

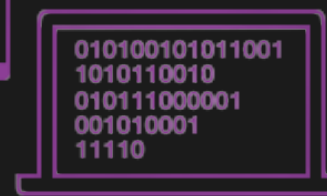
周佑康 口試報告

台中市立文華高級中學



國立清華大學 資訊工程學系

National Tsing Hua University Department of Computer Science



簡要介紹



文華高中
周佑康

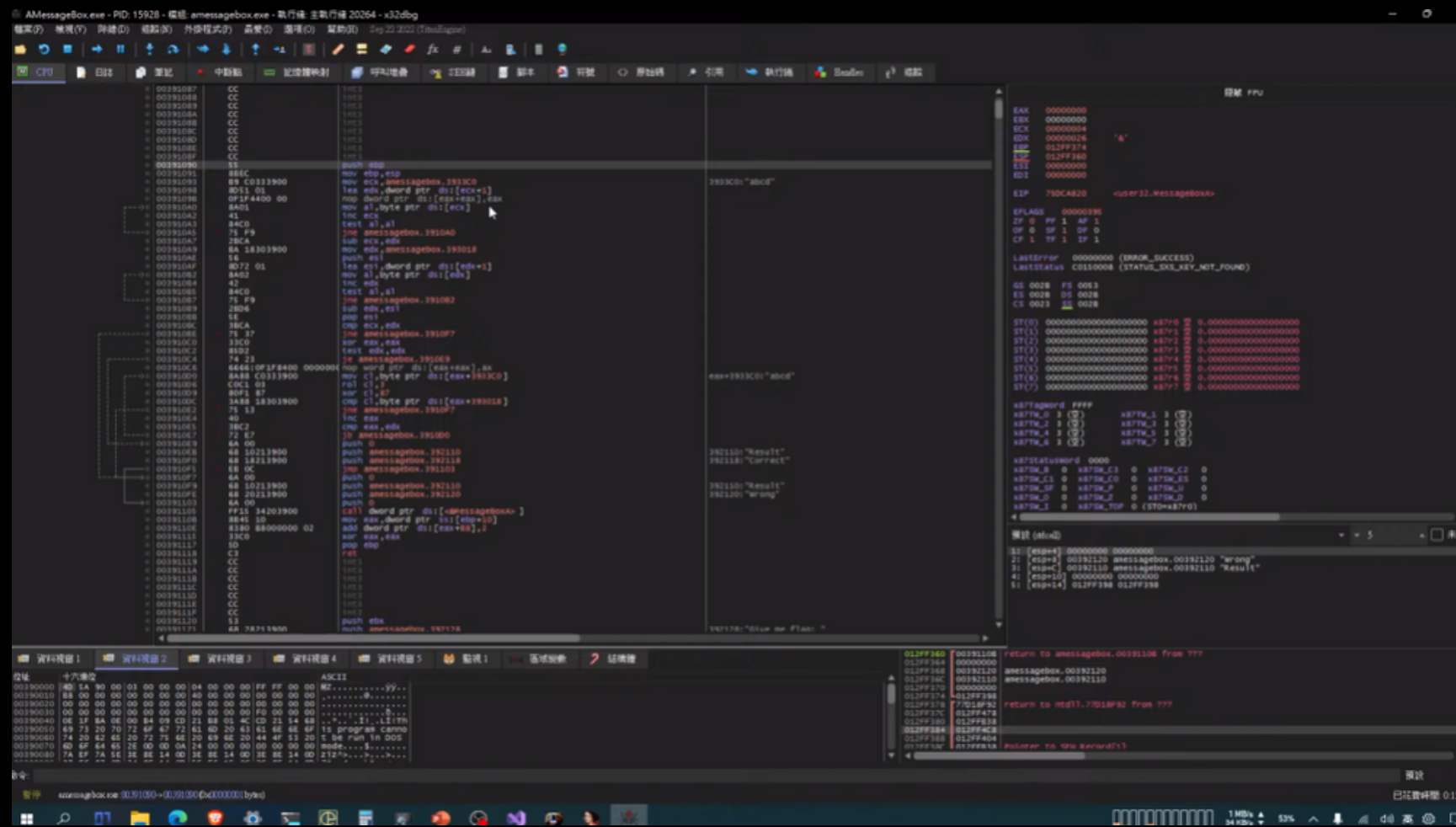
- 中部電資聯合會議 @會長/創會人
- 中部電資多項活動 @總召
- AIS3 Junior @助教 | AIS3 Club @講者
- 金盾獎 2022@第二名 2021@第三名
- 善於漏洞挖掘、工具開發、社群運營

資安專長

資訊之路

教學經驗

社群運營



資安專長

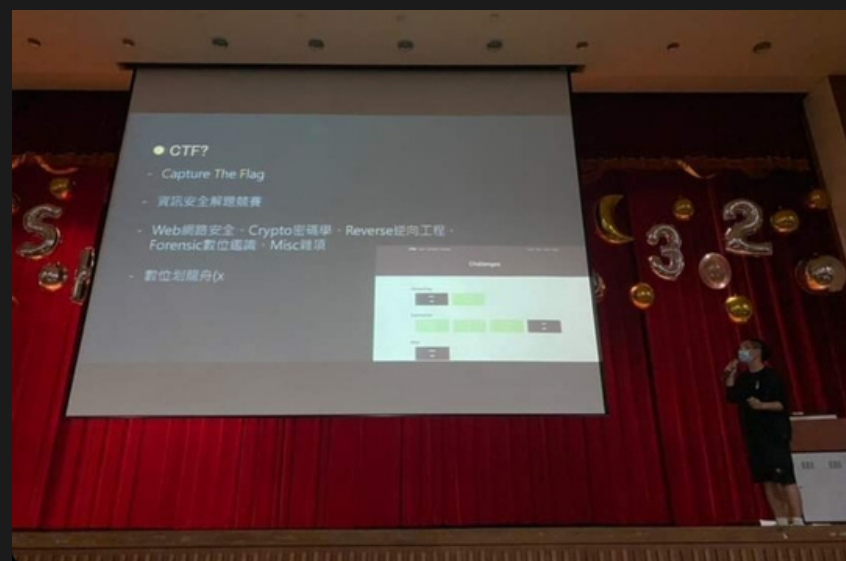
-windows 攻擊注入

學習方式

資安專長

途徑

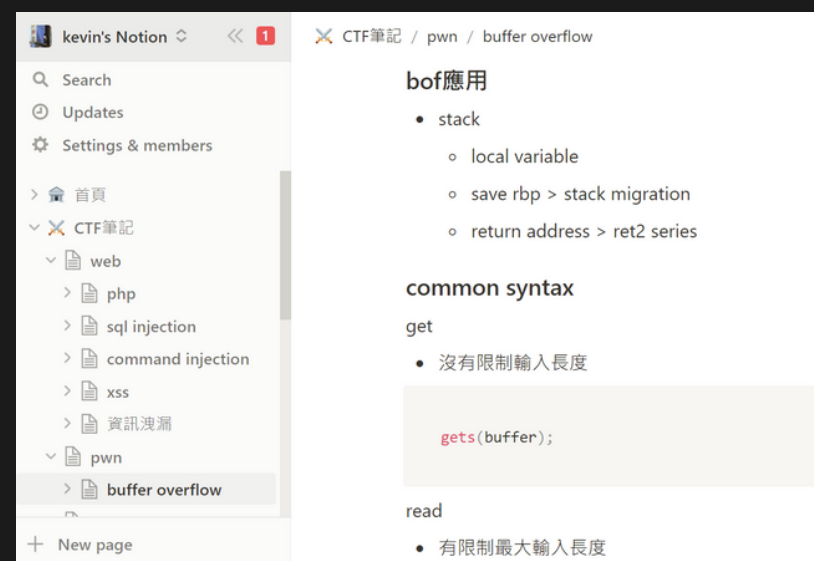
- 解題
- 從開發學起



校內自主學習成果發表
「CTF學習之路」

筆記／整理

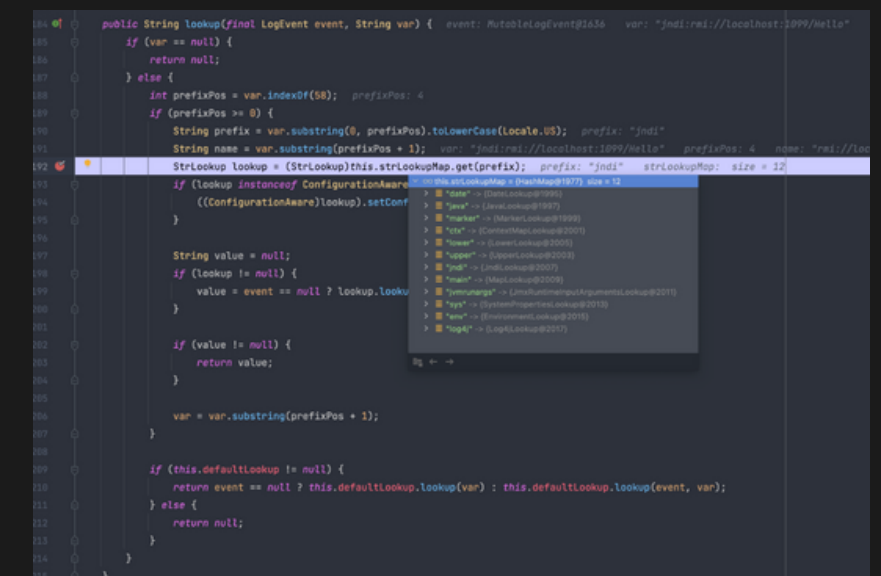
- Notion CTF筆記
- 個人blog



notion中的CTF筆記

漏洞重現

- exploit
- 靶機架設



log4j shell exploit

漏洞挖掘

資安專長

熟悉工具

```
Windows PowerShell x meowkb@DESKTOP-08JRMBC x + - □ x
[04:51:01] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[04:51:04] [WARNING] POST parameter 'password' does not seem to be injectable
[04:51:04] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--
level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of prote
ction mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2com
ment') and/or switch '--random-agent'
[04:51:04] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 68 times

[*] ending @ 04:51:04 /2022-12-11/

(meowkb@DESKTOP-08JRMBC)~[~/payload]
$ sqlmap -r sqlmap

  --H--
  --C-- {1.6.7#stable}
  --S--
  --V-- https://sqlmap.org

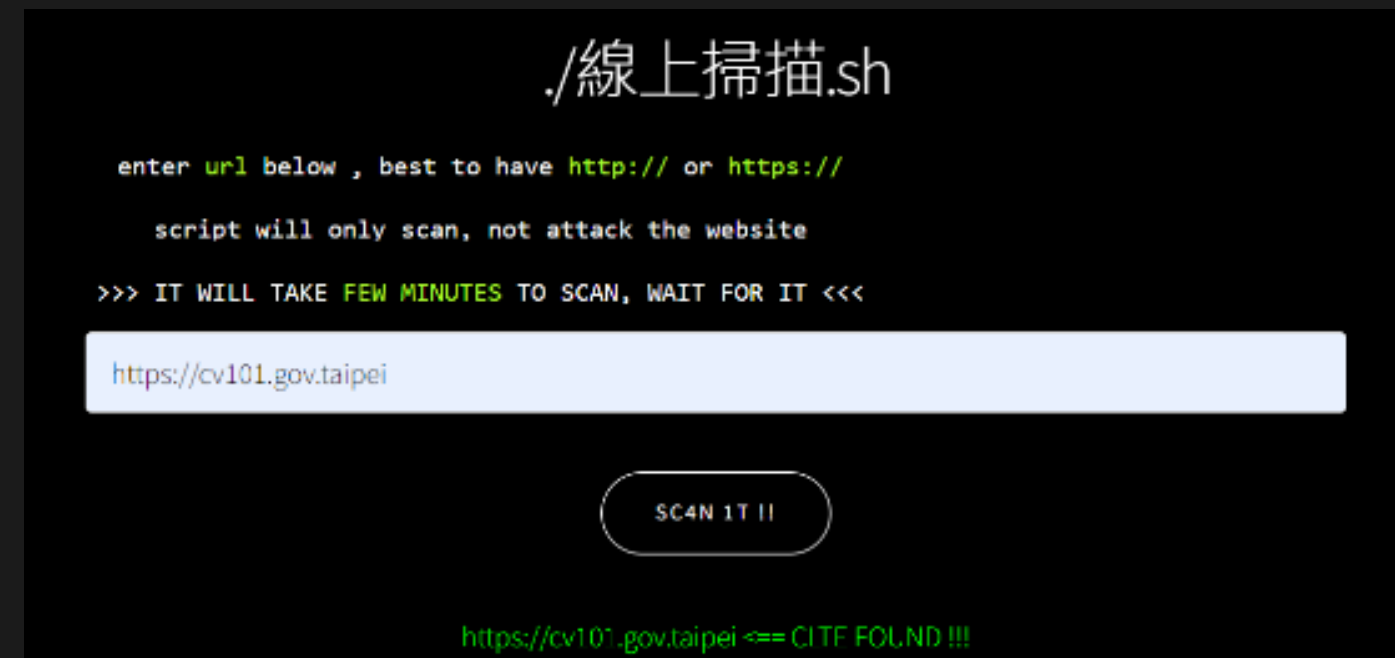
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is
the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no
liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 04:54:14 /2022-12-11/

[04:54:14] [INFO] parsing HTTP request from 'sqlmap'
[04:54:14] [INFO] testing connection to the target URL
got a 302 redirect to 'http://h4ck3r.quest:8200/?failed'. Do you want to follow? [Y/n] |
```

知名sqli偵測程式 sqlmap

自行開發&腳本撰寫



「模組化自動OWASP漏洞檢測工具」

漏洞挖掘

資安專長

2022 AIS3 專題發表

```
2 # -*- coding: utf-8 -*-
3 import os
4 import numpy as np
5 from tqdm import tqdm
6 import sys
7 import time
8 import timeout_decorator
9 from pathlib import Path
10
11 ## functions
12 def scanurl(url):
13     reurl = f'curl -s -o /dev/null -w "%{url}%" {url}'
14     result = os.popen(reurl).read()
15     context = re.findall(r'HTTP/1.1 200 OK', result)
16     state = ""
17     for line in result.splitlines():
18         state += line
19     result.close()
20     return(state)
21
22 def _handle_time_out(url):
23     raise TimeoutError
24
25 @timeout_decorator.timeout(10)
26 def test(url):
27     if sys.argv[1] == 'url':
28         meow = scanurl(url)
29         print(meow)
30         print(url)
31         if meow:
32             return '1'
33     else:
34         return '0'
```

```
thomaswang@thomaswang-PC:~/mnt/c/Users/thoma/Desktop/sublime/CTF/smuggler$ ./ais3.sh list.txt
```



根據利用腳本爆破出各部會相關 subdomain，並嘗試解析排出正常可使用的網域

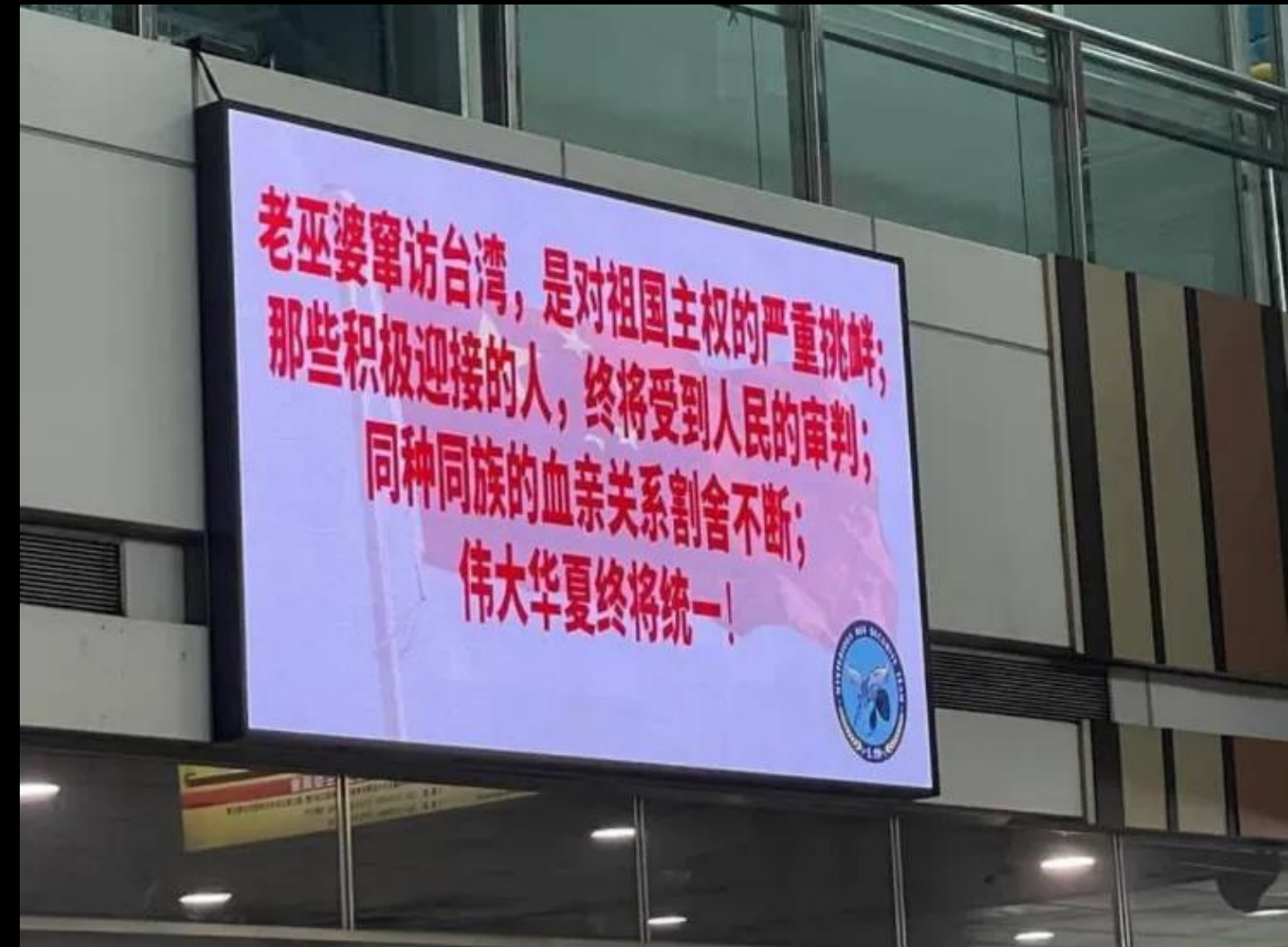
自行撰寫腳本，達成自動化掃描臺灣各大政府網站是否含有可利用的 http request smuggling 漏洞

以台北志工整合平台為例 驗證封包污染的可行性後進行相關單位的漏洞通報

漏洞挖掘

資安專長

2022 AIS3 專題發表



伺服器&網路

資安專長

伺服器



自家homelab
使用routeros作為主路由
搭配兩台塔型伺服器 兩台終端定位電腦

網頁開發

名稱	內容	類型	狀態	修改
ctfd	23.94.104.5	A	運行中	⋮
templatesite	23.94.104.7	A	運行中	⋮
meow1026	meow1026.github.io	CNAME	待處理	⋮
react			尚未註冊	⋮

利用flask搭配cloudflare api開發
「文華電腦研究社子域名註冊系統」

伺服器&網路

資安專長

IDC建置



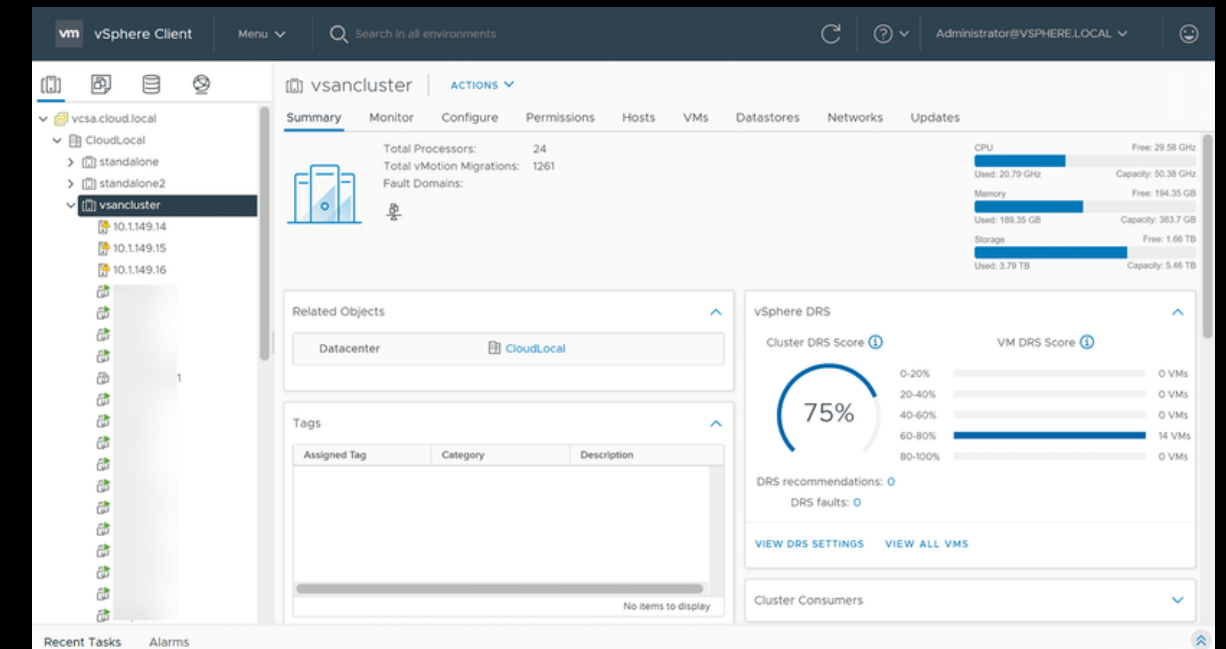
熟悉網路硬體
圖為使用附載均衡、switch、實體防火牆、路由器搭配機房多台主機使用

雲端運算

```
root@whcsc: ~  
PS C:\Users\User> ssh root@103.144.32.16  
root@103.144.32.16's password:  
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-132-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
System information as of Sun Dec 11 18:27:04 UTC 2022  
  
System load:  0.02          Processes:            124  
Usage of /:   23.9% of 28.89GB  Users logged in:    0  
Memory usage: 25%          IPv4 address for docker0: 172.17.0.1  
Swap usage:   0%           IPv4 address for eth0:  103.144.32.16  
  
* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.  
  
https://ubuntu.com/engage/secure-kubernetes-at-the-edge  
  
47 updates can be applied immediately.  
To see these additional updates run: apt list --upgradable  
  
New release '22.04.1 LTS' available.  
Run 'do-release-upgrade' to upgrade to it.  
  
*** System restart required ***  
Last login: Fri Dec  9 19:11:10 2022 from 123.241.59.71
```

在全球擁有多台雲主機
以利進行相關雲端運算功能，以及跨區瀏覽、VPN、驗證時間鉗形攻擊等

vSphere



利用vsphere管理多台虛擬機
開設多項網路功能如:校內NAS
網頁伺服器、GITLAB Server等

競賽參與

資安專長

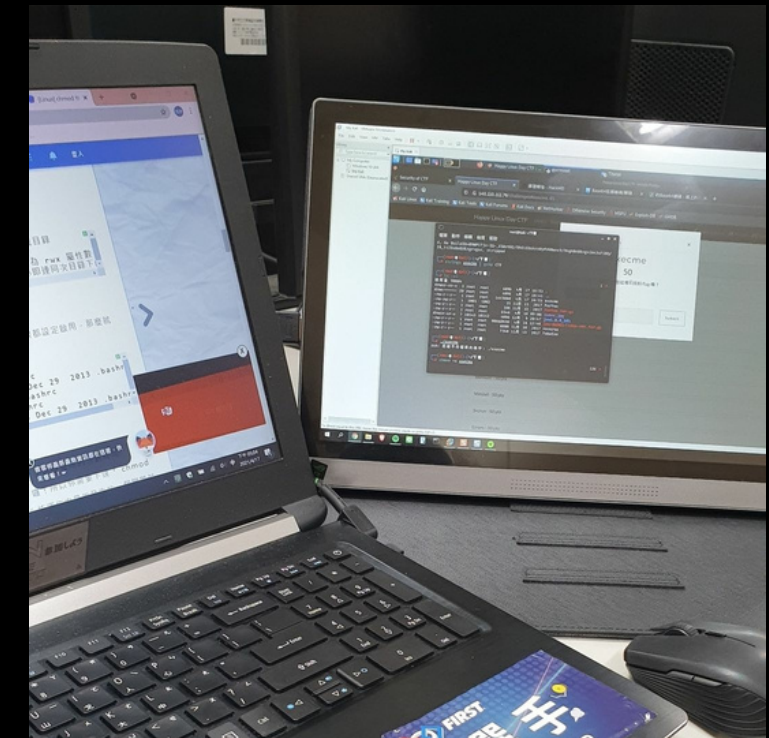
2021行政院資安技能金盾獎
第三名



2022行政院資安技能金盾獎
第二名



國內知名CTF競賽
balsn、TSJ、EoF



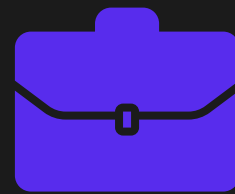
競賽參與

資安專長



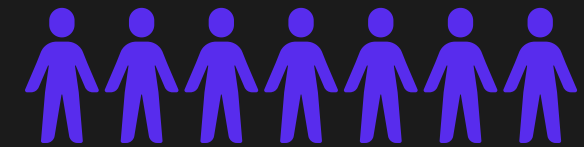
擅長題型

web、reverse、
crypto、MISC



通靈

利用自身的觀察力，協助
隊友挖掘漏洞



團隊分配

合理分配任務，
協助組內溝通、協調



資訊能力

python專案-口罩識別

學習路徑

國中時期

機器人、物聯網開發

- EV3-G / Arduino
- 樹梅派與linux
- 網頁開發
- 機器人競賽(WRO、FLL)

高一

程式競賽

- C++
- 演算法 & 資料結構
- 專題競賽

高二

資訊安全

- 深入網頁安全
- 逆向工程、密碼學
- 伺服器、linux系統
- 資安系列競賽

高三

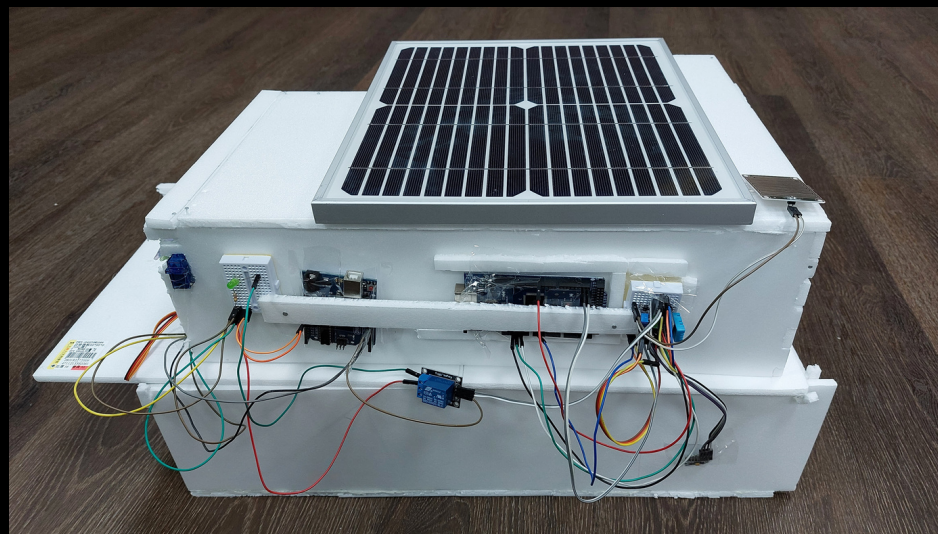
資訊安全+機器學習

- 初探機器學習
並結合資訊安全
- ADM 進階防禦模組

專案開發

資訊能力

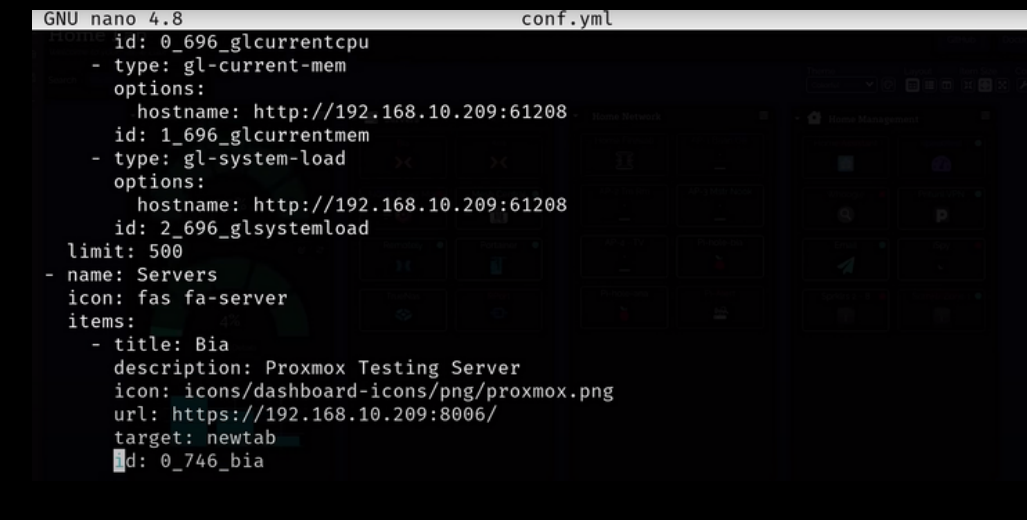
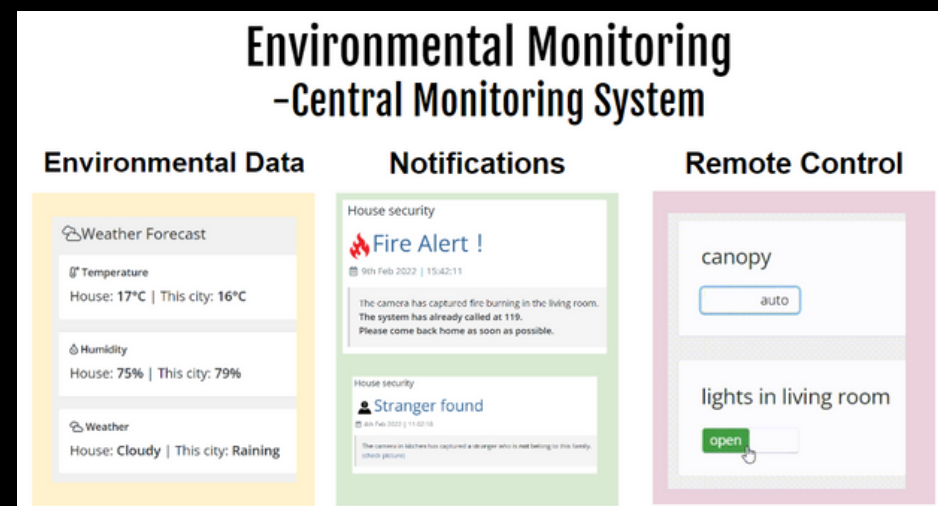
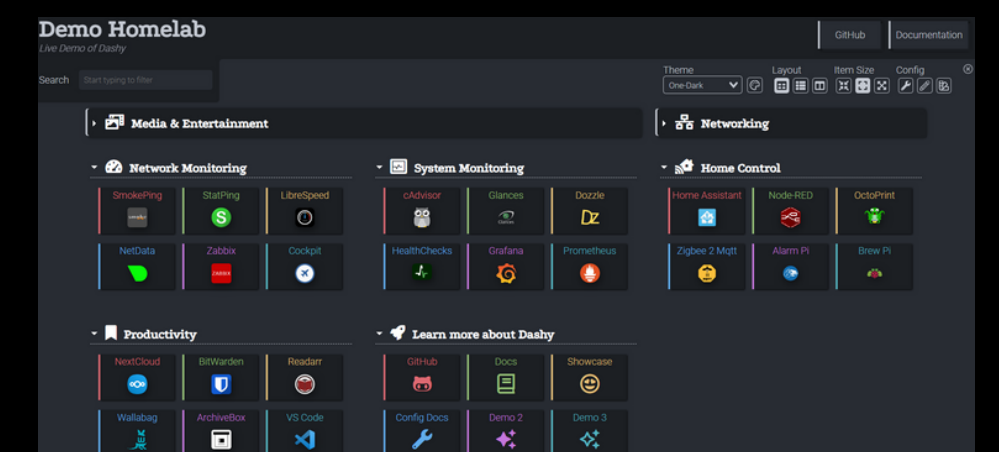
英國大學專題競賽
- 智能居家管理系統



「文華確診地圖」網頁



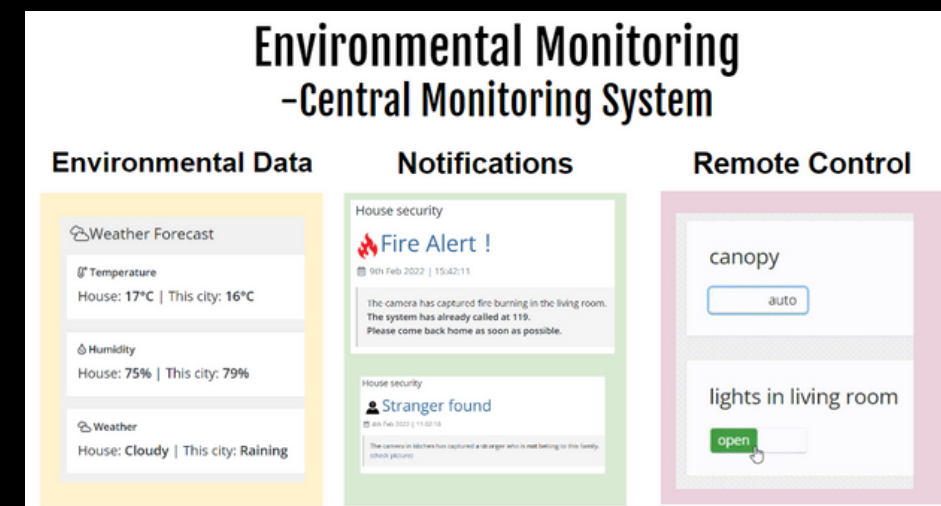
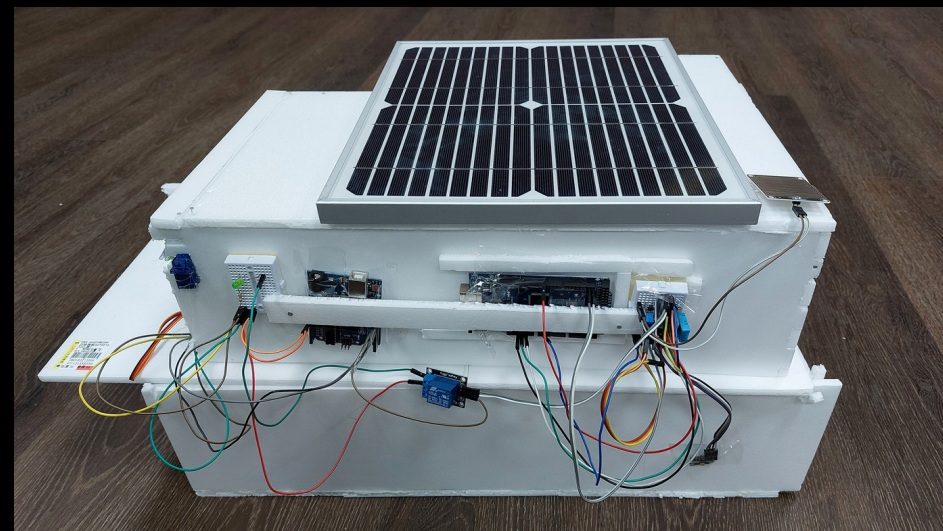
可模組化伺服器監控軟體



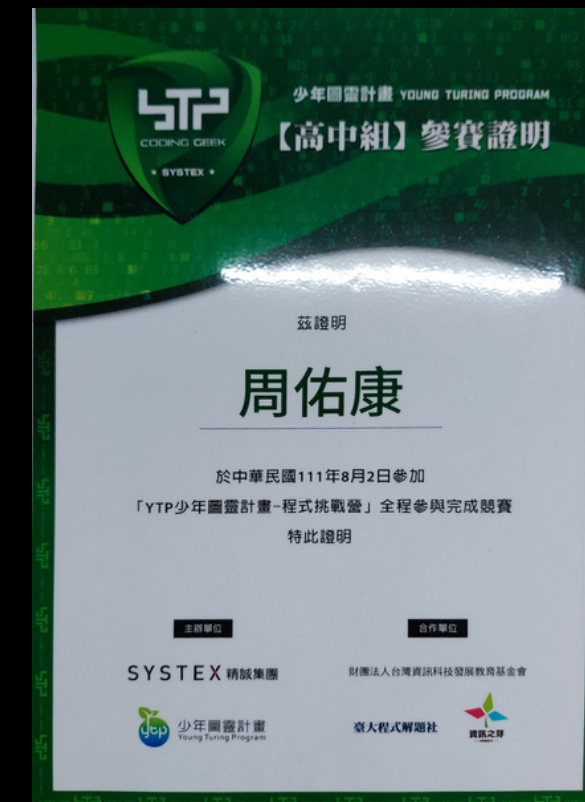
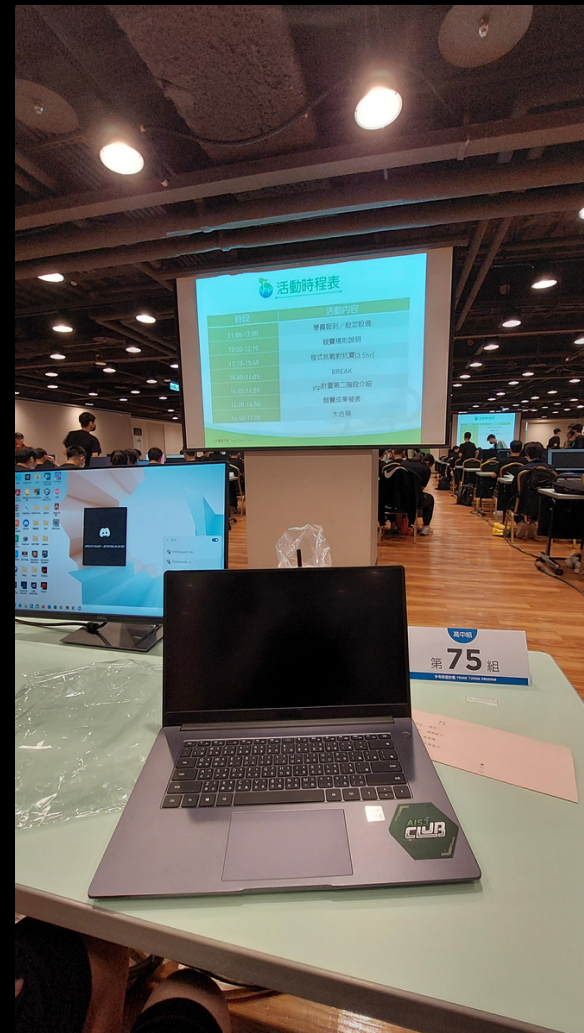
獲獎紀錄

資訊能力

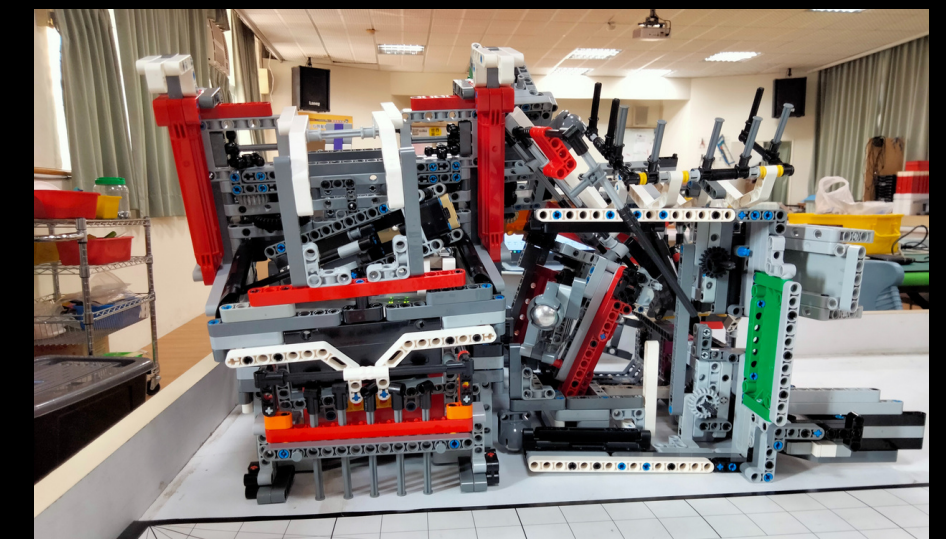
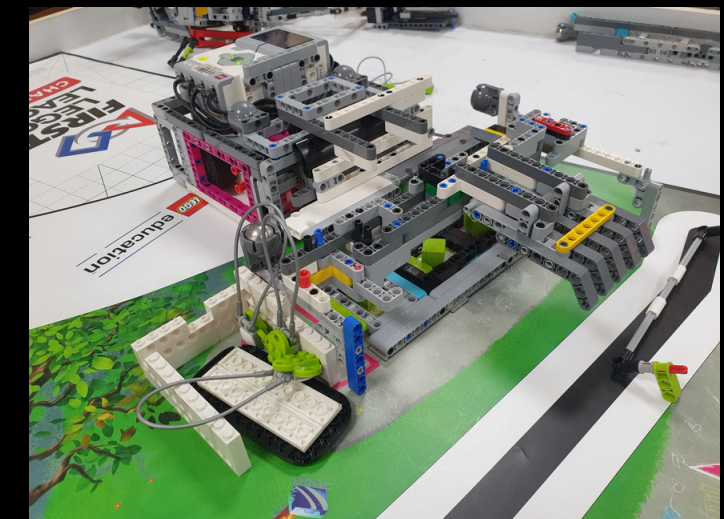
2022英國大學專題競賽
第七名



2022YTP少年圖靈計畫
佳作



2021-2020 FLL機器人大賽
最佳機器人設計獎



結合生活

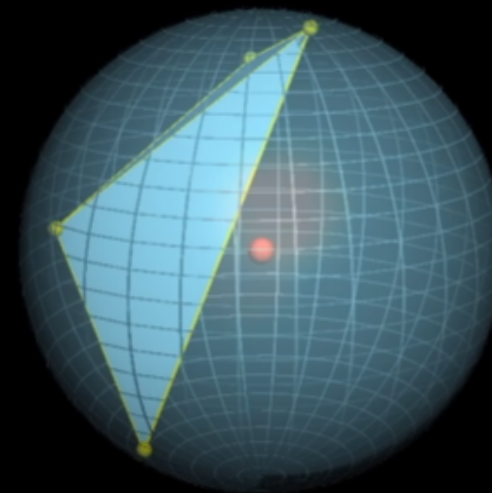
資訊能力

股票研究

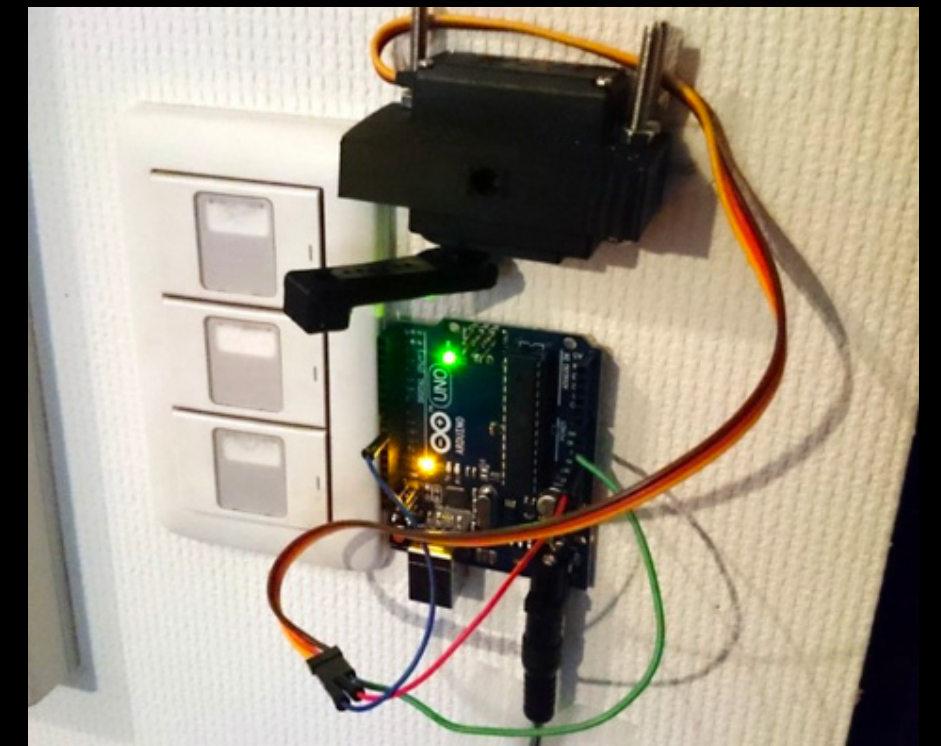


機率模擬

4 random* points on sphere
Probability that this tetrahedron
contains the sphere's center?



智能家居





社群運營

-中部電資聯合會議會長/創會人

經驗彙整

社群運營



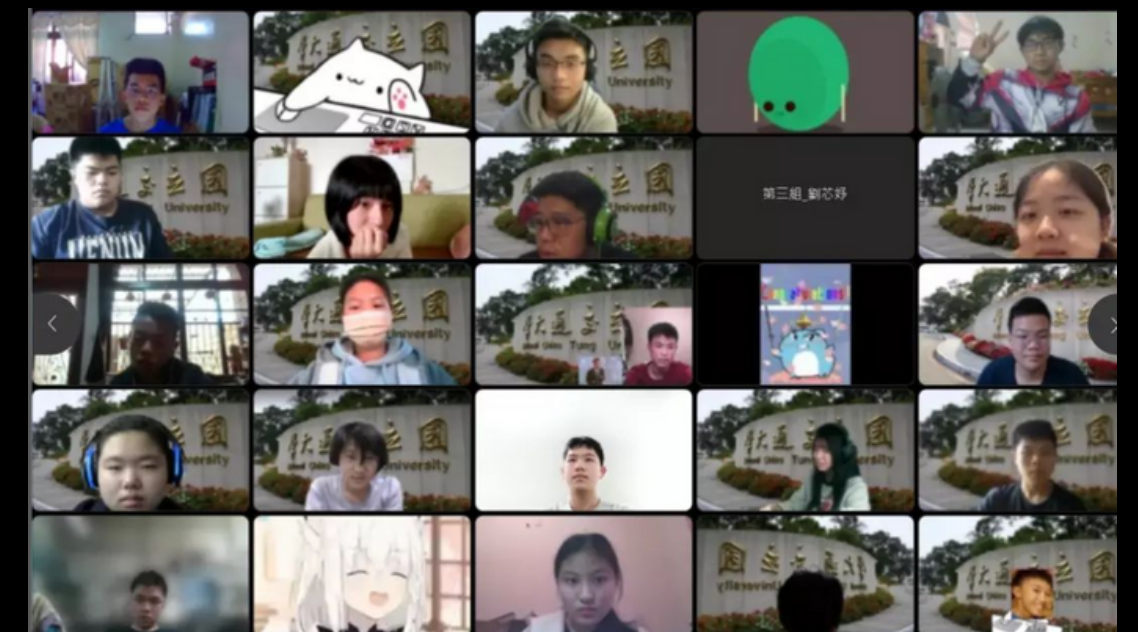
創立SCAICT
中部高中職電資聯合會議

社群

- SCAICT中部電資聯合會議第一屆 @會長/創會人
- g0v零時政府 @成員
- UCCU Hacker @成員
- OFDL 機器人研究社@隊長
- 文華數位投資群 @創群人
- SC41CT 資安戰隊創辦人 @逆向工程、密碼學

活動舉辦

- 2022 SCAICT中部電資聯合會議 @總召
- 2022 國立陽明交通大學中友會電資聯合寒訓 @總召
- 百土x百王中部三校四社電資交接茶會 @總召
- 2022 SITCON中部包車團 @總召
- 2021 中部三校四社電資聯合交接茶會 @總召
- GICS 資安女婕思 @選手群指導



擔任交大電資聯合寒訓總召
籌劃活動、規劃課程、團隊運營



教學經驗

-AIS3 Junior助教

經驗彙整

教學經驗

社團講師

- 文華高中電腦研究社
- 中女電腦科學讀書會
- 西苑高中資安多元選修
- 中電會密碼學講師



中女電科讀書會
長期python、網路程式開發

活動助教

- AIS3 Junior 助教
- AIS3 雲嘉資安體驗營 助教
- SITCON HoC 助教
- 中電會資安系列課程 助教



AIS3 Junior助教
指導學員解決課程問題、專題製作

社群 & 多元學習講者

- AIS3 Club 講者
- 幹部訓練-社群運營
- 校內多元學習課程
- 學習歷程製作



AIS3 Club中分享社群運營技巧
透過“RPG”的簡報方式

感謝聆聽！

時間用在哪裡，成就就在哪裡