NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE
School of Computer Science and Engineering
College of Engineering

Capture the Flag Challenges

Design and Implementation

Student: Oong Jie Xiang Supervisor: Asst Prof Li Yi

Background

NTU CZ4067 (Software Security) module assessment includes 20% grading in 1-week CTF competition

Objectives

1. Create challenges for future competitions
2. Examine design and implementation of challenges from ideation to testing that are (1) tailored to CZ4067 students' security education level, industrial exposure (2) engaging and interesting

Methodology

Design
- **Challenge Categories**: Pwn, Web, Forensics
- **3 Difficulty Levels**: Estimated based on
  1. Degree of concept chaining
  2. Familiarity with tools
  3. Presence of source code
  4. Extension of concepts

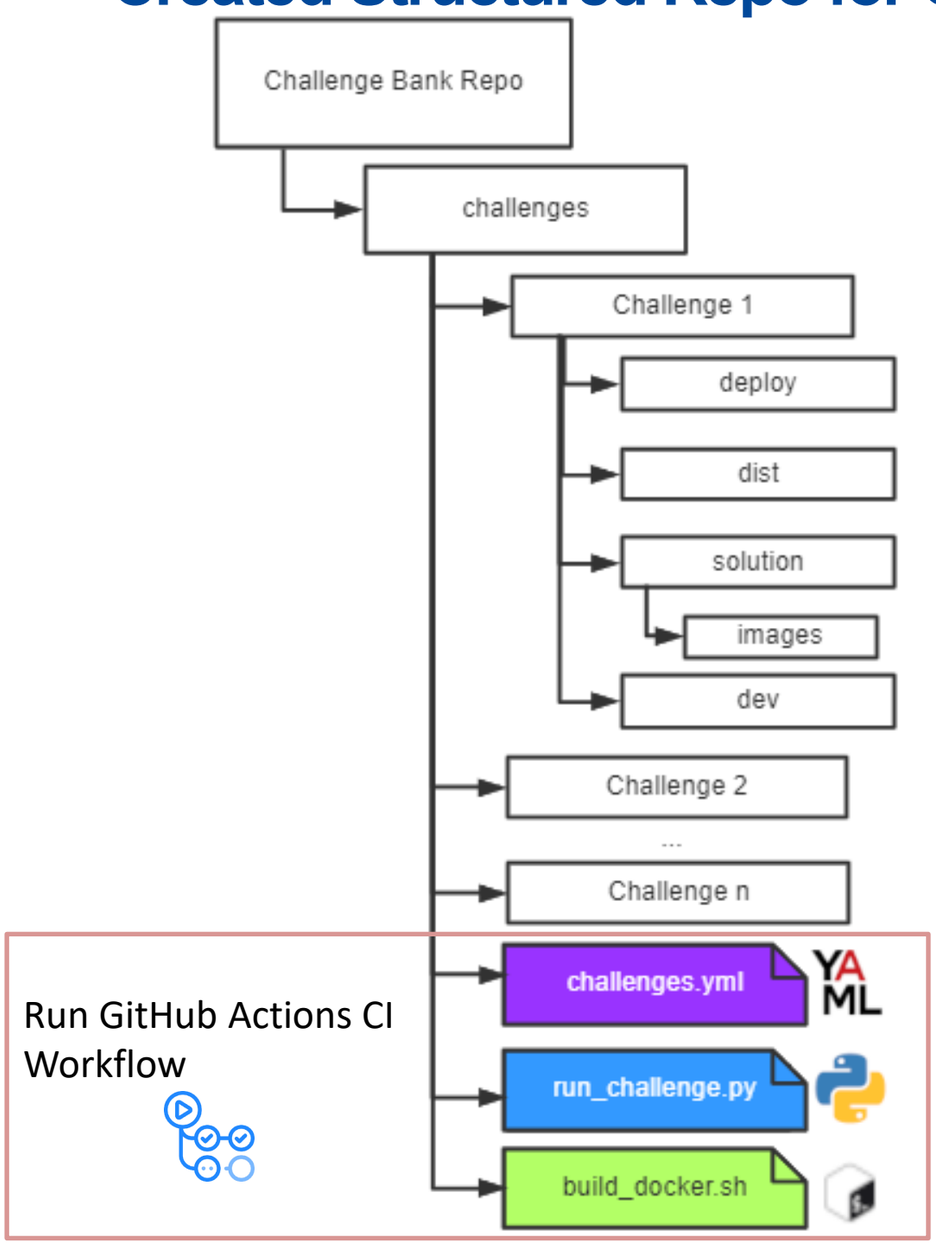
Implementation
- Development
  1. Containerisation for each deployable
  2. Jailing for Pwn reverse-shell attacks
  3. Obfuscation, framing, headless browser for XSS
- Host competition with >2 clusters (CTFd + Challenge)

Release
- **Handouts**: include scripts for CZ4067 students
- **Hints**: released dynamically
- **Limit failure attempts**: discourage brute-force
- **Release Write-ups**: improve students' security skills
- **Feedback form**

Testing
- **Competition trial**: update challenge difficulty based on solve statistics
- **Survey**: understand
  1. Students' security education profiles
  2. Subjective CTF experiences
  3. Potential admin issues

Results

Created Structured Repo for CI



16 Challenges Developed

7 Pwn | 6 Web | 3 Forensics

10 Tested

1 Week

82 Current Module Takers

Insights

- Out-of-syllabus challenges should go **in-breadth**
- Challenges should be interesting, solvable within timeframe with slight research
- **Good administration** affects CTF experience: clear hints, suitable difficulty levels, stable vulnerable containers
- Challenge Bank should have Continuous Integration (CI) to preserve challenge stability & solution correctness