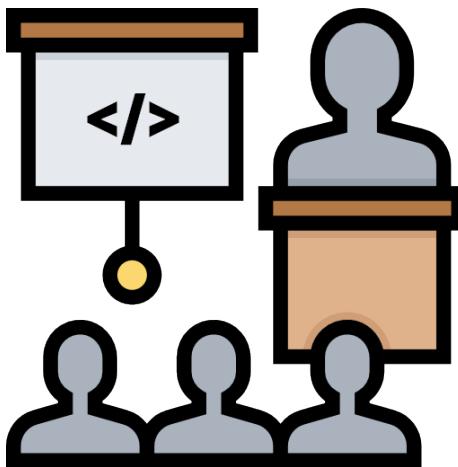


Remediate the Flag

Practical Application Security Training
for Developers

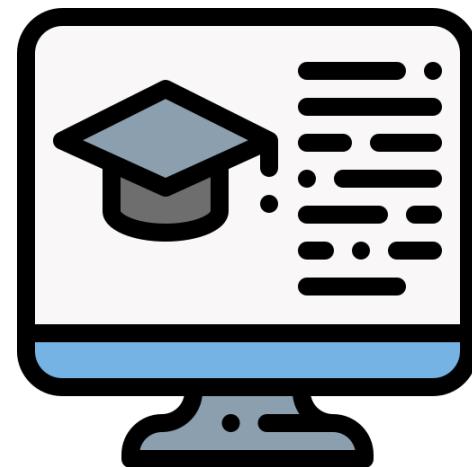
Andrea Scaduto

AppSec Training, today.



In Class Training

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

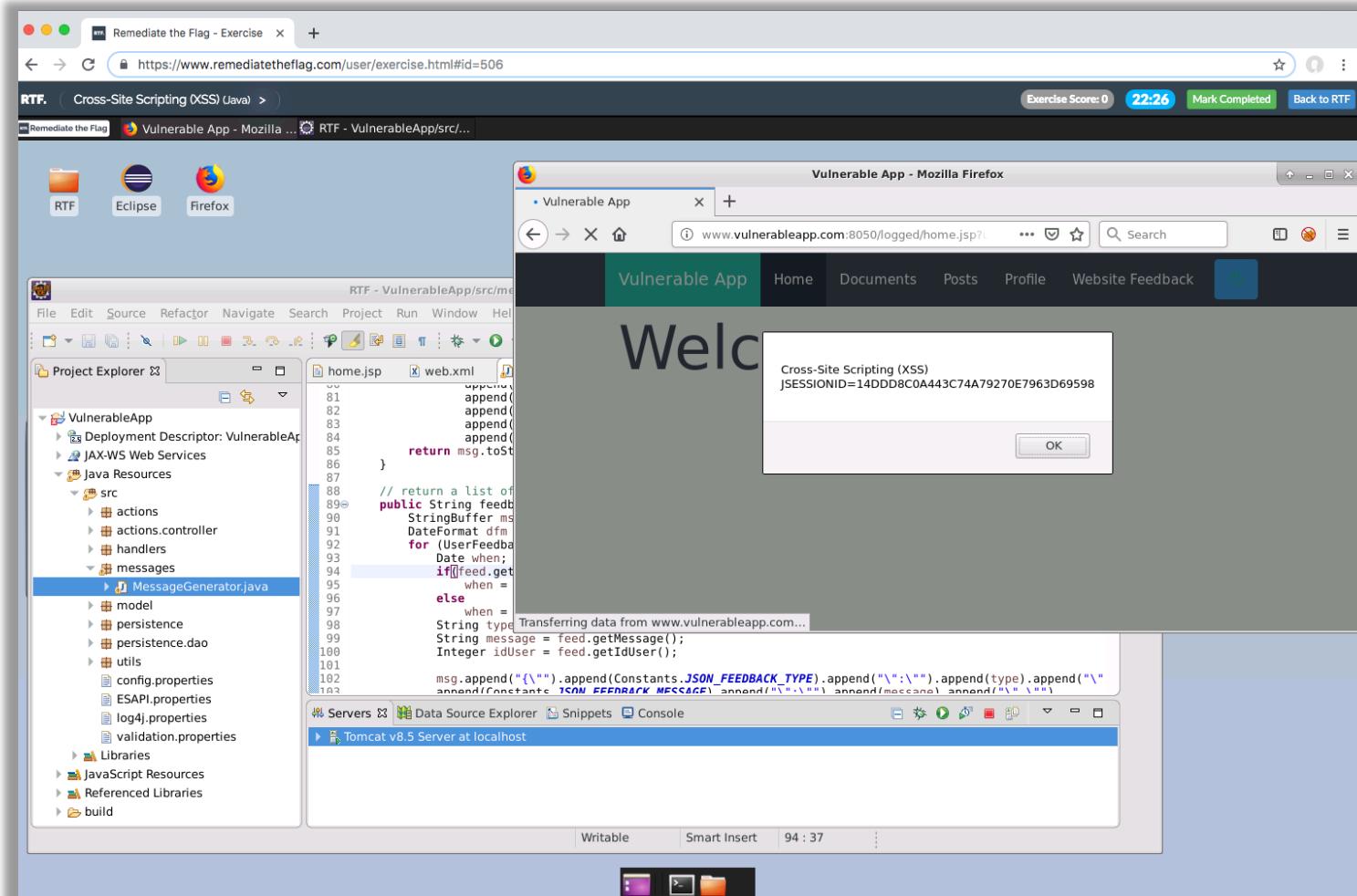


Computer Based Training

- ✗ No hands-on examples
- ✓ Scales well for large companies
- ✗ Difficult to assess competency

AppSec Training, tomorrow.

- 100% hands-on training
- Identify, exploit and fix security issues.
- Dedicated DEV environment accessed in seconds through a web browser.
- Learn using the same tools used at the workplace.



Engaging and Interactive

The screenshot shows a web browser window for the URL remediatetheflag.com/user/exercise.html?id=761. The page title is "RTF. Cross-Site Scripting (XSS) (Java) >". The main content area displays a Java code editor for a file named `MessageGenerator.java` within a project named `VulnerableApp`. The code contains logic for generating JSON messages based on user input. On the left, there's a sidebar with sections for "Exercise setup", "Score" (30), "Trophy" (Cross-Site Scripting Trophy), and several expandable sections for "Exploit Reflected Cross-Site Scripting", "Exploit Stored Cross-Site Scripting", "Remediate Stored Cross-Site Scripting", and "Remediate Reflected Cross-Site Scripting". A "References" section lists links to "Stored Cross-Site Scripting in Java" and "Reflected Cross-Site Scripting in Java". At the top right, there are buttons for "Exercise Score: 15", "29:17", "Mark Completed", and "Back to RTF". A modal window titled "Remediate Stored Cross-Site Scripting" is open, showing instructions and a feedback form. The feedback form shows an error message: "Oops! Your answer is not correct. Please try again." Below the code editor, status bars show "Writable" and "Smart Insert".

- Real-time results & Hints
- Automated scoring
- Gain Points & Trophies

Learning Paths

- Exercises are grouped into logically linked units.
- Learners become expert in a topic in small steps.
- When candidates complete a Learning Path, they receive a RTF certification.
- Certifications expire and they can be renewed by taking refresher exercises.

The screenshot shows a completed learning path titled "Java Secure Backend Developer" on the RTF platform. The path has a completion rate of 80% and an expiration date of 12 months. It includes five modules: Cross-Site Scripting (XSS), SQL Injection - Login, Horizontal Authorization Bypass, Session Fixation, and XML Entity Expansion (XXE). The XSS module is completed with 30 points and a trophy. The SQL Injection module is completed with 40 points and a trophy. The Authorization Bypass module is completed with 40 points and a trophy. The Session Fixation module is completed with 15 points and a trophy. The XXE module is not completed, with 50 points available and a trophy. Each module card includes a "Run again" button.

Browse as User HOME ORGS GATEWAYS & CLUSTERS USERS TEAMS AVAILABLE EXERCISES RUNNING EXERCISES CHALLENGES PENDING REVIEWS COMPLETED REVIEWS STATS Back Edit

Java Top Vulnerabilities

Exercises	Flags	Users	Completion	Remediation
5	6	5	56.0%	82.4%
Run Exercises	Run Flags	Total Exercises	Total Flags	Running Exercises
16	17	25	30	0
Start Date	End Date	Last Activity	Status	Organization
2018-09-23 09:00 (+01:00)	2019-03-30 18:00 (+00:00)	2019-01-04 22:16 (+00:00)	In Progress	Stark Industries

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

The radar chart displays remediation progress for six Java vulnerabilities across five users. The axes represent different vulnerability types: Authorization Bypass - Update User Profile, XML Entity Expansion, XSS Reflected - Url Parameter, XSS Reflected - User Parameter, XSS Stored, Session Fixation, and Session Not Invalidated On Logout. The legend indicates that blue segments represent remediated percentages.

User	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
aarav	Not Vulnerable	Vulnerable	Not Started	Not Started	Not Started	Not Started

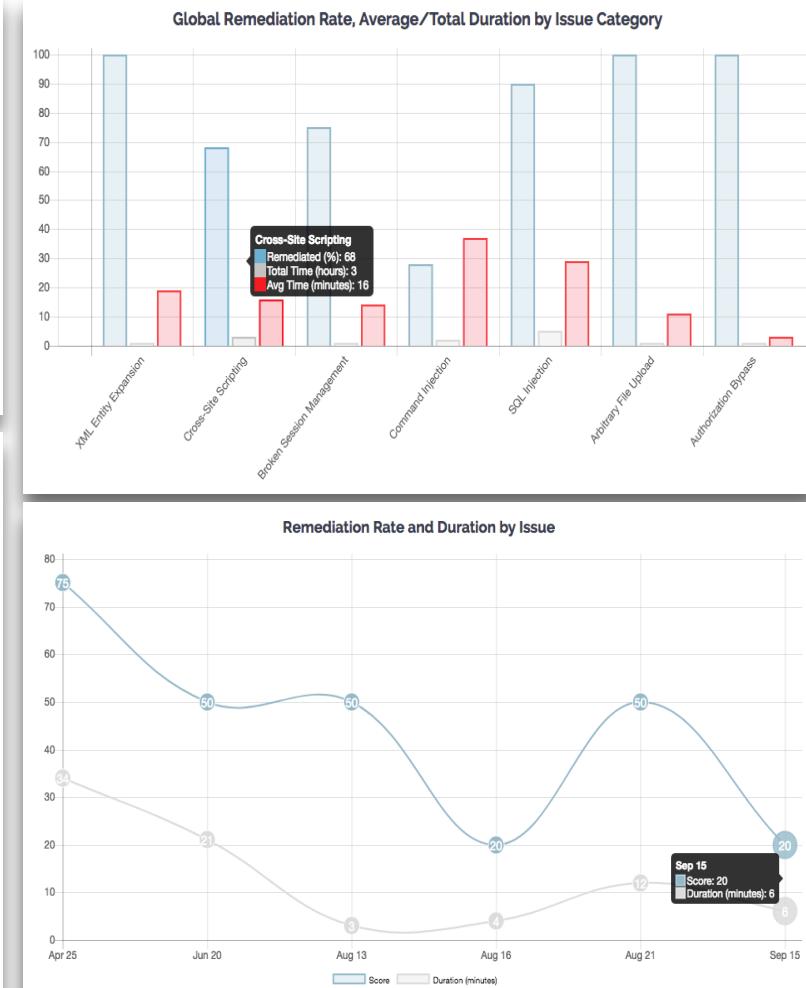
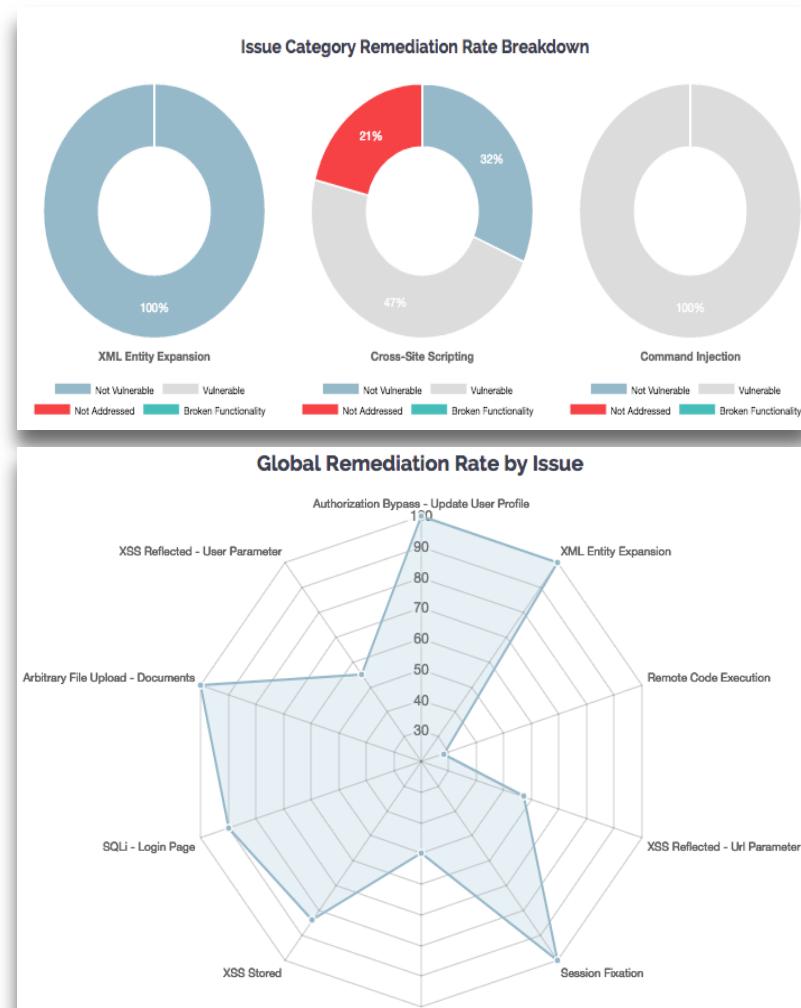
Last refreshed at 12:41 (+00:00) on Feb 10 2019

Tournaments

- Run time-boxed challenges.
- Users of the same Organization compete to remediate security issues.
- Engage the whole developer community.

Measure ROI for Training

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





Live Demo

• • •

1. Start an exercise
2. Exploit vulnerability
3. Remediate code
4. Check results

Installation

Step 1

- Signup to AWS
- Purchase a Domain
- Provision TLS certificate on AWS ACM



Step 2

- Import RTF template on AWS CloudFormation
- Tweak configuration (cluster size, passwords, hostnames, SSL certificate, etc.)



Step 3

- Run template
- Wait ~ 14 minutes
- Enjoy

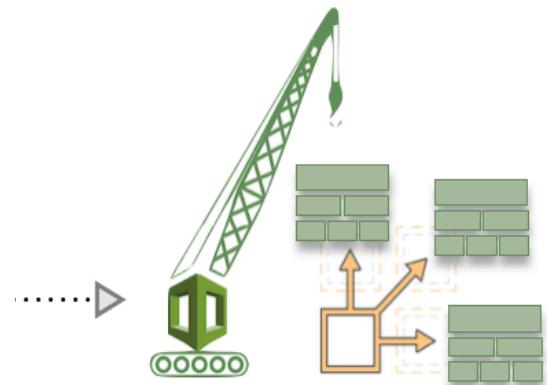


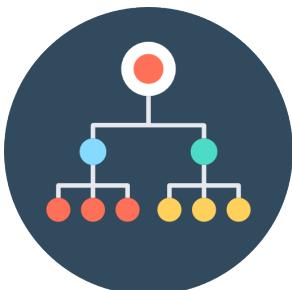
image from aws.amazon.com/cloudformation/

Configuration

Setup your structure

- Create Organizations and Teams based on your structure.
- Onboard/invite users.

Users in the same Team can compare their progress on a leaderboard.



Organizations



Teams



Users

Install Exercises

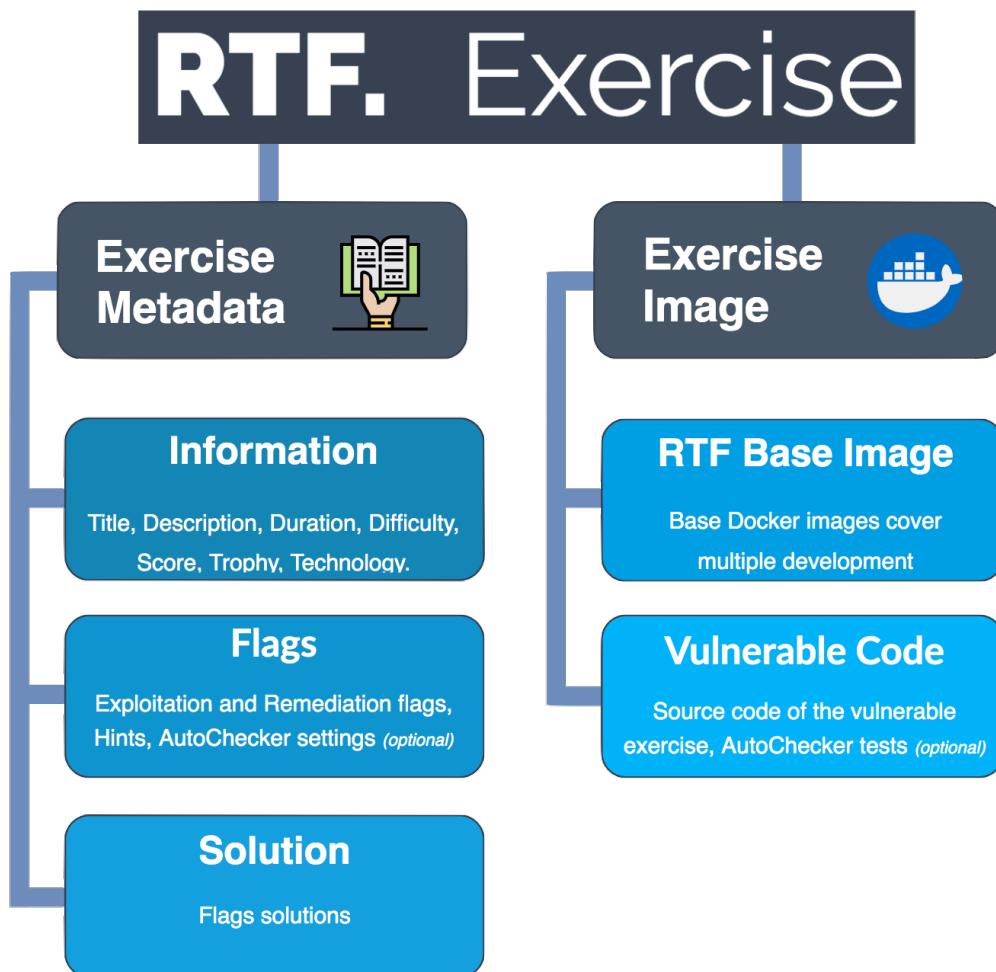
- Install Exercises from RTF Exercise Hub.
- Create your own exercises using the RTF SDK.

Exercises run in isolated DLP-friendly environments.

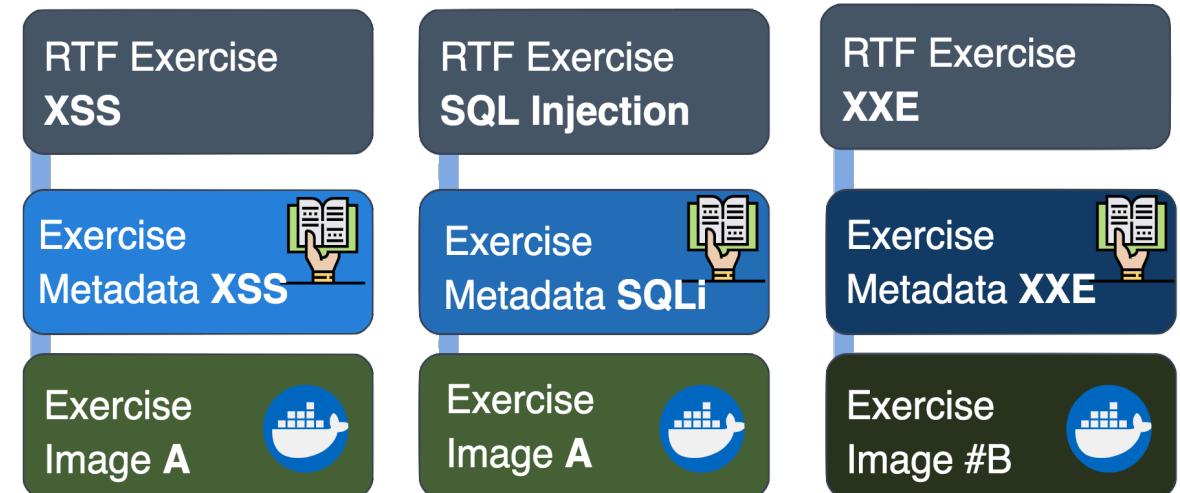
RTF. Exercise Hub

RTF. SDK

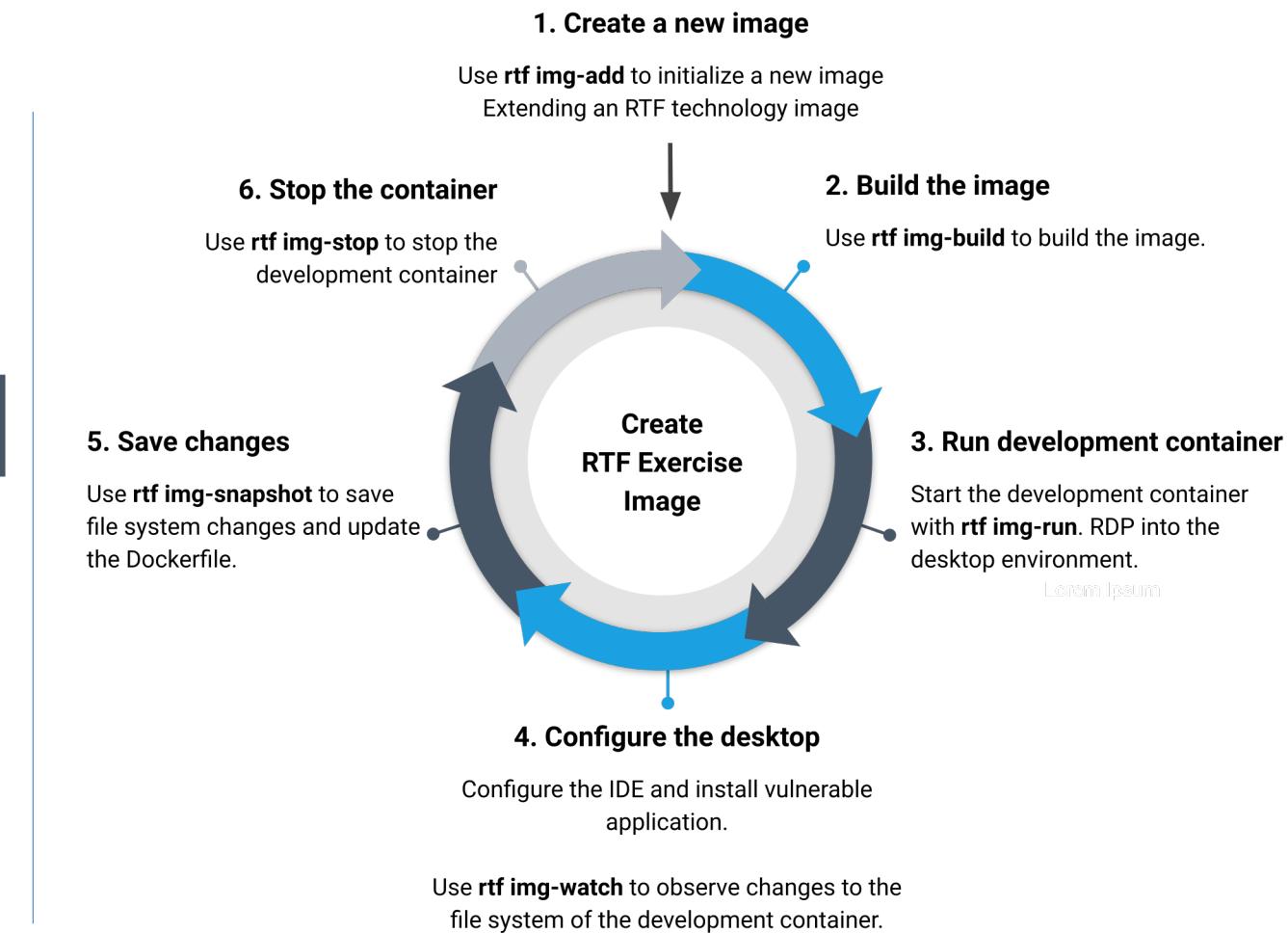
Exercise structure



It is possible to create multiple RTF Exercises reusing the same Exercise Image (e.g. one Vulnerable App with *many* vulnerabilities).

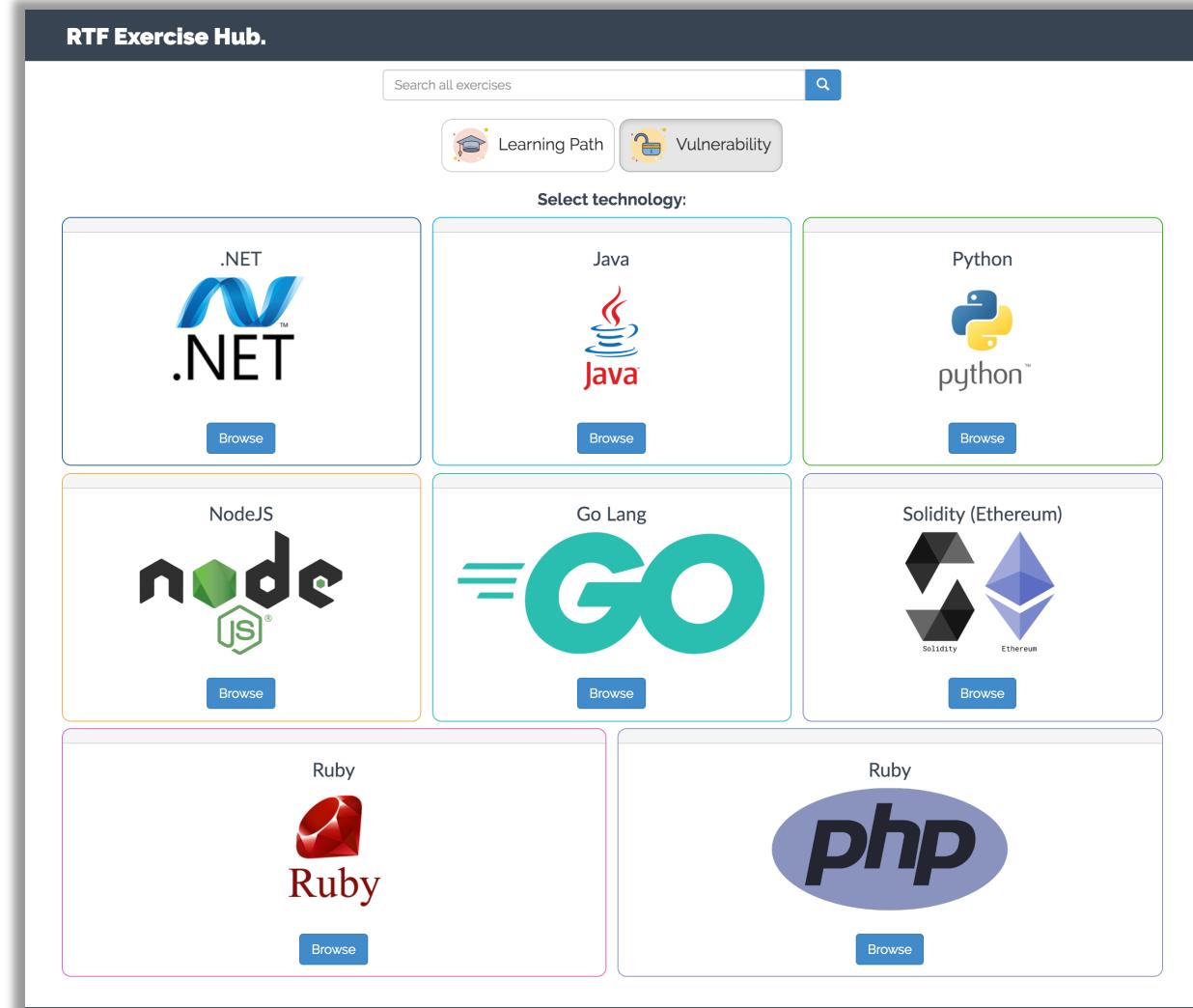
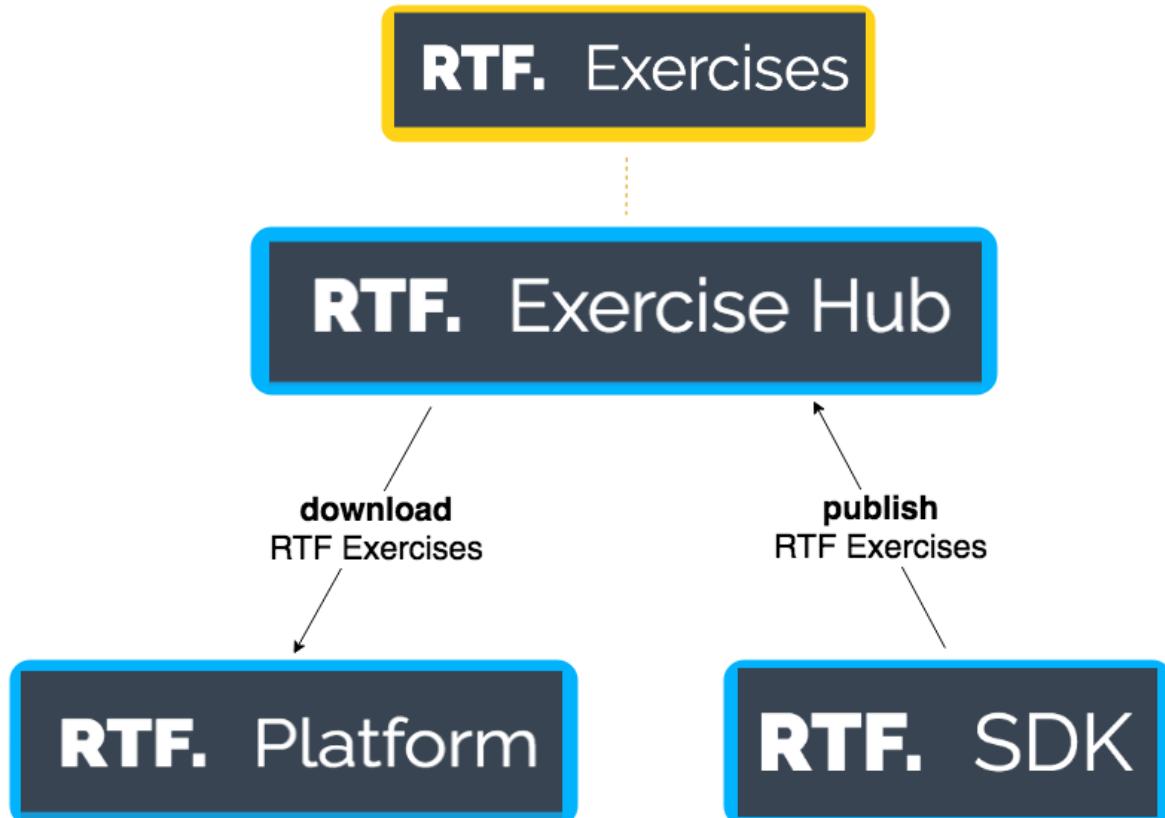


Creating new exercises

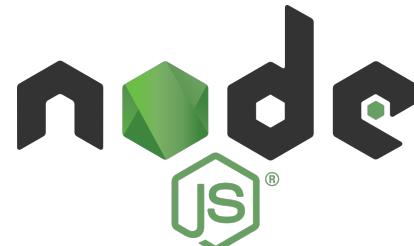


RTF.

RTF Exercise Hub



Supported Exercise Technologies



On the Roadmap



RTF.

Q&A

info@remediatetheflag.com

www.remediatetheflag.com