PYT201 - DEFENDING PYTHON

Course Learning Objectives

Defending Python explores the tools and development practices you need to start building secure Python applications, such as maintaining the Python interpreter and your dependencies, managing packages, and using community tools.

You'll also look at injection attacks, which attempt to insert malicious code or commands into an application. Finally, you'll see common attacks that target web applications, such as XSS, CSRF, and clickjacking attacks.

Description

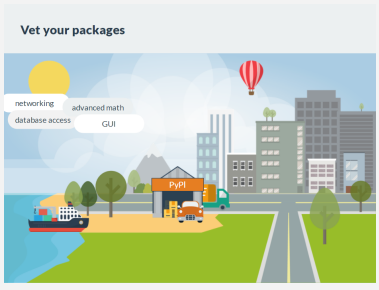
This course has been developed for Python and Web Application developers. It covers Python 3 versions 3.8 and later.

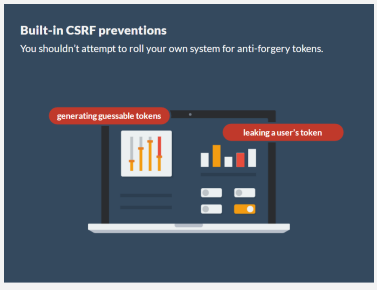
Audience

Python Developers
Web Application Developers

Time Required

Tailored learning - 50 minutes total





PYT201 - DEFENDING PYTHON

Course Outline

1. Securing the Python Environment

- The Python environment
- Use the latest version of the Python interpreter
- Checking your Python version
- Keeping track of new security risks
- Always use a virtual environment
- Anatomy of a virtual environment
- Creating a virtual environment
- Use dependency pinning with caution
- Vet your packages
- Evaluating packages
- Checking packages with Safety
- Perform static security analysis on your code

2. Injection Attacks

- What is an injection attack?
- Use parameterized queries with databases
- How SQL injection works
- The damage of SQL injection
- Parameterized queries
- Staying safe with SQL
- Don't use eval()
- eval() is evil
- Other vulnerable functions
- Don't use pickle for serialization
- Use defusedxml for untrusted XML
- Don't allow shell access with subprocess
- Don't let users specify format strings

3. Common Web Vulnerabilities

- Python web frameworks
- Start with security best practices
- Escape HTML to prevent XSS
- How XSS attacks work
- Escaping HTML
- Allowing limited markup with bleach
- Built-in XSS prevention
- Use tokens to prevent CSRF
- How CSRF attacks work
- How anti-forgery tokens work
- Built-in CSRF preventions
- CSRF defense in depth
- Use of Clickjacking
- Preventing frame-based attacks

SecurityCompass