ASSIGNMENT 1

What is OWASP?

The Open Web Application Security Project, or OWASP, is an international non-profit organization dedicated to web application security. One of OWASP's core principles is that all of their materials be freely available and easily accessible on their website, making it possible for anyone to improve their own web application security.

Top 5 Web Application Security Risks of 2021:

1. A01:2021-Broken Access Control
2. A02:2021-Cryptographic Failures
3. A03:2021-Injection
4. A04:2021-Insecure Design
5. A05:2021-Security Misconfiguration

Vulnerabilities:

1. Broken Access Control:

Broken access control is a security flaw where an application or system fails to properly restrict users' access to certain resources or actions. This may result in unauthorised users getting access to sensitive data or features, which may result in data breaches and security breaches. It frequently occurs as a result of weak user privilege protection and poor execution of authorisation checks.

CWE-284: Improper Access Control

Description: The Common Weakness Enumeration category CWE-285, often known as "Improper Authorization," includes flaws linked to ineffective access control. It deals with circumstances in which software systems or applications fail to effectively enforce access controls, allowing unauthorised users to carry out actions or access resources that they shouldn't have permission for. A number of security threats, including as data leaks, unauthorised data tampering, and privilege escalation, might result from this flaw.

Business Impact: The business impact of improper access control can be severe. It makes systems and data vulnerable to unauthorised access, which can result in data breaches, a decline in customer confidence, and even legal implications. This weakness may jeopardise the confidentiality, integrity, and accessibility of resources, damaging the business's brand, resulting in losses, and drawing regulatory attention. To lessen these harmful impacts, quick detection and mitigation are crucial.

2. **Cryptographic Failures:**

Security flaws resulting from mistakes in the application of encryption and related techniques are known as cryptographic failures. Due to defective encryption techniques, bad key management, or improper use of cryptographic tools, they can result in data breaches, privacy violations, and unauthorised access.

CWE-326: Inadequate Encryption Strength

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. A weak encryption scheme can be subjected to brute force attacks that have a reasonable chance of succeeding using current attack methods and resources.

Business Impact: It can have serious effects for businesses if the encryption is weak. This flaw develops when encryption algorithms used to safeguard sensitive data are rudimentary or out-of-date, making them vulnerable to breaching by attackers. Unauthorised access to sensitive data, weakened customer confidence, and potential legal implications as a result of data breaches can all have an impact on a firm. Data security is jeopardised by insufficient encryption, which may result in losses in money or reputational harm or non-compliance with regulations. In order to reduce these dangers and protect sensitive data, encryption techniques must be updated often.

3. **Injection:**

A security weakness known as an injection vulnerability occurs when untrusted data is poorly managed and executed as code inside the context of an application. Attackers may be able to manipulate databases, get unauthorised access to information, and possibly take over systems as a result of the injection and execution of malicious commands.

CWE-75: Failure to Sanitize Special Elements into a Different Plane (Special Element Injection)

Description: The product does not adequately filter user-controlled input for special elements with control implications.

Business Impact: Attackers may inject malicious commands when apps handle special characters improperly, which could result in unauthorised data access, data manipulation, or even system compromise. Data breaches, the loss of confidential information, legal ramifications, and reputational harm can all result from this. To avoid these vulnerabilities and the possible financial, legal, and reputational repercussions they could have, it is crucial to implement extensive input validation and appropriate sanitization strategies.

4. **Insecure Design:**

An insecure design vulnerability is a security problem that results from fundamental design choices in software or systems that do not effectively take security precautions into account or apply them. When a system's architecture, structure, or general design fall short of appropriately addressing possible security threats, this kind of vulnerability occurs.

CWE-256: Plaintext Storage of a Password

Description: Storing a password in plaintext may result in a system compromise. Password management issues occur when a password is stored in plaintext in an application's properties, configuration file, or memory. Storing a plaintext password in a configuration file allows anyone who can read the file access to the password-protected resource. In some contexts, even storage of a plaintext password in memory is considered a security risk if the password is not cleared immediately after it is used.

Business Impact: Plaintext password storage is a dangerous practise that can have serious effects on your business. In this case, private user information is recorded in plain text, making it possible for anyone with access to the stored data to simply view the information. Affected user accounts, data breaches, and unauthorised access may arise from this. Potential consumer distrust loss, reputational harm, legal liabilities, and non-compliance with regulations are some of the effects. Losses in money may result from such security lapses, particularly if confidential data is exposed. In order to minimise this risk and keep user accounts and sensitive data secure, proper password hashing and encryption are essential.

5. **Security Misconfiguration:**

Software, apps, or systems that have been poorly configured in terms of security are susceptible to assaults. When access controls or default settings are not appropriately modified, this can occur. Attackers may take advantage of these errors to obtain access without authorization, steal information, or disrupt services.

CWE-315: Cleartext Storage of Sensitive Information in a Cookie

Description: The product stores sensitive information in cleartext in a cookie.Attackers can use widely-available tools to view the cookie and read the sensitive information. Even if the information is encoded in a way that is not human-readable, certain techniques could determine which encoding is being used, then decode the information.

Business Impact: Serious commercial implications may result from storing private data in cookies in cleartext. Without encryption, sensitive information such as passwords or personal identification numbers (PINs) is easily intercepted and used

by attackers. This may lead to unauthorised account access, identity theft, and a breach of user privacy. Customer trust decline, reputational harm, legal liability, and potential regulatory infractions are some effects of data breaches. Such occurrences may result in monetary losses and discourage customers from using the impacted services. Sensitive information should be adequately encrypted before being saved in cookies to reduce these dangers while also protecting user privacy and the reputation of the company**.**

Name: Tharunya Bala S

Reg. No.: 21BCE0076