出國報告（出國類別：其他國際會議）

出席「國際資訊安全會議(DEF CON 25)」報告

服務機關：行政院資通安全處
姓名職稱：周智禾 科長
派赴國家：美國(拉斯維加斯)
出國期間：106 年 7 月 26 日至 106 年 8 月 1 日
報告日期：106 年 9 月 30 日

摘　　要

近年來，網路攻擊事件層出不窮，資通安全威脅已成為國際關注之重要議題，各國亦定期召開資安相關會議以促進最新資安發展趨勢之交流及分享，包含 RSA Conference、Blackhat 及 DEF CON 等。其中 DEF CON 係全球最知名的駭客技術會議之一，每年定期於美國拉斯維加斯舉辦，內容包含豐富的資安趨勢論壇、最新資安軟硬體設備展覽及國際間最重要的網路攻防奪旗賽(Capture the Flag, CTF)。

本(106)年(第 25 次)DEF CON 於美國拉斯維加斯 Caesar’s Palace 舉辦為期 4 日(7 月 27 至 30 日)會議，其內容包括各項軟硬體的最新漏洞發表，以及時下最熱門的物聯網(Internet of Thing, IoT)安全議題；其中，我國 DEVCORE 團隊的 Orange Tsai 於會議中發表伺服器端請求偽造(Server-Side Request Forgery, SSRF)攻擊，獲得與會人員熱烈迴響;另代表我國參加 CTF 比賽的隊伍(HITCON)則自 103 年起連續 4 年入選最後決賽，本年最後取得第 2 名的佳績。

經參加本次會議，建議後續可定期派員參與類此駭客盛會，以掌握最新資安威脅趨勢；建立資通安全科技研發整體規劃與推動機制，並針對新興技術建置相關實驗場域，以提升國家整體資安自主技術能量；由政府機關主動與相關資安社群合作，進一步帶動資安人才培育，循序充實各層級資安人才。

目　　錄

目　　錄 i
壹、會議介紹 1
　一、會議名稱 1
　二、會議時間 1
　三、會議地點 1
　四、會議相關文件 1
貳、參加會議目的 2
參、會議過程及重點議題 3
　一、會議議程 3
　二、重點議題 6
肆、心得建議 23
伍、會議照片 24

壹、會議介紹

一、會議名稱

DEF CON 25

二、會議時間

106 年 7 月 27 至 106 年 7 月 30 日

三、會議地點

美國拉斯維加斯 Caesar’s Palace 會議中心

四、會議相關文件

會議相關資料請詳見網站(https://www.defcon.org/html/defcon-25/dc-25-index.html)

貳、參加會議目的

DEF CON 為國際間極富盛名的駭客技術會議之一，會議中發表許多最新資安議題，不論是機器學習與資安領域的結合應用、物聯網設備的攻擊與防禦、數位鑑識、網路入侵偵測、惡意程式分析、雲端服務防護、工控系統安全及物聯網安全等，皆為會議議題之一；迄今已舉辦 25 屆，每年吸引超過 1 萬名的專業資安駭客，以及廠商、政府機關、學研界等資安專業人員齊聚於美國拉斯維加斯，旨在交流資安最新趨勢、攻防最新手法及系統最新弱點。

本次出國主要目的希望能從會議各類議題中瞭解最新資安威脅並掌握國際發展趨勢，除了提升本身對資安議題的認知外，亦期望藉由演講中所獲取的新知與技術，瞭解目前駭客最新的技術，增廣資安見聞，提供業務或決策方面上的協助；另藉由參觀不同主題的駭客村(Villages)，例如 car village、IoT village、social engineering village、crypto and privacy village 及 lockpick village 等，以掌握時下頂尖駭客對資安領域的研究成果，瞭解軟體安全、威脅分析及駭客攻擊手法等議題。

參、會議過程及重點議題

一、會議議程

DEF CON 25 演講議程自 7 月 27 日(四)至 7 月 30 日(日)，共分為 4 個廳進行演講，包括「DEF CON 101」、「Track 2」、「Track 3」及「Track 4」，議程詳如圖 1 至圖 4：

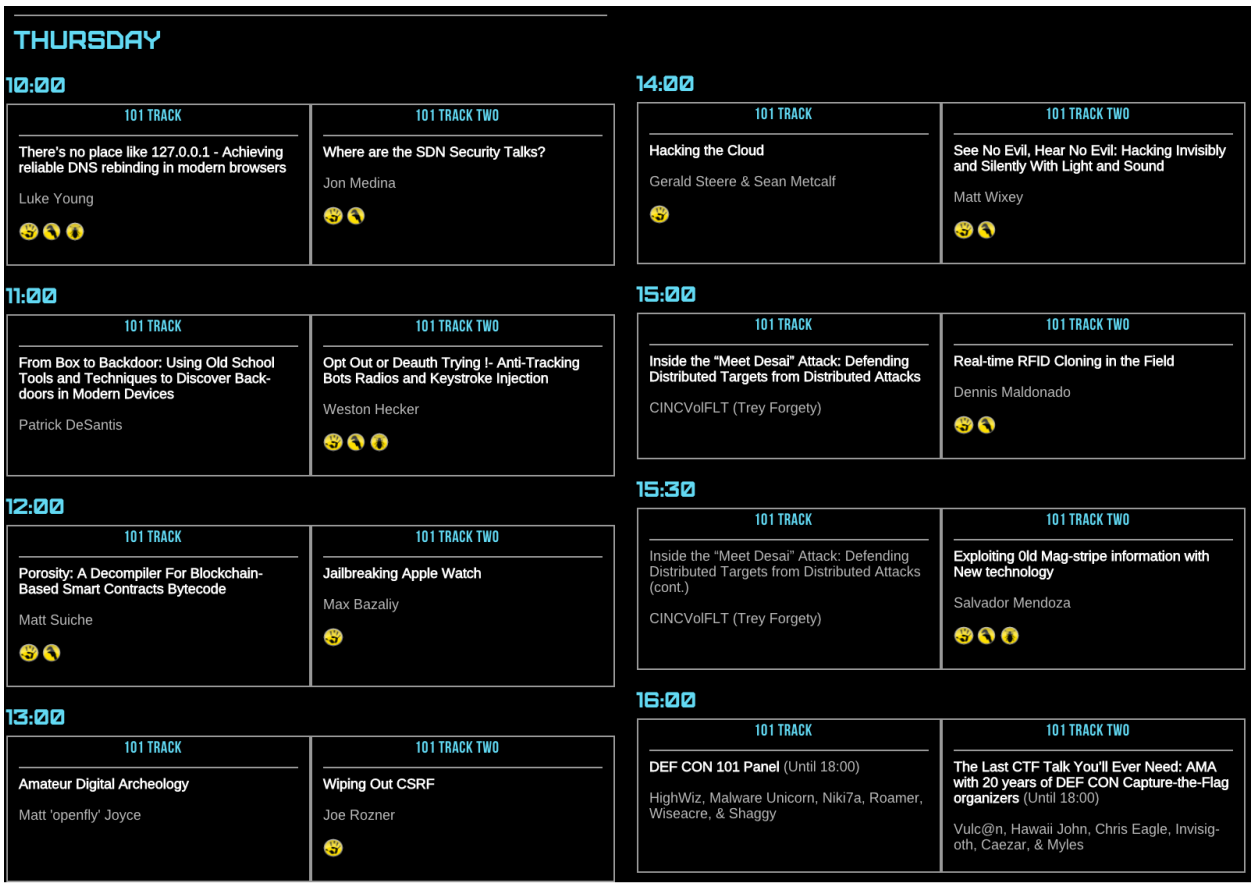

圖 1：DEF CON 25 會議第 1 日議程(7 月 27 日)

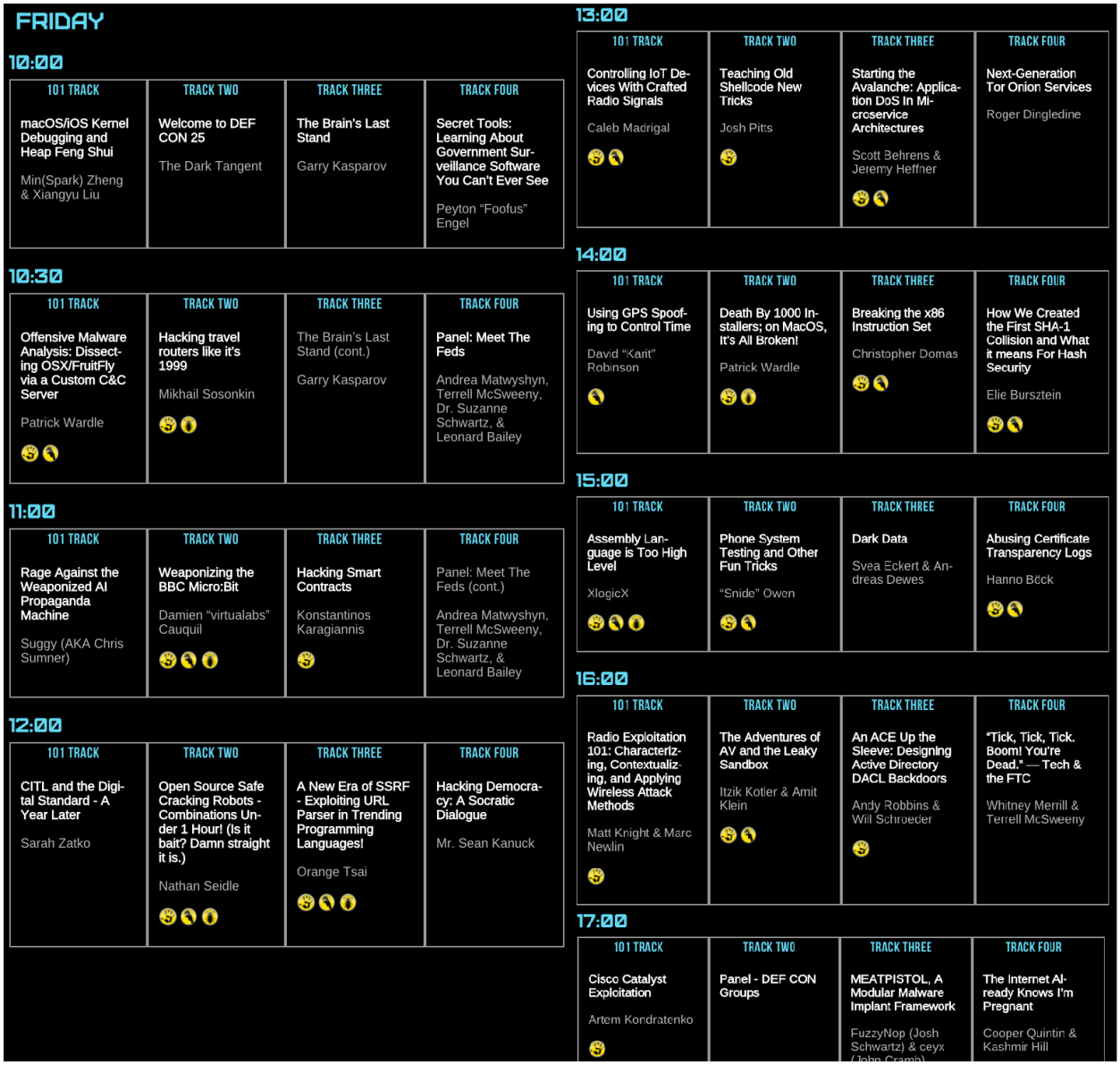

圖 2：DEF CON 25 會議第 2 日議程(7 月 28 日)

圖 3：DEF CON 25 會議第 3 日議程(7 月 29 日)

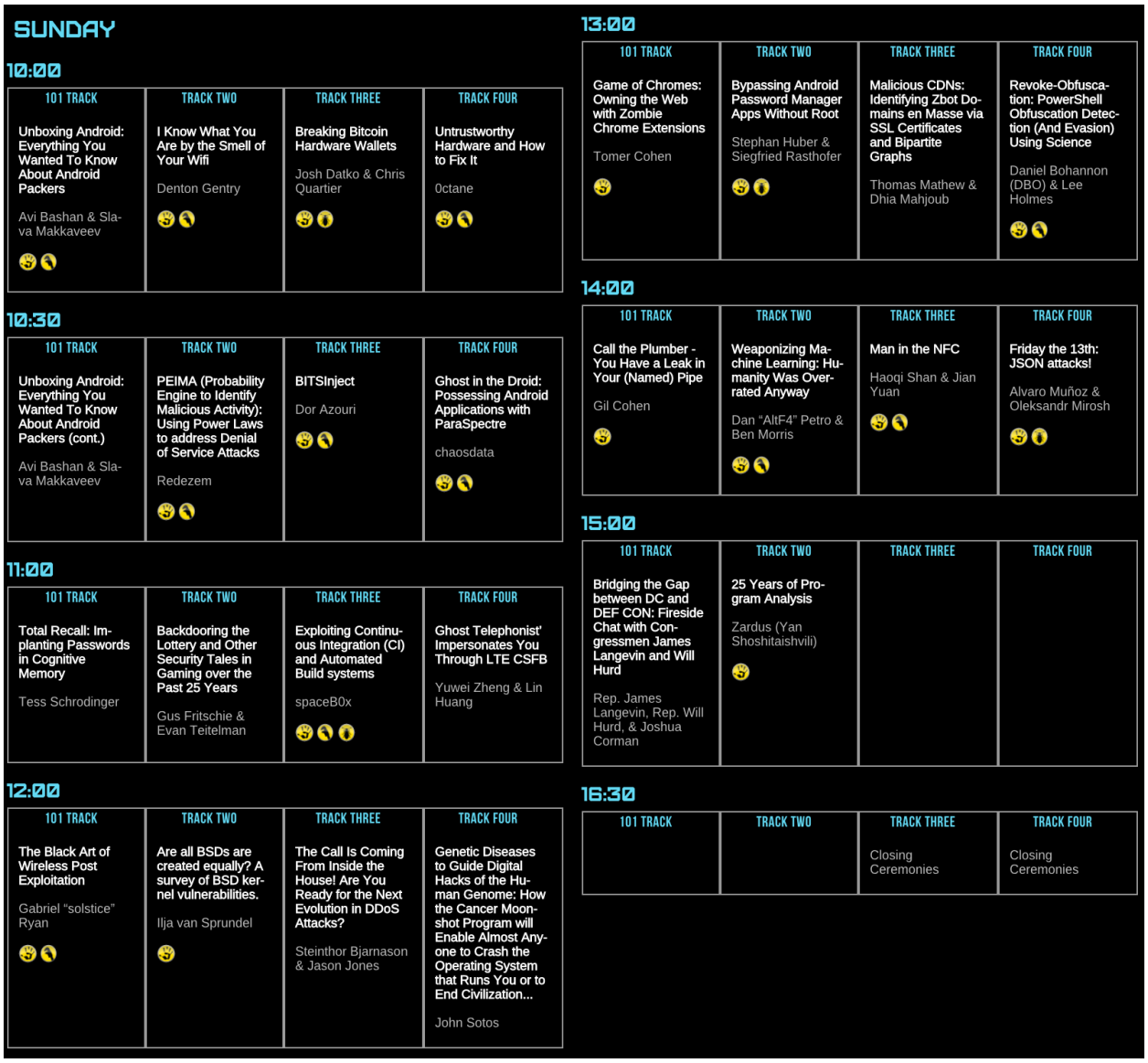

圖 4：DEF CON 25 會議第 4 日議程(7 月 30 日)

二、重點議題

(一)A New Era of SSRF - Exploiting URL Parser in Trending Programming Languages

伺服器端請求偽造(Server-Side Request Forgery, SSRF)為近年相當熱門的議題，本場演講受矚目之處為講者係我國戴夫寇爾(DEVCORE)團隊的蔡政達(Orange Tsai)，其內容主要係提出透過目前 URL Parsing 的漏洞進行攻擊，演講現況如圖 5。

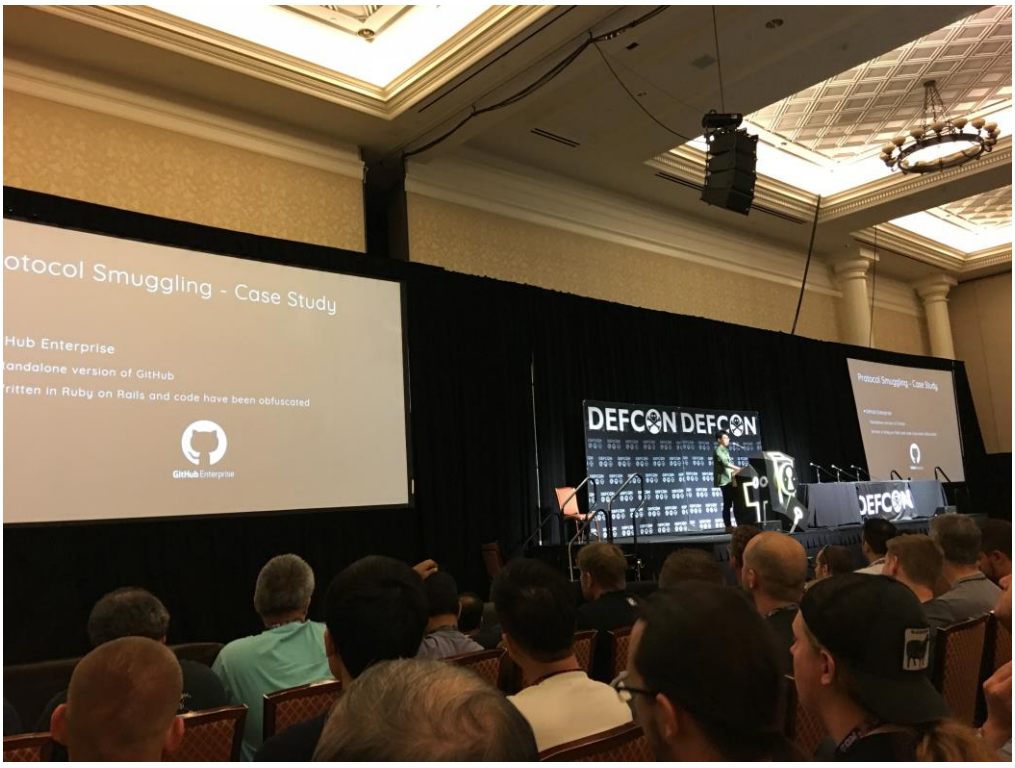

圖 5：A New Era of SSRF - Exploiting URL Parser in Trending Programming Languages 演講現況

1、SSRF 簡介

目前許多網站服務皆提供使用者輸入來源網址，由伺服器提供查詢或執行的服務，如搜尋引擎提供圖片搜尋或網頁內容擷取功能等。SSRF 係指由攻擊者傳送來源，透過伺服器端發起內網或外網的查詢請求，因為伺服器端通常不被防火牆阻擋，可繞過防火牆防護，惟來源參數內容為客戶端提供予伺服器端執行，倘若未進行檢查，可能造成內網攻擊或機敏資訊洩漏的可能，SSRF 攻擊架構詳如圖 6。

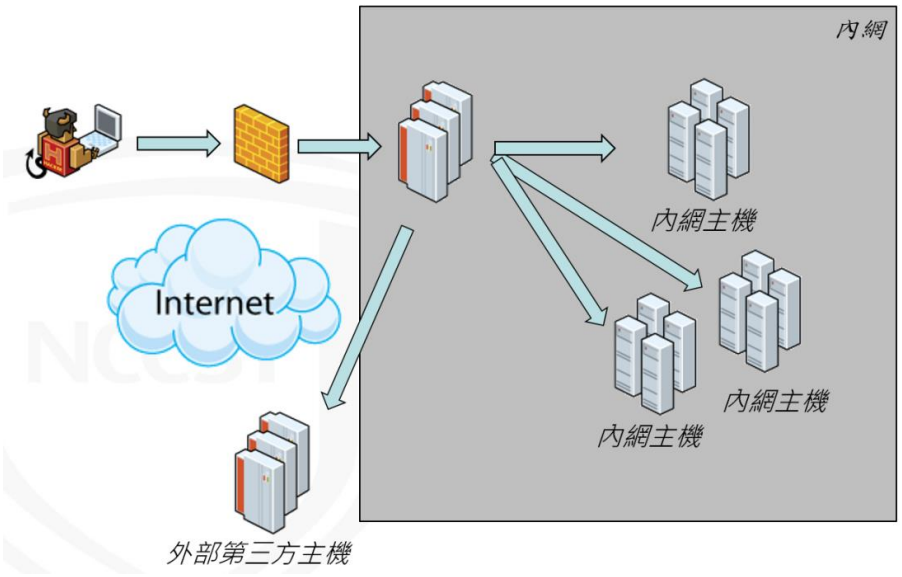

圖 6：SSRF 攻擊架構

2、URL Parsing

URL 的規範係定義於 RFC 2396 及 RFC 3986，WHATWG(Web Hypertext Application Technology Working Group)根據 RFC 定義了實作方式，但不同語言實作方式仍可能不同，URL 構成元件詳如圖 7。

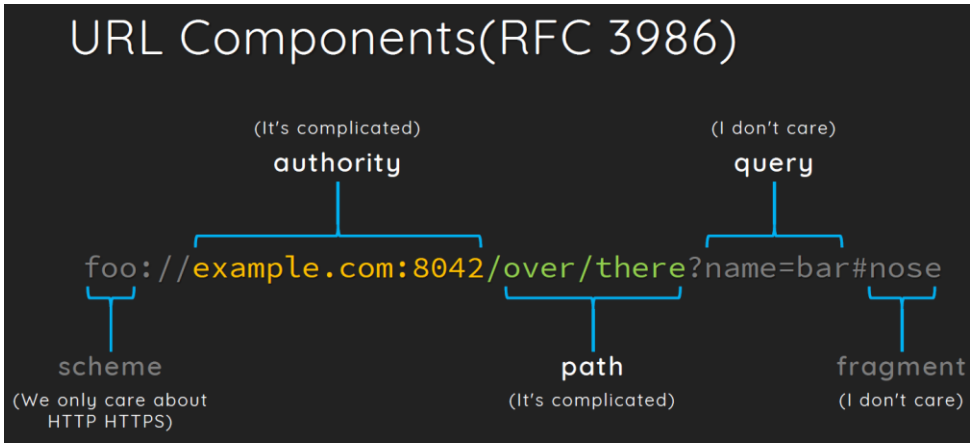

圖 7：URL Component

3、漏洞風險

有關 CR-LF injection 和 URL Parsing 部分，大多數程式語言皆存在相關漏洞風險，如 CR-LF injection 可能係針對 PATH、HOST 或 SNI (Server Name Indication)；

而 URL Parsing 則可能針對 Port、HOST 或 PATH 進行 injection，各種不同語言所實作的 library，針對 CR-LF injection 及 URL Parsing 可能存在弱點之處詳如圖 8。

Libraries/Vulns	CR-LF Injection			URL Parsing		
	Path	Host	SNI	Port Injection	Host Injection	Path Injection
Python httplib	☠	☠	☠			
Python urllib		☠	☠		☠	
Python urllib2		☠	☠			
Ruby Net::HTTP	☠	☠	☠			
Java net.URL		☠			☠	
Perl LWP			☠	☠		
NodeJS http	☠					☠
PHP http_wrapper				☠	☠	
Wget		☠	☠			
cURL				☠	☠	

圖 8：Library Vulnerability

4、Abusing URL Parsers

因 RFC 僅訂定 URL Parse 機制之標準，其實作方式或有差異，導致同一個 URL 查詢請求解析之後產生結果不同，講者表示目前已將結果不同之問題回報開發廠商進行修正，如@符號之後應為主機，而 cURL 和其他語言解析結果不同，因此可能遭攻擊者利用，詳如圖 9。

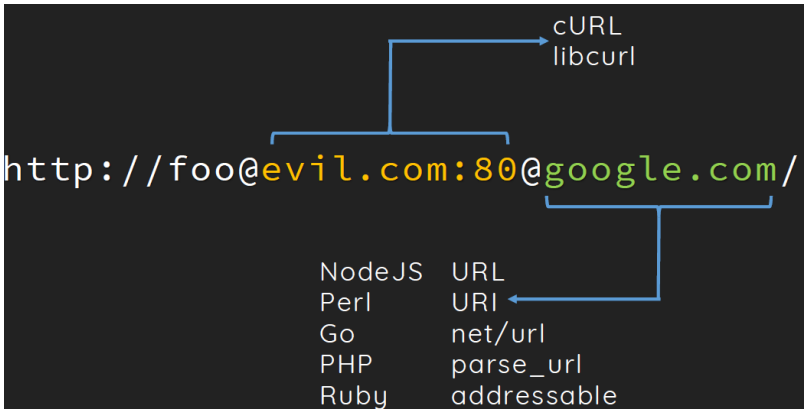

圖 9：URL Parser

5、SSRF Bypass Tech

有部分可以規避 SSRF 檢查的攻擊，例如第一個方法係因為程式檢查時間及程式開始使用時間存在時間差，可利用 DNS 的快速切換，造成執行目標網址的利用方式，

詳如圖 10。

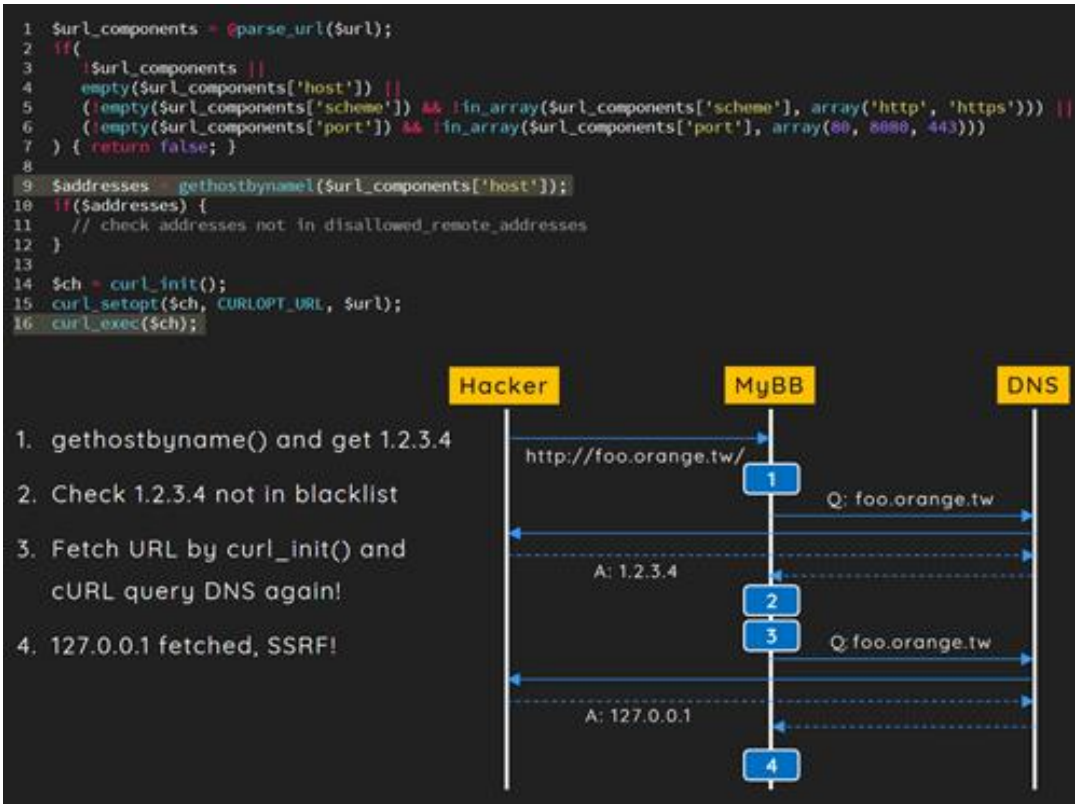

圖 10：SSRF Bypass

第二個方法是 IDNA (Internationalized Domain Names in Applications)的轉換問題，gethostbynamel 這個方法不會進行轉換，但 CURL 會進行轉換，因為這樣的差異，可以進行繞過攻擊，詳如圖 11。

```php
$url = 'http://ß.orange.tw/'; // 127.0.0.1

$host = parse_url($url)[host];
$addresses = gethostbynamel($host); // bool(false)
if ($address) {
  // check if address in white-list
}

$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $url);
curl_exec($ch);
```

圖 11：SSRF by IDNA Bypass

第三個方法是利用 URL parser 和 URL requester 的差異，可以利用其結果不同進而繞過網址檢查，cURL 未修補此項差異，詳如圖 12。

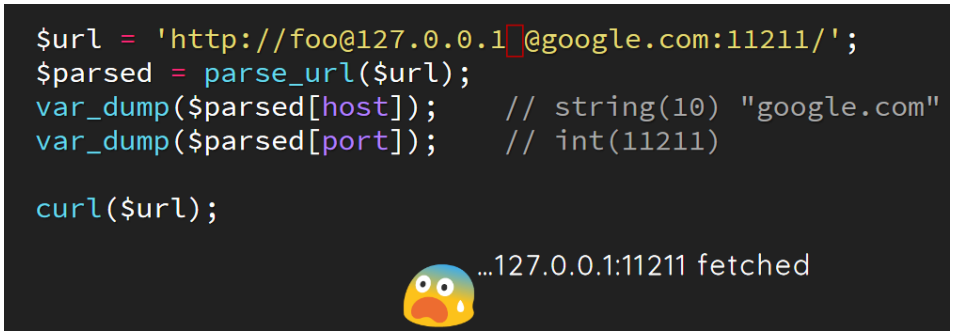

圖 12：SSRF by parse Bypass

6、如何減緩 SSRF 攻擊

有關減緩 SSRF 攻擊可分 3 個層面，應用層部分只使用 IP 或 Hostname，而不要重複利用使用者輸入的 URL 參數值；網路層部分使用防火牆或偵測規則以阻擋內網流量；最後撰寫專案時使用安全的 CURL 工具(如 SafeCurl 或 Advocate 等)以防止 SSRF 攻擊。

(二) Popping a Smart Gun

本場演講係討論駭侵智慧手槍(Smart Gun)，說明如何利用物理手法擊發 Smart Gun，對比於一般的傳統手機能夠使用電子的方式控制槍枝，例如限制本人才能扣板機，目前 Smart Gun 的操作需搭配一個控制器，例如手錶，透過控制器進行驗證才能發射子彈，控制器的距離也有一定限制，必須在一定距離內才能接收，例如 25 公分，詳如圖 13。

圖 13：Smart Gun 操作流程

本議程藉由三種不同方式突破手機的限制，分述如下：

1、Defeat proximity restriction

第 1 種方法係透過 Relay 方式，講者在 Amazon 網站花費 20 元美金購買相關設備，因為控制器係使用電波傳輸訊號，講者利用頻譜分析並錄製槍枝擊發時的電波，結果可成功錄下該段電波，再將結果 Relay 給 Smart Gun 擊發，詳如圖 14。講者建議若要降低此類攻擊，可將發射週期縮為極短，提升其複製難度，並建議不應使用 RF/NFC 等相對不安全的電波傳遞方式。

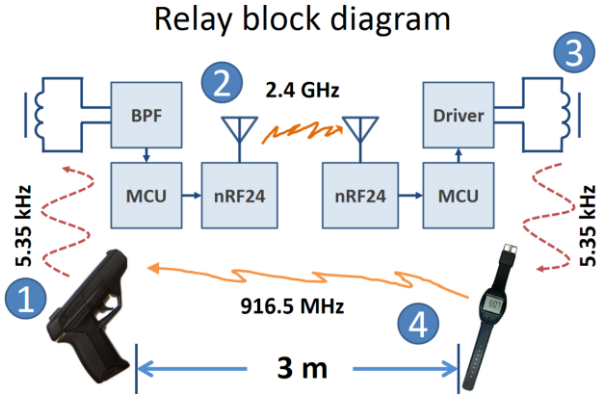

圖 14：Smart Gun Relay 攻擊流程

2、Denial of Service

講者所使用的 Smart Gun 使用 900 MHz 頻段，市面許多產品皆使用此頻段，如嬰兒監控、無線麥克風、無限遊戲控制器、無線耳機、遙測系統及無線電話等，講者利用同為 900 MHz 頻段的傳輸器，藉由控制訊號強度干擾訊號的輸出，講者針對

干擾器與控制器的訊號強度列出下列 3 種狀況，若干擾器訊號強度高於控制器，則訊號就無法順利被 Smart Gun 接收；若兩者訊號強度相同，則可能造成解碼錯誤；若干擾器訊號強度低於控制器，但高於 Slicer，則仍會造成解碼錯誤，詳如圖 15。講者建議若要降低此類攻擊，可將發射訊號強度增強，使用可錯誤矯正的編碼，最後是系統設計更周全。

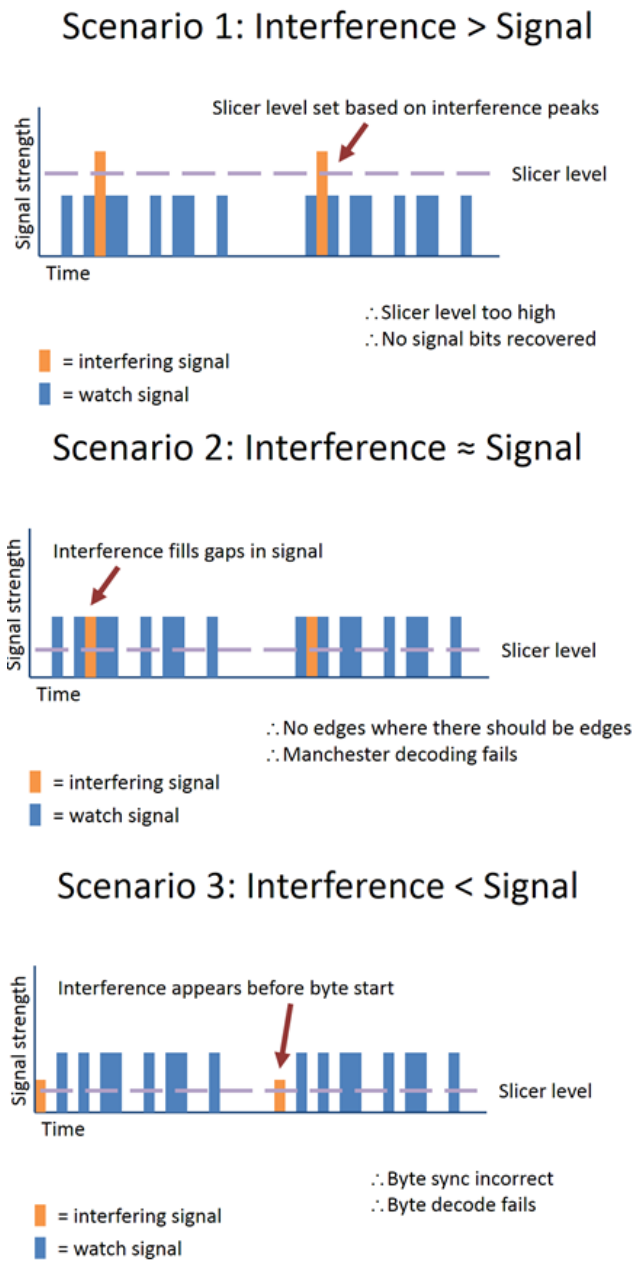

圖 15：Smart Gun 的 DoS 攻擊流程

3、Fire without authorization

最後的攻擊為難度最高，企圖使槍枝繞過驗證進行射擊動作，講者參考 Smart Gun 設計專利文件，發現其係使用磁力方式進行控制，講者利用強力磁力的載具進行磁力干擾，進而解開 pin 碼進行射擊，詳如圖 16。講者建議若要降低此類攻擊，不應使用磁力或螺線管做控制，因為有極高的可能可以進行操作，建議使用電動驅動是不易被攻擊的，或者做外部磁力的偵測進行槍枝鎖定可降低此類攻擊。

圖 16：Smart Gun 繞過驗證攻擊流程

(三) Get-$pwnd: Attacking Battle-Hardened Windows Server

本場演講主要說明 Windows PowerShell 安全議題，講者為微軟 Azure 管理安全首席架構師 Lee Holmes。

1、PowerShell 安全考量

PowerShell 目前為 Windows 環境系統管理的重要工具，主要是利用 JEA(Just Enough Administration)安全性技術做為授權管理，並區分角色功能(Role

Capabilities)、端點(Endpoint)和識別(Identity)等觀點，角色功能描述某人可以在 JEA 工作階段中做什麼，端點是說明可以存取的資源為何，而識別則是須以何種身分類別執行相關工作，綜合以上功能以實作權限控管功能，詳如圖 17 與圖 18。

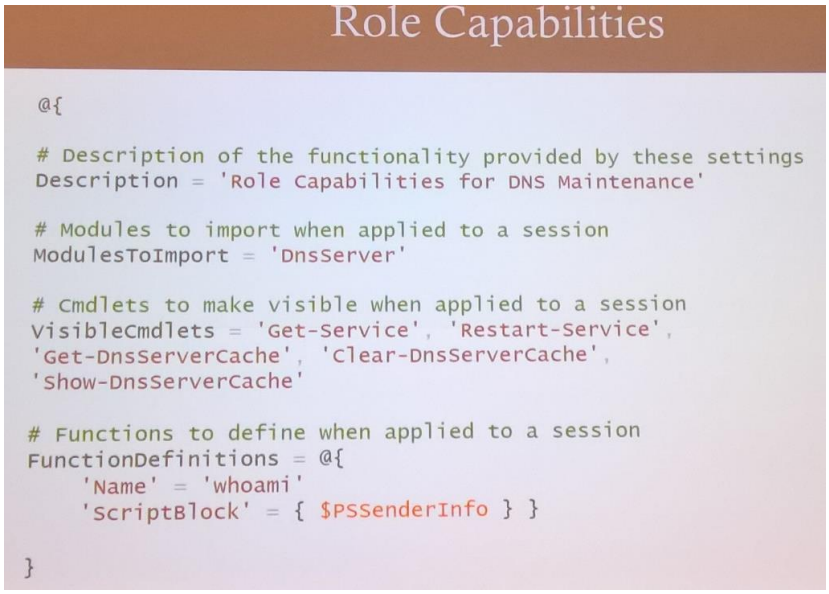

圖 17：PowerShell JEA (1/2)

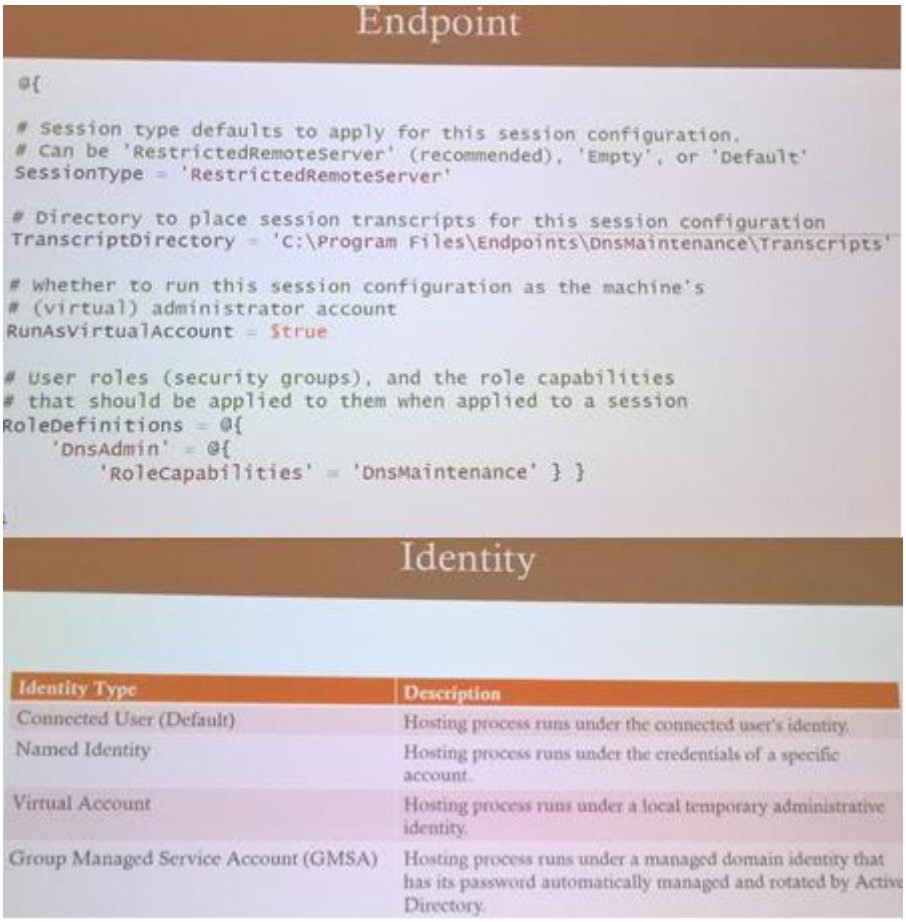

圖 18：PowerShell JEA (2/2)

2、Injection(PowerShell)

本場演講主要著墨於 PowerShell 的 Command Injection，討論各種不同寫法所可能產生的弱點，例如未對參數進行過濾，且指令又是執行系統相關呼叫，則可能造成 Command Injection，詳如圖 19。

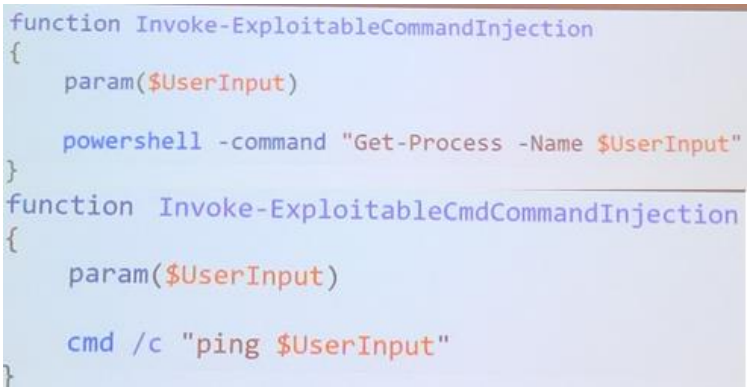

圖 19：PowerShell Command Injection

若是一般的指令，對參數進行過濾方法有問題亦有可能造成 Express Injection，例如單引號取代作法存在問題，詳如圖 20。

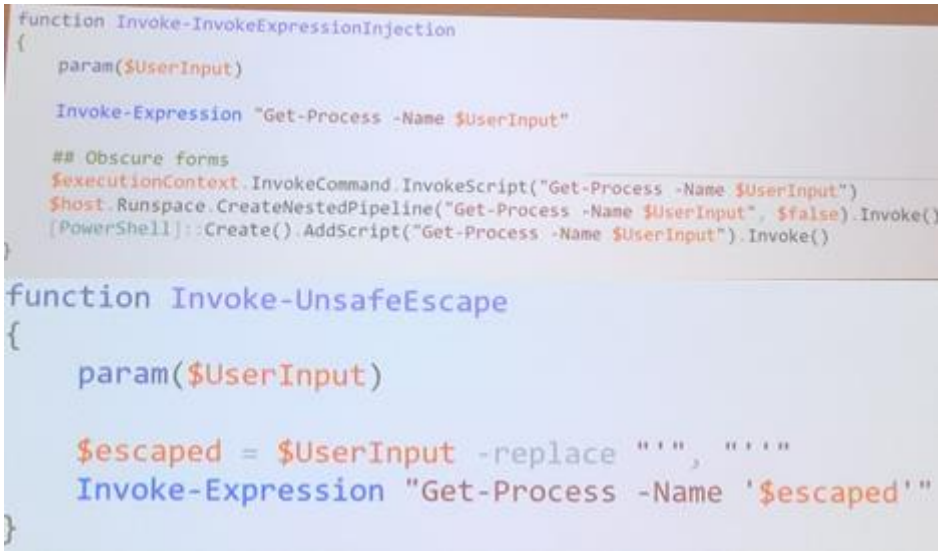

圖 20：PowerShell Express Injection

若指令置放於 script 區間，且利用 Invoke-Command 方式執行，則有可能造成 Script Block Injection，詳如圖 21。

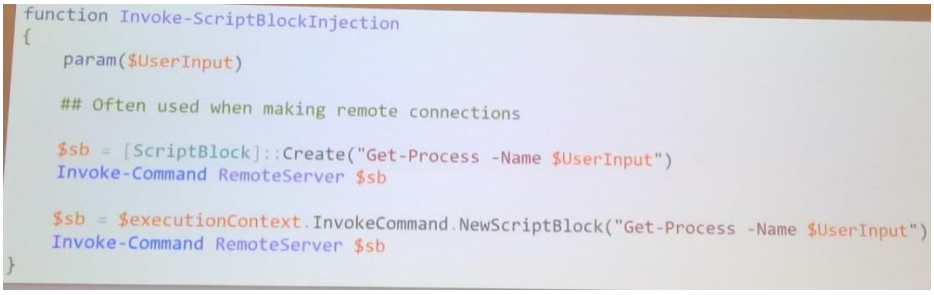

圖 21：PowerShell Script Block Injection

若指令利用 ExpandSting 執行，則有可能造成 String Expansion Injection，詳如圖 22。

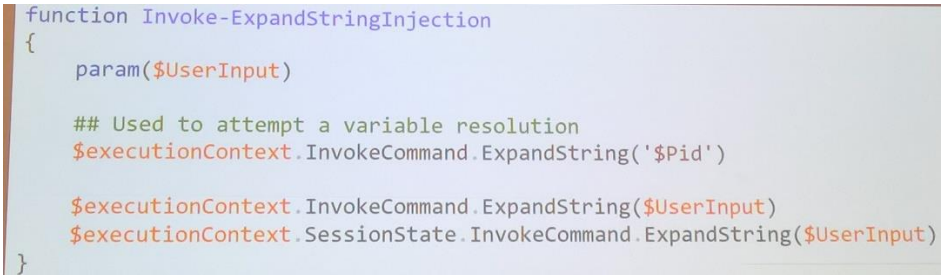

圖 22：PowerShell String Expansion Injection

若將指令當成 Method，則有可能造成 Method Injection，詳如圖 23。

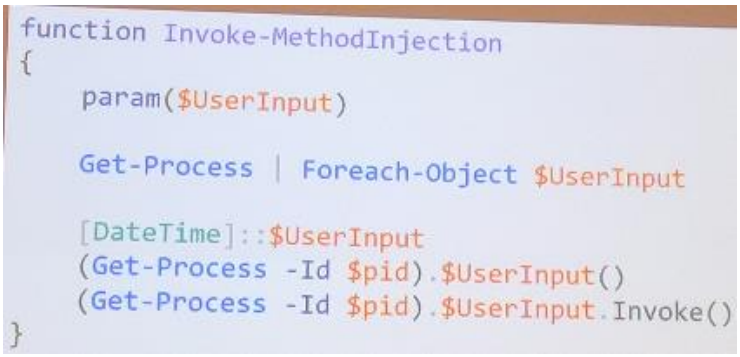

圖 23：PowerShell Method Injection

若指令當成程式呼叫的型態，則可能造成 Me Add-Type Injection，詳如圖 24。

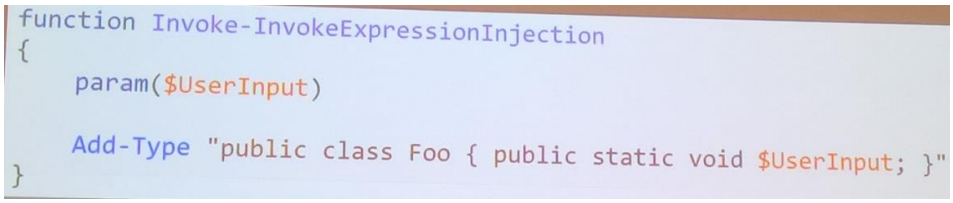

圖 24：PowerShell Add-Type Injection

3、Command Injection(PowerShell)減緩方法

要避免 PowerShellinjection 的問題，可考慮使用 token 和 AST (Abstract Syntax Tree)檢查結構是否符合，使用參數方式帶入，並使用 AST 進行檢查，詳如圖 25。

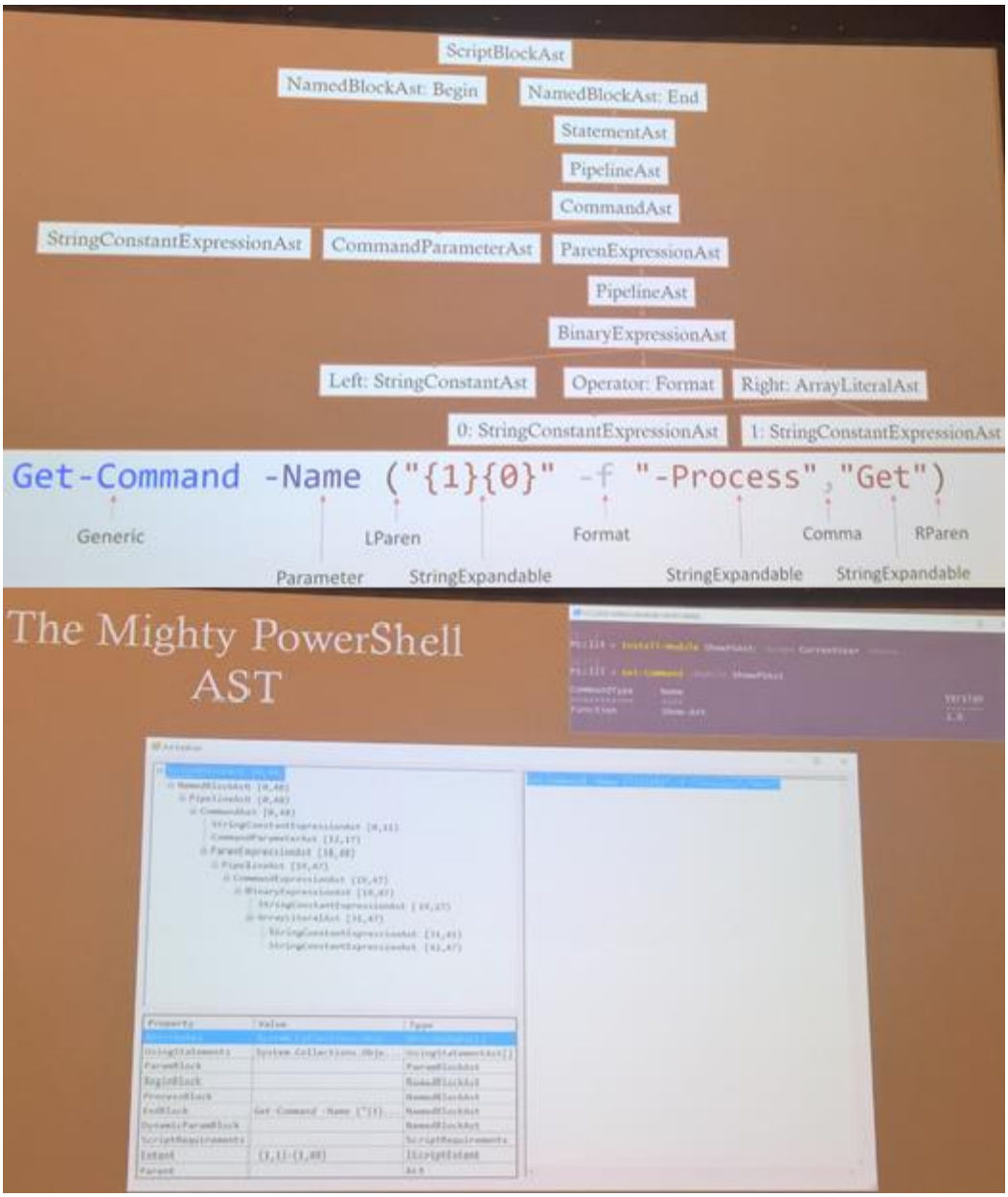

圖 25：PowerShell AST

撰寫 PowerShell 指令時也可利用工具檢查，例如 PSScriptAnalyzer，可提示權限問題，亦可整合至 Visual Studio Code 編輯器，詳如圖 26 與圖 27。

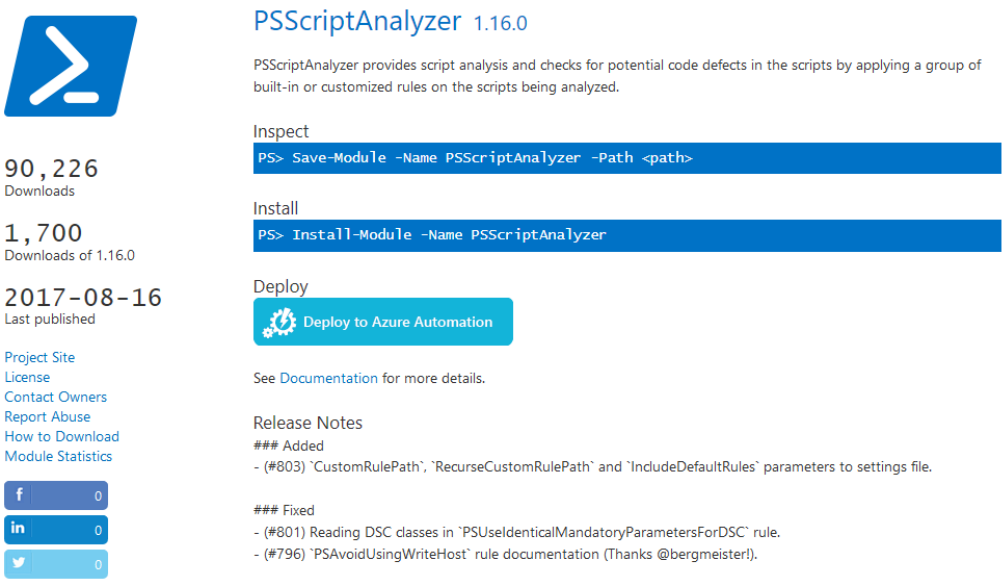

圖 26：PSScriptAnalyzer

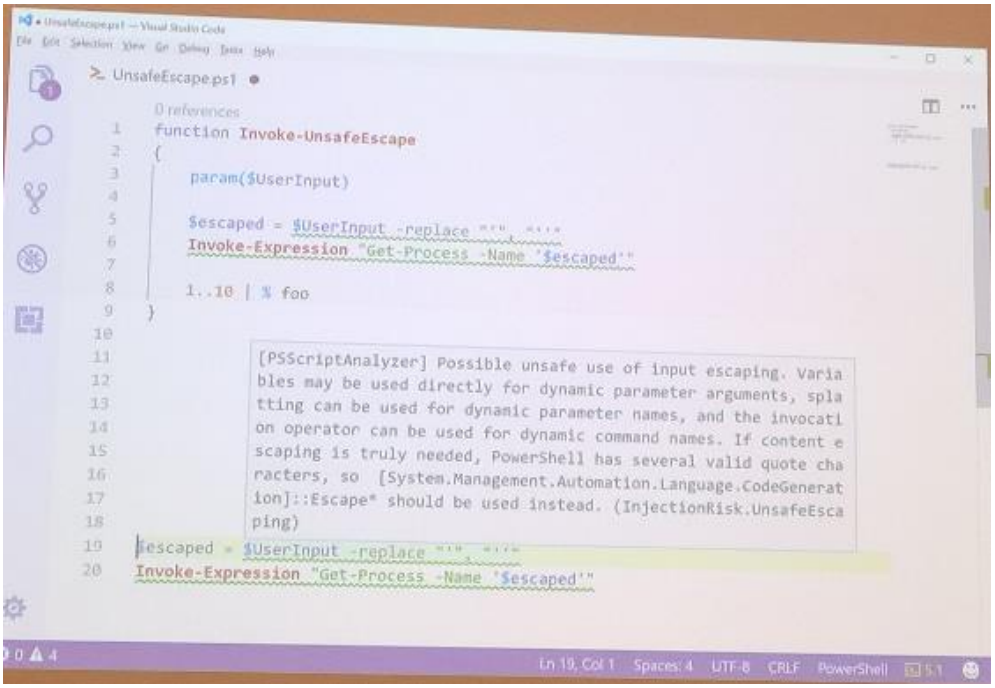

圖 27：PSScriptAnalyzer 執行範例

(四)CTF 競賽

本年依慣例舉辦 CTF 比賽，讓參賽隊伍彼此之間互相攻擊守護的主機，只要奪取對

手守護主機內的旗幟檔案即算得分，本次 CTF 比賽舉辦期間為 7 月 28 日上午 11 時至 7 月 30 日下午 2 時，大會於比賽前一天公布新的比賽規則，包括全新的 CPU 架構和指令集 cLEMENCy，並重新定義 1 個 byte 為 9 個 bit 的全新電腦運算規則，記憶體儲存資料的規則改為尾數居中儲存規則(Middle Endian)等，導致原有的駭客工具均得重新調整及設計，DEF CON 25 的 CTF 比賽現場如圖 28。

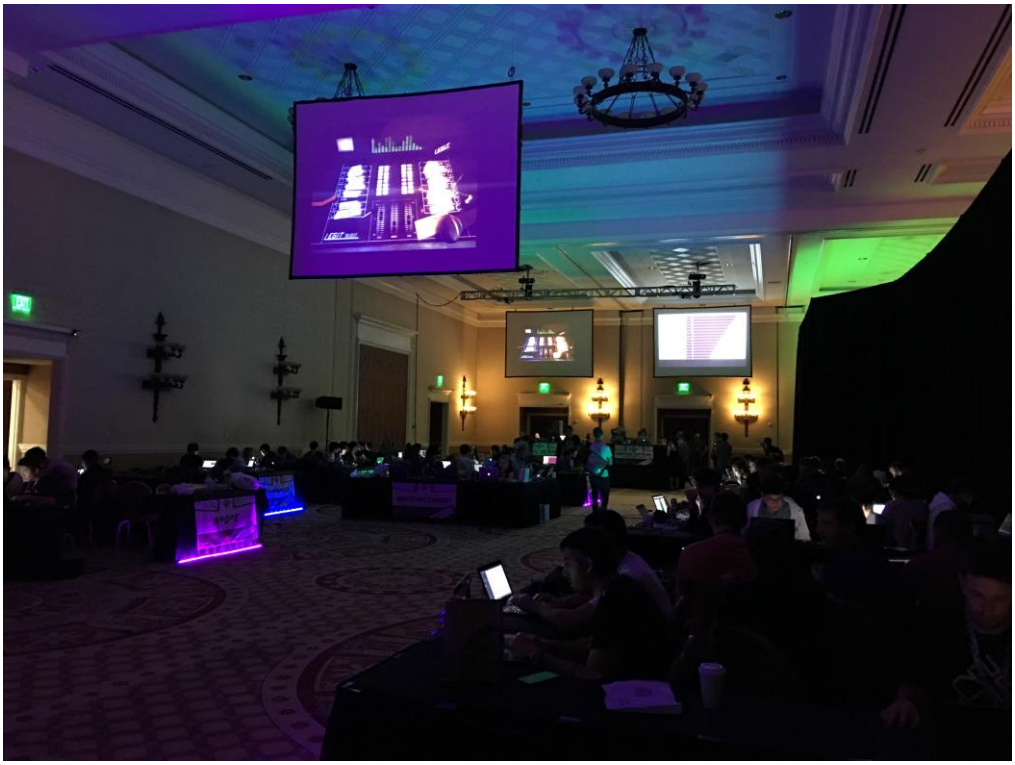

圖 28：DEF CON 25 CTF 比賽現況

本次 CTF 最後由美國隊 PPP 奪冠，另代表我國參賽的隊伍(HITCON)則自 103 年起連續 4 年入選最後決賽，本年最終獲得第 2 名的佳績，而由中國大陸騰訊公司網羅國內知名 CTF 戰隊所籌組的 A*0*E 則獲得第 3 名，值得注意的是韓國資安人才培育的結果逐漸展現，本次 CTF 計有 4 隊進入決賽，各隊分數如表 1 所示。

表 1：本年 DEF CON CTF 比賽最終成績

Qualifying Team	Score	Country
PPP	33850	美國
HITCON	30631	臺灣
A*0*E	19730	中國大陸
DEFKOR	18474	韓國
Tea Deliverers	13941	中國大陸
pasten	11332	以色列
Shellphish	10452	美國
Eat Sleep Pwn Repeat	9369	德國
RRR	9088	韓國
Lab RATs	8564	歐洲
hacking4danbi	8521	韓國
Team Rocket ☠	8496	歐洲
Bushwhackers	6894	俄羅斯
koreanbadass	6766	韓國
!SpamAndHex	4405	匈牙利

肆、心得建議

近年資安新興議題眾多，包括工業控制安全、物聯網安全及人工智慧等議題，經觀察發現許多國家在面對類此新興議題時，多採蒐集相關資訊及資源，並建置實驗場域以進行實務檢測，判斷是否存在相關資安漏洞，藉以強化其資安防護能量，建議我國可針對物聯網裝置，以民生需求為優先考量，併同納入國家需求及產業需求，訂定國家資安檢測共通標準，並扶植國內產業成立IoT設備軟體安全相關檢測實驗室，以提升我國物聯網整體安全性及產業發展。

最後，我國駭客社群近年於國際資安競賽屢獲佳績，代表我國的HITCON於本年DEF CON的CTF決賽再度獲得第2名，惟其他國家的代表隊實力亦不斷成長，如韓國曾於2015年獲得第1名，本年則有4隊進入決賽，顯示我國存在頂尖資安菁英量能不足問題，為補足所需人力，建議可透過推動大專院校增設資安系所(組)或學程、辦理國際資安競賽、培育產業所需資安頂尖人才及推動政府機關設置資安專責人力等措施，主動與相關資安社群合作，加速資安人才培育工作。

伍、會議照片

圖 29：DEF CON 25 會議舉辦場地(Caesar’ s Palace)

圖 30：DEF CON 25 會議識別證(badge)

圖 31：廠商展示區