RUB201 - DEFENDING RUBY ON RAILS

Course Learning Objectives

In this course, you'll be introduced to Ruby's built-in security features and other layers of protection that you should bear in mind for your Ruby applications. You'll learn how to set up your projects securely to prevent attacks at run-time and secure the admin console. You'll also learn how to identify secure and insecure practices to protect your application against common attacks.

By the end of this course, you'll be able to implement user registration to provide a customized user experience, manage an established session between an authenticated user, securely accept and process user input, and ensure the security of your web application's environments.

Description

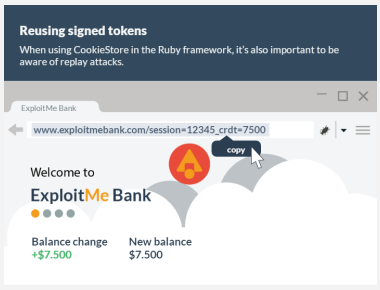
Defending Ruby on Rails was created for developers who already have some experience coding in Python and developing web applications with the Ruby platform, and will focus on creating secure web applications in Ruby.

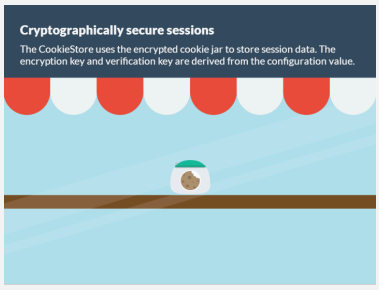
Audience

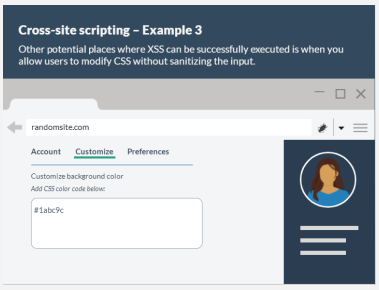
Developers

Time Required

Tailored learning - 40 minutes total







RUB201 - DEFENDING RUBY ON RAILS

Course Outline

1. Secure User Management

- Logging sensitive parameters
- Improper use of regular expressions
- Privilege escalation
- Do not log sensitive parameters
- Proper use of regular expressions
- Query user's access rights

2. Secure Session Management

- Session token encryption
- Reusing signed tokens
- Session fixation
- Cryptographically secure sessions
- Rotate, encrypt, and sign client cookies
- Prevent replay attacks

3. Secure Data Ingestion

- SQL injection attacks
- Cross-site scripting
- Header injection attacks
- Malicious file upload
- SQL injection countermeasure
- Input sanitization
- Header injection sanitization
- Secure file upload

4. Environmental Security

- Unencrypted traffic
- Unsafe Active Record Query generation
- Force SSL
- Safe query generation

SecurityCompass