Name :- Ch.V.S.Dhiraj Reg No :- 21BCE5717

Task - 3

Checking the Vulnerabilities with different CWE's :

:

CWE 89-Improper Neutralization of Special Elements used in an SQL Command :

- OWASP CATEGORY : A01 2021 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 : Attackers can potentially access, modify, or delete sensitive data from the database, leading to a breach in personal data and their financial records in the database.The attacker can also manipulate their data causing incorrect data calculations and data corruption.If the Consumer data is compromised then there can be loss of trust and credibility.

CWE 287-Improper Authentication:

- OWASP CATEGORY : A02 2021 Broken Authentication.

- Description: When an actor claims to have a given identity, the product does not prove or insufficiently proves that the claim is correct.

- Business Impact : Here as the authentication is inconsistent, attackers exploiting authentication bypass vulnerabilities can gain unauthorized access to sensitive data.The data breach can result in the authentication bypass can lead to financial losses due to fraudulent transactions, unauthorized fund transfers, for any financial transactions .The data breach can also result in consequences leading to legal actions, regulatory fines, and reputational damage.

CWE 213- Exposure of Sensitive Information due to incompatible policies :

- OWASP CATEGORY : A03 2021 Sensitive Data Exposure.

- Description : The product's intended functionality exposes information to certain actors in accordance with the developer's security policy, but this information is regarded as sensitive according to the intended security policies of other stakeholders such as the product's administrator, users, or others whose information is being processed.

- Business Impact : Here due to the exposed sensitive data, such as personally identifiable information (PII), can be used by attackers for identity theft and fraudulent activities.If sensitive business

information or intellectual property is exposed, competitors or malicious actors could exploit this information.Dealing with the aftermath of a sensitive data exposure incident can be resource-intensive, requiring investigation, data restoration, and security enhancement efforts.

CWE 611: Improper Restriction of XML External Entity

Reference : - OWASP CATEGORY : A04 2021 XML -

External Entity(XXE).

- Description : The product processes an XML document that can contain XML entities with URIs that resolve to documents outside of the intended sphere of control, causing the product to embed incorrect documents into its output.

- Business Impact : If the attackers exploit XXE vulnerabilities to read sensitive files and data from the system, potentially exposing confidential information such as user credentials, database contents, and configuration files.The aftermath of an XXE attack can result in financial losses due to operational disruptions, incident response efforts.In certain cases,attackers can execute arbitrary code on the targeted system This can lead to complete compromise of the system and further attacks.

CWE 611: Improper Restriction of XML External Entity

Reference : - OWASP CATEGORY : A05 2021 Broken

Access Control.

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

- Business Impact : If the access controls are applied incorrectly then any attacker may get access to our personal information which may use for some malicious purpose.They can also spread our information to our opponents or our enemies so they can use our information and target us.This can also lead to arbitrary code execution,information exposure etc.

END