Name : Veekshitha
Reg no: 21BCE8943

TASK - 2 : Vulnerabilities of top 5 OWASP

1. Broken Access Control (CWE-285)

Description:
Broken access control vulnerabilities occur when an application does not properly enforce restrictions on what authenticated users are allowed to do. This can lead to unauthorized access to certain functionalities or data.

Business Impact:
Exploiting broken access control can result in unauthorized access to sensitive functionality, data exposure, and even the compromise of user accounts. This can lead to data breaches, financial loss, and loss of user trust.

2. Cryptographic Failures (CWE-310)

Description:
Cryptographic failures refer to vulnerabilities related to the incorrect use or implementation of cryptographic algorithms. This can lead to weaknesses in data protection and encryption mechanisms.

Business Impact:
Exploiting cryptographic failures can lead to the compromise of sensitive data, including passwords and other confidential information. This can result in data breaches, regulatory non-compliance, and reputational damage.

3. Injection (CWE-89)

Description:
Injection vulnerabilities occur when untrusted data is inserted into an application and is executed as code. This can allow attackers to manipulate the application's behavior or access unauthorized data.

Business Impact:
Successful exploitation of injection vulnerabilities can lead to unauthorized data access, data manipulation, and even remote code execution. This can result in data breaches, system compromise, and financial loss.

4. Insecure Deserialization (CWE-502)

Description:
Insecure deserialization vulnerabilities happen when an application processes untrusted serialized data. Attackers can exploit this to execute arbitrary code or cause unintended behavior.

Business Impact:
Exploiting insecure deserialization can lead to remote code execution, denial of service, and potentially full compromise of the application. This can result in system downtime, data loss, and reputational damage.

5. Security Misconfiguration (CWE-396)

Description:
Security misconfiguration vulnerabilities occur when security settings are not properly configured, leaving potential vulnerabilities exposed. This can include default credentials, unnecessary features, and more.

Business Impact:
Exploiting security misconfigurations can lead to unauthorized access, data exposure, and other security breaches. This can result in data leaks, financial losses, and damage to an organization's reputation.
