Course Information

CSIE 7016 Computer Security, Fall 2017

https://csie.ctf.tw

計算機安全
Computer Security

(9:10-12:10) Fridays 234 Location: R204

https://csie.ctf.tw

Email: ctf@csie.ntu.edu.tw

討論室：https://tlk.io/edu-ctf

課程特色
Features

This is a non-traditional security course.

課程內容以實務攻防為主

- 本學期主軸為binary exploitation
- 大量的課後練習
- 還要參加CTF和bug bounty

課程特色
Features

This is a non-traditional security course.

跨校連線教學與競賽

- 講師來自臺大、交大、台科大，還有業界(黃金陣容!)
- 沒有期中考，但有期末競賽

課程特色
Features

This is a non-traditional security course.

建議具備資安基礎知識再選修

- 如修過密碼學、資訊安全
- 如參加過暑期資安課程、講習

課程目標
Course Objectives

提供學習和互動的機會給對hacking有興趣的同學

培育資安人才

招募CTF成員

尋找對自動化攻防有興趣的專題生和研究生

~~提升台灣整體資安防護的能力~~

Today’s Agenda

講師介紹和聯絡方式

課程大綱

加簽原則（台大only）

成績計算方式（台大only）

What is Capture the Flag?

Ethics of hacking

Course Website
https://csie.ctf.tw

Allowed IPs:

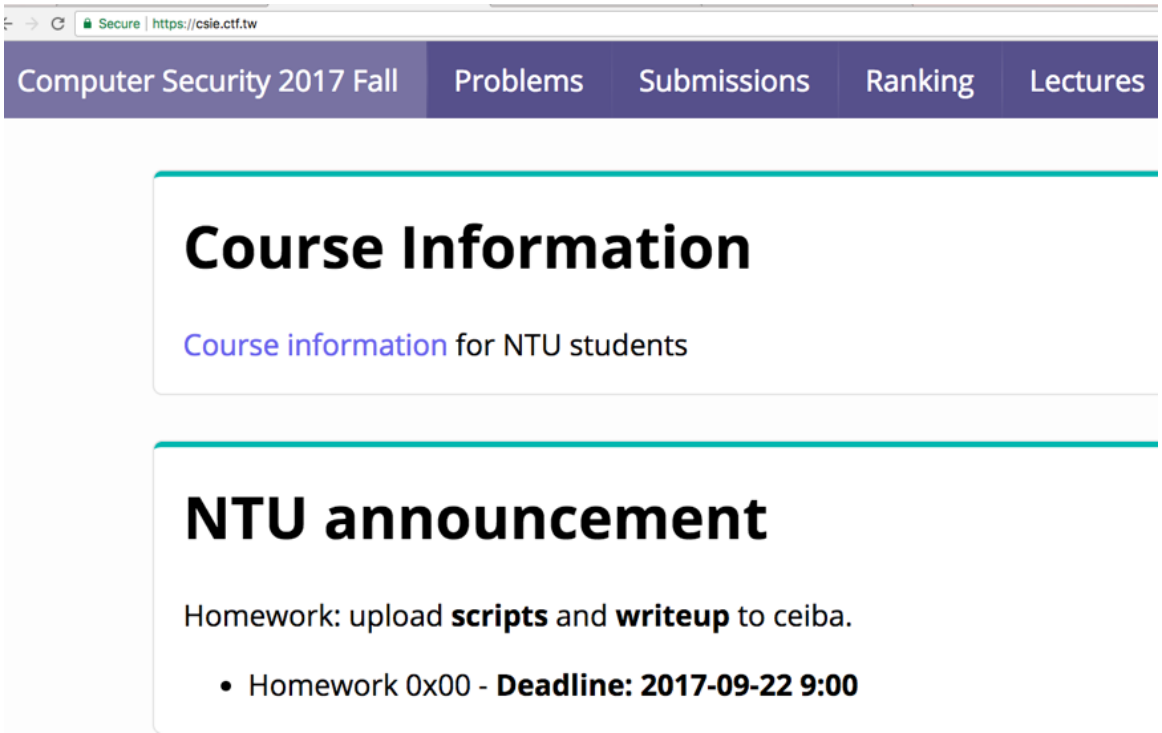
140.112.0.0/16

140.113.0.0/16

140.115.0.0/16

140.118.0.0/16

請愛用VPN



Teaching Team

台大	交大	台科大
蕭旭君	黃俊穎	鄭欣明
楊安傑 Angelboy	彭詩峰 Lays	蔡振華
陳威甯	陳仲寬	
王建元	王威擎	

Email: ctf@csie.ntu.edu.tw

Please DO NOT send to our personal emails

因各校規定略有不同，**寄信請註明學校**，方便教學團隊判斷如何回覆

Tentative Schedule

Wk.	Date	Topic
1	Sep 15	Course Introduction
2	Sep 22	Basic Tools & Concept
3	Sep 29	Assembly & Basic Knowledge
4	Oct 6	Linux Binary Exploitation - BOF
5	Oct 13	Linux Binary Exploitation - FMT/ROP
6	Oct 20	Linux Binary Exploitation - Heap
7	Oct 27	Introduction to Bug Bounty
8	Nov 3	Guest Lecture by QNAP
9	Nov 10	Mid-term Week (no exam, no class)

Tentative Schedule

Wk.	Date	Topic
10	Nov 17	Guest Lecture by Synology
11	Nov 24	Linux Binary Exploitation – Advanced
12	Dec 1	Symbolic Execution
13	Dec 8	Symbolic Execution
14	Dec 15	Windows Reverse
15	Dec 22	Windows Reverse
16	Dec 29	Guest Lecture (TBD)
17	Jan 5	Windows Exploitation
18	Jan 12	Final Week

Final CTF competition: 01/12 (9am) – 01/14 (5pm)

Make sure you can participate!

Attack & Defense in the Real World

Automated Analysis Techniques

Linux & Windows Exploitation

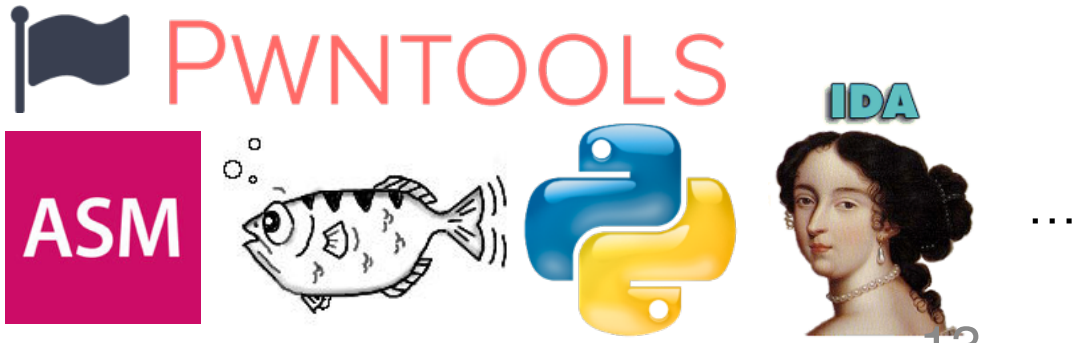
Basic Tools and Concepts

Attack & Defense in the Real World

Automated Analysis Techniques

Linux & Windows Exploitation

Basic Tools and Concepts



...

Attack & Defense in the Real World

Automated Analysis Techniques

Linux & Windows Exploitation

Basic Tools and Concepts

Attack & Defense in the Real World

Automated Analysis Techniques

Linux & Windows Exploitation

Basic Tools and Concepts

Attack & Defense in the Real World

Automated Analysis Techniques

Linux & Windows Exploitation

Basic Tools and Concepts

以下**加簽原則**與**評分方式**
只適用於台大修課的同學

加簽原則

根據HW0的成績來決定加簽的順序
人數上限依教室容量而定

開放旁聽，但不要佔到有選到課同學的座位

Homework 0x00

繳交期限：9/22 (Fri.) 9:00

繳交方式：請上課程網站註冊 (註冊完請填姓名與學號) 並詳細閱讀說明

加簽上的同學之後要在CEIBA上繳交HW0的code和說明，作為修課和評量的依據之一

＊＊＊作業只會越來越難，請審慎評估是否要修這門課＊＊＊

Grading Components

Homework assignments (65%)

Final CTF competition (25%)

Bug Bounty participation (10%)

Bonus: https://pwnable.tw/

- bonus = min (10, raw score/200)

Other bonus

- 課堂表現
- 課餘競賽表現優異
- 上台報告分享
- …

如有困難請儘早跟老師和助教聯絡

Final grade: criteria

百分數		等第	定義	等第績分
90-100	95	A+	All goals achieved beyond expectation 所有目標皆達成且超越期望	4.3
85-89	87	A	All goals achieved 所有目標皆達成	4.0
80-84	82	A-	All goals achieved, but need some polish 所有目標皆達成，但需一些精進	3.7
77-79	78	B+	Some goals well achieved 達成部分目標，且品質佳	3.3
73-76	75	B	Some goals adequately achieved 達成部分目標，但品質普通	3.0
70-72	70	B-	Some goals achieved with minor flaws 達成部分目標，但有些缺失	2.7
67-69	68	C+	Minimum goals achieved 達成最低目標	2.3
63-66	65	C	Minimum goals achieved with minor flaws 達成最低目標，但有些缺失	2.0
60-62	60	C-	Minimum goals achieved with major flaws 達成最低目標但有重大缺失	1.7
≦ 59	50	F	No goals achieved 所有目標皆未達成	0
0	0	X	Not graded due to unexcused absences or other reasons 因故不核予成績	0

Failing grade for grad students

Failing grade for undergrads

Warning: final grade is non-negotiable

http://www.oia.ntu.edu.tw/upload/files/20150616223619.pdf

Grading Component 1: Homework Assignments

CTF（capture the flag）形式

每週講師都會出作業

要在CEIBA上繳交code和writeup

作業不能遲交

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

抄襲行為: zero tolerance

作業抄襲(就算只有一次)：學期成績為F

考試作弊：學期成績為F

Grading Component 2: Final CTF Competition

CTF = Capture the Flag

Attack & Defense or Jeopardy

預計為期三天: 1/12-1/14

分組人數等確定總修課人數後決定

Grading Component 3:
Bug Bounty Participation（賞金獵人）

Grading Component 3: Bug Bounty Participation

參考UC Berkeley Prof. Doug Tygar的課程規劃

https://people.eecs.berkeley.edu/~tygar/cyberwarF17faq.html

同學自行選擇要參加哪個bug bounty

評分方式：寫參賽心得和漏洞解析

Bonus: 有得到獎金加分

Grading Component 3: Bug Bounty Participation

Don’t know where to start?

10/27: Introduction to Bug Bounty

List of bug bounty programs

- https://hackerone.com
- https://www.bugcrowd.com/bug-bounty-list/

QNAP講師熱情贊助，提供同學機器分析（詳情會在第三、第四週公佈）

TA Hours @ NTU

2-3pm (Wed.) @ R307

2-3pm (Thu.) @ R307

1-2pm (Fri.) @ 地下室 零度前面

雖然有許多週是同步視訊連線，但鼓勵同學還是來204電腦教室一起上課，因為：

- 隨時有問題可以問在現場的助教
- 可以和其他同學討論
- 課程影片不一定會公布

What is Capture the Flag?

Capture the Flag (CTF) Competition

Competitive cyber wargame for computer security

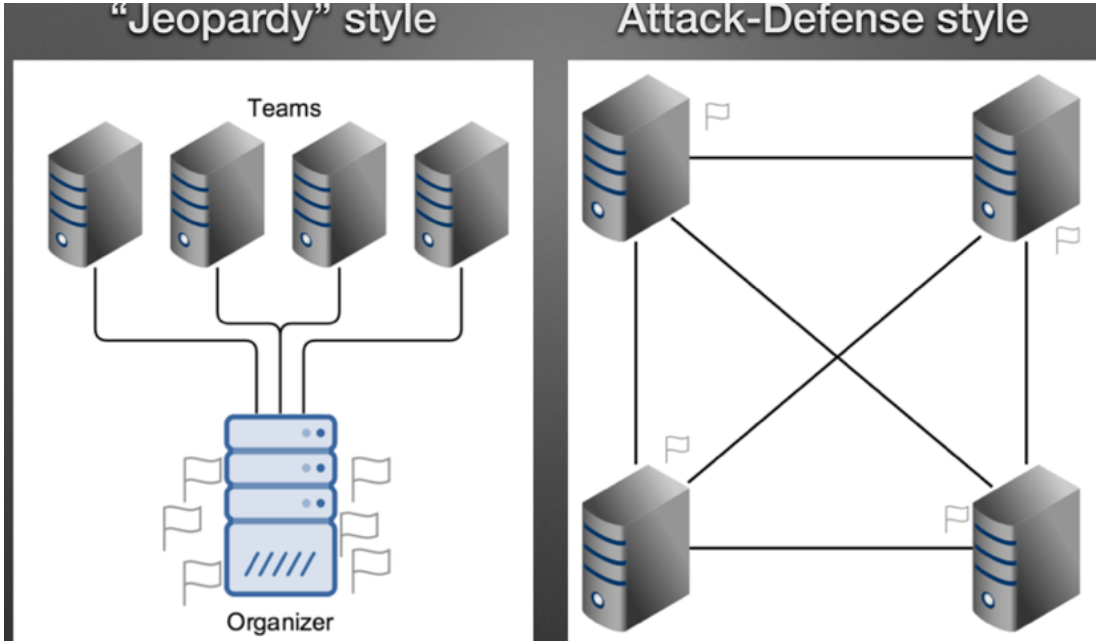
Teams compete to steal data (“flags”) from computers

Types of CTF

Jeopardy

Attack and Defense

King of the Hill



By Tyler Nighswander

Categories of CTF Problems

Cryptography

Forensics

Reverse engineering

Pwnable

Web exploitation

Misc

…

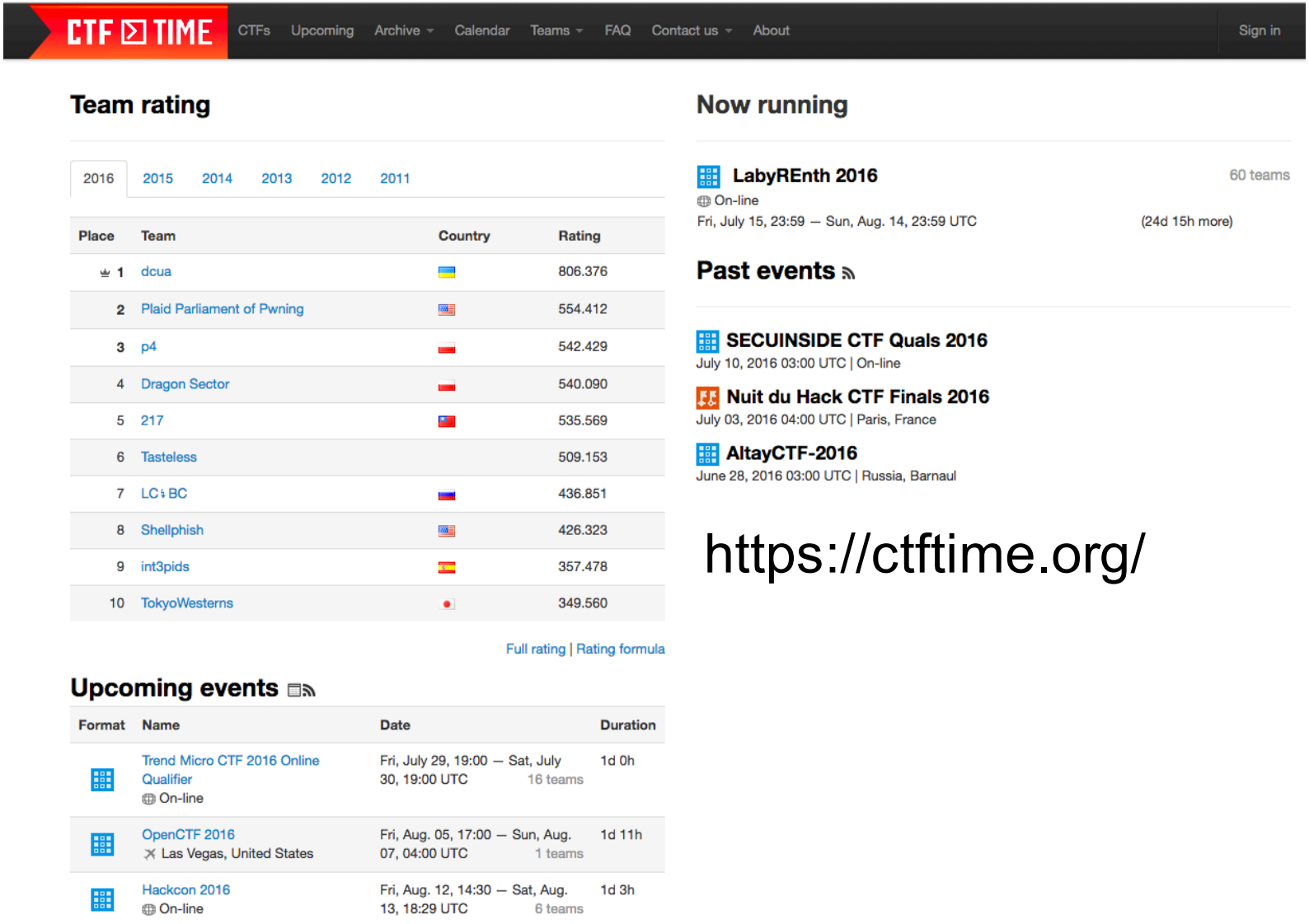
Many Online Practice Sites

http://overthewire.org/wargames/

http://pwnable.kr/

https://captf.com/practice-ctf/

....



https://ctftime.org/

工商服務

金盾獎 2017

- https://csc.udndigital.com.tw
- 網站報名日期106年9月1日(五)~10月2日(一)17:00止
- 初賽日期106年10月14日(六)

HITCON CTF 2017

- http://ctf.hitcon.org
- Online Jeopardy, Nov 4 10:00 AM ~ Nov 6 10:00 AM, 2017 (GMT+8, 48 hours)
- Online registration will open at Oct 28.

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

科技公司董事長及員工扮駭客，入侵高鐵售票系統修改票價自行升等

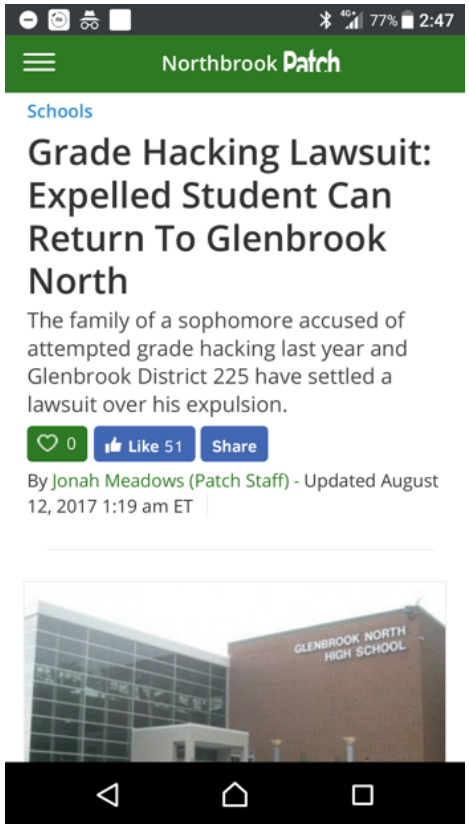
janus 發表於 2015年8月19日 17:05 | 收藏此文

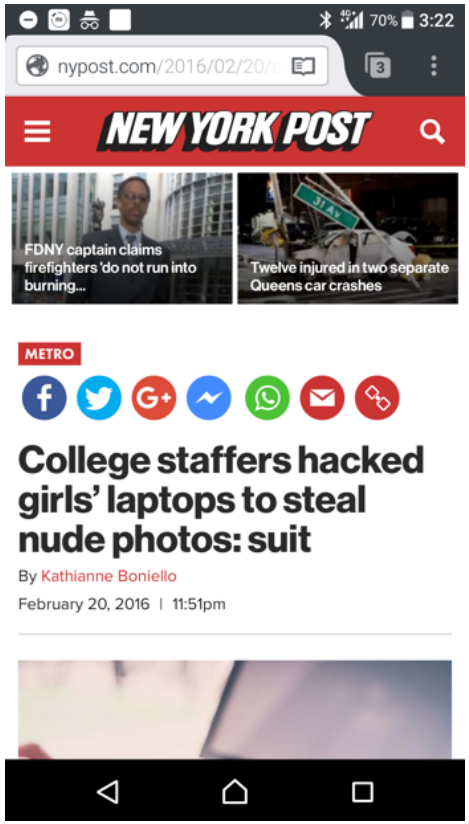
G+1 20 讚 1,497

高鐵公司在今年四月發現，網路購票系統從今年三月底開始，出現了九筆異常的交易狀況。經過鐵路警察局以及刑事局偵九隊調查發現，確認高鐵網站遭到駭客入侵付款系統，駭客竄改了票價的交易金額。而經過三個月的調查，刑事局昨天將駭入高鐵的兩名駭客逮捕。

Even More Lawsuit Cases

改成績　偷照片　搶銀行　駭手機





IF You Must Hack Something …

Consider BUG BONTY PROGRAMS

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

Any attempt to cheat or attack others (including the teaching team) may lead to a failing grade

Next Week

Basic Tools & Concept (by 振華)

- gdb
- readelf
- objdump
- IDA
- binary patching
- scripting
- …