Assignment 1- Cyber security with AI

1. Broken Access Control: Broken access control refers to a security vulnerability that occurs when an application or system fails to enforce proper restrictions on what users are allowed to access or do. Access control is a fundamental aspect of cybersecurity, ensuring that users are only able to interact with resources and perform actions that they are authorized to.

   Business Impact: Unauthorized access to sensitive data or intellectual property can result in data breaches. This can lead to the exposure of confidential customer information, trade secrets, proprietary algorithms, and other valuable assets.

2. Cryptographic failure refers to situations where cryptographic mechanisms or algorithms are compromised or fail to provide the expected level of security. Cryptography is widely used in information security to protect data confidentiality, integrity, authenticity, and more. When cryptographic systems fail, it can lead to various security vulnerabilities and risks.

   Business Impact: Customers, partners, and stakeholders expect their sensitive information to be protected. A cryptographic failure that leads to a data breach can erode trust in the organization's ability to secure data, damaging its reputation.

3. **Injection**-An injection attack is a type of cyber-security vulnerability that occurs when an attacker is able to insert malicious code or commands into an application, system, or database by exploiting improper input validation. These attacks can lead to the execution of unintended actions or the retrieval of sensitive information from the target system. Injection attacks can take various forms, including SQL injection, No-SQL injection, and OS command injection.

Business Impact-Cryptographic failures can lead to unauthorized access to sensitive data, resulting in data breaches. This can expose customer information, proprietary data, trade secrets, and other confidential information to malicious actors.

4. **Insecure Design –**Insecure design, also known as security design flaws or security architecture flaws, refers to the vulnerabilities and weaknesses that are inherent in the fundamental design of a system, application, or network. These vulnerabilities arise when security considerations are not adequately integrated into the design phase of a software or system development project. Insecure design can create serious security risks that might not be easily mitigated by patching or fixing individual components later on.

   Business Impact -Insecure design can have significant and far-reaching impacts on businesses. It can lead to security breaches, data exposure, financial losses, damage to reputation, and more. Dealing with the aftermath of a security breach caused by insecure design can incur substantial financial costs. This includes expenses related to incident response, forensic investigations, legal fees, regulatory fines, and potential lawsuits.

5. **Security misconfiguration** refers to the improper or inadequate configuration of software, applications, servers, or systems, leading to vulnerabilities and potential security breaches. It occurs when security settings

are not properly defined, default settings are not changed, unnecessary features remain enabled, or access controls are not appropriately configured. Security misconfiguration can arise at various levels, including the