ASSIGNMENT - 1

VISHNUBHATLA V L SRUTA KEERTHI
21BCE7726

WEB APPLICATIONS SECURITY RISKS

A. CWE: CWE-284: Improper Access Control
OWASP: A01: 2021 – Broken Access Control

DESCRIPTION

The product either doesn't restrict access to a resource from an unauthorized actor or restricts access to it wrongly.

BUSINESS IMPACT

Improper Authorization, CWE-285, directly endangers enterprises. Unauthorized access can expose sensitive data, which could result in legal problems, lost revenue, and reputational damage. Strict permission procedures must be followed in order to mitigate these dangers and keep stakeholders' trust.

B. CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm
OWASP: A02: 2021 – Cryptographic Failures

DESCRIPTION

The product uses a broken or risky cryptographic algorithm or protocol.

BUSINESS IMPACT

The authentication process in this approach entails taking an incoming password, computing its hash, and comparing it to the previously stored hash. An attacker can always use brute force offline after obtaining cached password hashes. Only using hash algorithms that are as resource-intensive as feasible can allow a defender to slow down offline attacks.

C. CWE: CWE-1395: Dependency on Vulnerable Third-party Component OWASP: A06: 2021 – Vulnerable and Outdated Components

DESCRIPTION

The product is dependent on a component from a third party that has one or more known security holes. In some hardware devices, for instance, even the full operating system may come from a third-party source. These parts, whether open-source or closed-source, might have publicly disclosed flaws that enemies could use to hack the device.

BUSINESS IMPACT

The dependency on Vulnerable Third-Party Component, CWE-1395, has important business repercussions. Relying on tainted external components exposes systems to security flaws, which can result in data leaks, system outages, and monetary losses. For operational integrity and brand protection, it is essential to reduce this risk through careful component screening and prompt updates.

D. CWE: CWE-287: Improper Authentication OWASP: A07: 2021 – Identification and Authentication Failures

DESCRIPTION

The product does not prove or does not sufficiently verify that an actor is who they say they are when they claim to have a particular identification.

BUSINESS IMPACT

Improper Authentication, CWE-287, poses serious business hazards. Inadequate authentication procedures can result in user account compromise, data breaches, and illegal access. Financial losses, legal liabilities, and reputational harm to the business could ensue from this. Secure authentication procedures are necessary to protect sensitive data and uphold client confidence.

E. CWE: CWE-918: Improper Authentication
OWASP: A10: 2021 – Server-Side Requests Forgery

DESCRIPTION

The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination.

BUSINESS IMPACT

Unauthorized users having access to important systems, applications, or data is the main risk of poor authentication. This can result in data being viewed, modified, or deleted without authorization. Data breaches caused by weak authentication might provide hackers access to private consumer information, financial data, or intellectual property. Data breaches can seriously damage one's finances and reputation.