HITCON Pacific 2018 / ZeroDay 漏洞獎勵計畫

台灣駭客年會 (Hacks In Taiwan Conference，簡稱 HITCON)，是台灣最大的駭客與資訊安全技術研討會，純技術的領域中沒有黑與白，我們認為「駭客」代表著高超的技術、挑戰的精神，因此 HITCON 始終致力於提供良好的舞台，讓世界各地的駭客們齊聚一堂，於一年一度的盛會中面對面交流最新、最深入的資安技術。

今年 HITCON Pacific 將結合 HITCON ZeroDay 舉辦 Bug Bounty 漏洞獎勵計畫，我們將邀請各單位提供其軟硬體產品、網站等，讓參加者進行漏洞挖掘，並提供獎勵予發現弱點或表現優異之參加者。參與漏洞獎勵計畫的各單位，不僅得以透過 HITCON 大會提升產品知名度，更能由白帽駭客為該產品的安全性與穩定度進行檢測，使各單位有機會對自家產品有更深一層的瞭解，創造參加者與參與單位雙贏的局面。

目的

我們期望 Bug Bounty 漏洞獎勵計畫的舉辦，除了讓世界各地的資安高手一同較勁、交流外，也透過參與單位願意公開檢測漏洞並修補的行為，協助證明該單位產品安全性的提升，同時令各界更加瞭解資訊安全的力量及重要性。

活動時程

活動預計在十月底公告參與的單位與該單位所提供的網站、軟體或硬體設備型號版本及測試位址，並於十一月開始供參加者進行測試，期間成功找到漏洞之參加者須在 HITCON Pacific (12 月 13 ~ 14 日) 會場展示攻擊過程。

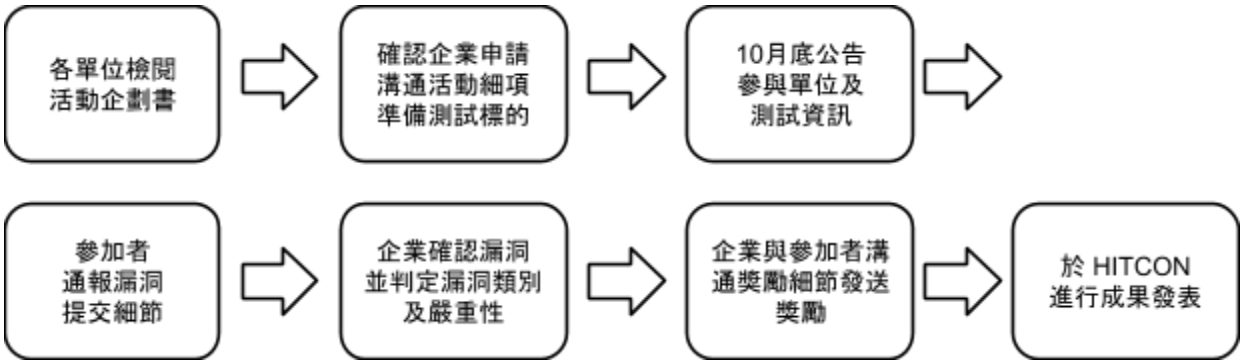
活動資訊

活動進行方式

- 參加漏洞獎勵計畫的企業，將在 HITCON ZeroDay 上公開上架計畫。
- 參加者於活動時限內找尋該企業許可範圍之漏洞，並至 HITCON ZeroDay 平台上該企業漏洞獎勵頁面通報，通報內容需註明清楚漏洞描述及截圖說明。
- 漏洞獎勵的通訊聯繫及獎勵細節皆由企業與參加者自行協議，HITCON 不介入獎勵流程。
- 在通報的漏洞當中擇優於 HITCON Pacific 大會當天進行展示。

企業合作方式

1. 企業與台灣駭客協會簽署合作契約書
2. HITCON 提供通報平台，包含通報介面、溝通機制等，並針對漏洞獎勵計畫的規範提出建議，若有漏洞爭議時協助仲裁。
3. 測試期間由甲方提供設備、網路，並維運該測試設備正常運作。
4. 擇優於 HITCON Pacific 會議時公開發表



企業需求準備

- 若測試目標為主機，建議準備獨立可供測試的主機，並公告此 IP 或網域名稱為測試專用。若欲測試正式站台，可直接公告正式站台之網域名稱。
- 若測試目標為硬體設備，需架設多組可供測試的設備，準備連線對外網路，並為獨立線路避免影響其他主機，公告此 IP 或網域名稱為測試專用。
- 若測試目標為軟體，須公告軟體的下載位置、版本、checksum，確認測試的版本與計畫中的相同。
- 定期監控設備及主機是否正常運作，若因測試故障，則排除故障後重新啟用。
- （選擇性）公布相關使用文件，如 Protocol、API 等。
- 決定接受測試漏洞種類及獎金，如 Remote Code Execution、Command Injection、Logic Flaw 等。
- 定義規範，如不得阻礙其他人測試、不得將服務惡意中斷。
- 企業需有人員負責裁判，如確認漏洞屬實、種類、獎金等，如有爭議，則請 HITCON 協調仲裁。
- 獎金多寡根據漏洞等級而定，由各參與單位自行制定詳細之獎勵發放條件。

參加者通報漏洞流程

1. 連至 HITCON ZeroDay 漏洞獎勵計畫頁面
2. 選擇本次參加漏洞獎勵計畫的企業
3. 點選通報漏洞
4. 詳細填寫漏洞描述、攻擊方式、指令、結果截圖、影響，說明漏洞是否存在

5. ZeroDay 平台根據通報將漏洞通報至企業
6. 企業確認完畢後，根據嚴重性、利用性評分後，決議給予獎金金額
7. 企業修復後，漏洞公開於平台

參加者活動規範

1. 參加者攻擊所用之漏洞必須是未知、未公佈且未向廠商提交過的，且不得重複利用。例如，參加者已經送 payload 進去得到遠端控制權限後，利用前述漏洞上傳網頁版遠端控制代碼，此種行為將不被接受。
2. 參加者執行遠端攻擊必須排除操作背後之人為干擾，必須出現在使用者正常的操作情況下，不得有重新啟動或下線、登入等情況。
3. 若有不同參加者使用相同漏洞之情形，建議將依照通報的順序為獎勵發放之依據。

企業申請流程

- 各單位如有意參與活動請將活動契約書寄到 service@hitcon.org 以供審核
- 契約書中需提出以下資訊：
    - 測試目標（如網站、或產品名稱與型號）
    - 給參加者測試的網站或韌體系統位址
    - 獎金或獎勵列表
    - 獎金或獎勵的領取時間、方式（現金、匯款等），如在 HITCON Pacific 大會現場頒發現金、在 HITCON 活動主辦單位見證下於兩週內匯款
    - 聯絡方式
    - 是否已在 HITCON ZeroDay 註冊企業帳號及發佈獎勵頁面
- 契約書收件時間：即日起至 **2018 年 11 月 09 日**

注意事項

1. 我們對成功提交漏洞的參加者之個人技術能力表示認可，但不認為活動結果與參加者所屬機構之技術能力存在對應關係，亦不認為活動結果能直接反映相關軟體或設備的安全水準。
2. 我們將要求參加者將漏洞的細節完整的至 HITCON ZeroDay 平台回報，由平台收到之後完整轉知給企業，不會利用漏洞資料進行任何額外利用，也不會透露給該通報者及企業以外的第三方。
3. 我們承諾在未經參加者同意的情況下，我們不會將參加者個人資訊透露給第三方，也不會利用參加者個人資訊及隱私從事任何商業活動。

聯絡方式

HITCON Pacific 活動小組 <service@hitcon.org>

HITCON Pacific 2018 漏洞獎勵計畫活動契約書

公司名稱			
通訊地址			
聯絡人		**電話**	
行動電話		**E-Mail**	
參加公約	1. 參加資格：國內外註冊登記之合法廠商。為尊重智慧財產權，無涉及仿冒商標及侵犯他人專利之公司 2. 本公司確認提供測試標的物網站、軟體或設備之所有權，以確保合法性，授權參加者對標的進行必要之檢測。 3. 參加者於測試時限內挖掘漏洞，將透過 HITCON ZeroDay 平台將完整漏洞說明報告以截圖加文字說明形式傳送，再由平台審核後完整提交給本公司資安窗口。參加者及大會必然會完整呈交相關資訊予公司，並承諾在各單位修補前不對任何第三方洩露資訊。 4. 本公司將指派專人擔任裁判，裁判得確認是否為漏洞並決定漏洞等級，依據漏洞等級給予對應之獎金或獎品。若判斷有爭議時，以本大會裁判為主。 5. 大會承諾在未經參加者同意的情況下，我們不會將參加者個人資訊透露給第三方，也不會利用參加者個人資訊及隱私從事任何商業活動。 6. 若有不同參加者使用相同漏洞之情形，建議將依照通報的順序為獎勵發放之依據。 7. 關於前揭合作夥伴企畫書內容，主辦單位保留變更之權利。 8. 以上相關事項如未盡事宜者，悉依本企劃書中規範及主辦單位決議辦理。		
測試標的	本公司願意提供以下網站、軟體、設備或產品參與測試： 1. [產品名稱] – [型號] – [測試站台位置] 2. [產品名稱] – [型號] – [測試站台位置] 3. [網站名稱] – [測試位址] 4. [軟體名稱] – [版本] – [下載位置]		
獎金及發放方式	漏洞分類請參閱附錄一，本公司同意給予獎金、獎品如下： 1. 遠端命令執行：_____ 2. 任意存取檔案系統或資料庫：_____ 3. 邏輯錯誤、繞過驗證機制：_____ 4. 攻擊客戶端：_____ 5. 其餘安全漏洞：_____ 於 HITCON Pacific 2018 結束兩週內，自行與參加者聯繫給予獎金/獎品。		
平台註冊確認	請確認已至 HITCON ZeroDay 註冊企業帳號，並至企業後台發佈漏洞獎勵頁面。 https://zeroday.hitcon.org □是否已在 HITCON ZeroDay 註冊企業帳號 □是否已在 HITCON ZeroDay 發佈獎勵頁面		

保證事項

本公司已知悉並承諾遵守 HITCON Pacific 2018 漏洞獎勵計畫活動之各項規定。如有違反規定，本公司除同意立即依主辦單位之要求終止參與外，且同意接受主辦單位之處分。

此致

公司印章：　　承辦人簽章：

中華民國_____年_____月_____日

附件一 漏洞參考獎金

針對受測的產品、伺服器，不同等級的漏洞給予不同的獎金。分級、獎金的標準，參考 Google Reward Program[1] 之 “Non-integrated acquisitions and other sandboxed or lower priority applications” 分類，類別分為以下五類：

1. Remote code execution (遠端命令執行)
2. Unrestricted file system or database access (任意存取檔案系統或資料庫)
3. Logic flaw bugs leaking or bypassing significant security controls (邏輯錯誤、繞過驗證機制)
4. Execute code on the client (攻擊客戶端)
5. Other valid security vulnerabilities (其餘安全漏洞)

考量不同企業資源的不同，可自行採取不同等級之獎金或等值獎品。參考金額如下表：

編號	類別	範例	參考獎金 (USD)
1	Remote code execution 遠端命令執行	Command injection, deserialization bugs, sandbox escapes	$5,000
2	Unrestricted file system or database access 任意存取檔案系統或資料庫	XXE, SQL injection	$5,000
3	Logic flaw bugs leaking or bypassing significant security controls 邏輯錯誤、繞過驗證機制	Insecure direct object reference, remote user impersonation, privilege escalation	$500
4	Execute code on the client 攻擊客戶端	Cross-site scripting, Client Code execution	$100
5	Other valid security vulnerabilities 其餘安全漏洞	CSRF, Clickjacking, Information leakage	$100

Reference
1: http://www.google.com/about/appsecurity/reward-program/