Code Injection

Code injection, also known as remote code execution **(RCE)**, is a security vulnerability that allows an attacker to execute arbitrary code on a targeted system by injecting malicious code into an application. This vulnerability is often caused by improper input validation or lack of input sanitization in an application.

The benefits of code injection are very few, if any, as it is a security vulnerability that can be exploited by attackers to gain unauthorized access to a system, steal data, or execute arbitrary code. Attackers can use code injection to bypass authentication mechanisms, escalate privileges, or execute malicious payloads, among other things.

To prevent code injection attacks, it is important to follow secure coding practices, including input validation and sanitization, and to use secure coding techniques such as parameterized queries and prepared statements when working with databases. Additionally, it is important to keep all software and applications up-to-date with the latest security patches and to regularly perform vulnerability assessments and penetration testing to identify and address potential security vulnerabilities.

Examples of code injection attacks include **SQL** injection, which allows attackers to execute **SQL** queries on a database, and cross-site scripting **(XSS)**, which allows attackers to inject malicious scripts into a web page. Other types of code injection attacks include command injection, which allows attackers to execute arbitrary commands on a system, and **LDAP** injection, which allows attackers to manipulate **LDAP** queries to gain unauthorized access to a system.