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:**
   An application or system that improperly restricts users' access to particular resources or actions is considered to have broken access control. This could lead to unauthorized users gaining access to private information or features, which could lead to security and data breaches. It frequently happens as a result of inadequate authorisation checks and user privilege protection.

   CWE-284: Improper Access Control

   Description: Instances where an application improperly enforces access rules, letting unauthorized users to access resources or carry out actions they shouldn't be allowed to, are referred to as CWE-284. This flaw may result from improper implementation of authorisation methods, insufficient user role and permission validation, or other oversights in access control

   Business Impact: Unauthorized data breaches, financial losses, reputational harm, operational interruptions, regulatory violations, and intellectual property loss can all result from improper Access Control vulnerabilities (CWE-284) that can be exploited. Customer mistrust, legal obligations, and lost business prospects can all be caused by these problems. Strong access restrictions, frequent security reviews, incident response strategies, and compliance activities are all part of mitigation, which aims to lessen these effects.

2. Cryptographic Failures

Cryptographic failures are mistakes or flaws in how cryptographic procedures are applied to secure data. These mistakes can result in regulatory non-compliance, financial losses, reputational damage, privacy violations, and data breaches. Strong cryptographic procedures and appropriate encryption techniques must be used to avoid these problems.

CWE-261: Weak Encoding for Password

Description: 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.

Business Impact: The use of subpar or insufficient encoding techniques for password storage is highlighted by CWE-261. By using shoddy encoding methods, attackers can easily obtain and abuse passwords. This weakness could result in user privacy being violated, data breaches, and unauthorized account access. Strong password hashing techniques, like bcrypt or Argon2, should be used to securely store passwords and improve system security as a whole to lessen this risk.

3. Injection

It entails intentionally introducing dubious data into an application's input so that it can be translated into code. Unauthorized access, data modification, and even remote code execution may result from this. SQL injection, where attackers alter database queries, and Cross-Site Scripting (XSS), when nefarious scripts are inserted into web pages, are two frequent examples. Data breaches, unauthorized access, system compromise, and reputational harm can all be caused by injection attacks. Input validation, parameterized queries, and output encoding are crucial security precautions to take in order to stop them.

CWE-89: Improper Neutralization of special Elements used in SQL command

Description: Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data. This can be used to alter query logic to bypass security checks, or to insert additional statements that modify the back-end database, possibly including execution of system commands.

SQL injection has become a common issue with database-driven web sites. The flaw is easily detected, and easily exploited, and as such, any site or product package with even a minimal user base is likely to be subject to an attempted attack of this kind. This flaw depends on the fact that SQL makes no real distinction between the control and data planes.

Business Impact: Attackers can modify database queries made by an application using CWE-89 vulnerabilities, also known as SQL injection, which could result in unauthorized data access, modification, or deletion. Data breaches, the disclosure of sensitive information, illegal account access, financial losses as a result of fraud, and reputational harm can all arise from this. Organizations may experience legal repercussions, regulatory issues, and a decline in customer confidence. To prevent these negative business results, preventive steps are essential, such as input validation and parameterized queries.

4. Insecure Design

The process of developing software systems, applications, or products without fully considering and putting in place security measures during the design phase is known as insecure design. It entails failing to foresee and address potential security dangers and flaws that could be abused by bad actors. A system that has been designed insecurely may have structural, functional, and architectural defects that leave it open to numerous security concerns such unauthorized access, data breaches, and system compromises.

CWE-73: External control of file name or path

Description: This could allow an attacker to access or modify system files or other files that are critical to the application.

Path manipulation errors occur when the following two conditions are met:

1. An attacker can specify a path used in an operation on the filesystem.

2. By specifying the resource, the attacker gains a capability that would not otherwise be permitted.

For example, the program may give the attacker the ability to overwrite the specified file or run with a configuration controlled by the attacker.

Business Impact: CWE-73 draws attention to flaws where an attacker could change the file names or application paths used. This might result in remote code execution, data spillage, and unwanted access. Attackers have the ability to upload harmful files, overwrite important files, or modify paths to access sensitive data. Data breaches, the disclosure of sensitive information, the compromise of system integrity, and potential system disruptions are some of the commercial effects of CWE-73. In order to stop illegal file access and modification, remediation measures include verifying and sanitizing file paths, limiting access to sensitive folders, and putting in place the right access controls.

5. Security Misconfiguration

When software, apps, servers, or other systems are configured incorrectly so they are susceptible to security risks, this is referred to as security misconfiguration. It happens when superfluous features and services are enabled or when default settings, permissions, or configurations are maintained. These errors can disclose confidential information, give intruders access points, and jeopardize an organization's general security posture.

CWE-260: Password in Configuration File

Description: 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.

Business Impact: Passwords are kept in configuration files either in plain text or with insufficient encryption, which is a CWE-260 vulnerability. Unauthorized access to private systems, accounts, and data may result from this. These credentials are simple for attackers to recover, which might lead to data breaches, unlawful actions, and financial losses. Reputational harm, regulatory non-compliance, and legal repercussions could be experienced by organizations. Use of secure password storage systems and encryption methods is required for proper mitigation in order to protect sensitive data and stop these negative effects.

Student Name: Kamalnath R