Name: Sarath Rajan Senthilkumar Register No: 21BCE5965

Assignment-1

Broken Access Control	CWE-285: Improper Authorization
Cryptographic Failure	CWE-327: Use of a Broken or Risky Cryptographic Algorithm
Injection	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
Insecure Design	CWE-657: Violation of Secure Design Principles
Security Misconfiguration	

Broken Access Control

CWE-285: Improper Authorization

Description:

The product does not perform or incorrectly performs an authorization check when an actor attempts to access a resource or perform an action.

Business impact:

If a user with a low-level clearance who is a corporate spy but does not have access to the company's latest innovation. He/she can easily steal the latest innovation which is generally only accessible by the high-level management.

Cryptographic Failure

CWE-327: Use of a Broken or Risky Cryptographic Algorithm

Description:

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

Business impact:

Weak cryptographic algorithms can be exploited by attackers to decipher encrypted data, leading to unauthorized access to sensitive information. This can result in data breaches, leaks of proprietary information, and violations of privacy regulations.

Injection

CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Description:

The product constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component.

Business impact:

A hacker can easily manipulate an SQL command which is being sent from the website to the server. By doing so he can easily access data that was previously unavailable to him/her.

Insecure Design

CWE-657: Violation of Secure Design Principles

Description:

The product violates well-established principles for secure design.

Business impact:

Security incidents caused by inadequate secure design can erode an organization's reputation and trust among customers, partners, and stakeholders. News of a data breach or security vulnerability can lead to negative media coverage, public scrutiny, and loss of customer confidence.