Code injection

Code injection is a technique in computer programming where an attacker inserts code into a program or system with the intent of altering its behavior or gaining unauthorized access.

For example, in a web application, an attacker may use code injection to inject malicious code into a form field or URL parameter that is not properly sanitized or validated by the application. This code may then be executed by the application's server, allowing the attacker to perform various actions such as stealing sensitive information or taking control of the system.

Code injection can take many forms, including SQL injection, cross-site scripting (XSS), and command injection. In each case, the attacker takes advantage of a vulnerability in the target system to insert their own code and cause it to execute.

Preventing code injection attacks requires a combination of secure coding practices, input validation and sanitization, and access control. Developers should always validate and sanitize any input received from users or external sources, and use parameterized queries to prevent SQL injection. Additionally, access to sensitive system resources should be restricted to only authorized users and processes, and security updates and patches should be applied regularly to prevent newly discovered vulnerabilities from being exploited.

Resourses: chat gpt