In an injection attack, an attacker supplies untrusted/malicious input to a program. This input gets processed by an interpreter as part of a command or query. In turn, this alters the execution of that program.

Injection attacks can lead to Data Loss,Denial of service as well as full system compromise.

Injection attacks are one of the most common and dangerous web attacks and ranked #1 in OWASP Top Ten Web Application Vulnerabilities.

Types of Injection Attacks :

1. SQL Injection :
SQL is a query language to communicate with a database.
The attacker injects SQL statements that can read or modify database data. In the case of advanced SQL Injection attacks, the attacker can use SQL commands to write arbitrary files to the server and even execute OS commands. This may lead to full system compromise.

It can potentially impact :

-Authentication Bypass
-Information Disclosure
-Data Loss
-Sensitive Data Theft
-Loss of Data Integrity
-Denial of Service
-Full System Compromise

2. Cross-Site Scripting (XSS) :
The attacker injects an arbitrary script (usually in JavaScript) into a legitimate website or web application.This script is then executed inside the victim’s browser.

XSS Attack occurs when :
 1. Data enters a Web application through an untrusted source, most frequently a web request.
 2. The Data is sent to a web user without being validated for malicious content.

It can potentially impact :

-Account Impersonation
-Defacement
-Run Arbitrary JavaScript in victim's browser

3. Code Injection :
Code is injected in the language of the targeted application and executed by the server-side interpreter.
It executes Operating system commands with user privilege who is running web application.
An application is vulnerable to code injection when :

1. Lack of proper input validation
2. Dynamic Evaluation of user input in a dangerous way

This involves eval() or equivalent function code.
Once the attack is successful the attackers get access to system information And database.

4. Command Injection :
OS command injection (also known as shell injection) is a web security vulnerability that allows an attacker to execute arbitrary operating system (OS) commands on the server that is running an application, and typically fully compromise the application and all its data.

Sometimes web applications need to call a system command on the webserver that is running them. In such instances, if user input is not validated and restricted, a command injection can occur.

An attacker could compromise full system and gain complete control of O.S.
There is difference in code injection and Command injection, Code injection can submit executable input to a program and trick the software into running that input, Whereas Command Injection exploits the weakness of unprotected system which can execute arbitrary commands without having to inject code.

5. LDAP Injection : Lightweight Directory Access Protocol (LDAP) Injection is a vulnerability in which an attacker injects LDAP statements to execute LDAP commands.

LDAP injection attacks primarily occur due to missing or weak input validation.

It can potentially impact :

-Authentication Bypass
-Information Disclosure
-Privilege Escalation