ASSIGNMENT – 1

AI FOR CYBER SECURITY

21BRS1283

SANJAYKRISHNAA R S

CSE with AI and Robotics

Chennai campus

Task :

To understand and implement the top 5 OWASP security risks with their business impacts.

1. Broken Access Control (A01): This vulnerability allows attackers to gain unauthorized access to sensitive data or resources. One common CWE that contributes to broken access control is CWE-287: Improper Authorization. This CWE occurs when an application does not properly verify the authorization of a user or system before granting them access to a resource. This can allow attackers to gain access to resources that they should not have access to, such as sensitive data or restricted areas of a website.

   Business impact: Broken access control can have a significant impact on businesses, as it can lead to the unauthorized disclosure of sensitive data, financial losses, and reputational damage.

2. Cryptographic Failures (A02): This vulnerability allows attackers to decrypt sensitive data that has been encrypted by an application. One common CWE that contributes to cryptographic failures is CWE-327: Use of Weak or Improperly Implemented Cryptographic Algorithm. This CWE occurs when an application uses a weak or improperly implemented cryptographic algorithm to encrypt sensitive data. This can allow attackers to decrypt the data using a brute-force attack or other method.

   Business impact: An attacker could exploit a vulnerability in the cryptographic algorithm to decrypt sensitive data or to impersonate a legitimate user.

3. Injection (A03): This vulnerability allows attackers to inject malicious code into an application. One common CWE that contributes to injection is CWE-89: Improper Input Validation. This CWE occurs when an application does not properly validate input from users or other sources. This can allow attackers to inject malicious code into the application, which can then be executed by the application.

Business impact: An attacker could inject malicious code into a web application, which could lead to a denial-of-service attack, data theft, or arbitrary code execution.

4. Insecure Design (A04): This vulnerability allows attackers to exploit design flaws in an application to gain unauthorized access or cause other damage. One common CWE that contributes to insecure design is CWE-79: Improper Control of Information Flow. This CWE occurs when an application does not properly control the flow of information between different parts of the application. This can allow attackers to gain access to sensitive data or cause other damage.

   Business impact: An insecure design could make it easier for attackers to exploit other security vulnerabilities, such as injection or broken authentication.

5. Security Misconfiguration (A05): This vulnerability allows attackers to exploit misconfigurations in an application's security settings. One common CWE that contributes to security misconfiguration is CWE-284: Improper Access Control Configuration. This CWE occurs when an application's access control configuration is not properly configured. This can allow attackers to gain unauthorized access to sensitive data or resources.

   Business impact: An insecure default configuration could leave a web application vulnerable to attack, even if the application itself is properly coded.

These are just a few of the many security risks that businesses face. By understanding these risks and taking steps to mitigate them, businesses can help to protect themselves from attack.