PYT201 - DEFENDING PYTHON

Course Learning Objectives

In this course, you'll learn about the vulnerabilities that affect your Python web and non-web applications. We'll cover a variety of techniques for securing your application against injection attacks, cross-site scripting and request forgery, information disclosure and file attacks.

Description

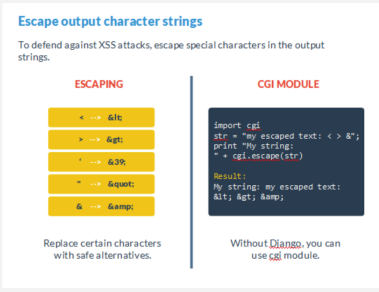
We'll cover topics on using secure database queries, avoiding risky Python functions, how to handle serialization safely, validating, encoding and sanitizing input, protecting your files and folders, and securing temporary files. You'll complete this course with an understanding of important defenses for your application against various vulnerabilities.

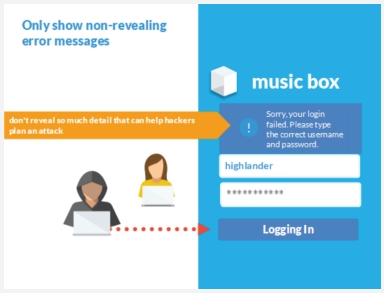
Audience

Python developers
Web application developers

Time Required

Tailored learning - 35 minutes total





PYT201- DEFENDING PYTHON

Course Outline

1. Injection Attacks

- About the vulnerability
- SQL injection
- Command and code injection
- Serialization injection
- Parameterized queries
- Block Python code injection
- Other functions that run Python code
- Don't allow shell access
- Serialization/Input parsing

2. Cross-Site Attacks

- About the vulnerability
- Reflected/Non-persistent XSS
- Stored/Persistent XSS
- Cross-site request forgery (CSRF)
- Stored CSRF
- CSRF in network administrator sites
- CSRF in unauthenticated sites
- Validate input
- Escaping output character strings
- Sanitize your code
- Block cross-site request forgeries

3. File Attacks and Disclosures

- About the vulnerability
- Forced browsing
- Directory traversal
- Object references
- Information disclosure
- Block file attacks
- Non-revealing error messages
- Secure the temp files

SecurityCompass