an encryption scheme that's theoretically secure but insufficient for necessary protection can lead to various adverse business outcomes. It heightens vulnerability to cyberattacks, increasing the likelihood of data breaches and eroding trust. Compliance with data protection regulations might be compromised, resulting in legal penalties. Financially, the fallout

encompasses direct costs like legal fees and compensation, while indirect losses arise from damaged reputation and reduced customer trust. Ultimately, such incidents tarnish a company's image.

CWE-94: Improper Control of Generation of Code ('Code Injection')

OWASP CATEGORY: A03 2021 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 code generation, often referred to as 'code injection,' can have severe consequences for software systems. It enables attackers to insert malicious code into an application, potentially leading to unauthorized access and system compromise. This can result in the theft of sensitive information, disruption of services, and even complete system takeover. Additionally, code injection vulnerabilities can damage a company's reputation and require extensive resources to identify, fix, and mitigate the impact. It's crucial for organizations to implement robust input validation, sanitize user inputs, and adhere to secure coding practices to prevent code injection attacks and safeguard their applications and users' data.

CWE-15: External Control of System or Configuration Setting

OWASP CATEGORY: A05 2021 Security Misconfiguration

Description:

Allowing external control of system settings can disrupt service or cause an application to behave in unexpected, and potentially malicious ways.

Business Impact:

External control of system or configuration settings can have significant and detrimental impacts on software and systems. It allows attackers to manipulate crucial settings, leading to unauthorized access and potential compromise of the entire system. This can result in the theft of sensitive information, disruption of services, and unauthorized modifications to critical functionalities. Additionally, such control could enable attackers to plant malicious code, execute arbitrary commands, and escalate privileges, further exacerbating the security risks.

CWE-1104: Use of Unmaintained Third-Party Components

OWASP CATEGORY: A06 2021 Vulnerable and Outdated Components

Description:

The product relies on third-party components that are not actively supported or maintained by the original developer or a trusted proxy for the original developer.

Business Impact:

The use of unmaintained third-party components in software can have serious cyber-related consequences. Such components often lack crucial security updates, making them vulnerable to exploitation by cybercriminals. Hackers can exploit known vulnerabilities in these components to gain unauthorized access, compromise data, and even launch attacks against other parts of the system. Additionally, unmaintained components might not adhere to the latest security standards, leading to weak encryption or authentication mechanisms that can be exploited. These components could also serve as entry points for malware or ransomware attacks, potentially spreading throughout the system.