

時間	題目	主講者
13:00- 13:30	記者會 – VulReport 發表會	Sylphid Su
13:30- 14:00	聽眾報到	
14:00- 14:30	開場及 2014 年度回顧 / HITCON 2015	TT
14:30- 15:00	2014 年台灣企業安全常見風險剖析	Bowen Hsu
15:00- 15:20	下午茶	
15:20- 15:50	駭客如何弄垮企業？ 從索尼影業與南韓核電廠事件說起	GasGas / Fyodor
15:50- 16:40	Operation GG 台灣最熱門網遊安裝檔 驚見網軍後門	Kenny / PK / Kaspersky Trend Micro
16:40- 17:40	座談	



Hacks
In Taiwan
Conference

Free Talk

2015.01.09

TT@HITCON.org



致謝



公民攝影守護民主陣線

Live broadcasting

注意事項

可以拍照，但只能對著台上拍

不可以錄影

會議室內禁止飲食

手機請調成靜音

連 wifi 自己要小心

不要踢到攝護線

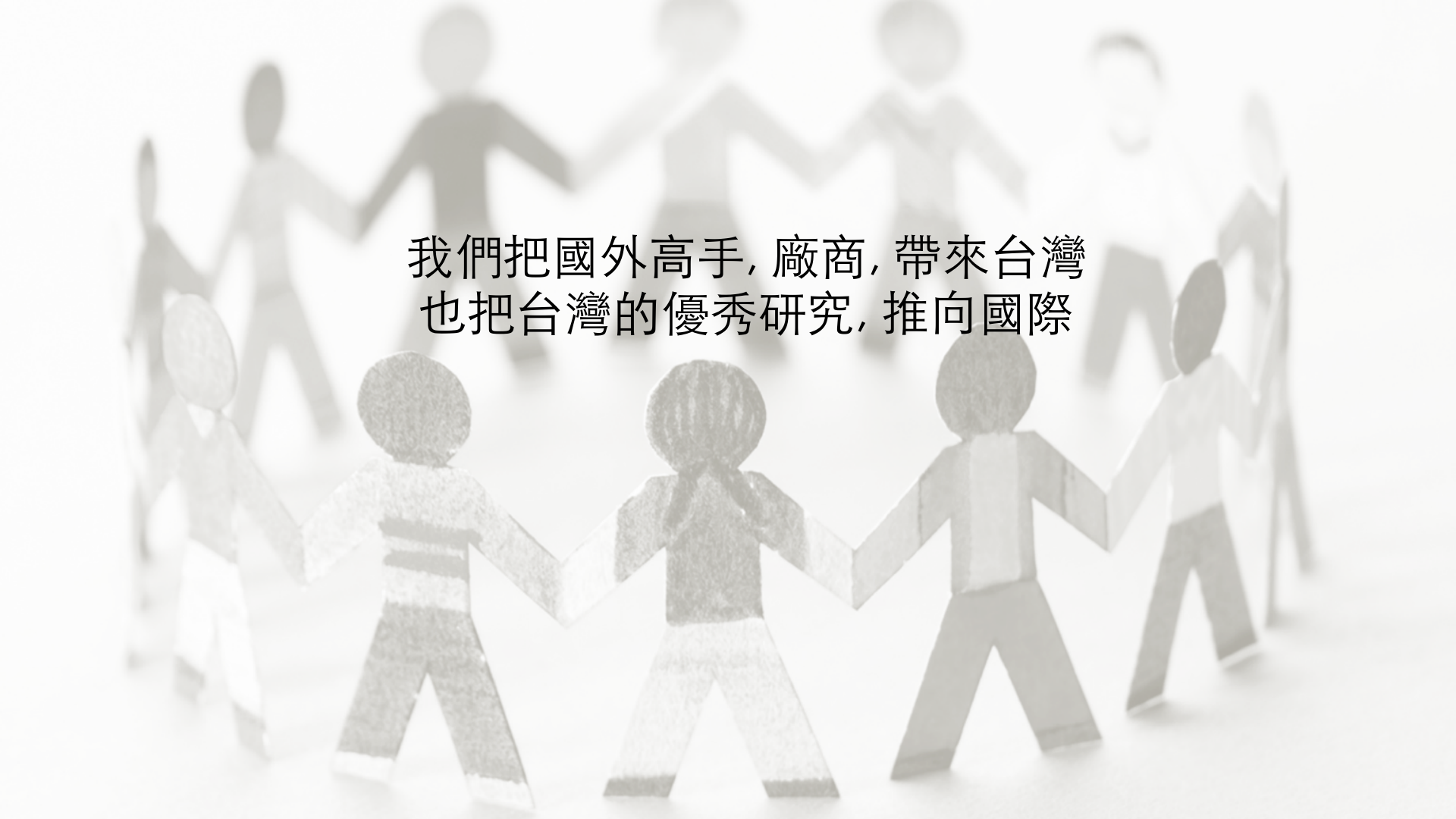


台灣駭客年會默默的推動國家資安的發展



數百場世界頂尖資安研究分享
國際大廠持續關注台灣資安研究
國內外資安社群交流
讓更多人願意關注資安, 學習資安



The background of the image features a group of stylized, cut-out human figures in various shades of gray. They are arranged in a circular formation, holding hands, which symbolizes unity, teamwork, and global collaboration. The figures are simple in design, with some wearing hats or having different hairstyles. The overall tone is light and positive.

我們把國外高手, 廠商, 帶來台灣
也把台灣的優秀研究, 推向國際

傳遞最新資安訊息



HITCON Free Talk

2014 回顧與 2015 展望

The logo features the word "Hitl00" in a bold, black, 3D block font. Below it, the word "Playground" is written in a black, cursive script. The background is white with several light gray diamond shapes of varying sizes and orientations scattered around the text.

Hitl00
Playground

The logo features the word "Hitl00" in a bold, white, 3D block font. Below it, the word "Enterprise" is written in a white, cursive script. The background is solid black with several dark gray diamond shapes of varying sizes and orientations scattered around the text.

Hitl00
Enterprise

A group of approximately 12 young men, members of the HITCON CTF team, are posing for a photo in a large, modern hallway. They are dressed in a mix of casual and semi-formal attire, including t-shirts, jackets, and lab coats. Several team members are wearing lanyards with identification badges. In the background, a sign on the wall reads "CAPTURE THE FLAG". The hallway has a high ceiling with a large square light fixture and a patterned floor.

HITCON CTF 戦隊

HITCON CTF 2014

8/16 12:00 ~ 8/18 12:00 (UTC+8)

Online Registration: 7/1 ~ 8/17

[Goto Contest](#)

SONY

CHROOT / HITCON

實習生計畫

**INTERN
WANTED**



HITCON GIRLS

「女孩的第一堂資安課」，

歡迎對資安有興趣，想學習資安技術的女孩們來參加我們精心規劃、為期兩天的WORKSHOP活動。

趕快報名參加，一起加入HITCON GIRLS吧!

2015 ?

2015 CTCTF

台交網路攻防搶旗賽

2014年8月，有一群對資安技術充滿熱誠，以學生為主的台灣HITCON駭客團隊，在美國拉斯維加斯舉辦的DEF CON CTF 駭客競賽，獲得了第二名的成績，是國內資安史重要的里程碑。這種駭客競賽，參加的選手需同時具備演算法分析、程式設計、系統程式概念、系統漏洞分析、系統防禦和攻擊程式撰寫能力等等，這種競賽可說是全方位的電腦科學競技，各國為了培養這類高階資安技術人才，均舉辦此類CTF (Capture the Flag)駭客競賽來厚植防禦能量。

為了培訓更多優秀高階資安技術選手，台灣大學與交通大學兩校設立軟體安全課程，訓練學生能夠具備軟體安全的實務經驗，並於學期末共同舉辦台交網路攻防搶旗賽 (Attack and Defense)，讓修課學生互相驗證實力。這也是台灣首度嘗試舉辦與美國DEF CON CTF相同的Attack Defense競賽，也期待未來能有更多隊伍能參與，提昇台灣學生的資訊安全實務能力。



和沛科技
最專業的雲端儲存及運算解決方案



中華電信 hicloud
國內最專業、完整的雲端服務提供商

企業註冊

登入 / 註冊



Adobe Flash Player Heap Overflow

There is a heap overflow in Adobe Flash Player 14.0.0.125 on Windows 7 , which results in remote code execution.

🚀 最新提交

- Incident **JAN-08** Lobsiinvok
某縣市公共圖書館目錄洩漏導致大量資訊流
- Application **JAN-06** M4LORcl
某上網服務 SQLi

✅ 最新確認

- Application **JAN-08** Orange
某防毒軟體意見中心 Stored XSS
- Application **JAN-08** DMC
某連鎖餐飲餐點情報頁面 SQL Injection

⚠️ 最新公開

- Service **JAN-07** Orange
某防毒軟體線上檔案系統密碼洩漏
- Incident **DEC-16** beichen
VulReport 重置密碼問題



HITCON Junior

HITCON Junior 計畫

走出台北，到各地或校園推廣資安

我們歡迎各地資安社團與我們聯繫

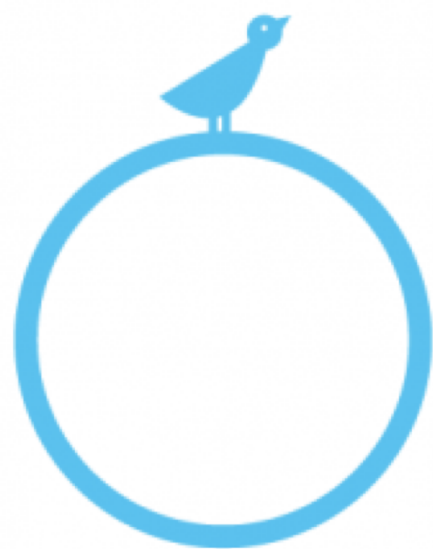
近期推出，請密切注意 HITCON Facebook

也徵求贊助商



2014 的資安狀況？





和平佔中

OCCUPY CENTRAL WITH
LOVE AND PEACE

6.20-22

全民投票

POPVOTE.HK

Sony Pictures hackers leak scripts, celebrity phone numbers and aliases

Apps and Software

By Lee Mathews Dec. 9, 2014 9:30 am



Follow @geekdotcom



354,353 people like Geek.com.

The group calling themselves Guardians of Peace continue to leak

2014 – The Year of ~~Today~~ Legacy Vulnerabilities

CVE - 2014 - 0160



Heartbleed

OpenSSL

Critical information
leakage

CVE - 2014 -1761



Microsoft Office

Word

RTF Document

CVE - 2014 -1776



Internet Explorer

0day

Spear phishing with
waterhole attack

CVE - 2014 - 6271

A terminal window titled 'masscan - sh - 35x9' showing a shellshock exploit. The prompt is 'sh-3.2\$'. The command entered is 'env x='() { :}; echo vulnerable' bash -c "echo this is a test"'. The output is 'vulnerable' followed by 'this is a test' on a new line.

```
sh-3.2$ env x='() { :}; echo vulnerable' bash -c "echo this is a test"
vulnerable
this is a test
```

Shellshock

25 years old

CVE - 2014 - 7169

CVE - 2014 - 4114



Sand Worm

Microsoft Office
Powerpoint

Logical flaw
MS-12-005

CVE - 2014 - 6332



Internet Explorer

19 years

IE 3.0 - IE 11

Windows 95 - Windows 8.1



GG 的一年

時間	題目	主講者
13:00 - 13:30	記者會 – VulReport 發表會	Sylphid Su
13:30 - 14:00	聽眾報到	
14:00 - 14:30	開場及 2014 年度回顧 / HITCON 2015	TT / Alan
14:30 - 15:00	2014 年台灣企業安全常見風險剖析	Bowen Hsu
15:00 - 15:20	下午茶	
15:20 - 15:50	駭客如何弄垮企業？ 從索尼影業與南韓核電廠事件說起	GasGas / Fyodor
15:50 - 16:40	Operation GG 台灣最熱門網遊安裝檔 驚見網軍後門	Kenny / PK / Kaspersky Trend Micro
16:40 - 17:40	座談	