TYP201 - DEFENDING TYPESCRIPT

Course Learning Objectives

In the four modules of this course, we'll explore how to protect TypeScript applications by detecting, scoring, fixing, and monitoring vulnerabilities that could otherwise lead to injection attacks, cross-site scripting, denial of service, cross-site request forgeries, path traversal, and timing attacks, as well as securing the Software Composition Analysis process through the correct use of types, modes, declarations, code review tools, linters, input validation, settings, and configurations.

Description

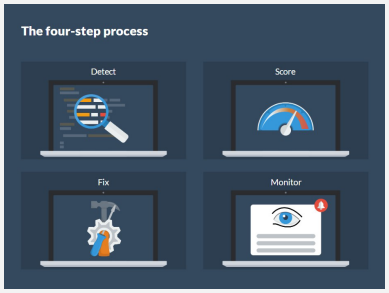
Defending TypeScript is for developers, testers, and security professionals who are familiar with JavaScript. This course is designed to help learners follow best practices for resolving security vulnerabilities and avoiding common pitfalls.

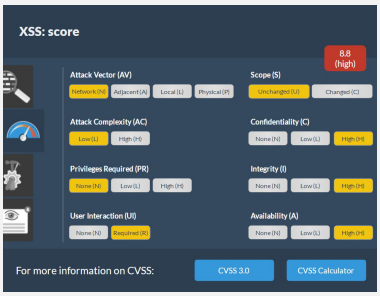
Audience

Developers
Testers
Security Professionals

Time Required

Tailored learning - 45 minutes total





TYP201 - DEFENDING TYPESCRIPT

Course Outline

1. Security Fundamentals

- TypeScript security: the big picture
- Injection attacks
- XSS and DDoS attacks
- Analyzing an application using SAST tools
- Borrowed vulnerabilities
- Leaked secrets
- SCA tools and open-source risk
- Ignoring best practices
- Protecting secrets, API keys, and credentials
- The biggest software development challenge

2. Code Security Issues Part 1

- The four-step process
- Cross-site scripting
- Command injection
- Denial of service

3. Code Security Issues Part 2

- Cross-site request forgery
- Path traversal
- Timing attack
- Analyzing a TypeScript application using SAST tools

4. Code Security Issues Part 3

- SCA vulnerabilities
- Correct types, modes, and declarations
- Code review tools and linters
- Input validation
- Preventing security flaws

SecurityCompass