**Types of vulnerabilities**

1. **Types of SQL injection:**

* Error-Based SQLI: Exploits database error messages to reveal database structure and content by intentionally causing errors through injected SQL code.
* Boolean-Based SQLI: Utilizes Boolean logic to infer information from the database by manipulating queries to return true or false conditions based on injected SQL code.
* Union-Based SQLI: Leverages the UNION SQL operator to combine the result sets of multiple queries, allowing attackers to retrieve additional data from other tables.
* Time-Based Blind SQLI: Exploits conditional SQL queries that cause delays in the server's response, allowing attackers to infer information based on the delay in response time. rewrite in human language.

1. **Types of XSS:**

* reflected XSS: cur when a malicious script is reflected off of a web application to the victim's browser.
* Stored XSS: Malicious script is permanently stored on the server, executing when users access affected pages.

1. **LFI Vulnerability:**

* A vulnerability that allows files on the server to be read without requesting any permissions by writing simple commands.

1. **SSRF Vulnerability:**

* A Server-Side Request Forgery (SSRF) vulnerability occurs when an attacker manipulates a web application to make unintended requests. In an SSRF attack, the attacker might make the server connect to internal-only services within the organization's infrastructure.

1. **IDOR Vulnerability:**

* occur when an application provides direct access to objects based on user-supplied input. As a result of this vulnerability attackers can bypass authorization and access resources in the system directly, for example database records or files.

1. **Brute Force**

* attackers using excessively forceful attempts to gain access to user accounts.