

國立清華大學資訊工程系 106 學年度上學期專題報告

專題名稱	雲端攻防平台之容器管理系統				
參加競賽或計畫	<input type="checkbox"/> 參加對外競賽		<input type="checkbox"/> 參與其他計畫		<input checked="" type="checkbox"/> 無參加對外競賽或任何計畫
學號	103062121	102000039	103062305	103062116	
姓名	劉亮廷	林杰	林宛萱	楊澤仁	

摘要

此專題在於學習資安基礎知識及各面向攻擊防禦手法，參加各 CTF 搶旗賽，然後熟悉 CTF 形式的比賽以後，建立一個線上、附帶有沙箱功能的 CTF 練習平台，分為兩個部份：

一、CTF 競賽培訓：

資訊安全競賽幫助我們藉由賽前的練習和比賽來將所學到的知識加以整合與應用。此專題一開始加強專題生在資安方面的基礎知識，並透過每週 Write-up 報告中運用所學的知識去解決資安競賽題目。

二、雲端攻防平台之容器管理系統：

由於在台灣資安方面的教學資源相當稀少，而且提供沙箱功能的 CTF 網站也非常少，因此我們決定架設常駐於線上、附帶有沙箱功能的 CTF 練習站，期望能提供未來資安人才一個練習平台，並透過架設的過程中，研究網站之沙箱管理，以及對於資安方面更進一步的瞭解。

中華民國 106 年 11 月

一、CTF 競賽培訓

甲、簡介：

CTF，全稱 Capture The Flag，即為奪旗賽，起源於 DEFCON 大會(1996/4)，現已發展為全球性質的網路資安比賽。大致流程為：參賽隊伍之間透過進行攻防對抗、程序分析，進而從主辦方得到一串具有一定格式的字串(稱作 Flag)，再將此交給主辦方奪得分數。其中題型大致分為：

1. Reverse 逆向工程
通常由主辦方給一個或多個 Binary，過關所需之 Flag 通常藏在執行檔裡，要將程式逆向分析才能找出。
2. Pwnable 弱點漏洞分析
從伺服器運行的弱點程式或 Server 執行檔，透過靜態分析(static analyze)或動態分析(dynamic analyze)來找出該程式的弱點(Buffer overflow)，進一步取得在遠端 Server 的金鑰。
3. Crypto 密碼學
從密文、加密程式分析加解密演算法找出演算法的弱點來解出真正的明文。
4. Forensics 鑑識
從封包、Log、Memory Dump、Disk Image、VM image 等鑑識出隱藏在之中的金鑰。
5. Web Security 網路安全
有 SQL Injection / Command Injection / Cookie / Race Condition 這幾類。
6. Misc 綜合類型
非處於上述所提類型的題目。

乙、培訓過程

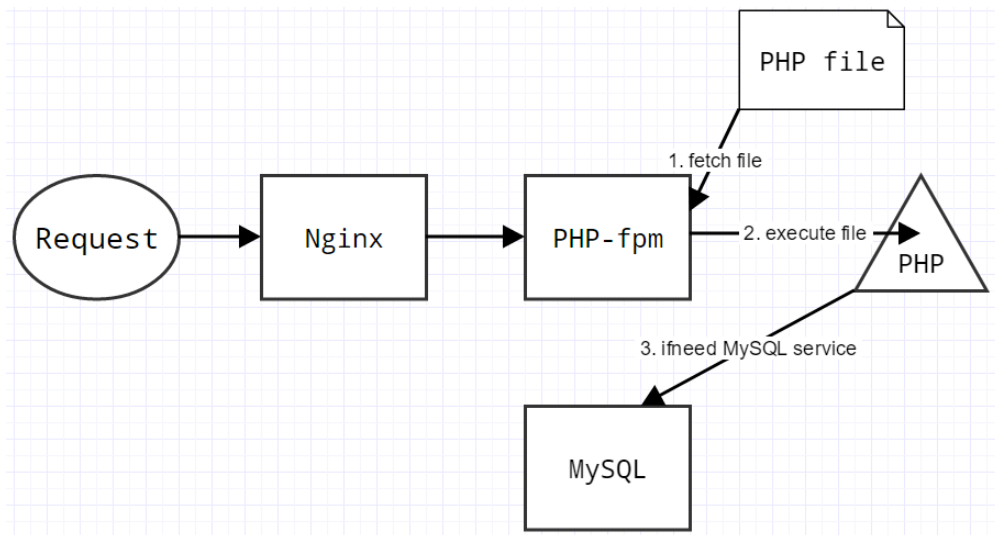
我們在大三上學期即開始進行培訓，從去年 10 月開始，每週由學長講解資安方面的知識，每位學生須於每週解出一題 CTF 競賽的題目，並於 Meeting 時進行報告，相關上課內容也有上傳至 YOUTUBE 供日後之複習(相關影音網址: <https://goo.gl/Twjbce>)。學習的主題大致有：

1. Docker 之使用與指令
2. 熟悉 Linux, Tmux 環境操作
3. 靜態分析程式(IDA PRO、QIRA...)
4. 動態分析程式(GDB)
5. Pwn Tool 之操作
6. Format String 漏洞利用與防禦
7. Stack Overflow 漏洞利用與防禦
8. Shellcode 覆蓋正常程式碼返回地址
9. Web server、Database 架設



圖表 1

其中在每周的報告看到了許多 Crypto、Forensics 以及 Web 類型，主要是教授 Pwnable 及 Reverse。從大三上學期至今約有 17 堂課，另外也有參加了兩次 CTF 線上賽，在當周六日專題生在台達會議室一起打比賽。也會統整寫下 write-up 供日後參考及同儕間互相觀摩學習。



圖表 2

在大三下學期時，為了做出第二部分的雲端攻防平台之容器管理系統，我們開始研讀架設網站相關知識，學習伺服器架設，以及資料庫操作，學習 PHP, MySQL, HTML, CSS 等等語言，並做了多項練習，如寫出簡易的會員網站。透過這些基礎使得我們能夠建置一個 CTF 管理系統，並以近期熱門的 Docker 技術來實現，將使用者的攻擊行為與主機隔離，使得這些攻防行為不會影響主機的運行，達到極高的真實性模擬。

丙、競賽成果





The image shows a colorful poster for the 106th National Cyber Security Skills Competition (資安技能金盾獎). The title is in large, stylized orange and yellow characters. Below it, the subtitle '入圍決賽名單 (依隊伍名稱排序)' is in blue. The main content is a table with two columns: '學校' (School) and '隊伍名稱' (Team Name). The table lists 30 teams. The team '清華大學' (Tsinghua University) with the name '打錯QQ' is highlighted with a red rectangular box. The poster also features cartoon characters of a boy and a girl in superhero costumes, and various icons related to cybersecurity like a padlock, a key, and a computer monitor.

學校	隊伍名稱
臺灣大學	S1
交通大學	0xb43b00f0xb43b00f
臺灣科技大學	11894666
中央大學	127.0.0.1
臺灣科技大學	9136
暨南國際大學	BlueDoT
中正大學	CCU_SAF
中正大學	CTF從入門到放棄
交通大學	CT's bar
中央大學	DoubleSigma
交通大學	DSNS_Love_Learning_Machine_Learning
臺灣科技大學	FIN
臺灣大學	how2hack
高雄第一科技大學	NKFUST
高雄第一科技大學	or 1=1 -童年
中央大學	PDC
清華大學	PentaKill
新北市立清水高級中學	Sean
成功大學	Spot : 謝隨!
成功大學	Spot 2.0
交通大學	SQLab_RETURN
臺灣大學	ZeroDegree
清華大學	人語仁道並未有
清華大學	打錯QQ
交通大學	志在把殼不往參加
臺灣科技大學	孤單寂寞覺得冷
臺灣科技大學	所有參賽隊伍
中央大學	留包子大撒幣
臺灣大學	森77
中央大學	結果被打爆
臺灣科技大學	想想隊名

圖表 3













我們於 106 年 10 月 14 日參與行政院所舉辦的金盾獎競賽，此競賽為國內相當大的資安競賽，我們從一百多隊的激烈競爭中脫穎而出，獲得決賽資格，初賽內容分為資安學術題與實作題，由於在專題培訓期間訓練扎實，實作題做得相當順手，我們也在初賽前複習不少基礎知識，因此在學術題獲得了不錯的成績。近期內我們將為繼續為比賽做準備，期許能在決賽獲得不錯的成績。圖 3 為晉級名單，紅框標示我們的隊伍。

另外，我們於培訓期間參加過兩場 CTF 線上賽: Pragma CTF 2017 以及 AlexCTF，取得的成績如下網址：<https://ctftime.org/team/33347>，專題生每人至少能完成一題，再加上助教的幫忙才有此成績。

41	b1n4ry4rms	
42	True0xA3	
43	ukk1337	
44	flagish	
45	PentaKill	

圖表 4

首先是 AlexCTF，作為大三上學期的驗收，這次比賽中遇到較多困難的是 Reverse 方面的題目，大部分是在助教引導下完成題目，我們學到了如何處理經過加殼及混淆的程式，還有 python 檔的逆向分析。而我們也解出了其他較為簡單的 Forensics 題目，像是 PNG 檔的編碼處理，特殊格式檔案處理。附圖 figure 3 是在第二天結束後的成績(比賽持續一周，但是我們用那一周的六日兩天比線上賽)。比賽結束後大家將解題的過程放到網路筆記上，讓彼此互相觀摩一下解法([Write-up 連結](#))。

#	Team	Country	Points
1	217		1,060
2	ASIS		885
3	khack40		885
4	tushalien		660
5	Scrypter		660
6	REU		610
7	ShortSpicy		510
8	Aravinth Ramesh		510
9	Abhijith V		510
10	Beers4Flags		510
11	bi0s		510
12	PentaKill		510

圖表 5

再來是 Pragma CTF，這一次的題型較上次難一點，而我們進行的模式也是和上次一樣，選六日兩天來打這個線上賽，當作經驗的累積。彼此討論出題目從哪個方向著手最適當，解出題目後專題生也有寫 Write-up([Write-up 連結](#))讓彼此觀摩。

二、雲端攻防平台之容器管理系統

甲、動機與目的：

資安、軟體安全議題一向是軟體開發中極為重要的領域，近期由於 WannaCry 等 malware 猖獗，而使得資安議題再次受到重視。而資安是一項除了知識以外，實作、經驗均非常重要的研究領域，許多教學中會使用隔離環境（沙箱）與打線上比賽（CTF）的形式學輔助學習。

但一方面至今很少有常駐於線上、附帶有沙箱功能的 CTF 練習站，另一方面台灣在資安方面的開放教學資源缺乏，所以我們希望提供一個開放的、附有線上即時沙箱模擬的 CTF 平台，以供研究、教學、比賽使用。

乙、現有相關研究概況與比較：

國外經常舉辦 CTF 競賽，但多數網站僅在競賽期間（三天至一週）開放使用，並非常駐、難度也參差不齊，即便有少數網站提供常駐的練習服務，但大多只是簡化版的題目。

此外，提供沙箱功能的網站也非常少數，大多是提供靜態的網站，難以提供可能會對服務造成破壞性干涉的題目，我們希望藉由 Docker 實現個人化的沙箱模擬實際環境，可以提供更多樣的題目類型與擬真的環境。

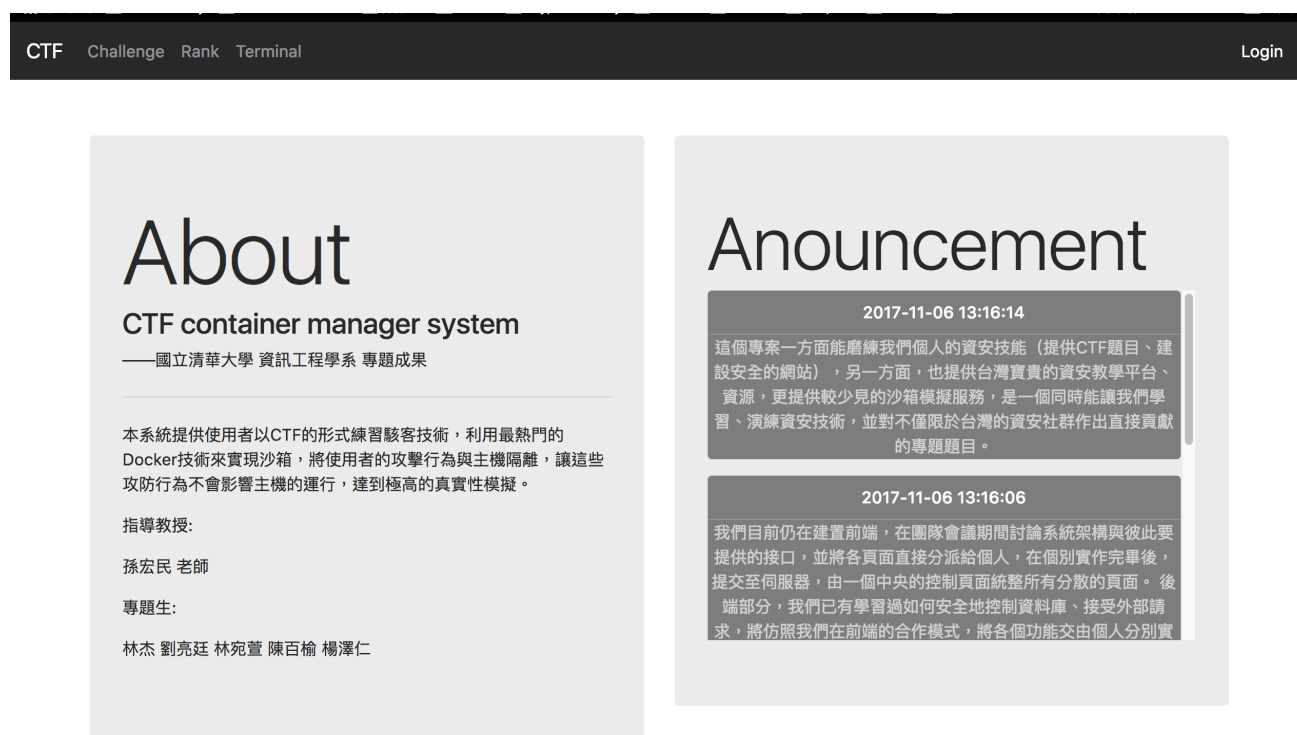
丙、設計原理與實現：

i. 整體框架

因 CTF 競賽主要目的是以實際操作、攻擊的方式，演習、練習資安相關技術，所以希望環境愈擬真愈好，並且我們的網站本身也要安全、不能被隨意攻破，所以我們的前後端、使用比較成熟的框架，前端使用 jQuery 與 Bootstrap，後端則使用 PHP 與 MySQL。

而沙箱模擬、管理部分，由於觀察到近日熱門的 Docker，其容器的啟動可以在秒級實作，這相比傳統的虛擬機方式要快得多。另外，Docker 對系統資源的使用率很高，一台主機上可以同時執行數千個 Docker 容器。這些特性十分符合我們架設 CTF 練習站

的需求，因此我們決定使用 Docker 來針對不同題目、使用者，建置獨立的沙箱環境，在能讓使用者得到高度擬真的體驗同時，也確保網站本身後台的安全性。



圖表 6

整體網站以導覽列為網站主體(圖 6)，根據使用者前往不同的頁面而嵌入對應的頁面至中心顯示區域，並同時檢查使用者的權限，對符合權限的使用者主動顯示連往管理頁面的連結，並在管理頁面內會再次檢查權限。

ii. 容器與 Web terminal

首先在 Web terminal 部份中，我們修改開源專案，針對我們的使用情境進行底層原始碼修正，提供使用者獨立的虛擬環境進行解題，以供教學、練習使用。架構上，在網站本體之外會開啟另一個處理 web terminal 使用請求的伺服器，接受、檢查使用者是否具有權限訪問 docker 虛擬容器。

```
CTF Challenge Rank Terminal [admin] challenge [admin] about [admin] post [admin] docker [admin] user Hello! admin

root@a319b492a691:/# ls
afl-2.51b boot etc lib32 media pin qemu run sys var
bd_build challenge home lib64 mnt proc qira sbin tmp
bin dev lib libx32 opt QAQ root srv usr
root@a319b492a691:/# python
Python 2.7.12 (default, Nov 19 2016, 06:48:10)
[GCC 5.4.0 20160609] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

0 python

圖表 7

若是使用者權限符合，則此伺服器會將 docker 虛擬容器的 command line 與前端的 web terminal 進行雙向連接，此連接會將所有資訊直接通過兩層 port forward 進入雙層的 docker 虛擬容器內部，確保使用者間無法互相訪問，也確保沙箱的周密性、絕對不會被打穿。

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES	
7d4f9f94cc0d	duckll/ctf-box	"/sbin/my_init"	10 days ago	Exited (0) 10 days ago		user-28	<div>Kill</div> <div>Remove</div>
e6656ad4cdca	duckll/ctf-box	"/sbin/my_init"	10 days ago	Up 10 days	3002/tcp, 0.0.0.0:9489->4000/tcp	q-fd	<div>Kill</div> <div>Remove</div>
4833c2680ad3	duckll/ctf-box	"/sbin/my_init"	10 days ago	Exited (0) 15 hours ago		user-26	<div>Kill</div> <div>Remove</div>
94bbf9de65fb	duckll/ctf-box	"/sbin/my_init"	10 days ago	Up 10 days	3002/tcp, 0.0.0.0:9488->3000/tcp	q-limited_users	<div>Kill</div> <div>Remove</div>
c256c6c2e5c4	duckll/ctf-box	"/sbin/my_init"	10 days ago	Up 10 days	3002/tcp, 0.0.0.0:9487->5000/tcp	q-flask_injection	<div>Kill</div> <div>Remove</div>

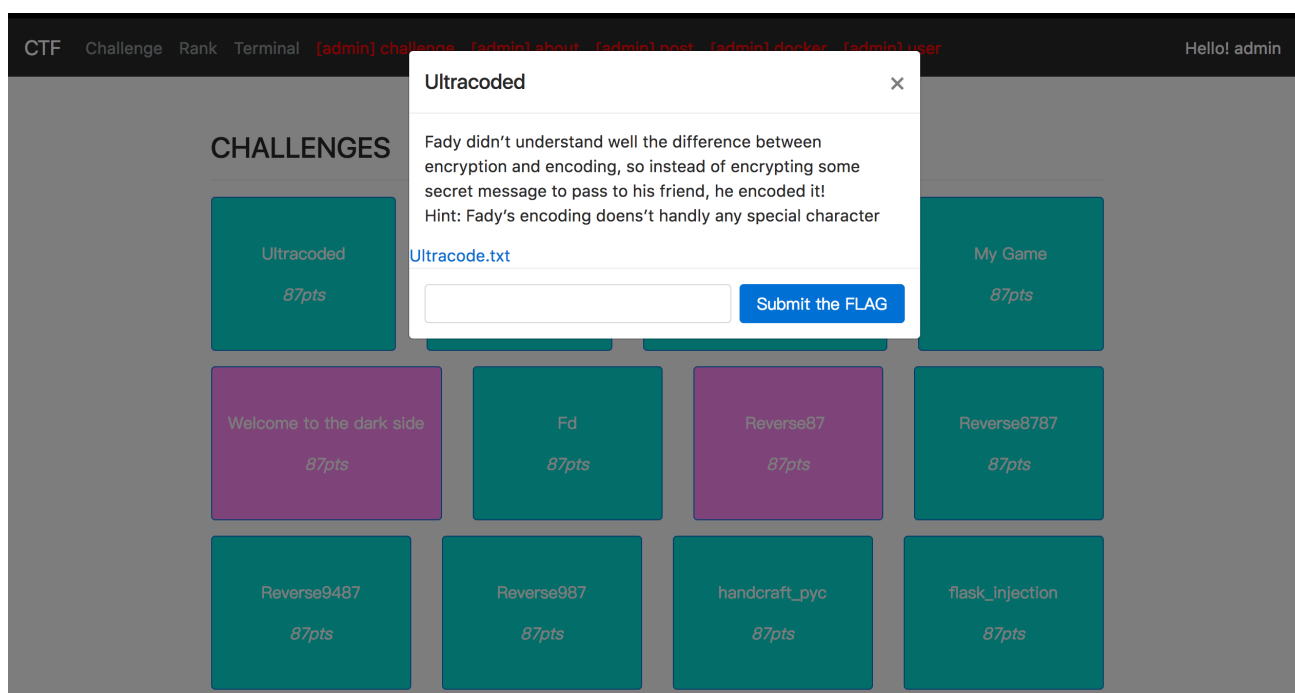
圖表 8

在 Docker 部分中，當使用者註冊帳號成功時，伺服器會創立一個容器給該名使用者，使用者可在登入以後，使用 web terminal 來操作此容器，並透過容器來競賽、解題。另外在管理方面，我們在 Docker 管理頁面(圖 8)，透過 docker 內建的指令，並經由我們做字串處理後顯示於管理頁面中，方便監控所有使用者的資源使用量，並根據管理者需求開啟、停止、刪除使用者的個別容器，以達到方便、即時的管理。

iii. 題目部份

1. Challenge :

Challenge 為使用者挑戰解題的頁面(圖 9)，將我們所設計的不同的 CTF 題目分別顯示在頁面上一個個可點擊的藍色小方格內，點擊每一個方格即可看見所對應的題目敘述跟附加檔案，點及檔案連結即可下載檔案，題目敘述的下方為 Flag 的欄位，使用者解出題目的 Flag 後，將 Flag 打在這個欄位中。



圖表 9

按下「Submit the flag」後，即會送出使用者填寫的 Flag 到伺服器，伺服器會判斷使用者填入的 Flag 是否正確，若使用者解出正確的 Flag，會跳出「恭喜解出 Flag」的訊息，藍色的小方格也會變成粉色。

CHALLENGES

Ultracoded 87pts	unVM me 87pts	1magePr1son- Nozambique 87pts	My Game 87pts
Welcome to the dark side 87pts	Fd 87pts	Reverse87 87pts	Reverse8787 87pts
Reverse9487 87pts	Reverse987 87pts	handcraft_pyc 87pts	flask_injection 87pts

圖表 10

2. 題目設計

目前網站上已放有我們設計的題目，這些題目都是透過我們在這一年當中所習得的資安知識所設計出，期望能在網站架設之初提供使用者練習，日後會陸續新增題目，如同 CTF，題目分為以下幾類：

Reverse 逆向工程：目前網站上的 Reverse 題皆為較基礎的題目，使用者會獲得題目檔案，並透過反組譯該檔案，觀察其組合語言，從中找出檔案的加密規則，並取得 flag。另外也有針對 python 檔案的題目，使用者必須了解 python 編譯的過程，才能取得 flag。

Web 網路安全：Web 題目的設計理念在於如何管理最小資訊顯示，並警覺於任何模板注入(template injection)攻擊，我們提供 flask injection 與 cookie 管理的題目，達到警醒解題者應警覺於「處理使用者輸入字串」、「不應任意儲存資料於使用者端」的目的，並提升使用者對於網頁設計時應遵行的安全守則警覺度。

Crypto 密碼學：使用者必須將亂碼透過常見的加密解密技術來取得 flag，其中包含常見的 base64 以及 md5，另外也有結合圖片的題目，使用者需將亂碼透過 python 印成圖片以取得 flag。

Forensics 鑑識：使用者需從提供的檔案中找出 flag，如處理圖片的 pixel 以計算出 flag，透過多樣化的設計，要求使用者擁有處理不同類型檔案的能力。

iv. 管理者部分

為了方便管理者管理此平台，我們建設許多管理頁面，其中包含使用者管理、發佈新題目、發佈新公告以及管理容器，管理者在使用管理帳號登入以後，網站上方會出現數個管理頁面(以紅字顯示)可供點選，將管理者導向各個管理頁面。

CTF	Challenge	Rank	Terminal	[admin] challenge	[admin] about	[admin] post	[admin] docker	[admin] user	Hello! admin
uid	ID	Password							
0	admin	\$2y\$12\$Cjwdf60usEL5Nm9Uy.ib.sFgk.VICqbKmN7yn6qvgM9vbOluA5aG				#FuckPhpBtw	174	abc@gg.gg.gggg	1.161.220.57
8	test	\$2y\$12\$uOOHPqmAaJ1hd9i1o0tCzeL6lMA3MDv/fhAF7aG2tQiiyn6SGjXu				test	0	test@test.test	111.254.119.198
9	test2	\$2y\$12\$imklvhF3dURM78LSOjqU6eb0GTCnbpWbu8xqQ4V4VI729ABvdl/7G				test2	0	test2@test.test	140.114.40.187
10	abc	\$2y\$12\$WdFy0nFKiuQYVeMQJj03rOdmZVEdqMR0tO36HGJwQr0mPeS9t8AvS				abc	0	abc@gmail.com	
11	DuckLL	\$2y\$12\$uOTnHJmK4TZtr5s7BDjBte0VXwXX8xMHdACWloiV9Yy7bkoyuQLJS				pwn the world	0	a347liao@gmail.com	
12	aaa	\$2y\$12\$M0Xt7LwLMX38dD9C1We4KusWYdnr27pykZez.qX3qOVyqtbD2dZv6				aaa	0	a@a.com	
13	zzz	\$2y\$12\$15/.H7.LBjiNuS/YKyWbu.N1kBzA7LQikfm2.3ZQHqhb0VoCpw032				z.z	0	a@a.com	
14	asdf	\$2y\$12\$zxAzjhY.657lm9EVUJvCb.Pk50N9aao6/rIYL4iul2kTIEGkU9N7W				asdf	0	a@a.com	

圖表 11

圖 11 為管理使用者的頁面，在這邊記錄著各個使用者的資訊，若在競賽進行中發現使用者作出違規行為，管理者也透過此頁面可以刪除使用者。

CTF

Challenge

Rank

Terminal

[admin] challenge

[admin] about

[admin] post

[admin] docker

[admin] user

Hello! admin

Add problem

Name

Point

Description

Flag

File input

選擇檔案

未選擇任何檔案

reset

Submit

圖表 12

Modify problems		
Problem		
Ultracoded	<div>Delete</div>	<div>Modify</div>
unVM me	<div>Delete</div>	<div>Modify</div>
1magePr1son- Nozambique	<div>Delete</div>	<div>Modify</div>
My Game	<div>Delete</div>	<div>Modify</div>
Welcome to the dark side	<div>Delete</div>	<div>Modify</div>
Fd	<div>Delete</div>	<div>Modify</div>
Reverse87	<div>Delete</div>	<div>Modify</div>
Reverse8787	<div>Delete</div>	<div>Modify</div>

圖表 13

除此之外，也有管理題目的頁面(圖 12 及圖 13)，讓管理者能夠新增題目以及修改現有的題目。

Adding New Announcement

Description

Submit

aid	Description	Time	Delete
26	Testing	2017-11-06 13:04:00	<input type="radio"/>
28	本系統提供使用者以CTF的形式練習駭客技術，利用最熱門的Docker技術來實現沙箱，將使用者的攻擊行為與主機隔離，讓這些攻防行為不會影響主機的運行，達到極高的真實性模擬。	2017-11-06 13:05:03	<input type="radio"/>
30	整體網站以導覽列為網站主體，根據使用者前往不同的頁面而嵌入對應的頁面至中心顯示區域，並同時檢查使用者的權限，	2017-11-06	<input type="radio"/>

圖表 14

圖 14 為管理公告的頁面，管理可在此發佈新公告以及修改公告。

CTFChallengeRankTerminal[admin] challenge [admin] about [admin] post [admin] docker [admin] userHello! admin

容器管理

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES	
7d4f9f94cc0d	duckll/ctf-box	"/sbin/my_init"	10 days ago	Exited (0) 10 days ago		user-28	<div>Kill</div> <div>Remove</div>
e6656ad4cdca	duckll/ctf-box	"/sbin/my_init"	10 days ago	Up 10 days	3002/tcp, 0.0.0.0:9489->4000/tcp	q-fd	<div>Kill</div> <div>Remove</div>
4833c2680ad3	duckll/ctf-box	"/sbin/my_init"	10 days ago	Exited (0) 16 hours ago		user-26	<div>Kill</div> <div>Remove</div>
94bbf9de65fb	duckll/ctf-box	"/sbin/my_init"	10 days ago	Up 10 days	3002/tcp, 0.0.0.0:9488->3000/tcp	q-limited_users	<div>Kill</div> <div>Remove</div>
c256c6c2e5c4	duckll/ctf-box	"/sbin/my_init"	10 days ago	Up 10 days	3002/tcp, 0.0.0.0:9487->5000/tcp	q-flask_injection	<div>Kill</div> <div>Remove</div>

圖表 15

圖 15 則是容器管理頁面，此頁面能夠讓管理者監控所有使用者的資源使用量，並根據管理者需求開啟、停止、刪除使用者的個別容器，以達到方便、即時的管理。

丁、專題重要貢獻

- 1.提供國內外資安競賽、練習環境
- 2.提供高度擬真的沙箱環境，增加練習題目的多樣性與練習效果

戊、團隊合作方式

我們在團隊會議期間討論系統架構與彼此要提供的接口，前端部分，將各頁面直接分派給個人，在個別實作完畢後，提交至伺服器，由一個中央的控制頁面統整所有分散的頁面。後端部分，由於我們已有學習過如何安全地控制資料庫、接受外部請求，將仿照我們在前端的合作模式，將各個功能交由個人分別實作、測試。最後題目部分，則是由每人參考自己的長項，研究過去所寫過的題目，將其做過變化後，製作出五題題目，放至網站上提供使用者練習。

己、效能評估與成果

一方面考慮經費，另一方面資安目前並不是非常熱門的研究領域，我們目前預計提供一百個使用者同時上線、使用沙箱，未來在專案完成後，若有需要繼續拓展，也許能考慮分散式系統。

庚、結論

這個專案一方面能磨練我們個人的資安技能（提供 CTF 題目、建設安全的網站），另一方面，也提供台灣寶貴的資安教學平台、資源，更提供較少見的沙箱模擬服務，是一個同時能讓我們學習、演練資安技術，並對不僅限於台灣的資安社群作出直接貢獻的專題題目。

參考文獻：

1. 俞甲子、石凡、潘愛民(2009)。《程式設計師的自我修養：連結、載入、程式庫》。賴榮樞譯。台灣。碁峰。
2. HOW TO Binary Patching. The Brute Force of Reverse Engineering with IDA and Hopper (And a Hex Editor), from <https://goo.gl/259N9m>
3. Iman Karim. How to inject code into a exe file, from <https://goo.gl/tnFwyd>