

Security testing C and C++ applications

Ziel und Nutzen

Your application written in C and C++ is tested functionally, so you are done, right? But did you consider feeding in incorrect values? 16Gbs of data? A null? An apostrophe? Negative numbers, or specifically -1 or -231? Because that's what the bad guys will do - and the list is far from complete.

Testing for security needs a remarkable software security expertise and a healthy level of paranoia, and this is what this course provides: a strong emotional engagement by lots of hands-on labs and stories from real life.

A special focus is given to finding all discussed issues during testing, and an overview is provided on security testing methodology, techniques and tools.

So that you are prepared for the forces of the dark side.

So that nothing unexpected happens.

Nothing.

Inhalt

Dieser Kurs wird von Fastlane durchgeführt

- Getting familiar with essential cyber security concepts,
- Understanding security testing methodology and approaches
- Correctly implementing various security features
- Identify vulnerabilities and their consequences
- Learn the security best practices in C and C++
- Input validation approaches and principles
- Getting familiar with security testing techniques and tools
- Cyber security basics
- Memory management vulnerabilities
- Memory management hardening
- Security testing
- Common software security weaknesses
- Wrap up

Voraussetzungen

C/C++ Entwickler und Tester