A Platform for
Cyber Security Training
and
Holding CTF competitions

COMP 4801 Final Year Project
Department of Computer Science
The University of Hong Kong

Name: Han Yu
UID: 3035141736
Supervisor: Dr. S. M. Yiu
1. Project Background and Objective

Along with the widely use of information technology in both business and daily life, data streams flowing among electronic devices contains valuable private information and any loss or damage may cause huge cause to both individuals and organizations. Ranging from the software platform embedded in everyone’s laptop to the electronic gate people entered every day, as long as it is under the control of the programming logic stored inside, it can be the target of cyber criminals.

Cybercrime is now attracting more attention than traditional crimes because of the serious loss it can cause. In contrast, there is a lack of cyber security professionals all over the world to provide proper solutions for such problems. According to the statistic, there would be a vacancy of 3.5 million cybersecurity jobs in 2021 (Cybersecurity Ventures, 2017). To meet the need of cyber security professionals, many companies and universities are now holding cyber security education programmes as well as competitions to enhance the skills of young people who are planning a career towards this field. Capture the Flag (CTF) is one of these events aimed at selecting skilled students or professionals in different areas in cyber security. It has attracted a lot of young participants and professionals all over the world to take part in since it is first held all around the world in 1990s. (Harmon, 2016)

CTF has evolved into various forms and keeps embracing popular topics in the industry during its history. The narrow meaning of CTF refers to either attack and defense or jeopardy style competitions, while it is more often to be used to refer to all the competitive events including games and other before-competition training materials nowadays. As one of the traditional styles of CTF competition, attack and defense contest requires teams to patch their own vulnerable server as well as seeking for ways to hack other servers, while jeopardy style allows teams to get marks by solving a set of challenges provided within limited time.

As one of the oldest CTF, Defcon adapts the traditional form of CTF competition, including both attack and defense style and jeopardy style contests. In Defcon CTF teams are first required to solve a set of challenges online and then the selected ones are invited to take the onsite attack and defense contest. (Vulcan) Attack and defense style competitions are much more difficult to hold as building available vulnerable virtual machine for participants is highly time consuming.
In addition, it is often arranged as the onsite competition considering the coherency of the whole contest system which consists of multiple virtual machines and other components.

This project aims to design and implement an online CTF platform supporting both of the traditional styles competitions. The whole system would be allocated in the Cyber Security lab in the University of Hong Kong and contribute to the cybersecurity training on campus. It should be able to hold the onsite attack and defense style competitions for multiple users on campus.

Furthermore, based on the education purpose, some CTFs are accompanied with related lectures and tutorials for being a qualified teaching tool for cybersecurity knowledge. (Werther, Zhivich, Leek and Zeldovich, 2011) However, most of the cybersecurity trainings are held temporarily or even consists of only a few workshops in weeks. Other training programmes, like picoCTF, are in the form of electronic games, facing only high school students or even lower age. There is a lack of the stable online platform that provides comprehensive cyber security education for self-taught young people as well as competitions for exercising practical skills.

Our project aims to develop a CTF platform which holds both of the competitions of two traditional styles and cooperates with online and offline training materials to assist the students in self-taught learning process. The training materials will be presented both in the form of online knowledge sheets and in offline workshop by tutors. Such workshop may hold several times per year depending on the actual situation to help students get familiar with the CTF platform and get a quick start for online self-taught learning. Additionally, in order to provide students with hand-on exercises about what theories they have learnt, the competitive contests provided by CTF platform will be highly matched with the training materials and thus encourage students to apply theories to practical problems.

With the close cooperation of online contests and learning materials, students are expected to establish solid cybersecurity theory foundation and develop a high level of practical skills towards real life challenges. Additionally, it could also be used by the university to evaluate the skills of students through CTF competitions supported by the platform.
2. Methodology

To build the suitable CTF training platform for HKU students, this project performs careful analysis on existing open source platform CTFd and FBctf from multiple aspects and then choose one of them to add designed functionalities.

The two platforms FBctf and CTFd are analyzed based on interface design, supporting functionalities and source code. They both support default jeopardy style competition but leave ample space for customization. After analysis, this project will choose one of them as basic platform and design desired functionality to build on top of it.
3. Current Work

By now, the default functionalities of platforms FBctf and CTFd have been analyzed and this section will present the comparison of game interface design, administrator control and source code.

Part 1: Administration panel:

1. Registration control:

They both provide options for free registration or reserving the rights for administrators to manually register new teams. In addition, FBctf also can approve new teams by registration tokens sent by administrators. CTFd discloses some of the functionalities, including certain pages, challenges, to anonymous users while FBctf only serves registered users.

2. Game control:

Both FBctf and CTFd keep the records of the game start and end time, but only FBctf includes timer in game panel and can hold events in competitive way. During the game, FBctf supports in time announcements and game pause or termination. On the other hand, CTFd is more suitable for a training platform as it sets no time limit for solving challenges and provide a interface while clearly divide challenges into different challenges.

3. Database refresh and game storage

Both FBctf and CTFd support game import and export. The content could be full game or particular part of settings, such as team logos and challenges. Each time administrators make challenges to CTFd, it will be automatically saved with the account and when come back to CTFd, these changes will remain. However, changes made to FBctf will lose after restart of the server and recompilation of the source code. So it is necessary for administrators to import necessary part of the game before exit and import it again after next login.

4. Challenge Setting

FBctf support different categories of challenges by default, including quiz level, flag level and base level with different setting layout, while CTFd use the same template for all challenges. For FBctf, Level Quiz is the basic level designed for challenges with simple question and simple answer format. The basic layout includes title, description, flag, keep point, capture point fields, and hint, hint penalty, countries (a symbol for challenges) fields are optional. Level Flags and Bases are built based on this layout but added attachment and link fields.
Level Flags challenges are mostly associated with additional files or links to provide interactive problems during the competition. Teams may be directed to vulnerable servers for exploitation or manipulate certain files.

Unlike jeopardy style challenges involved in Level Flags and Quiz, a special King of the Hill game type is introduced in Level Bases. The link will direct teams to a target server and each team compete to take control of the server. The scores depend on the time that they can hold the target server.

In the contrast, CTFd use one default template for creating challenges, which includes name, category, value(points), static/regex key (flags), file attachments and hints. It supports two different type of answers, static key which is the simple answer in text format and regex keys which is compared with regular expressions. As shown in figure 1, Regex keys is checked by match() method in python and administrators have to write specific regular expression for answers of each challenge.

```python

class CTFdRegExKey(BaseKey):
    id = 1
    name = "regex"

    @staticmethod
    def compare(saved, provided):
        res = re.match(saved, provided, re.IGNORECASE)
        return res and res.group() == provided
```

*Figure 1: Part of the source code of CTFd, which shows the correctness check for regex keys*

But FBctf only support simple text answers in Level Quiz and Level Flag.

5. Challenge Setting

As introduced in the above, FBctf uses different levels to differentiate challenges through their supplement materials and format. In addition, both FBctf and CTFd use field tag to indicate challenges in different knowledge area, including programming, cryptography and web hacking.

*Figure 2: Challenges page of CTFd.*
CTFd directly group challenges based on tags and present them in groups. In contrast, FBctf uses countries in World Map to represent each challenge and allow teams to use filter to select challenges in particular category as shown in figure 3.

Also as shown in the figure 2, solved challenges are colored in green in CTFd while FBctf use status filter to select solved and unsolved challenges.

6. Grading Mechanism

CTFd simply assign points to each challenge and add up those of solved problems for final score, while FBctf employs a more complicated grading mechanism for different levels of challenges.

For levels, FBctf sets two fields Default Bonus and Default Bonus Dec. Default Bonus represents the value received when the first team reaches particular level and scores received by following teams will be Default Bonus minus corresponding Bonus Dec. The later a team arrives at a new level, the less bonus it is awarded.

Additionally, FBctf also uses similar mechanism for each challenge. Bonus field represents scores for the first team to capture this challenge and -Dec field is used to calculate scores for following teams. And both -Dec and Default Bonus Dec can be set to zero, that is all teams arrive at the same stage can get equal scores regardless of their precedence.

As discussed in the above, FBctf needs to assign score to teams based on the length of time they hold the control of the target system in Level Bases. So it needs some mechanism to keep track of the duration time. In control panel, it includes a field called Base Cycle, which represents the number of seconds between two Base check. Each time a Base check is made, team holding the target system will be awarded with certain amount of scores.
Part 2: Team Panel:

1. Game board:

Both FBctf and CTFd includes basic information fields, like team account, scoreboard and challenges. As shown in figure 4, CTFd separates these fields to different pages and allow administrators to add new pages with HTML and CSS.

Figure 4: page options in CTFd

But FBctf includes all fields on the same page and add additional timer to show the remaining time of the game, announcements for administrators to communicate with teams and activity block to update information, as shown in figure 5.

Figure 5: gameboard for competitions
Part 3: Source Code

1. CTFd

CTFd is developed with python, which is easy to read and understand. It is also very friendly to customization as it leaves a plugin folder in source code for developer to add new functionalities. Plugins are supposed to be implemented as Python modules under the instructions in CTFd website.

Figure 6: plugin folder in CTFd and content of _init_.py file

In figure 6, there are two folders challenges and keys in plugin folder now. And the file _init_.py is the main code that is to be compiled. To add a new plugin, developers just need to add additional folder containing the new plugin and then update the _init_.py file to make sure new plugin will be included in load() method.

Similarly, CTFd also supports adding and modifying routes, replacing templates and registering assets.

What’s more, when the platform is running, information about commands submitted to web server will show in the terminal window and it is easier for developers and administrator to keep track of what is happening.
Figure 7: terminal information when CTFd platform is running

2. FBctf

FBctf is developed with Hack, a dialect of PHP language, which is not very familiar for most developers. It doesn’t provide plugin folder for developer to directly add new functionalities. But if one gets familiar with Hack and PHP language, the source code is rather well-structured and easy to modify. As shown in the below, each controller class is in separate files and modification will have little influence on other classes.

Figure 8: files contained in controller folder of FBctf source code
4. Future Work

After analysis, I found that FBctf contains more sophisticated settings, such as timer and announcements block, which can better support a CTF competition. At the same time, as shown in figure, it provides detailed instructions and enough technical support for setting vulnerable servers for attack and defense competition. So FBctf will be chosen as the basic platform to enhance by adding desired functionalities.

Functionality 1: Target System of Level Bases

In Level Bases of FBctf, target systems are expected to hold the King of the Hill competition and some agent files are also needed to be added. The future plan of this project is to design such a target system which can be hold by various teams and include vulnerabilities. At the same time, the system is expected to record the actions and commands of the teams for evaluation.

Functionality 2: Training and Answer Page

In additional to competition mode, FBctf doesn’t provide training materials or answers for participants. So one of the goals is to add new pages or blocks in FBctf, and all necessary learning materials or answers to the challenges can be disclosed with the permission of the administrators.

These two functionalities will be started to be implemented right after the first presentation. The final product of the first functionality will be prepared at the end of February, and the implementation of second one can be expected in March.
Reference:
Cybersecurity Research and Market Intelligence, (2017), Cybersecurity Ventures
Retrieved from https://cybersecurityventures.com/jobs/


Vulcan of DDTek, A history of Capture the Flag at DEF CON

Werther J, Zhivich M, Leek T and Zeldovich N, (2011), Experiences In Cyber Security Education: The MIT Lincoln Laboratory Capture-the-Flag Exercise