Code Injection

Code Injection is the general term for attack types which consist of injecting code that is then interpreted/executed by the application. This type of attack exploits poor handling of untrusted data. These types of attacks are usually made possible due to a lack of proper input/output data validation,

for example:

- allowed characters (standard regular expressions classes or custom)
- data format
- amount of expected data

Code Injection differs from Command Injection in that an attacker is only limited by the functionality of the injected language itself. If an attacker is able to inject PHP code into an application and have it executed, they are only limited by what PHP is capable of. Command injection consists of leveraging existing code to execute commands, usually within the context of a shell.

Risk Factors

These types of vulnerabilities can range from very hard to find, to easy to find If found, are usually moderately hard to exploit, depending of scenario If successfully exploited, impact could cover loss of confidentiality, loss of integrity, loss of availability, and/or loss of accountability