

**RTF.**

# Remediate the Flag

Practical Application Security Training

Andrea Scaduto

[info@remediatetheflag.com](mailto:info@remediatetheflag.com)

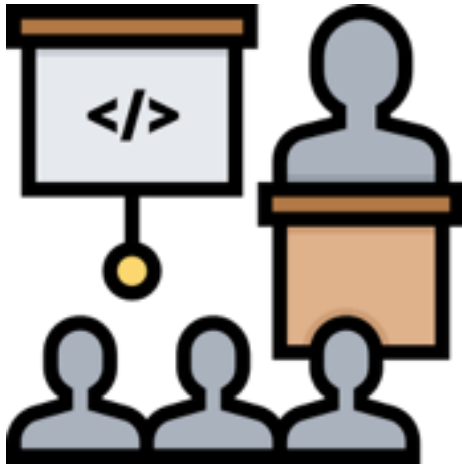
[github.com/sk4ddy/remediatetheflag](https://github.com/sk4ddy/remediatetheflag)

## AppSec Training for Developers



- Developing secure software is a key component in enterprise defense strategy.
- AppSec training is part of cyber security programs for most companies operating in regulated industries.
- Companies still suffering from 20 year old vulnerabilities.
- Assessing competency in secure development is challenging
- Hard to measure ROI for AppSec training

## AppSec Training, today.



### In Class Training

- ✓ Provides real-world examples
- ✗ Expensive (Cost / Time)
- ✗ Often a one time event

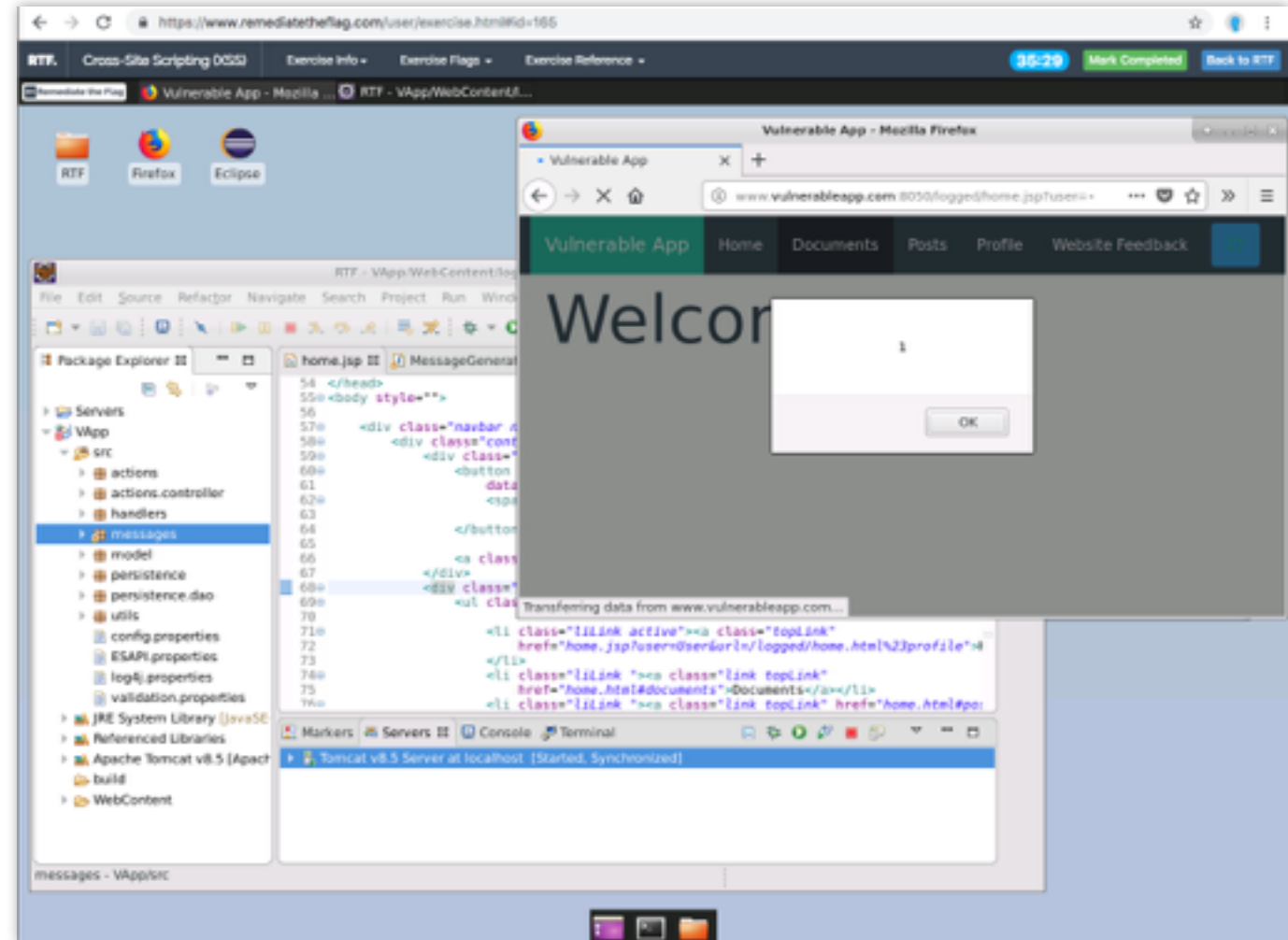


### Computer Based Training

- ✗ No hands-on examples
- ✓ Scales well for large companies
- ✗ Lacks the scope and depth to cover companies' technology.

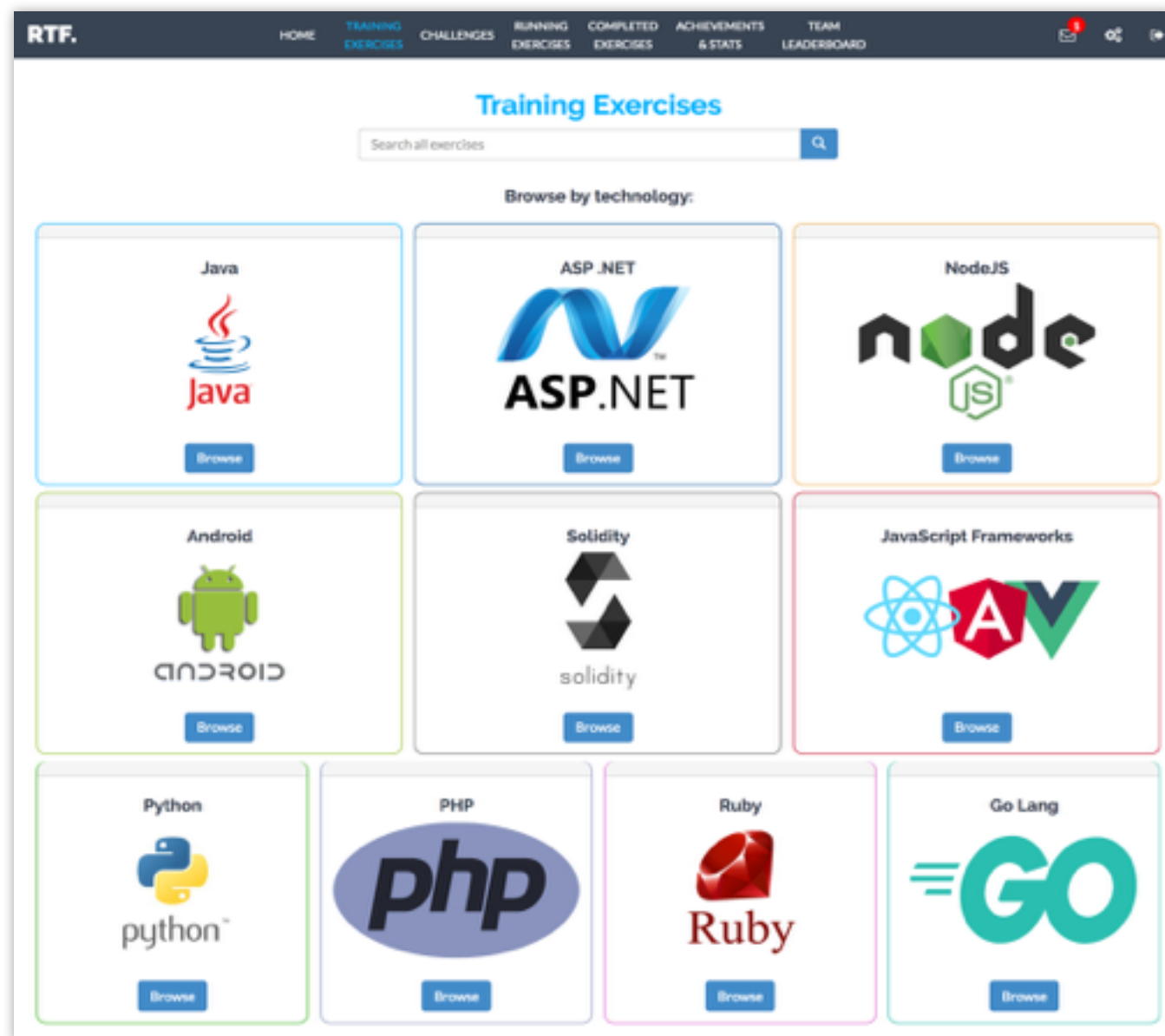
# AppSec Training, tomorrow.

- Open source platform to teach modern secure coding practices.
- Candidates learn how to identify, exploit and remediate security issues.
- Same familiar environment and tools used at the workplace.
- Dedicated desktop accessed in seconds through a web browser.



# Tailored Exercises

- Exercises address the most prevalent security issues and can focus on:
  - Exploitation
  - Remediation
  - Secure Coding
- Multiple tech stacks supported
- New exercises can be easily integrated



## Engaging and Interactive

- Real-time results & automated scoring
- Points, Trophies & Leaderboard
- Time-boxed Tournaments

Java

### Cross-Site Scripting (XSS)

Improper Neutralization of Input During Web Page Generation

Exploit and remediate Reflected and Stored Cross-Site Scripting (XSS) exposures. XSS attacks affect web applications that do not neutralize user input before it is placed in output as a web-page. This could result in the attacker stealing sensitive information or performing actions on behalf of the victim on the vulnerable site.

Duration: 40 minutes | Difficulty: Easy

Score

50

gain up to 50 points

Trophy

Cross-Site Scripting Trophy

---

#### Stored Cross-Site Scripting

Type	Instructions	Required	Hint	Check result
EXPLOITATION	Exploit the Stored XSS in the 'Add Feedback' functionality of the 'Website Feedback' page.	Optional	<a href="#">Show Hint</a>	
REMEDIATION	Remediate the vulnerability by performing Output Encoding in the String feedback.getListMessage().setUserFeedback("feedback") method in the messages.MessageGenerator.java class.	Required	<a href="#">Show Hint</a>	Not Vulnerable

---

#### Reflected Cross-Site Scripting (User parameter)

Type	Instructions	Required	Hint	Check result
EXPLOITATION	Exploit the Reflected XSS in the 'user' query-string parameter of the 'Home' page of the application.	Optional	<a href="#">Show Hint</a>	
REMEDIATION	Remediate the vulnerability by performing the correct Output Encoding for the 'user' parameter in the JSP atWebContent/logged/home.jsp.	Required	<a href="#">Show Hint</a>	Vulnerable

RTF. [Browse as User](#) [HOME](#) [ORGS](#) [GATEWAYS & CLUSTERS](#) [USERS](#) [TEAMS](#) [AVAILABLE EXERCISES](#) [RUNNING EXERCISES](#) [CHALLENGES](#) [PENDING REVIEWS](#) [COMPLETED REVIEWS](#) [STATS](#) [📄](#) [🔍](#) [👤](#)

## Java Top Vulnerabilities

Exercises

5

Run Exercises

16

Start Date

2018-09-21 09:00 (+00:00)

Flags

6

Run Flags

17

End Date

2019-03-30 18:00 (+00:00)

Users

5

Total Exercises

25

Last Activity

2019-01-04 22:34 (+00:00)

Completion

56.0%

Total Flags

30

Status

In Progress

Remediation

82.4%

Running Exercises

0

Organization

Start Industries

[Back](#) [Edit](#)

#### Challenge Exercises

- SQL Injection
- XML Entity Expansion (XXE)
- Broken Session Management
- Horizontal Authorization Bypass
- OS Command Injection

#### Challenge Scoring

Automated Scoring

**Challenge Details:**

Exploit and remediate a number of Java vulnerabilities. This challenge includes the following exercises: Session Fixation, Ineffective Logout, XML Entity Expansion, Horizontal Authorization Bypass, and OS Command Execution and Arbitrary File Upload. A reference document is available for each exercise.

#### Challenge Table

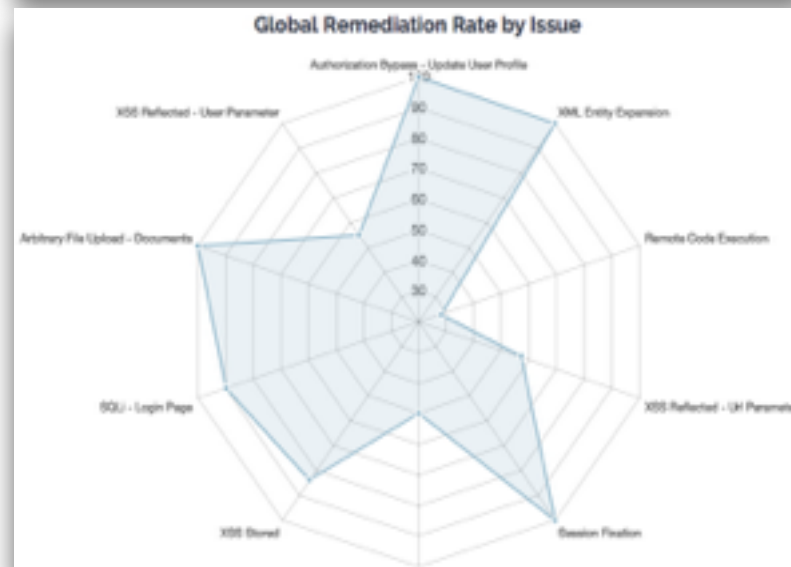
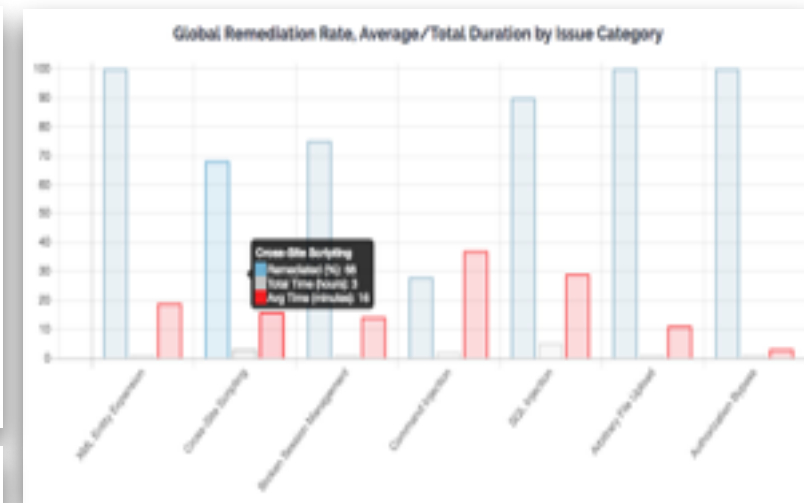
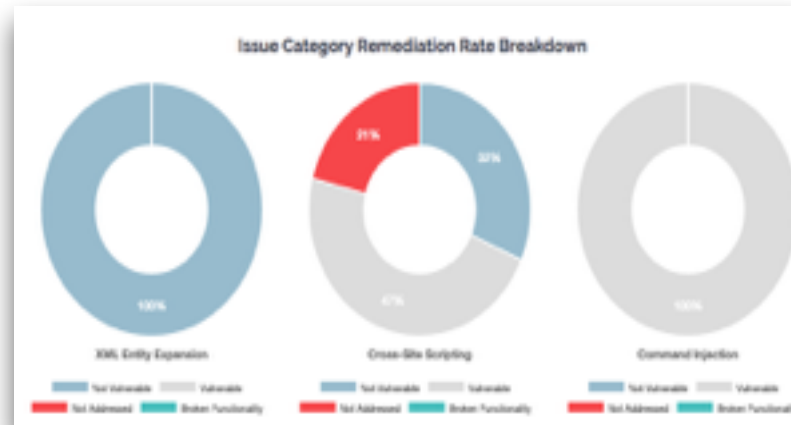
User	Country	Score	Run Exercises
michael	United Kingdom	215	4
andrea	Italy	165	5
joanne	United States	85	5
frank	United Kingdom	50	3
john	United States	30	2

	SQL Injection leading to Authentication Bypass	XML Entity Expansion	Session Fixation	Session Not Invalidated On Logout	Horizontal Authorization Bypass	OS Command Injection
andrea	Not Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Not Started
joanne	Broken Functionality	Not Started	Not Vulnerable	Not Vulnerable	Vulnerable	Not Started
michael	Not Vulnerable	Not Vulnerable	Not Started	Not Started	Not Started	Not Started
frank	Not Started	Not Vulnerable	Not Vulnerable	Not Vulnerable	Not Started	Not Vulnerable
arav	Not Vulnerable	Vulnerable	Not Started	Not Started	Not Started	Not Started

Last refreshed at 12:41 (+00:00) on Feb 10 2019

## Measure ROI for Training

- Measure *real* competency in secure coding and remediation
- Metrics allow for rapid discovery and closure of gaps
  - User
  - Team
  - Region
  - Organization



**RTF.**

**RTF.**

Live Demo





**100% Hands-on Training**  
Open Source Platform  
Automated Deployment on AWS

**New Features Coming Soon**  
Exercise Hub  
Exercise Creation SDK

[info@remediatetheflag.com](mailto:info@remediatetheflag.com)  
[github.com/sk4ddy/remediatetheflag](https://github.com/sk4ddy/remediatetheflag)