Fall 2021: Computer Security

Discord 討論群組
今天請使用 #ntu-discuss 提問

Course Information

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

Today’s Agenda

- 課程資訊一覽
- 台大課程如何加簽？
- 課程目標與大綱
- 教學團隊介紹
- 台大成績計算方式
- CTF 是什麼？
- 資安倫理
- 相關線上資源

課程資訊一覽

Course name	計算機安全 Computer Security
Time	9:30-12:10, Fridays 234 # 配合各校上課時程，若開始時間有調整會再公布
Location	Online # 直播連結會於課前公布於課程網站和 Discord
Course website	https://edu-ctf.csie.org # Allowed IPs: 140.{112, 113, 114, 115, 118, 122}.0.0/16
Email	ctf@csie.ntu.edu.tw
Discussion board	https://discord.gg/q3GdaCkMJV
Writeup submission	https://cool.ntu.edu.tw/courses/9014

台大課程如何加簽？

- 下週五 (10/1) 9:30 前，完成以下三件事

1. 寫 HW0
   - 上傳 flags 即可，下下週才需繳交 writeup（解題說明）
   - 根據 HW0 的成績決定加簽順序，同分同順序
   - 作業只會越來越難，請審慎評估是否要修這門課
2. 於課程網站上登錄姓名和學號
3. 登記選課意願
   - 台大同學：請上 NTU COOL 登記選課意願，利於寄送授權碼
   - 師大同學：請用學校信箱來信 ctf@csie.ntu.edu.tw，信件主旨「[edu-ctf 2021] 台大課程意願登記」，信中請註明姓名和學號

Problems

- Don't share flags!
- Don't DoS the server or services!
- Don't attack non-specified services or ports!
- Services only allow connections from 140.(112|113|114|115|118|122).0.0/16 (VPN is your friend)
- Updates or bug fixes will be announced here and on the change log :)

#	✓	Title	Tag	Point	AC
1		[HW0] to bf or not to bf	Crypto	50	181
3		[HW0] XAYB	Rev	50	144
4		[HW0] Arch Check	Pwn	50	121
5		[HW0] text2emoji	Web	50	130

Update Account

Old Password

Old Password

User Group ○ User ◉ admin

Password (optional)

New Password

Password Again (optional)

New Password Again

Email

Email

Realname (optional)

Realname

Student ID (optional)

Student ID

Edit

https://edu-ctf.csie.org

課程目標

透過實務操作，學習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

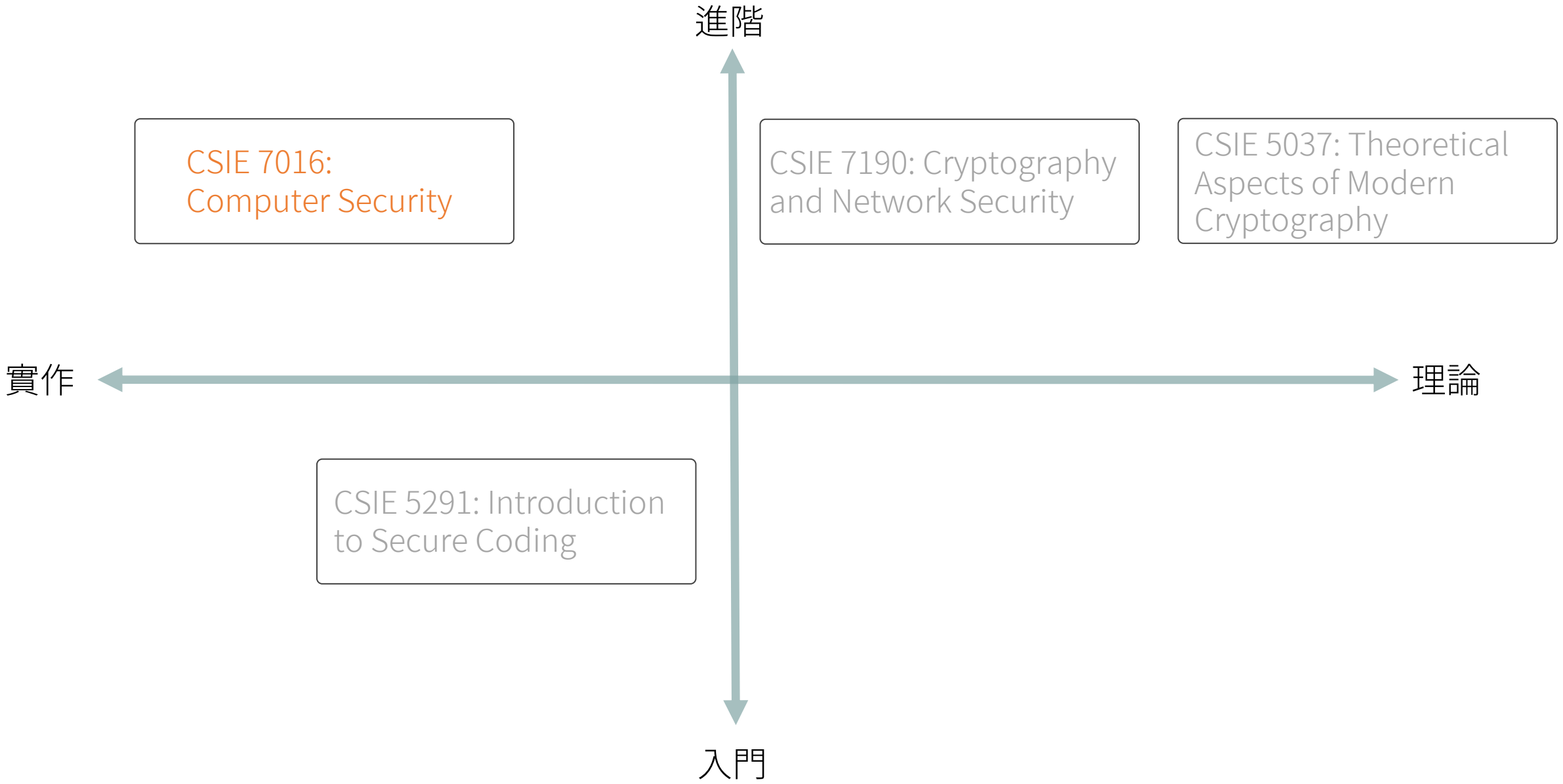
課程特色

透過實務操作，學習資訊安全的核心概念與技術

- ✓ 課程內容以實務攻防為主
- ✓ 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
- ✓ 講師來自世界知名 CTF 戰隊
- ✓ 與臺大、交大、台科大同學交流


進階
CSIE 7016:
Computer Security
CSIE 7190: Cryptography and Network Security
CSIE 5037: Theoretical Aspects of Modern Cryptography
實作
理論
CSIE 5291: Introduction to Secure Coding
入門

建議具備以下所有條件再選修

- 資安基礎知識
  - 如修過密碼學、資訊安全
  - 如參加過暑期資安課程、講習
- 程式與系統基礎知識
  - 如修過計算機程式
  - 如摸過 Unix/Linux
- 這學期時間很多很多很多

Computer Security 2021 Fall | Problems | Submissions | Ranking | Lectures | Admin | Feedback

Change Log

[2021-09-23 17:01] Another new announcement for NTU students! (Please scroll down to view it)

[2021-09-21 15:38] New announcement for NTU students! (Please scroll down to view it)

[2021-09-14 23:30] Hello world! ☺

Course Information

Discord Channel

Feel free to join our discord channel via this link: https://discord.gg/BQKdmygwwu

You can chat, find TA, or discuss with other students in this channel.
Do NOT share flags or solutions in discord channel!

https://edu-ctf.csie.org

課程大綱（暫定）

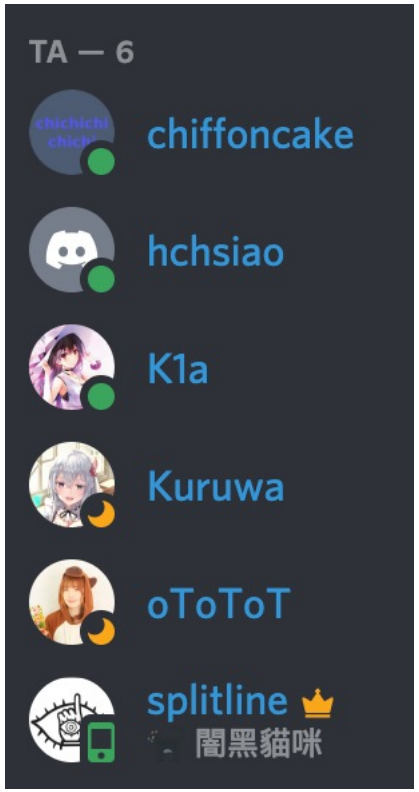
Wk.	Date	Topic	Note
1	Sep 24	Introduction	HW0 out
2	Oct 01	Crypto	HW0 due
3	Oct 08	Crypto	HW0 writeup due; HW1 out
4	Oct 15	Crypto	
5	Oct 22	Web security	
6	Oct 29	Web security	HW1 writeup due; HW2 out
7	Nov 05	Web security	
8	Nov 12	No class	
9	Nov 19	Reverse engineering	HW2 writeup due
10	Nov 26	Reverse engineering	HW3 out
11	Dec 03	Reverse engineering	
12	Dec 10	Binary exploitation	
13	Dec 17	Binary exploitation	HW3 writeup due
14	Dec 24	Binary exploitation	HW4 out
15	Dec 31	Holiday; No class	
16	Jan 07	No class # make sure you can participate!	
17	Jan 14	Final CTF (01/14 9am - 01/16 5pm)	HW4 writeup due
18	Jan 21	No class	Final CTF writeup due

線上直播授課

- 目前規劃整學期都線上直播授課
  - 影片課後會放上課程網站
- 上課時段仍有借用 204 電腦教室，供同學自行使用
- 直播工具
  - Google meet, youtube, webex 都有考慮
  - 直播連結會於課前公布於課程網站和 Discord

Teaching Team

- 無固定 office hours
- 聯絡方式之一：ctf@csie.ntu.edu.tw
  - 所有人都會收到
  - 寄信請註明學校
- 聯絡方式之二：discord
  - @TA, 請認明藍色 IDs
  - 各校特定問題請分別使用 {ntu, nycu, ntust}-discuss



Name	Discord ID	
蕭旭君	hchsiao#1776	台大老師
黃俊穎		陽交大老師
鄭欣明		台科大老師
蔡奇夆	chiffoncake#0750	台大助教
江昱勳	oToToT#0148	台大助教
陳冠廷	HexRabbit#2410	陽交大助教
林子婷	飛飛#6341	台科大助教
陳昱暢	K1a#8092	pwn 助教
張智諺		pwn 助教
郭彥廷	Kuruwa#7773	crypto 助教
黃志仁	splitline#4881	Web 助教
張書銘	LJP#5728	Reverse 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

- Homework assignments (65%)
  - HW0: 5%
  - Others: 15 % each
- Final CTF competition (25%)
- Other CTF or bug bounty participation (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 1: Homework Assignments （10/08 補充）

- CTF (capture the flag) 形式
- 四個單元，每個單元各佔 15%；HW0 佔 5%
- 約三週完成，不能遲交
- 在 NTU COOL 繳交 code & writeup
  - Writeup 是評分的主要依據，沒解出來也能繳交
- 各單元的分數計算方式：
  - Lab 題：只看 judge 上的分數，當題有上傳正確的 flag 即得全部的分數
  - HW 題：只看 writeup 分數，writeup 每題的滿分跟 judge 的題分一樣
  - 單元總分為 min(1000, lab 總分 + HW 總分)，亦即拿到 1000 分此單元就滿分

Grading Component 2: Final CTF Competition

- Jeopardy style
- 為期三天：Jan 1/14-16, 2022
- 搭配 EOF 初賽
- 4 個人一組

AIS3 EOF CTF決賽隊伍

排名	隊伍名稱
1	元元T^T
2	LYB
3	KuruwA
4	國際邀請隊（不列入名次計算）
5	0x41414141
6	lysCSYaznya19
7	Xmas
8	CTF2NOP
9	乂卍進吉ㄉ煞氣a星爆氣流斬卍乂
10	kcjjntu
11	20H
12	被程安隊員拋棄的邊緣人們
13	CRyptoGRapheR
14	10秒烤麵包
15	MYLK

Grading Component 3: Other CTF or Bug Bounty Participation

- 在學期結束前參加至少一次課外資安競賽或 bug bounty
  - Balsn CTF
  - 金盾獎
  - …
  - Check CTFTime for CTF competitions
  - Check HackerOne for bug bounties

- 評分方式：寫參賽心得和題目解析
- Bonus: 有得獎或獲得獎金，斟酌加分

歡迎參加資安系列競賽

https://csc.nccst.nat.gov.tw/member.aspx

We are here again! This year, Balsn CTF 2021 will feature creative and interesting challenges. We cordially invite you to join our party. Don't forget to mark it on your calendar!

- >> Date: 20 Nov. 2021, 10:00 (UCT+8) ~ 22 Nov. 2020, 10:00 (UTC+8)
- >> Format: 48-hour Online Jeopardy
- >> CTFTime: event/1376
- >> Official URL: Coming soon
- >> Prize:
  - >> 1st place: $30,000 TWD
  - >> 2nd place: $23,000 TWD
  - >> 3rd place: $15,000 TWD
  - >> Balsn CTF 2021 Taiwan Stars (top 3 domestic teams):
    - >> 1st place: $15,000 TWD
    - >> 2nd place: $10,000 TWD
    - >> 3rd place: $5,000 TWD
  - >> All the prize will be transferred in ETH.
- >> All of the above information is subject to change.

In Balsn CTF 2021, we will be featuring a new "homework" category, which consists of unsolved challenges from the previous year. See our twitter post for more details.

抄襲行為: zero tolerance

- 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、考試作弊：學期成績為 F
- 複製貼上別人的 flag、分享 flag 也是抄襲

CTF 介紹

Capture the Flag (CTF) 搶旗賽

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

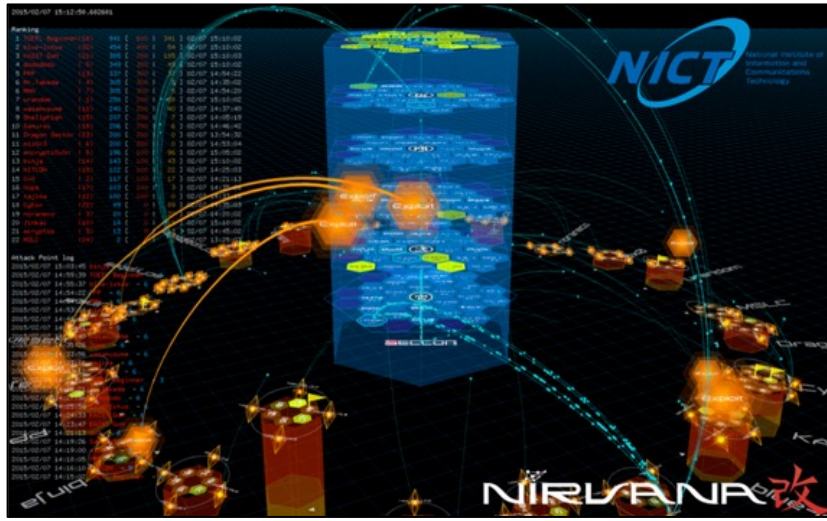
Capture the Flag (CTF) for Computer Security

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

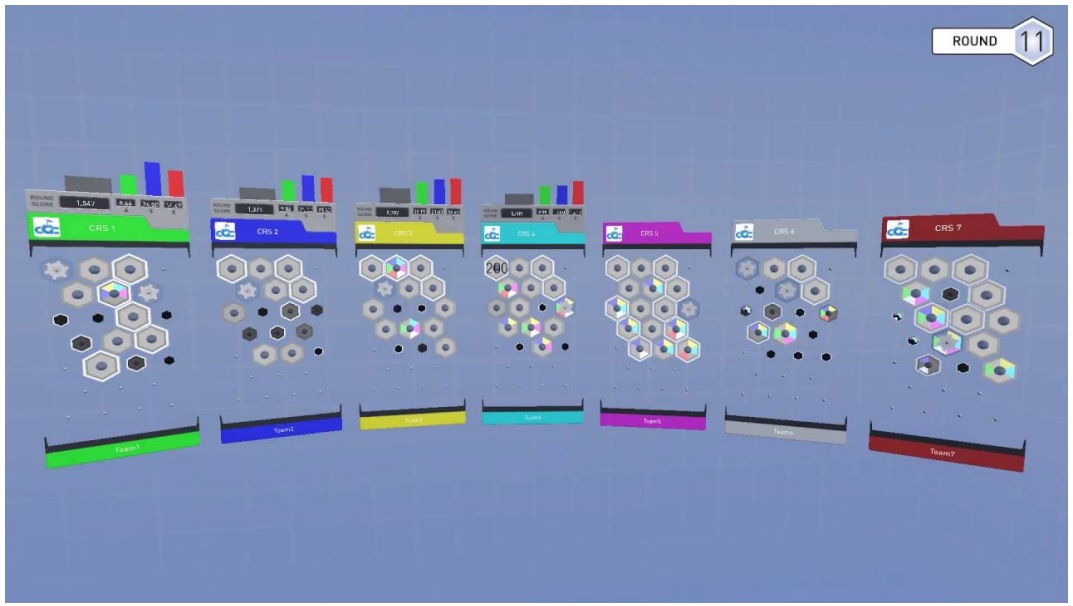
https://www.cna.com.tw/news/ait/201912010114.aspx

CTF Types

- Jeopardy
- Attack and Defense
- King of the Hill



- DARPA Cyber Grand Challenge (CGC)
  - 電腦之間的駭客競賽
  - 全自動的攻擊與防禦



CTF 競賽類型

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

CTF vs. security in the real world

- 雖然 CTF != 實戰的攻防

- CTF 的優點
  - 將重要的資安概念和實務技術包裝成競賽題目，寓教於樂，好玩有成就感

OWASP Top 10
Web Application Security Risks

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

CWE/SANS TOP 25
Most Dangerous Software Errors

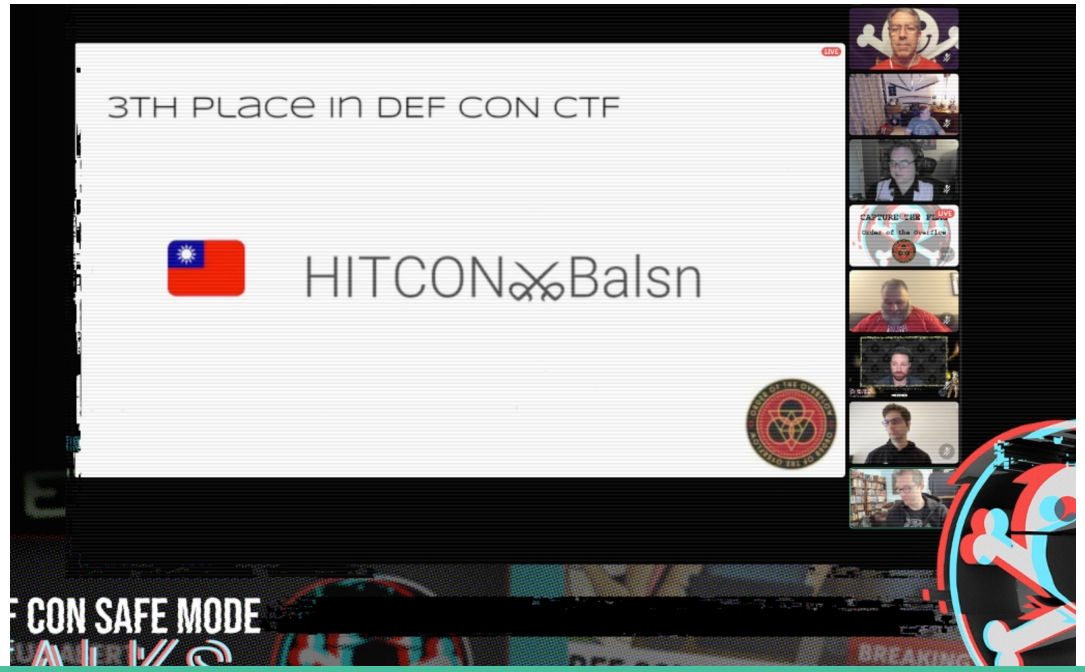
Rank	ID	Name	Score
[1]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	75.56
[2]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.69
[3]	CWE-20	Improper Input Validation	43.61
[4]	CWE-200	Information Exposure	32.12
[5]	CWE-125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

CTF vs. security in the real world

- 雖然 CTF != 實戰的攻防

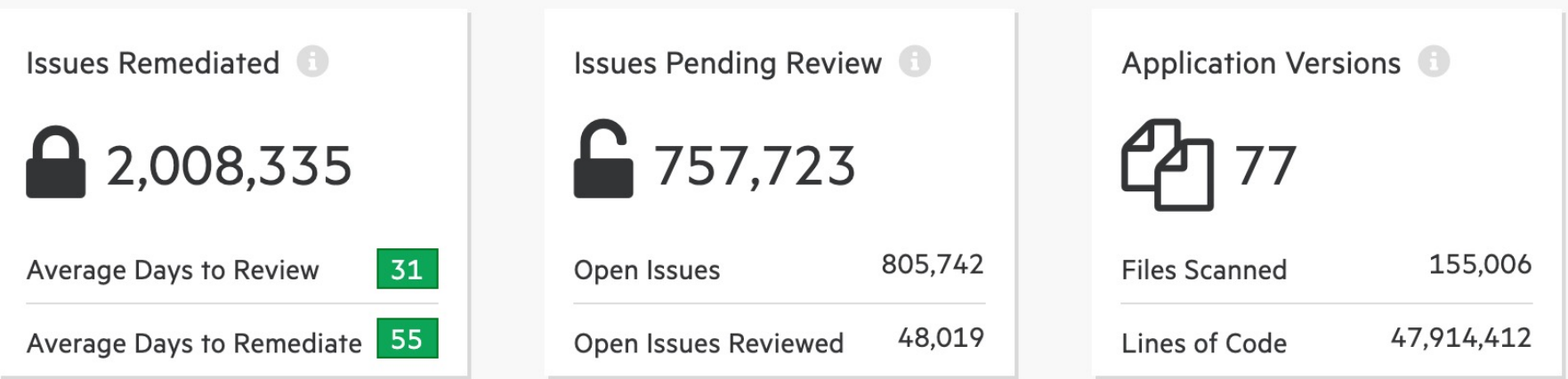
- CTF 的優點
  - 將重要的資安概念和實務技術包裝成競賽題目，寓教於樂，好玩有成就感
  - 能常常出國比賽（？


HITCON X BALSN
資安交流經典賽
2020 TAIWAN CTF


3TH PLACE IN DEF CON CTF
HITCON Balsn
F CON SAFE MODE

CTF vs. security in the real world

- 雖然 CTF != 實戰的攻防
- CTF 的優點
  - 將重要的資安概念和實務技術包裝成競賽題目，寓教於樂，好玩有成就感
  - 能常常出國比賽（？
  - 知道漏洞很容易產生，以後寫 code 會更小心



CTF vs. security in the real world

- 雖然 CTF != 實戰的攻防
- CTF 的優點
  - 將重要的資安概念和實務技術包裝成競賽題目，寓教於樂，好玩有成就感
  - 能常常出國比賽（？
  - 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

- 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自動化、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
- Vulnerability -> Exploit -> Patch

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

SQL Injection	LFI	XSS	Information Leak
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

資安倫理
Ethics of Hacking

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。

刑法第36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、拘役或科或併科二十萬元以下罰金。
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、拘役或科或併科二十萬元以下罰金。

超級駭客蘇柏榕再犯！盜百萬個資

xC

http://www.tvbs.com.tw/index/

更新日期:2007/09/22 15:18

國內爆發治安史上最嚴重的駭客事件，包括中華電信、無名小站">無名小站以及BBS網站，都遭駭客入侵，3百多萬名會員資料被竊取，而嫌犯就是超級駭客蘇柏榕，他曾在就讀建中期間，入侵總統府及大考中心網站，聲名大噪。現在疑似遭黑幫利用，竊取資料販售牟利。讓他的父母很心痛，說家裡沒有這個人。

蘇柏榕父親：「沒有這個人（蘇柏榕）啦！」記者：「您是蘇爸爸嗎？」蘇柏榕父親：「不是啦。」
轉過頭，不認蘇柏榕就是自己的兒子，蘇爸爸態度冷漠，或許是太過心痛失望。因為國內爆發治安史上，最嚴重的駭客事件，包括中華電話、無名小站以及知名BBS網站，有多達3百多萬名的會員資料，都遭到駭客入侵竊取。

刑法§358+§359

< APT目標攻擊 >冒用健保局名義,攻擊中小企業案,使用惡名昭彰的Ghost遠端存取木馬

POSTED ON 2013 年 07 月 02 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

作者：Maharlito Aquino（威脅研究員）

從逮捕勒索軟體集團的首腦之一，到成功打下Rove Digital(請參考:趨勢科技協助 FBI 破獲史上最大殭屍網路始末)，我們可以時常地看到執法單位和安全廠商間的合作行動，並且有著豐碩的成果。這一次，台灣刑事單位和趨勢科技合作偵破駭客假冒健保局,盜取萬筆中小企業個資案件，解決利用知名的Ghost遠端存取木馬家族所進行的APT-進階持續性滲透攻擊 (Advanced Persistent Threat, APT)目標攻擊。執法單位也逮捕了一名對象。

駭客假冒健保局寄帶有惡意程式的email
刑法§359+§360

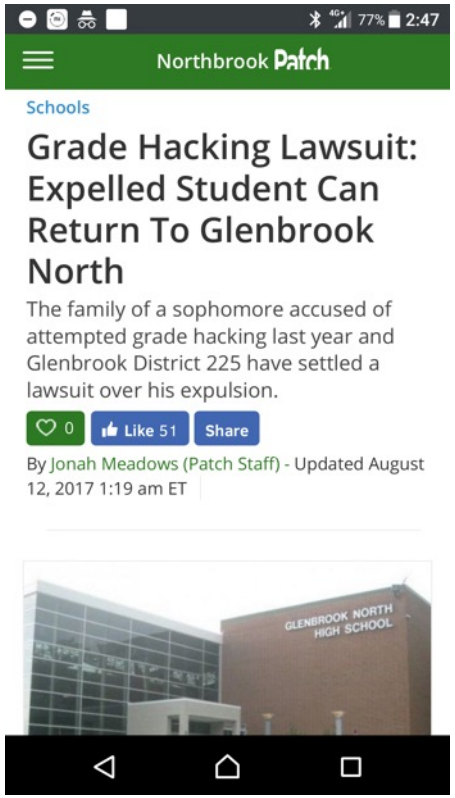
演唱會門票「秒殺」竟是黃牛集團電腦程式搶票

電腦程式搶票流程圖。（記者姚岳宏翻攝）

2017-01-16 15:05

拓元售票網黃牛票案
刑法§360+§362

Even More Lawsuit Cases



Respect for Law is the minimum requirement

Principle	Application
Respect for Persons	Participation as a research subject is voluntary, and follows from informed consent; Treat individuals as autonomous agents and respect their right to determine their own best interests; Respect individuals who are not targets of research yet are impacted; Individuals with diminished autonomy, who are incapable of deciding for themselves, are entitled to protection.
Beneficence	Do not harm; Maximize probable benefits and minimize probable harms; Systematically assess both risk of harm and benefit.
Justice	Each person deserves equal consideration in how to be treated, and the benefits of research should be fairly distributed according to individual need, effort, societal contribution, and merit; Selection of subjects should be fair, and burdens should be allocated equitably across impacted subjects.
Respect for Law and Public Interest	*Engage in legal due diligence; Be transparent in methods and results; Be accountable for actions.*

Source: Dr. Shehar Bano

Respect for person

- In the name of good will and science?
  - Hack in vulnerable devices and patch them?
  - Hijack spam botnets for research purposes?
  - Infiltrate the administration team of an underground market to study sales of illegal drug and weapon?

IF You Must Hack Something …

- Consider BUG BONTY PROGRAMS
  - https://hackerone.com
  - https://www.bugcrowd.com/bug-bounty-list

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

Resources

- Basic and Concepts by Weber Tsai (2017 TA)
  - https://www.youtube.com/watch?v=T_TJABTuL0o
- Tools
  - gdb/gdb-peda, ltrace, strace
  - strings, readelf, objdump, IDA/Ghidra, xxd
  - scripting/pwntools