Security Misconfiguration

<1 min

Security Misconfiguration is a broad category of vulnerabilities caused by software configuration. Someone might have changed the configuration to a less secure state, or the default configuration might have had security vulnerabilities; to use an earlier example, many XML processors allow external entities by default.

Security misconfiguration might be manageable while writing code, but programs rarely stand alone. It's common for programs to use other programs for data storage or specialized tasks, which need to be configured properly.

There needs to be a strategy for preventing security misconfiguration. Still, it's a good idea to search for known vulnerabilities or configuration issues if you're writing code that uses other programs. And, of course, try to secure the default configuration for programs you write.