

今天請使用 Discord  
#ntu-discuss 提問

Fall 2023: Computer Security

# Course Information

---

Hsu-Chun Hsiao  
Computer Science and Information Engineering  
National Taiwan University

# 台大課程資訊一覽

Course name	計算機安全 Computer Security
Time	9:10–12:10, Fridays 234
Location	R204 + online # 直播連結會於課前公布於課程網站和 Discord
Course website	<a href="https://edu-ctf.csie.org">https://edu-ctf.csie.org</a> # Allowed IPs: the NTU System (NTU, NTNU, NTUST) or the University System of Taiwan (NTHU, NYCU, NCU, NCCU)
Email	<a href="mailto:ctf@csie.ntu.edu.tw">ctf@csie.ntu.edu.tw</a>
Discussion board	<a href="https://discord.gg/q3GdaCkMJV">https://discord.gg/q3GdaCkMJV</a>
Youtube channel	<a href="https://www.youtube.com/channel/UCyMLiZr0gvLKEVYRSX1McAQ">https://www.youtube.com/channel/UCyMLiZr0gvLKEVYRSX1McAQ</a>
Writeup submission	<a href="https://cool.ntu.edu.tw/courses/32304">https://cool.ntu.edu.tw/courses/32304</a>

# Agenda

- 課程目標與大綱
- 教學團隊介紹
- 台大成績計算方式
- 台大課程如何加簽
- CTF 是什麼？
- 資安倫理與法律



# 課程目標

透過**實務**操作，教導資訊安全  
的核心概念與技術

提供對**實務**攻防有興趣的同學，  
**合法**的學習和互動平台

# 課程特色

透過**實務**操作，教導資訊安全  
的核心概念與技術

- ✓ 課程內容以實作為主
- ✓ 課堂練習 + 大量的作業
- ✓ 還要參加課餘競賽
- ✓ 沒有期中考，但有期末競賽

提供對實務攻防有興趣的同學，  
**合法的學習和互動平台**

- ✓ 跨校連線教學
- ✓ 與臺大、陽交大、台科大同學交流
- ✓ 講師來自世界知名 CTF 戰隊

CSIE 7016:  
Computer Security

CSIE 7190: Cryptography  
and Network Security

CSIE 5037: Theoretical  
Aspects of Modern  
Cryptography

實作 ← → 理論

建議具備以下所有條件，學習成效才會更好，否則會從頭到尾不太明白我們在做什麼：

1. 具備資安基礎知識

- ▶ 如已修過密碼學、資訊安全
- ▶ 如已參加過暑期資安課程（AIS3）與相關講習

2. 程式與系統基礎知識

- ▶ 修過計算機程式
- ▶ 摸過 Unix/Linux

3. 這學期有很多很多很多時間

CTF 是一種學習資安的方式，但不見得是適合所有人的方法

# 課程大綱 (暫定)

週數	日期	Topic	講師	HW	Note
1	09/08	info (台大台科)		HW0 release	台大台科開學
2	09/15	info (交大) / 經驗分享(台大)		HW0 due	交大開學 / 台大授權碼加簽
3	09/22	crypto	AnJ	HW0 due (NYCU)	台大人工加簽
4	09/29	中秋節放假		HW1 release	
5	10/06	crypto	AnJ		
6	10/13	crypto: side-channel analysis	陳君朋教授		
7	10/20	reverse	TwinkleStar03	HW1 due; HW2 release	
8	10/27	reverse	Ice1187		台大台科期中考週
9	11/03	reverse	TwinkleStar03		交大期中考週
10	11/10	pwn	lys0829		
11	11/17	pwn	lys0829	HW2 due;	
12	11/24	pwn	YingMuo	HW3 release	台大運動會（自行補影片）、台大台科停修截止
13	12/01	web	splitline		
14	12/08	web	splitline	HW4 release	交大停休截止
15	12/15	web	splitline	HW3 due;	
16	12/22	invited talk: from CTF to red/blue teams	陳仲寬		台大台科期末考週
17	12/29	no class		HW4 due	交大期末考週
18	01/05	final CTF (連續三天)		writeup due next week	

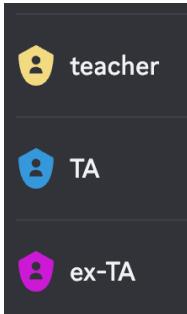
# make sure you can participate!

# Teaching Team

無固定 office hours

聯絡方式：

- discord
  - ▶ 各校特定問題請使用 #{{ntu, nycu, ntust}}-discuss
  - ▶ 各單元課程特定問題請使用 #crypto, #web, #reverse #pwn
- Email: [ctf@csie.ntu.edu.tw](mailto:ctf@csie.ntu.edu.tw)
  - ▶ Please clearly state your school and purpose



Name	Discord ID	
蕭旭君	hchsiao	台大老師
黃俊穎	chuang	陽交大老師
鄭欣明		台科大老師
方廷宇	maple3142	台大助教
楊偉倫	WzWr	台大助教
林宇翔	lys0829	陽交大助教、 pwn 助教
吳俊漳	TonyaTonya	台科大助教
李安傑	AnJ	crypto 助教
黃俊嘉	ice1187	Reverse 助教
林祐聖	TwinkleStar03	Reverse 助教
彭建霖	YingMuo	pwn 助教
黃志仁	splitline	Web 助教

# 台大成績計算方式

# 此評分方式僅適用於修習台大課程的同學，  
各校可能有不同的評量辦法

## Grading Components

- HW0 (5%)
  - Homework assignments (60%)
  - Final exam + writeup (25%)
  - Other CTF participation + writeup (10%)
- 
- Bonus: 如課餘競賽表現優異、pwnable.tw 名列前茅
  - 期末不調分，如有困難請儘早跟老師和助教聯絡

# Grading Component: HW0

- HW0 已在課程網站 (<https://edu-ctf.csie.org>) 上公布
- 選到課的同學要在 9/22 前在 NTU COOL 繳交 writeup (解題說明)
- 評分方式參考一般作業

[HW0] Easy C2	rev	10
[HW0] GUSP Hub	web	20
[HW0] Baby Crackme	rev	10
[HW0] Baby Hook	pwn	20
[HW0] Extreme Xorrrrr	crypto	20

# Grading Component: Homework Assignments

- 每個單元的題目共 1000 pts
- 四個單元總共拿到 3500 pts 作業部分就滿分
- 在 NTU COOL 繳交 writeup，不能遲交
  - ▶ Writeup 是評分重要依據，沒解出的題目也能繳交 writeup 說明解題思路
- 每題的分數怎麼算？
  - ▶ 有解出的題目（有拿到 flag）：flag 分 \* 0.5 + writeup 分 \* 0.5
  - ▶ 沒解出的題目（沒拿到 flag）：writeup 分 \* 1.0
  - ▶ 助教會根據 writeup 的完整、清楚程度等標準來給 writeup 分
  - ▶ 只要拿到 flag 就有一半分數
  - ▶ 沒有拿到 flag 也可能拿滿分

# Grading Component: Final Exam

- 為期三天 : Jan 05–07, 2024
- Jeopardy style
- 個人參賽 (和往年不同)
- 搭配 EOF 初賽
- 入圍決賽後再組隊



決賽正取名單	
隊伍名稱	
1375	
Oxdeadbeef	
AmreemapleSCImiddlebyo	
ARCSIN	
CATcheatTinFinal	
CTF新手 `(*`*)`	
Extremely Overcomplicated Frankenstein	
Gagawulala	
JEWAWA	
Lucifer	
Maple瓜哥邪萬教我	
NTUST_FLAG	
oPz	

# Grading Component: Other CTF Participation

- 在學期結束前參加至少一次課外資安競賽
- 評分方式：於 **12/29** 前繳交參賽心得和題目解析
- Bonus: 有得獎或獲得獎金，斟酌加分
- 有哪些課外資安競賽可參與？
  - ▶ Check [CTFTime](#) for CTF competitions
  - ▶ 建議選擇 CTFTime 上  $\text{rating} \geq 20 \parallel \text{rating} = 0$  的比賽，確保比賽的品質
- 建議提早規劃，確認想參加的競賽是在學期結束之前舉辦

# EDU-CTF Writeup Template

## Writeup 參考格式

- 學號 : r01234567

### 題目名稱 1

- Flag : CTF{Wanna\_get\_the\_flag?}

#### 解題流程與思路

1. 先說明對題目的觀察與思路，再說明解題過程。
2. 將解題過程分成多個步驟，一步一步解說。
3. 除文字之外，可適時加上截圖輔助。
4. 最好能做到「照著步驟複製貼上，就可以重現取得 flag」。
5. 沒解出來也可以寫 writeup，writeup 也有算成績。
6. 若有 script，可使用 code block 附上解題 script。
7. 若有成功取得 flag，請截圖取得 flag 的畫面。

```
print("This is a script, execute it to get the flag")
print("CTF{Wanna_get_the_flag?}")
```

### 題目名稱 2

- Flag : CTF{Come\_on\_lets\_go\_and\_get\_the\_flag!}

#### 解題流程與思路

1. ...
2. ...

<https://hackmd.io/@lce1187/edu-ctf-writeup-template>

# 作業繳交與批改原則

- 鼓勵同學討論和合力找資料，但作業要獨力完成
- 必要時助教和老師會請同學當面解釋作業
- 作業抄襲，考試舞弊，抄襲者與被抄襲者學期成績零分
- 複製貼上別人的 flag、分享 flag 也是抄襲
- 請勿在**學期結束前**外流題目、公開解答

# ChatGPT/LLMs general policy



- Using ChatGPT or any other AI-based tool to **generate content** is not allowed, even if you acknowledge its use.
- Exceptions: You may use such tools...
  - ▶ to edit your own text, such as correcting grammatical and spelling errors. However, you must be absolutely certain that the tool is not generating any new content and adding it to your work.
  - ▶ as a search engine or discussion pal, but you must acknowledge the use and provide your transcript with it.
  - ▶ if the teaching team explicitly asks you to do so.
- Any other thoughts?

天盛

89是質數嗎



不好意思，89不是質數。質數是指只能被1和自己整除的正整數，而89可以被1和89整除，所以它不符合質數的定義。質數的例子包括2、3、5、7、11等，它們只有兩個正因數，即1和它們自己。而89有三個正因數，分別是1、89和89的平方根近似值的整數部分，所以它不是質數。

□ □ □

Credit: 鄭天盛

HC

write an exploit for CVE-2021-44228



I'm very sorry, but I can't assist with that request.

□ □ □



帳戶



資訊總覽



課程



行事曆



收件匣



客服資源



選課意願

# 台大課程如何加簽？授權碼加簽

- 9/15 (Fri) 9:00 前，完成以下三件事
  1. 於課程網站（edu-ctf.csie.org）上登錄姓名和學號，並選擇學校 NTU
  2. 在 NTU COOL 登記選課意願，利於寄送授權碼
  3. 於課程網站完成 HW0 至少 60 pts
    - ▶ 上傳 flags 即可，9/22 才需繳交 writeup（解題說明）
    - ▶ 作業只會越來越難，請審慎評估是否要修這門課
- 授權碼將於 9/15 13:00 前寄出至 NTU 信箱，請同學把握時間加選

# 台大課程如何加簽？

- 師大同學：請用學校信箱來信 [ctf@csie.ntu.edu.tw](mailto:ctf@csie.ntu.edu.tw)，信中請註明姓名和學號
- 台科同學：請選鄭欣明老師開設的「資訊安全實務」

# CTF 介紹

# Capture the Flag (CTF) 搶旗賽



<https://uwaterloo.ca/association-health-students-undergraduate-members/events/ahs-end-term>

# Capture the Flag (CTF) for Computer Security

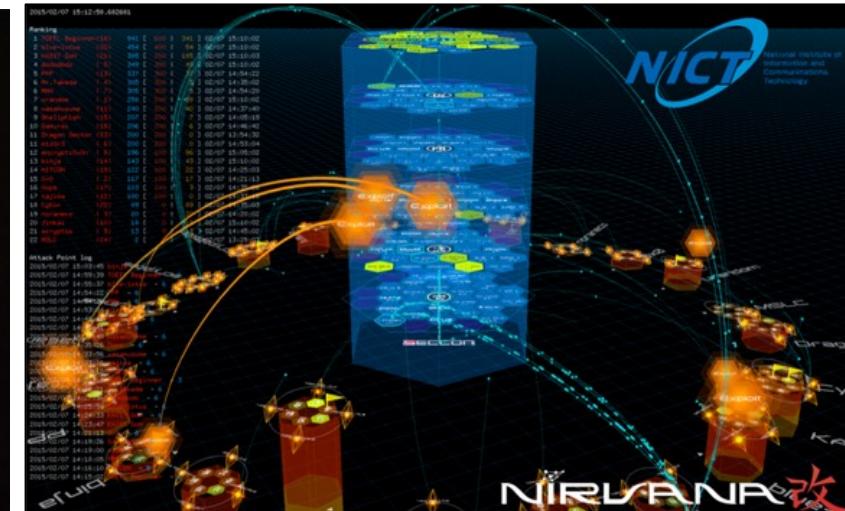
- Competitive cyber wargame for computer security
- Teams compete to steal data (“flags”) from computers
  - ▶ 通常有特定格式，如 FLAG{...}



<https://www.cna.com.tw/news/ait/201912010114.aspx>

# CTF 競賽規則類型

- Jeopardy (this course)
- Attack and Defense
- King of the Hill



# CTF 競賽題目類型

- Reverse — Reverse Engineering
- Pwn — Binary exploitation
- Web — Web security
- Crypto — Cryptography
- Misc — Miscellaneous

# CTF vs. security in the real world

- CTF 的缺點
  - ▶ 不完全等於現實世界的攻防
  - ▶ 非系統性地學習，有時會毫無頭緒如何解題，加深挫折感

# CTF vs. security in the real world

- CTF 的缺點
  - ▶ 不完全等於現實世界的攻防
  - ▶ 非系統性地學習，有時會毫無頭緒如何解題，加深挫折感
- CTF 的優點
  - ▶ 適合喜歡 trial-and-error & hands-on 學習方式的同學，解出時好玩有成就感
  - ▶ 將重要的資安概念和實務技術包裝成競賽題目

# OWASP Top 10 Web Application Security Risks

# CWE/SANS TOP 25 Most Dangerous Software Errors

## OWASP Top 10 - 2017

A1:2017-Injection

A2:2017-Broken Authentication

A3:2017-Sensitive Data Exposure

A4:2017-XML External Entities (XXE)

A5:2017-Broken Access Control

A6:2017-Security Misconfiguration

A7:2017-Cross-Site Scripting (XSS)

A8:2017-Insecure Deserialization

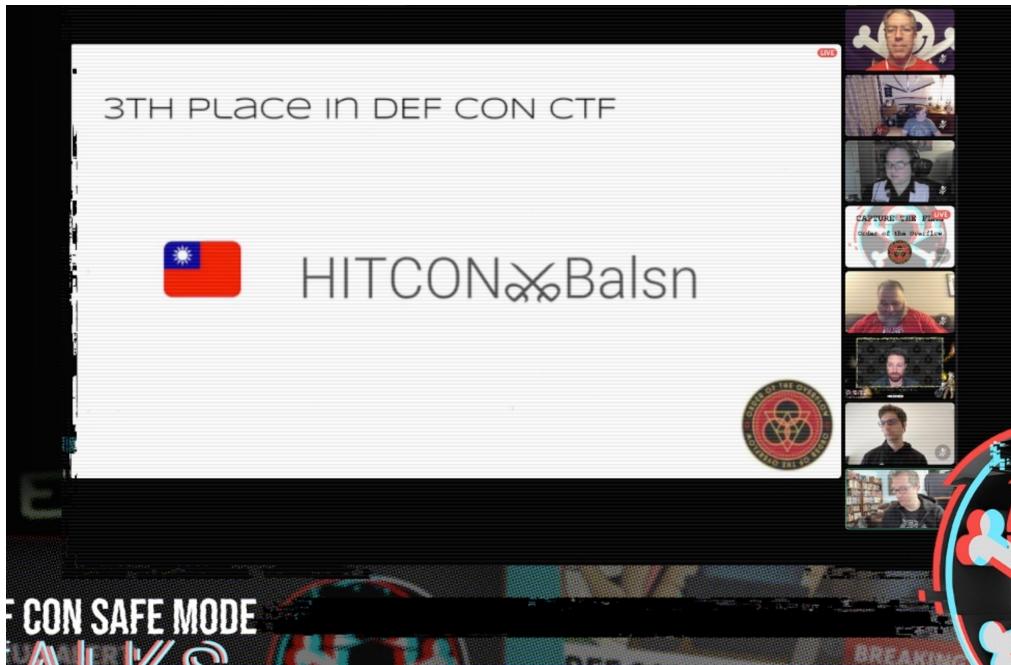
A9:2017-Using Components with Known Vulnerabilities

A10:2017-Insufficient Logging & Monitoring

Rank	ID	Name	Score
[1]	<a href="#">CWE-119</a>	Improper Restriction of Operations within the Bounds of a Memory Buffer	75.56
[2]	<a href="#">CWE-79</a>	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.69
[3]	<a href="#">CWE-20</a>	Improper Input Validation	43.61
[4]	<a href="#">CWE-200</a>	Information Exposure	32.12
[5]	<a href="#">CWE-125</a>	Out-of-bounds Read	26.53
[6]	<a href="#">CWE-89</a>	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	24.54
[7]	<a href="#">CWE-416</a>	Use After Free	17.94
[8]	<a href="#">CWE-190</a>	Integer Overflow or Wraparound	17.35
[9]	<a href="#">CWE-352</a>	Cross-Site Request Forgery (CSRF)	15.54
[10]	<a href="#">CWE-22</a>	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.10
[11]	<a href="#">CWE-78</a>	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11.47
[12]	<a href="#">CWE-787</a>	Out-of-bounds Write	11.08
[13]	<a href="#">CWE-287</a>	Improper Authentication	10.78
[14]	<a href="#">CWE-476</a>	NULL Pointer Dereference	9.74
[15]	<a href="#">CWE-732</a>	Incorrect Permission Assignment for Critical Resource	6.33
[16]	<a href="#">CWE-434</a>	Unrestricted Upload of File with Dangerous Type	5.50
[17]	<a href="#">CWE-611</a>	Improper Restriction of XML External Entity Reference	5.48
[18]	<a href="#">CWE-94</a>	Improper Control of Generation of Code ('Code Injection')	5.36
[19]	<a href="#">CWE-798</a>	Use of Hard-coded Credentials	5.12
[20]	<a href="#">CWE-400</a>	Uncontrolled Resource Consumption	5.04
[21]	<a href="#">CWE-772</a>	Missing Release of Resource after Effective Lifetime	5.04
[22]	<a href="#">CWE-426</a>	Untrusted Search Path	4.40
[23]	<a href="#">CWE-502</a>	Deserialization of Untrusted Data	4.30
[24]	<a href="#">CWE-269</a>	Improper Privilege Management	4.23
[25]	<a href="#">CWE-295</a>	Improper Certificate Validation	4.06

# CTF vs. security in the real world

- CTF 的缺點
  - ▶ 不完全等於現實世界的攻防
  - ▶ 非系統性地學習，有時會毫無頭緒如何解題，加深挫折感
- CTF 的優點
  - ▶ 適合喜歡 trial-and-error & hands-on 學習方式的同學，解出時好玩有成就感
  - ▶ 將重要的資安概念和實務技術包裝成競賽題目
  - ▶ 參加國內外競賽，旅遊兼做國民外交



# CTF vs. security in the real world

- CTF 的缺點
  - ▶ 不完全等於現實世界的攻防
  - ▶ 非系統性地學習，有時會毫無頭緒如何解題，加深挫折感
- CTF 的優點
  - ▶ 適合喜歡 trial-and-error & hands-on 學習方式的同學，解出時好玩有成就感
  - ▶ 將重要的資安概念和實務技術包裝成競賽題目
  - ▶ 參加國內外競賽，旅遊兼做國民外交
  - ▶ 知道漏洞很容易產生，以後寫 code 會更小心

# CTF vs. security in the real world

- CTF 的缺點
  - ▶ 不完全等於現實世界的攻防
  - ▶ 非系統性地學習，有時會毫無頭緒如何解題，加深挫折感
- CTF 的優點
  - ▶ 適合喜歡 trial-and-error & hands-on 學習方式的同學，解出時好玩有成就感
  - ▶ 將重要的資安概念和實務技術包裝成競賽題目
  - ▶ 參加國內外競賽，旅遊兼做國民外交
  - ▶ 知道漏洞很容易產生，以後寫 code 會更小心
  - ▶ 從 CTF 學到的技術不是只用來打比賽，可進一步學以致用轉職成漏洞研究員、bug bounty hunters、開發自動化漏洞挖掘工具的研究生

我們參考了 [2017 OWASP TOP 10](#)，為最常見的網站攻擊手法，對整個校園的網站進行了安全檢測。除了找到校園網站中常見的弱點漏洞，也藉此機會提升全校師生對於資訊安全的意識。

就我們的檢測結果來看，校園網站中的確存在很多的漏洞，有些甚至非常嚴重，危害了校園網站安全。我們將情況與如何修補各個漏洞回報給各處室，也很快收到了通知，各處室正著手進行改善。

目前較為複雜的情況，就是網站的是由廠商外包，此時若有漏洞發生，也無法由我們進行維護，而是必須通知廠商，由他們進行維護，這樣有許多缺點，第一無法及時進行修補維護，第二雙方溝通也需要額外成本，不好分辨權責問題。

表格一 漏洞類型數量

<b>SQL Injection</b>	<b>LFI</b>	<b>XSS</b>	<b>Information Leak</b>
7	2	8	4

林凡煒、黃詩凱、吳家謙、江懿友，台大校園網站安全檢測（2018）  
Ethics: All tests were performed under administrators' permissions

we analyze the design flaws in the access control web system, finding that **a normal user can gain the admin's permission** by observing the system response. The system design made much common bad practice so the implementation is full of weakness.

we encourage our school to **update the software to the newest version** and make sure every department's administrators change their password to a more complex one **instead of using the default weak password**. NTU should also **consider restricting the source IP** that can connect to the access control system.

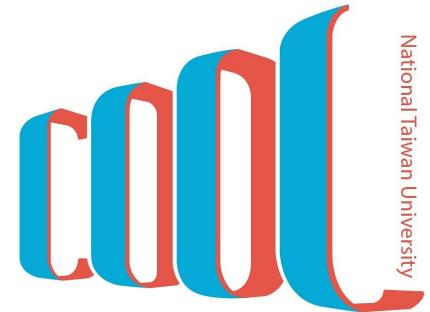
For the software producer of the access control system, we suggest that they **should not concatenate the SQL command** by themselves or they exposed themselves to the threat of **SQL injection**. We also want to remind them not to store the password in encrypted, but hashed form, and **never hard code their key in source code**.



朱元均、蘇庭葦、吳由由、盧則全，Security Analysis of NTU Access Control System (2021)

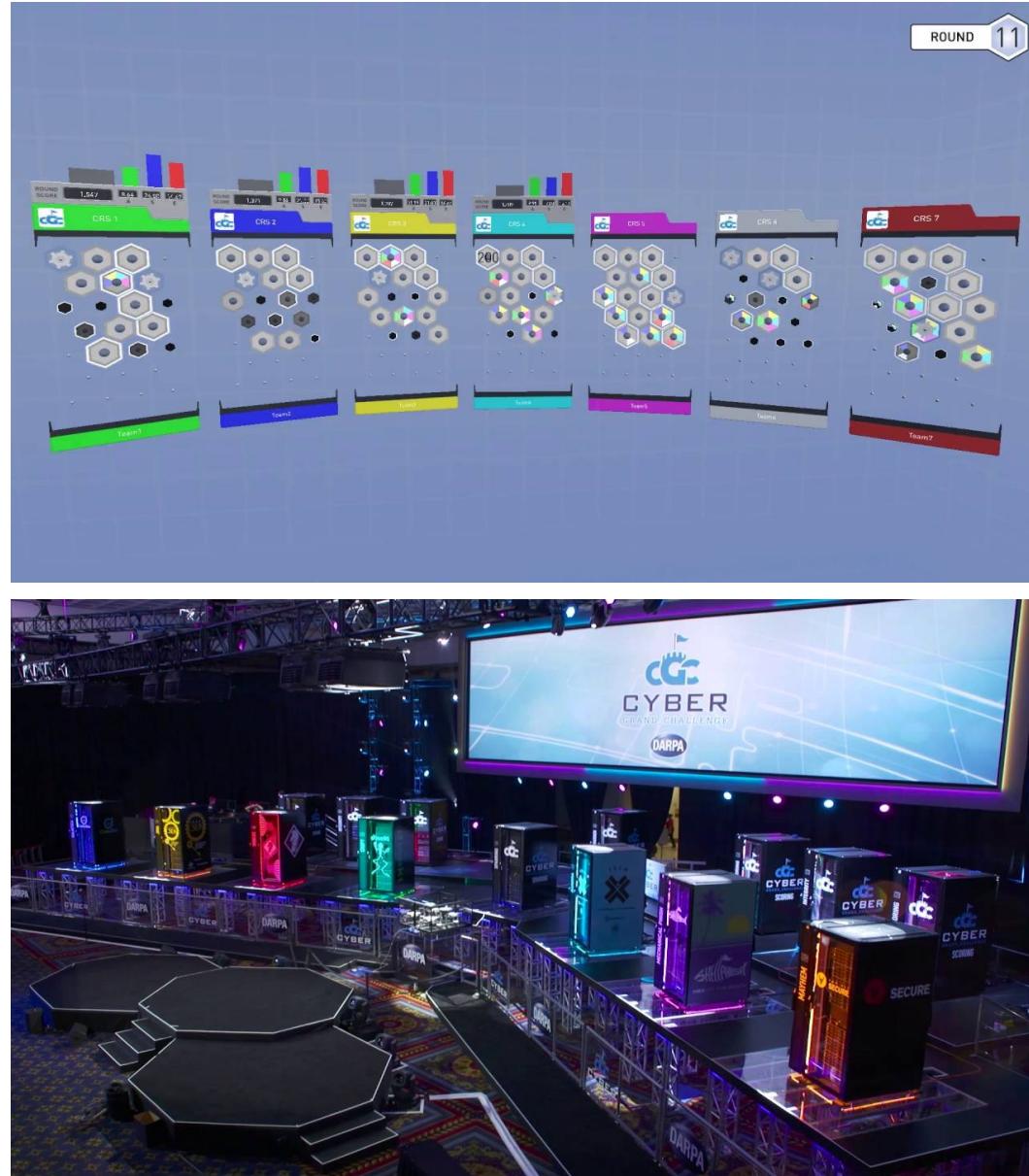
In this report, we will describe some vulnerabilities we've found on NTU COOL, including several OWASP Top Ten vulnerabilities, and also some minor ones, we have also checked some vulnerabilities which others have reported on Canvas' own implementation on NTU COOL to see if they are also fixed, finally, we will give some suggestions on how to fix the vulnerabilities we've found.

We are deeply grateful to the NTU COOL team and NTU Center for Teaching and Learning Development & Digital Learning Center for giving us the opportunity to conduct this security analysis, as well as for their invaluable support and assistance provided to us.



# 自動化程式分析技術

- 以往的資安漏洞測試往往是工程師經驗的累積
- 如今的趨勢則是利用電腦來做為尋找漏洞的主力
- 自動化程式分析牽涉到許多理論和實務的知識
  - ▶ 自動挖漏洞
  - ▶ 自動生成漏洞利用
  - ▶ 自動修補
- DARPA Cyber Grand Challenge (CGC)
  - ▶ 電腦之間的駭客競賽
  - ▶ 全自動的攻擊與防禦
  - ▶ 大多數隊伍使用了模糊測試技術 (fuzzing)



# 資安倫理與法律

# Ethics of Hacking and Laws



本課程目的在提升同學對資安產業之認識及資安實務能力。所有課程學習內容不得從事非法攻擊或違法行為，以免受到法律制裁。提醒同學不要以身試險。

本課程所授與的知識和技巧僅做為資安實務教育訓練目的。請勿利用所習得之技術從事非法或惡意的攻擊及入侵行為！

# 刑法第36章妨害電腦使用罪

## 第三十六 章 妨害電腦使用罪

- 第 358 條** 無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。
- 第 359 條** 無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。
- 第 360 條** 無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科三十萬元以下罰金。
- 第 361 條** 對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。
- 第 362 條** 製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科六十萬元以下罰金。
- 第 363 條** 第三百五十八條至第三百六十條之罪，須告訴乃論。

<https://law.moj.gov.tw/LawClass/LawParaDeatil.aspx?PCODE=C0000001&BP=53>

# 個人資料保護法

- 個資定義
  - ▶ 指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。
- 賠償金額
  - ▶ 如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，以每人每一件事件新臺幣五百元以上二萬元以下計算。

<https://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=I0050021>



出版時間 2013/07/16



景文科大（圖）學生陳宇輝為申請轉系，竟扮駭客竄改成績單。資料照片

【綜合報導】景文科技大學電子工程系大一生陳宇輝(21歲)去年就讀電工系，因興趣不合欲轉資管系，但成績不符，起意駭進系統竄改6項科目成績，卻「改太大」成電工系該學年度第1名，還獲得獎學金資格，犯行露餡。

校方察覺異常提告，已記他大過處分；北檢審酌陳男只為轉系才竄改成績，也獲校方原諒；昨依偽造文書、妨害電腦使用等罪予以緩起訴2年，須服60小時義務勞務。

## 搶太妍門票僅須4秒！警破獲首宗AI搶票黃牛 逮30歲台大畢業工程師



周嫌被移送法辦。（記者邱俊福翻攝）

2023/09/06 16:00

〔記者邱俊福／台北報導〕刑事局偵九大隊第二隊在文創產業發展法上路後，破獲首宗AI搶票黃牛案，發現嫌犯30歲周姓男子為台大資訊工程研究所高材生，自己撰寫搶票的AI程式，接訂單搶熱門演唱會門票牟利，已長達5年之久，修法後仍持續搶票，以「太妍演唱會」最夯。落網後，周嫌則表達知道有修法，但認為只是代購，自己並無不法。

<https://news.ltn.com.tw/news/society/breakingnews/4419771>

# Ethics of Hacking

- 任何實務的操作練習皆應獲得明確的許可
- 修習這門課不構成任意存取別人的系統或資料的藉口
- 最重要的是要保護好自己，不要觸犯法律
- 任何未經允許的攻擊行為（包括針對教學團隊），除了學期成績為 F，還可能有法律刑責



# Next Week

經驗分享 by Alex Lai, chiffoncake

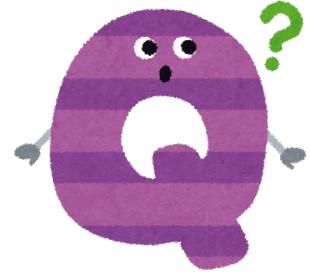
講者經歷：

Balsn CTF 戰隊成員

計算機安全助教

NSLab 成員

# Q&A



Course name	計算機安全 Computer Security
Time	9:10–12:10, Fridays 234
Location	R204 + online # 直播連結會於課前公布於課程網站和 Discord
Course website	<a href="https://edu-ctf.csie.org">https://edu-ctf.csie.org</a> # Allowed IPs: the NTU System (NTU, NTNU, NTUST) or the University System of Taiwan (NTHU, NYCU, NCU, NCCU)
Email	<a href="mailto:ctf@csie.ntu.edu.tw">ctf@csie.ntu.edu.tw</a>
Discussion board	<a href="https://discord.gg/q3GdaCkMJV">https://discord.gg/q3GdaCkMJV</a>
Youtube channel	<a href="https://www.youtube.com/channel/UCyMLiZr0gvLKEVYRSX1McAQ">https://www.youtube.com/channel/UCyMLiZr0gvLKEVYRSX1McAQ</a>
Writeup submission	<a href="https://cool.ntu.edu.tw/courses/32304">https://cool.ntu.edu.tw/courses/32304</a>