NAME- HARSHIT RAJ REG- 21BCE8673 ASSIGNMENT-1

1. 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: Access control involves the use of several protection mechanisms such as:

- **Authentication (proving the identity of an actor)**
- **Authorization (ensuring that a given actor can access a resource), and**
- **Accountability (tracking of activities that were performed)**

When any mechanism is not applied or otherwise fails, attackers can compromise the security of the product by gaining privileges, reading sensitive information, executing commands, evading detection, etc.

There are two distinct behaviors that can introduce access control weaknesses:

- **Specification: incorrect privileges, permissions, ownership, etc. are explicitly specified for either the user or the resource (for example, setting a password file to be world-writable, or giving administrator capabilities to a guest user). This action could be performed by the program or the administrator.**
- **Enforcement: the mechanism contains errors that prevent it from properly enforcing the specified access control requirements (e.g., allowing the user to specify their own privileges, or allowing a syntactically-incorrect ACL to produce insecure settings). This problem occurs within the program itself, in that it does not actually enforce the intended security policy that the administrator specifies.**

2) CWE: CWE-261: Weak Encoding for Password

OWASP CATEGORY : A02 2021 Cryptographic Failures

Description Obscuring a password with a trivial encoding does not protect the password.

BUSINESS IMPACT:

Password management issues occur when a password is stored in plaintext in an application's properties or configuration file. A programmer can attempt to remedy the password management problem by obscuring the password with an encoding function, such as base 64 encoding, but this effort does not adequately protect the password.

3) CWE: CWE-184: Incomplete List of Disallowed Inputs

OWASP CATEGORY : A03 2021 Injection

DESCRIPTION:The product implements a protection mechanism that relies on a list of inputs (or properties of inputs) that are not allowed by policy or otherwise require other action to neutralize before additional processing takes place, but the list is incomplete, leading to resultant weaknesses

BUSINESS IMPACT:

Developers often try to protect their products against malicious input by performing tests against inputs that are known to be bad, such as special characters that can invoke new commands. However, such lists often only account for the most well-known bad inputs. Attackers may be able to find other malicious inputs that were not expected by the developer, allowing them to bypass the intended protection mechanism.

4) CWE: CWE-501: Trust Boundary Violation

OWASP CATEGORY : A04 2021 Insecure Design

Description

The product mixes trusted and untrusted data in the same data structure or structured message.

BUSINESS IMPACT: A trust boundary can be thought of as line drawn through a program. On one side of the line, data is untrusted. On the other side of the line, data is assumed to be trustworthy. The purpose of validation logic is to allow data to safely cross the trust boundary - to move from untrusted to trusted. A trust boundary violation occurs when a program blurs the line between what is trusted and what is untrusted. By combining trusted and untrusted data in the same data structure, it becomes easier for programmers to mistakenly trust unvalidated data.

5) CWE: CWE-260: Password in Configuration File

OWASP CATEGORY : A05 2021 Security Misconfiguration

Description

The product stores a password in a configuration file that might be accessible to actors who do not know the password.

BUSINESS IMPACT: This can result in compromise of the system for which the password is used. An attacker could gain access to this file and learn the stored password or worse yet, change the password to one of their choosing.