



VulReport

sylphid@vulreport.net

Agenda

- 弱點揭露現狀
- 為什麼要建置VulReport
- 負責任的弱點揭露

VulReport

"高超的電腦技術，卻沒有用在正途"

Y 入侵1237個網站 高二生被逮

https://tw.news.yahoo.com/入侵1237個網站-高二生被逮-120422257.html

YAHOO! 奇摩 新聞 新聞搜尋 網頁搜尋 登入 信箱

入侵1237個網站 高二生被逮

民視新聞 民視 - 2013年10月16日 下午8:04

新北市刑大日前接獲學校和民間網站報案，指出有電腦駭客入侵網站，而且從2月犯案至今，已經有1237個網站受害，高居全球駭客網站排名第19名，警方深入追查，赫然發現，這名駭客竟然是雲林一名高二學生，前往家中逮人時，這名學生正在入侵網站。

躲在遠端電腦前的駭客，透過指尖敲鍵盤，就能癱瘓聯邦調查局的監控系統，竊取機密資料，沒想到類似的電影情節，也在台灣真實上演。

點進網站，就出現震耳欲聾的音樂聲，還有這名穿著白色襯衫的男子，戴著V怪客的面具，伸手比出不雅姿勢，如果看到這個頁面，就代表網站被駭了，這個駭客，破解各大網站，取得管理權限的帳號密碼後，竄改網站內容，把商家的LOGO拿掉，放上自創的駭客標誌，彰顯入侵能力，今年2月犯案至今，駭進全球1237個網站，在全球被黑點統計，排名高達第19名，最讓警方吃驚的是，這個駭客竟是一名年僅17歲的高二學生。

警方查出，這名學生平時就在家中電腦，入侵他人網站，各科學業成績不理想，惟獨電腦科目表現突出，還曾在個人臉書網頁上說，我不喜歡上學，因為這樣就不能駭了。

高超的電腦技術，卻沒有用在正途，警方也覺得可惜，這名學生對於犯行坦承不諱，警方訊後依妨害電腦使用函送法辦，最高可被判處三年以下刑期。

新聞相關影音

正在等候 s.yung.com...

你可能還會想看

- 柯P上任前夕 趙少康閃辭富邦金獨董
- 中年大叔靠一枝眼線筆 負債3千萬翻身年營收3億
- NBA/湖人沒Kobe更強？ 史考特：這些人瘋了
- 女大生堅提告：給他教訓
- 台灣第一小生 魏少朋病逝
- 炒飯遭前夫捉姦 女星矢口真里驚：糟糕了
- 岳父貼心一句話 高山峰大鯢男兒淚
- 周刊：郭美珠爆白冰冰曾是性工作者？

心情排行 »

- 一哥休兵 湖人意外痛宰勇士
- NBA/沒有Kobe更好？ 湖人痛宰聯盟龍頭勇士
- NBA/聖誕驚魂！沒Kobe更棒 湖人宰勇士
- MIT航母殺手 沱江艦亞洲最強
- 老古不在家 湖人上陣勇士

zone-h

Zone-H.org - Unrestricted info x

www.zone-h.org/archive

zone-h
unrestricted information

Home News Events Archive Archive ★ Onhold Notify Stats Register Login search...

NOTIFIER DOMAIN

Special defacements only ☒ Fulltext/Wildcard ☒ Onhold (Unpublished) only ☐

Date :

Total notifications: **1,508** of which **1,189** single ip and **319** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H M R L ★	Domain	OS	View
2014/12/28	ymh	H M	★ iht.nstm.gov.tw	Win 2003	mirror
2014/11/27	BY DRISS		★ 1999.taitung.gov.tw/attach/201...	Linux	mirror
2014/10/20	Bunglon_Ijo		★ work.tnvtc.gov.tw/xampp/lang.tmp	Win 2003	mirror
2014/10/12	Kkk1337	R	★ www.yuanli.gov.tw/index.html	Win 2003	mirror
2014/09/15	Dbuzz	H	★ job.tainan.gov.tw	Linux	mirror
2014/09/04	1923Turk		★ www.xh-land.gov.tw/EvreN.htm	Win 2003	mirror
2014/09/02	OxSiT	M R	★ casio.com.tw/baby-g/	FreeBSD	mirror
2014/09/02	OxSiT	R	★ casio.tw/baby-g/	FreeBSD	mirror
2014/08/12	Dz-Secur	M R	★ www.thermaltake.com.tw/db/dz06...	Win 2003	mirror
2014/07/21	SlayersHackTeam	M	★ fsi.forest.gov.tw/ss.html	Win 2003	mirror
2014/06/21	علي حافظ الاسد	H R	★ www.guanyin.gov.tw	Linux	mirror
2014/06/17	HighTech	H	★ dns.ilccb.gov.tw	Linux	mirror
2014/06/17	HighTech	H M	★ apt.ilccb.gov.tw	Linux	mirror
2014/06/15	HighTech	H R	★ www.ilccb.gov.tw	Linux	mirror
2014/05/27	Karim-TN	H M	★ www.junglicity.gov.tw	Win 2008	mirror
2014/05/27	Karim-TN	H	★ www.chundlicity.gov.tw	Win 2008	mirror

Underground Economy



The Black Market

\$980-\$4,900

Trojan program to steal online account information

\$490

Credit card number with PIN

\$78-\$294

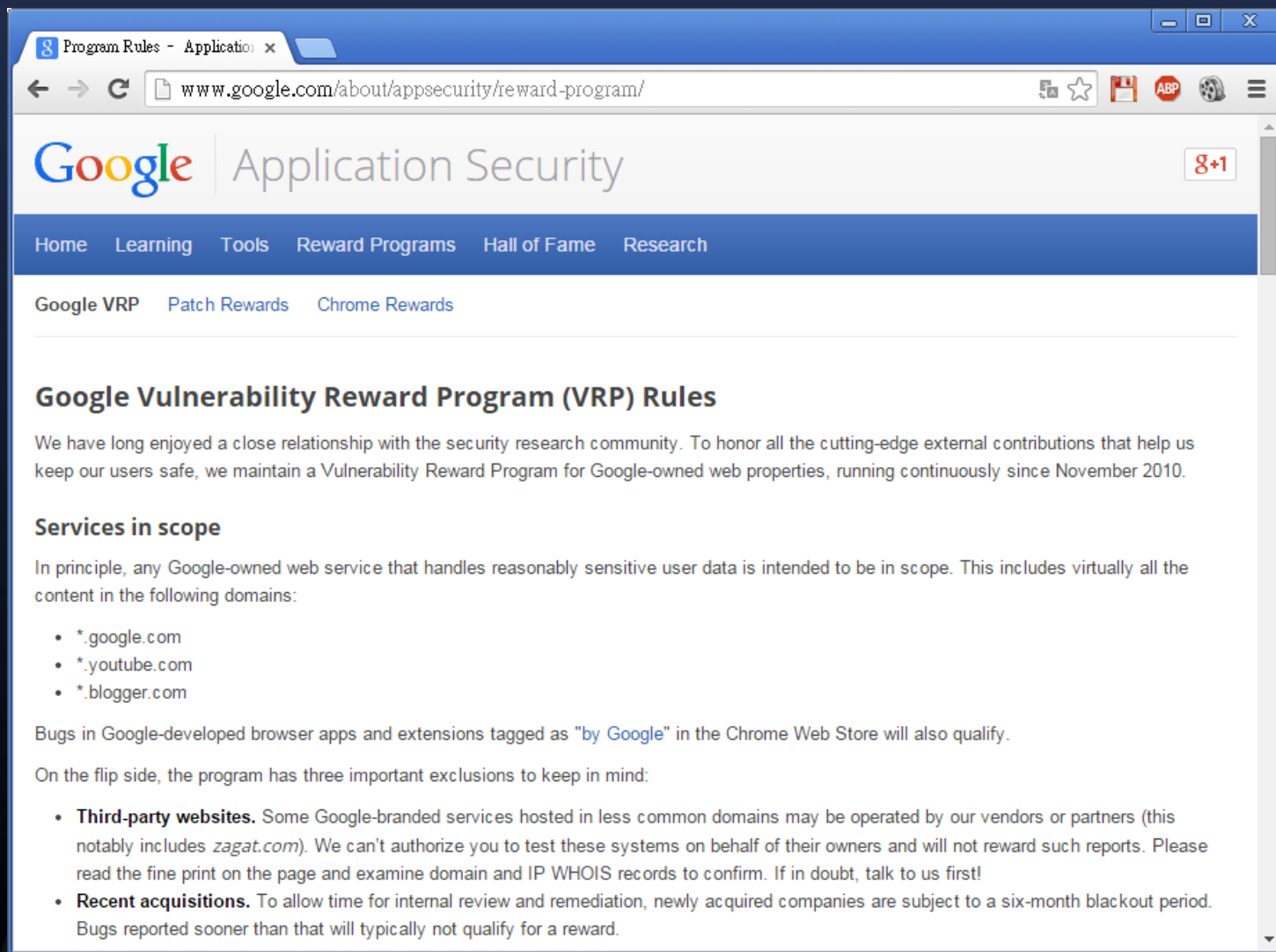
Billing data, including account number, address, Social Security number, home address, and birth date

別讓駭客不開心

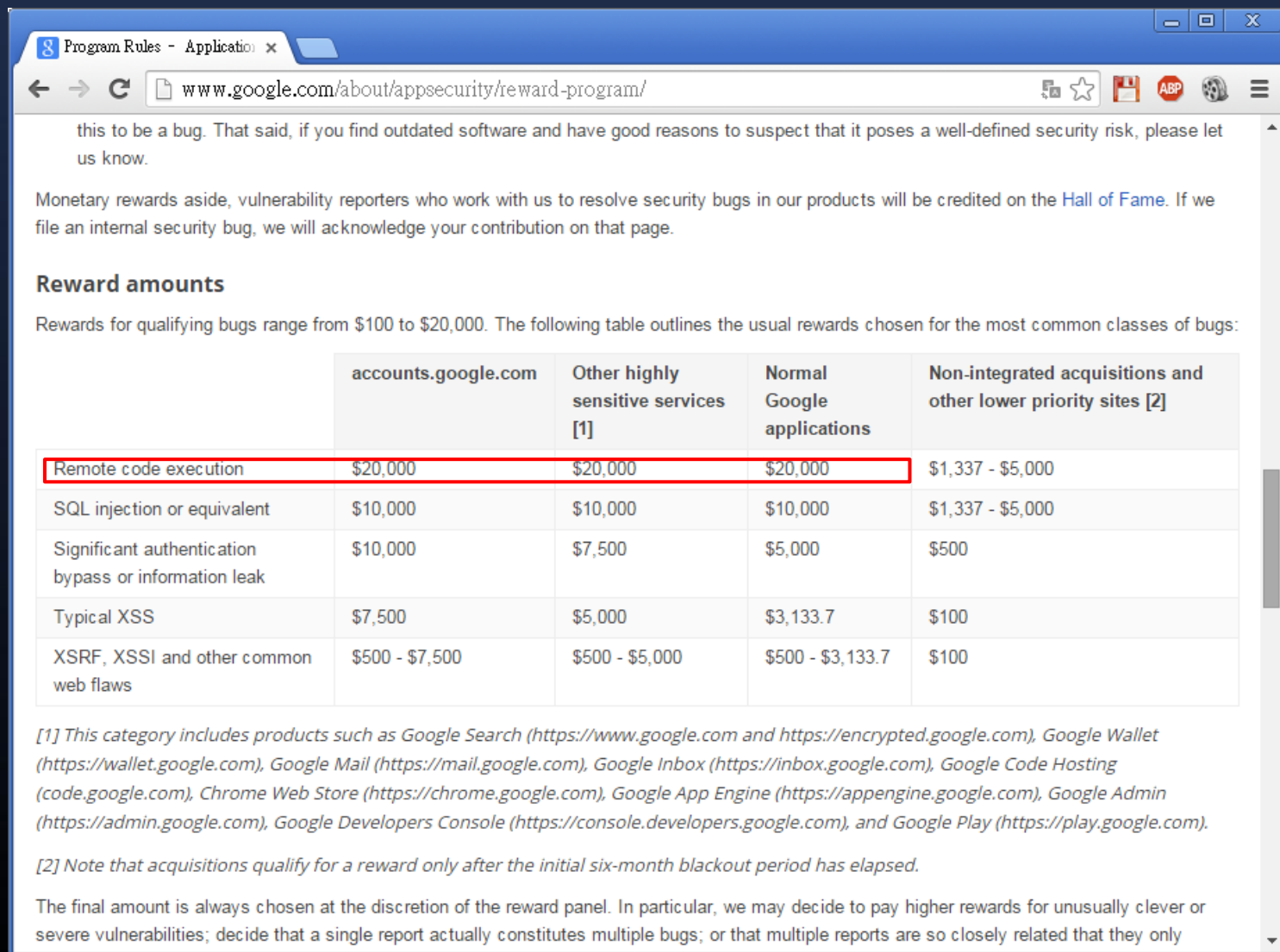
- 黑色產業 -> 資安產業/公益
- 技術的交流與提昇
- 正面形象的轉變

VulReport

Google VRP - 1



Google VRP - 2

A screenshot of a web browser displaying the Google VRP Program Rules page. The browser's address bar shows the URL 'www.google.com/about/appsecurity/reward-program/'. The page content includes a paragraph about reporting bugs, a section on monetary rewards, and a table of reward amounts for different bug classes. The table has five columns: bug type, accounts.google.com, Other highly sensitive services, Normal Google applications, and Non-integrated acquisitions. The 'Remote code execution' row is highlighted with a red border. Below the table, there are two footnotes providing additional context on the reward categories and the discretion of the reward panel.

this to be a bug. That said, if you find outdated software and have good reasons to suspect that it poses a well-defined security risk, please let us know.

Monetary rewards aside, vulnerability reporters who work with us to resolve security bugs in our products will be credited on the [Hall of Fame](#). If we file an internal security bug, we will acknowledge your contribution on that page.

Reward amounts

Rewards for qualifying bugs range from \$100 to \$20,000. The following table outlines the usual rewards chosen for the most common classes of bugs:

	accounts.google.com	Other highly sensitive services [1]	Normal Google applications	Non-integrated acquisitions and other lower priority sites [2]
Remote code execution	\$20,000	\$20,000	\$20,000	\$1,337 - \$5,000
SQL injection or equivalent	\$10,000	\$10,000	\$10,000	\$1,337 - \$5,000
Significant authentication bypass or information leak	\$10,000	\$7,500	\$5,000	\$500
Typical XSS	\$7,500	\$5,000	\$3,133.7	\$100
XSRF, XSSI and other common web flaws	\$500 - \$7,500	\$500 - \$5,000	\$500 - \$3,133.7	\$100

[1] This category includes products such as Google Search (<https://www.google.com> and <https://encrypted.google.com>), Google Wallet (<https://wallet.google.com>), Google Mail (<https://mail.google.com>), Google Inbox (<https://inbox.google.com>), Google Code Hosting (code.google.com), Chrome Web Store (<https://chrome.google.com>), Google App Engine (<https://appengine.google.com>), Google Admin (<https://admin.google.com>), Google Developers Console (<https://console.developers.google.com>), and Google Play (<https://play.google.com>).

[2] Note that acquisitions qualify for a reward only after the initial six-month blackout period has elapsed.

The final amount is always chosen at the discretion of the reward panel. In particular, we may decide to pay higher rewards for unusually clever or severe vulnerabilities; decide that a single report actually constitutes multiple bugs; or that multiple reports are so closely related that they only

Google Project Zero - 1

Google成立專職的網路抓蟲小組

www.ithome.com.tw/news/89430

iThome

新聞 產品評測 CIO 技術 專題 專欄 主題頻道 研討會 社群

搜尋

Google成立專職的網路抓蟲小組，Project Zero公開徵人

Google表示，過去Googlers們業餘研究的成功，讓他們想要成立一個真正的強大團隊，也就是Project Zero。這個團隊將網羅最優秀的資安人才，百分百專注於改進網際網路的安全。

✓讚

1萬

按讚加入iThome粉絲團

f讚

分享

201

g+

6

文/ 林妍湊 | 2014-07-16 發表



iThome Weekly

按讚追蹤 iThome 最新報導

✓讚 1萬

熱門新聞

【第5代Core處理器搶先預覽】Intel超低電壓CPU打頭陣，全面進化14奈米

2015-01-05

【第5代Core處理器搶先預覽】Intel超低電壓CPU打頭陣，全面進化14奈米

2015-01-05

Google Project Zero - 2

Google成立專職的網路抓蟲 Issues - google-security-research

www.ithome.com.tw/news/89430

iThome 新聞 產品評測 CIO 技術 專題 專欄 主題頻道 研討會 社群 搜尋

Google研究中心人員Chris Evans解釋這個小組成立的動機指出，過去一些有心的Googlers會使用自己的閒暇時間研究網路安全，像Heaetbleed臭蟲也是這樣被發現的。過去Googlers們業餘研究的成功，讓他們想要成立一個真正的大團隊，也就是Project Zero。這個團隊將網羅最優秀的資安人才，百分百專注於改進網際網路的安全。

他進一步表示，使用者應該能安心上網，不用害怕罪犯或國家支持的駭客入侵軟體漏洞，感染電腦，竊取機密或監視使用者的通訊。然而一些高明的攻擊利用零時差漏洞鎖定人權運動人士或從事產業間諜行為。這些行為必須遏止，因此Google認為，要解決這個問題，還有許多待努力的地方。Evans指出，這個團隊的宗旨即是大幅降低精準攻擊的受害者人數。

Wired 報導，Google已找到的Project Zero成員包括曾發現Adobe及Microsoft Office中多個臭蟲的紐西蘭高手Ben

2015-01-06

【第5代Core處理器搶先預覽】SST智慧型聲音技術帶來更省電的效果，並支援語音喚醒

2015-01-06

【CES 2015焦點】華碩發表第二代ZenFone及照相手機ZenFone Zoom

2015-01-06

Windows 8.1零時差漏洞90天通告期已過，微軟未修補，Google揭露

2015-01-05

【CES 2015焦點】微軟推出29美元的Nokia 215連網手機

2015-01-06

【CES 2015焦點】聯想發表比MacBook Air還輕薄的13吋LaVie Z筆電，只有780公克

2015-01-06

Alibaba



烏雲 - 1

乌云平台 - 通用性软件安全漏洞奖励计划

支撑厂商：绿盟、知道创宇、安全宝等 监督单位：国家互联网安全应急中心

1, 乌云漏洞报告平台的通用型软件安全漏洞奖励计划低调运营4个月后, 已经有**100多位**白帽子踊跃参加, 共反馈了**200多个**通用型安全漏洞, 在多家安全厂商的支持下已发出了**数十万**的现金奖励。



2, 这期间收到多家通用型软件厂商不同影响等级的安全漏洞, 帮厂商与其用户及时发现了并杜绝了多起因安全漏洞导致的攻击隐患。

Discuz!

ecshop®

DEDECMS

ESPCMS
易思企业网站管理系统

phpwind

ShopEx



烏雲 - 台灣



“台灣是全球殭屍網路第四大國”

DDoS 攻擊需要大量的殭屍電腦

www.techbang.com/posts/18717-ddos

加入粉絲團

讚 13 萬

登入 註冊 訂閱本站

搜尋 T客邦 搜尋

首頁 新聞 評測 教學 手機 平板 筆電 影音 相機 零組件 周邊 遊戲 生活 討論區 體驗會

網路 手機 平板 筆電 零組件 網通 影音 電信 軟體 周邊 社會話題

現在加入T客邦會員，留言、登入拿積分，每個月都有機會拿到好禮，請看 [會員好康機制說明](#)。 Close

DDoS 攻擊需要大量的殭屍電腦，台灣是全球殭屍網路第 4 大國

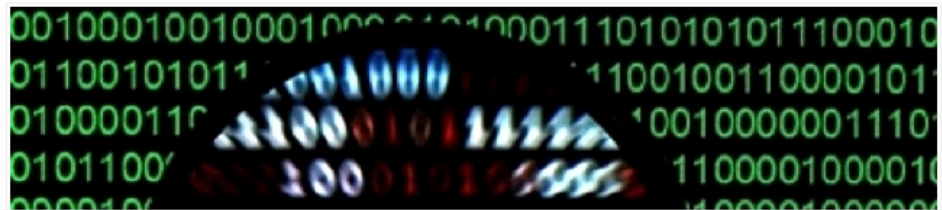
 老巴 發表於 2014年6月20日 10:02 | [收藏此文](#) 8+1 60 6 6 6 讚 1,114

GO2/CryptoLocker Scope

- More than 1 million GO2 infections globally
- Roughly 20% of infected computers are located in the United States
- Losses estimated globally in the hundreds of millions of dollars
- Key participation of 18 partner countries in support of ransomware operation



香港大學的民意網站（PopVote）投票系統、壹傳媒的網站這幾天遭受到的 DDoS 攻擊（分散式阻斷服務攻擊），主要的攻擊手法，就是利用大量的殭屍電腦，在特定時間內，大量向所要攻擊的伺服器發出密集的數據，造成伺服器的主機、頻寬等資源耗盡，而無法提供服務及回應給真正需要的使用者。



最愛排行榜

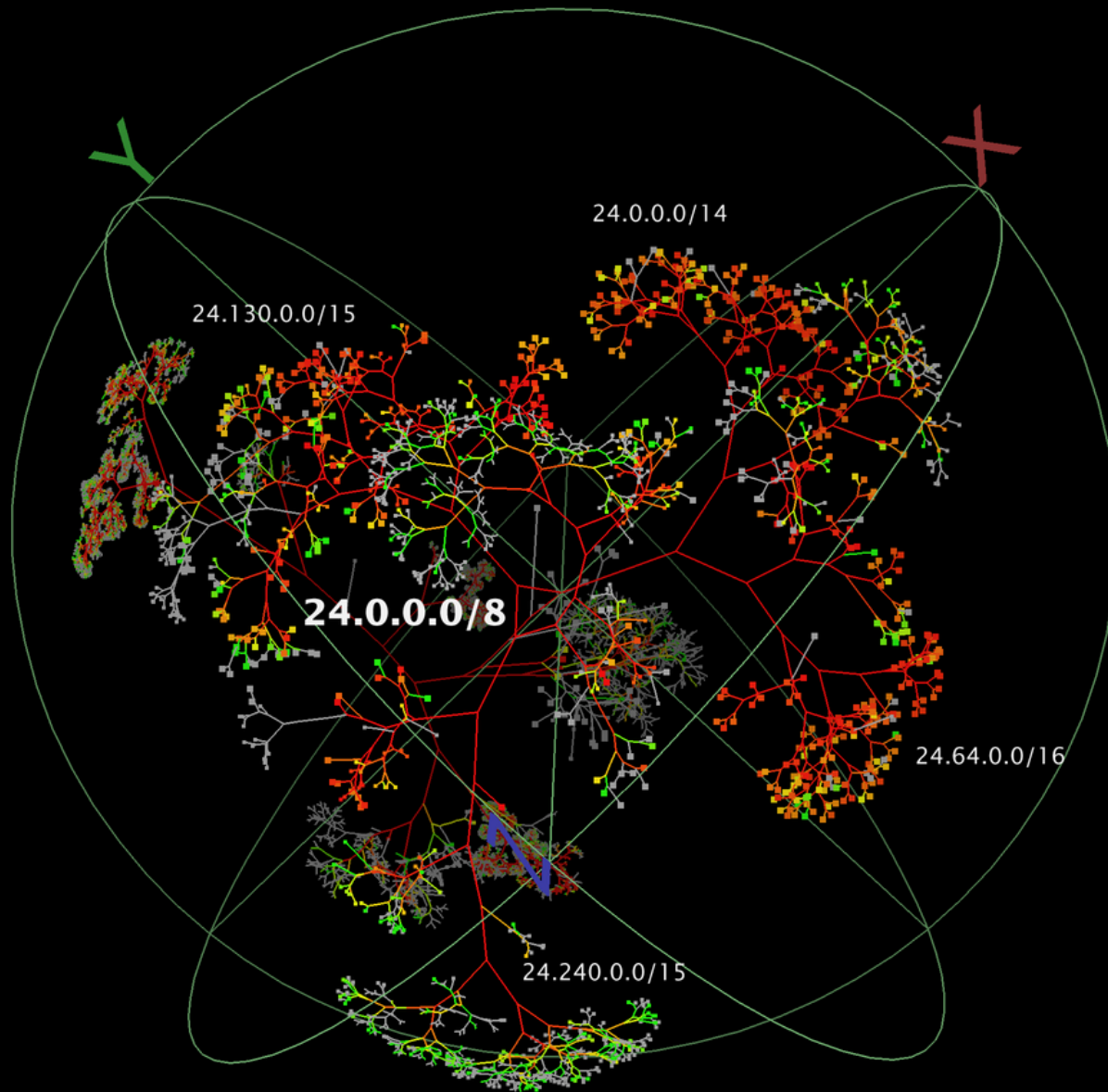
- 1/ 免破解，內建11招讓 Windows 7 效能大提升
- 2/ 不可不知的 Line 10大密技，你一定要會！
- 3/ SSD 固態硬碟 6 大優化技巧：提昇讀寫效能，延長使用壽命
- 4/ 臉書又見新型混合攻擊病毒！Private Video+OMG 傳播方式以及中毒徵兆完全公開
- 5/ 歲末年終敗家守則：新手採購電腦，從無到有手把手教學
- 6/ 國軍上兵偷用衛星網路看色情網站，上網費用高達一百多萬，他到底看了幾支片？
- 7/ 把 mSATA 固態硬碟變外接，比 USB 3.0 隨身碟便宜又更快
- 8/ Facebook 年度回顧，看看自己的 2013 年重要時刻

全民大亂鬥

 李婉語 說：

全世界都留一手





漏洞 - 資安攻防的關鍵

為何建置VulReport

- 台灣版的弱點資料庫
- 在地化通報及溝通讓修補時間縮短
- 提供NGO/無自行修復能力的小型企業修補服務或諮詢
- 提供學校資安社團參與資安弱點修補實務訓練
- 整合原本零散的安全研究人員或社群
- 提升台灣整體資安防禦實力

VulReport

[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	DEC-18	KNowlet
某知名新聞網子網域目錄洩漏造成部分內網		
Incident	DEC-18	cR@B

☑ 最新確認

Incident	DEC-16	beichen
某網站重置密碼問題		
Incident	DEC-16	beichen

⚠ 最新公開

Incident	DEC-16	beichen
某網站修改會員資料問題		
Other	DEC-16	beichen

漏洞通報範例

通報漏洞範例

← → ↺ <https://www.facebook.com/notes/vulreport-漏洞回報平台/通報漏洞範例/1592733567623990> ☆   

搜尋人、地點和事物 Sylphid 首頁 20+ 尋找朋友    

通報漏洞範例

編輯

由 Sylphid Su 發佈 · 2014年12月17日 18:52

標題: 某大學網頁 **command injection** (請隱蔽廠商關鍵字)

廠商: 國立台北教育大學 計算機與網路中心

簡述: 國立台北教育大學計算機與網路中心網頁存在 **command injection**

詳述: (麻煩盡可能詳盡，以利 VulReport 平台審核及廠商重現漏洞)
<http://cc.ntue.edu.tw/CheckWAN/trace3.php> 是測試校內對外連線的工具，由於POST參數IP過濾不夠嚴謹，將輸入值改為168.95.1.1; sed 'a;N;\$!ba;s/\n/ /g' /etc/passwd; ls 可造成 **command injection**，請見上傳附圖

思路: (可提升發掘漏洞的技術交流深度)
起初是發現有可以查詢北教大校內對外連線的網站，就覺得可以測試看看學校有沒有對這個功能有一點資安意識，因此就用了最基本的判斷，在後面接分號再接其他指令跑跑看，一開始嘗試後發現沒辦法返回構造的指令，就在繼續想辦法繞過，於是又接了一個分號，結果發現夾在中間的指令是會response的。
這裡停頓了一下，為什麼只有夾在中間的指令結果會返回？這邊暫緩腳步，繼續測試，後來發現只會跑出指令執行完後的結果的最後一項，因此就用sed將指令執行的結果串在一行，便成功利用此漏洞。
再回頭看trace3.php的程式碼發現是這樣判斷的：`exec("ping " . $_POST['IP'] . " | grep PING | cut --delimiter=' ' -f 2 | cut --delimiter=' ' -f 1");`
因此第一個ping的結果會有很多行，接著是我們中間的指令結果(已將結果串成一行)，而最後的指令會經過其他後面的過濾。最後的想法是，只要想辦法讓最後一行指令不產生任何結果，那依據這行程式碼便會返回最後一行結果回來，也就是我們構造的指令結果囉。

修補建議: (可加速存在漏洞廠商修復漏洞的正確性及效率)
由後來取得trace3.php的程式碼，可發現IP參數未經過檢查就直接放進exec()，這是非常危險的!! 建議在放入\$_POST['IP']前先將這個參數使用regular expression進行白名單過濾，或審慎思考這個功能的必要性，如沒有必要就取消這個功能。

 VulReport 漏洞回報平台

VulReport 漏洞回報平台的網誌
網誌一覽

新增標籤
透過 RSS 訂閱網誌
嵌入貼文

推薦粉絲專頁 顯示全部

 奧修生命之道學苑
1,310 人說讚。
讚

聊天室(13)

漏洞揭露流程

- 弱點審核(5人天)
- 廠商/企業組織弱點通知與確認(5人天)
- 對安全合作夥伴公開 (3天)
- 向核心成員及相關領域專家公開(10天)
- 對大眾公開(30/45/65/90天)

VulReport

VulReport 使用規範與聲明

VulReport 使用規範與聲明

歡迎你加入成為VulReport的會員，當完成註冊手續、或開始使用本平台所提供的服務及資訊時，就視為已知悉、並完全同意本文件的所有規範與聲明：

- 1 我們反對和譴責一切以漏洞測試為藉口，利用安全漏洞進行破壞、損害對方利益的惡意行為，包括但不限於利用漏洞竊取用戶資料、隱私及虛擬財產與影響商業營運等行為。
- 2 我們反對和譴責一切利用安全漏洞恐嚇個人、組織與影響競爭對手的行為。
- 3 通報漏洞或使用VulReport相關服務，必須遵守中華民國相關法律規定，使用者同意不會利用本平台及所提供資訊進行任何違法或不正當行為，包括但不限於下列法律：

3.1 刑法 第三十六章 妨害電腦使用罪

[http://law.moj.gov.tw/LawClass/LawParaDeatil.aspx?
Pcode=C0000001&LCNOS=%20358&LCC=2](http://law.moj.gov.tw/LawClass/LawParaDeatil.aspx?Pcode=C0000001&LCNOS=%20358&LCC=2)

3.2 個人資料保護法

<http://law.moj.gov.tw/LawClass/LawAllIf.aspx?PCode=I0050021>

刑法 第三十六章 妨害電腦使用罪

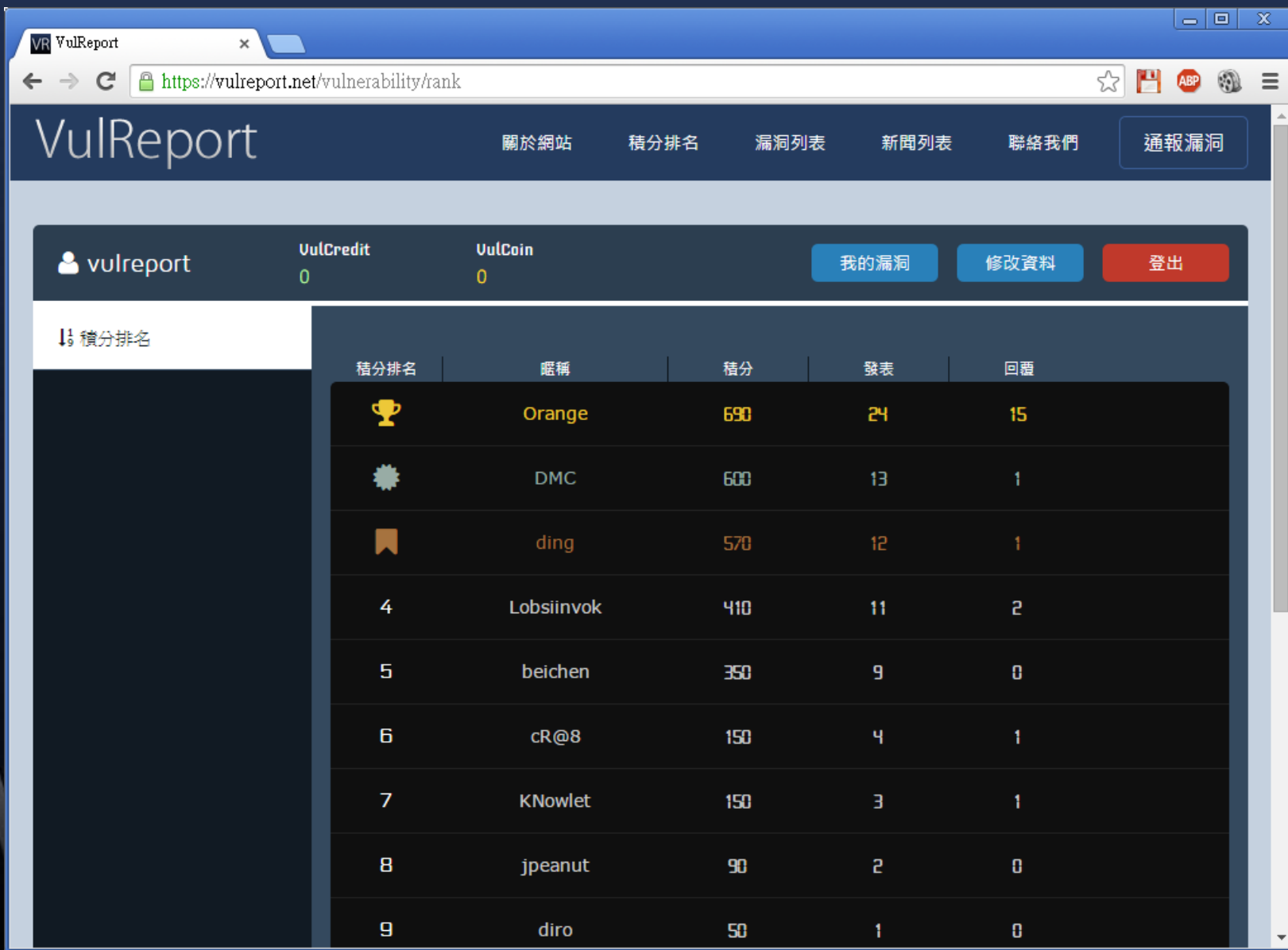
- 第 358 條
無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
- 第 359 條
無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。
- 第 360 條
無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
- 第 361 條
對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。
- 第 362 條
製作專供犯本章之罪之電腦程式，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。
- 第 363 條
第三百五十八條至第三百六十條之罪，須告訴乃論。

VulReport 里程碑

- 2014 Q1 開始籌備
- 2014 Q2 網站雛形(HITCON FreeTalk 短暫公開)
- 2014/11/24 公開測試
- 2014/12/23 粉絲團 500 讚(藉由社群力量宣傳及擴散)
- 2015/01/9 公開記者會
- 2015/01/10 公測/第一屆VR漏洞積分賽結束

VulReport

漏洞積分排名 (2015 $\frac{1}{8}$)



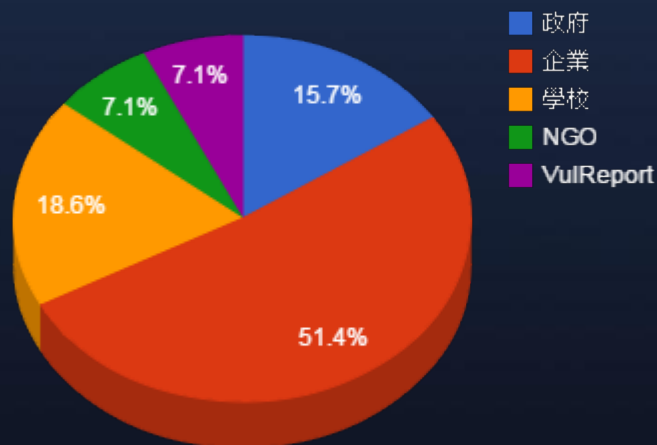
The screenshot shows the VulReport website interface. The browser address bar displays `https://vulreport.net/vulnerability/rank`. The site header includes the VulReport logo and navigation links: 關於網站, 積分排名, 漏洞列表, 新聞列表, 聯絡我們, and 通報漏洞. The user profile section shows 'vulreport' with 0 VulCredit and 0 VulCoin, and buttons for 我的漏洞, 修改資料, and 登出. The main content area is titled '積分排名' and displays a table of the top 9 users.

積分排名	暱稱	積分	發表	回覆
1	Orange	690	24	15
2	DMC	600	13	1
3	ding	570	12	1
4	Lobsiinvok	410	11	2
5	beichen	350	9	0
6	cR@8	150	4	1
7	KNowlet	150	3	1
8	jpeanut	90	2	0
9	diro	50	1	0

通報漏洞統計 (2015/1/8)

- 政府: 11
- 企業: 36
- 學校: 13
- NGO: 5
- VulReport: 5

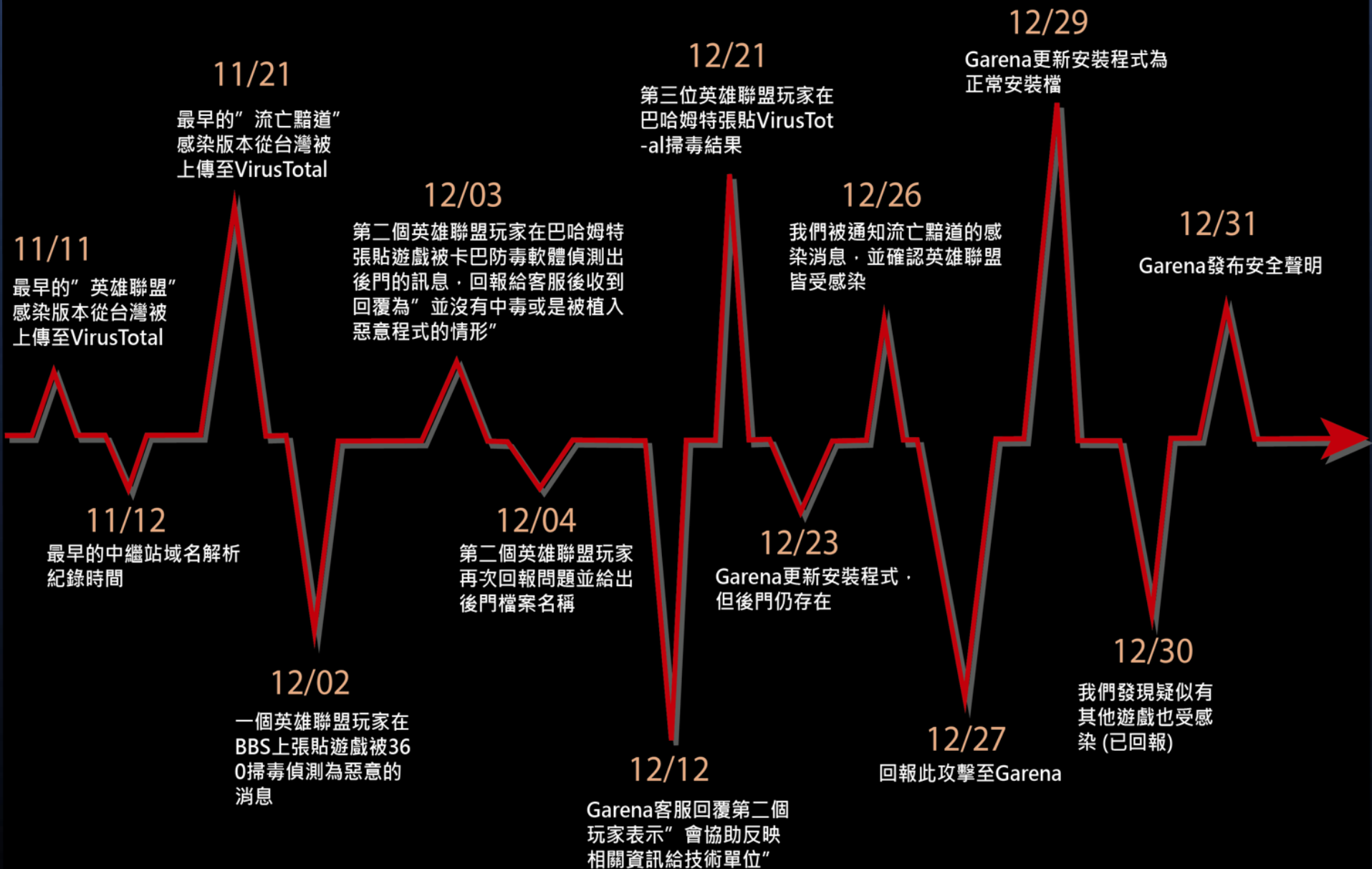
通報漏洞統計



VulReport 企業帳號

- 等級: 免費/正式/黃金/鑽石
- 優先通知漏洞通報
- 通報期限: 30/45/65/90
- 資安諮詢服務
- Logo連結
- 資安人才招聘
- 漏洞資訊提供研究
- 資安產品或服務推薦
- 對外服務檢測(研議中)
- 詳見: <http://goo.gl/9cbFgN>

VulReport



wiki - responsible disclosure

The screenshot shows a web browser window with the Wikipedia page for 'Responsible disclosure'. The browser's address bar shows the URL 'en.wikipedia.org/wiki/Responsible_disclosure'. The page layout includes a left sidebar with navigation links, a main content area with text and a list of references, and a right sidebar. The left sidebar contains sections for 'Interaction' (Help, About Wikipedia, Community portal, Recent changes, Contact page), 'Tools' (What links here, Related changes, Upload file, Special pages, Permanent link, Page information, Wikidata item, Cite this page), 'Print/export' (Create a book, Download as PDF, Printable version), and 'Languages' (Čeština, Español, Magyar, Edit links). The main content area starts with a paragraph about repairing vulnerabilities, followed by a paragraph on responsible disclosure as a process, then a paragraph about Vendor-sec, and a section on selected security vulnerabilities resolved by applying responsible disclosure. The references section lists two items.

Responsible disclosure - Wiki x

en.wikipedia.org/wiki/Responsible_disclosure

Interaction

- Help
- About Wikipedia
- Community portal
- Recent changes
- Contact page

Tools

- What links here
- Related changes
- Upload file
- Special pages
- Permanent link
- Page information
- Wikidata item
- Cite this page

Print/export

- Create a book
- Download as PDF
- Printable version

Languages

- Čeština
- Español
- Magyar

Edit links

repairing the vulnerability and preventing any future damage. Depending on the potential impact of the vulnerability, the expected time needed for an emergency fix or workaround to be developed and applied and other factors, this period may vary between a few days and several months. It is easier to patch software by using the [Internet](#) as a distribution channel.

Responsible disclosure fails to satisfy security researchers who expect to be financially compensated, while reporting vulnerabilities to the vendor with the expectation of compensation might be viewed as extortion. While a market for vulnerabilities has developed, vulnerability commercialization remains a hotly debated topic tied to the concept of vulnerability disclosure. Today, the two primary players in the commercial vulnerability market are iDefense, which started their vulnerability contributor program (VCP) in 2003, and [TippingPoint](#), with their zero-day initiative (ZDI) started in 2005. These organisations follow the responsible disclosure process with the material bought. Between March 2003 and December 2007 an average 7.5% of the vulnerabilities affecting Microsoft and Apple were processed by either VCD or ZDI.^[1] Independent firms financially supporting responsible disclosure by paying bug bounties include [Facebook](#), [Google](#), [Mozilla](#), and [Barracuda Networks](#).^[2]

[Vendor-sec](#) was a responsible disclosure mailing list. Many, if not all, of the [CERT](#) groups coordinate responsible disclosures.

Selected [security vulnerabilities](#) resolved by applying responsible disclosure:

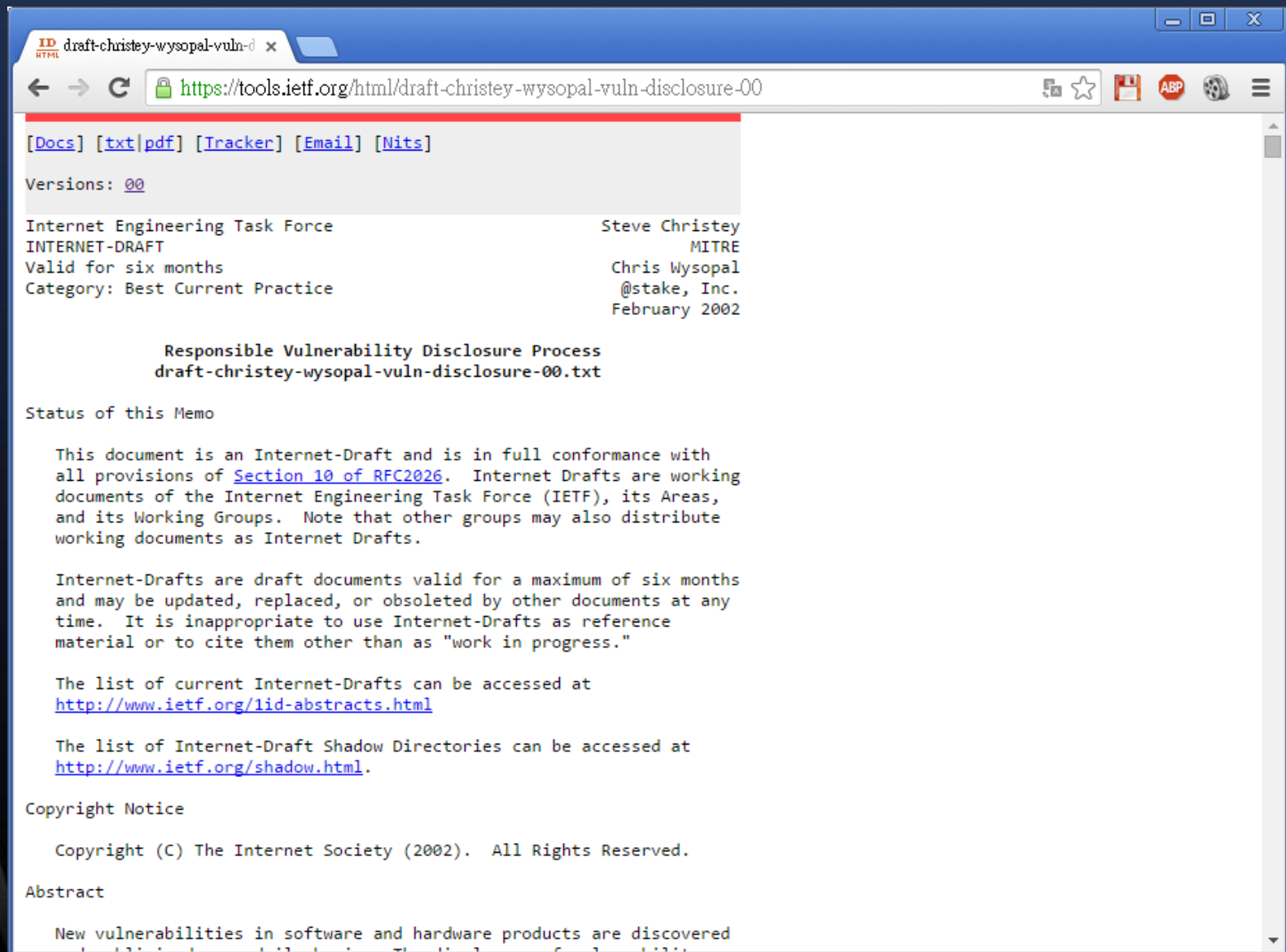
- [Dan Kaminsky](#) discovery of [DNS cache poisoning](#), 5 months^[3]
- [Radboud University Nijmegen](#) breaks the security of the [MIFARE](#) Classic cards, 6 months^[4]
- [MBTA vs. Anderson](#), MIT students find vulnerability in the Massachusetts subway security, 5 months^[5]
- [MD5](#) collision attack that shows how to create false CA certificates, 1 week^[6]

References

[edit]

- ¹ ["Paper measuring the prevalence of responsible disclosure and model of the processes of the security ecosystem"](#)
- ² [^](#)

Responsible Vulnerability Disclosure Process



The screenshot shows a web browser window with the address bar displaying <https://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00>. The page content includes a header with links [Docs], [txt|pdf], [Tracker], [Email], and [Nits]. Below this, it states "Versions: 00". The main body of the document is titled "Responsible Vulnerability Disclosure Process" and "draft-christey-wysopal-vuln-disclosure-00.txt". It includes a "Status of this Memo" section, a "Copyright Notice", and an "Abstract".

[Docs] [txt|pdf] [Tracker] [Email] [Nits]

Versions: 00

Internet Engineering Task Force
INTERNET-DRAFT
Valid for six months
Category: Best Current Practice

Steve Christey
MITRE
Chris Wysopal
@stake, Inc.
February 2002

Responsible Vulnerability Disclosure Process
draft-christey-wysopal-vuln-disclosure-00.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#). Internet Drafts are working documents of the Internet Engineering Task Force (IETF), its Areas, and its Working Groups. Note that other groups may also distribute working documents as Internet Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/lid-abstracts.html>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

Abstract

New vulnerabilities in software and hardware products are discovered

Security Response Center

阿里巴巴集团安全应急响应中心

security.alibaba.com/index.htm?spm=0.0.0.0.hWlzeO

Alibaba Group

安全应急响应中心

security.alibaba.com

English

首页

公告

报告漏洞

贡献榜

博客

阿里巴巴安全应急响应中心

诚邀您共同打造健康安全的电子商务生态!

↑

报告漏洞



平台简介

阿里巴巴集团一直致力于建设诚信、共赢、繁荣的电子商务产业生态圈。安全是其健康成长的核心要素，为此特成立集团安全部，隶属于其的安全响应中心（Alibaba Security Response Center，简称ASRC）欢迎广大用户向我们反馈阿里巴巴集团各事业部旗下相关产品及业务的安全漏洞，以帮助我们提升自身产品及业务的安全性，同时也希望借此平台加强与安全业界同仁的合作与交流。我们诚邀您共同为打造健康安全的电子商务产业生态圈贡献力量。

反馈途径

公告

更多>

阿里巴巴招聘公告	2014-09-04
2014年7月白帽子获奖公告	2014-08-18
阿里500万安全赏金计划2014年8月奖励公告	2014-08-06
阿里安全赏金计划	2014-02-18
漏洞评分标准	2013-10-14
漏洞奖励计划(期)	2013-10-13
漏洞报告与处理流程	2013-10-12

責任揭密政策 - Uber



The screenshot shows a web browser window with the title 'Uber Security'. The address bar displays 'https://www.uber.com/zh-TW/security'. The page header includes a navigation menu with '主選單' (Main Menu) and 'LEGAL UBER' branding. On the right, there are links for '登入' (Login) and '註冊' (Register). Below the header, there are five tabs: '使用者條款' (Terms of Use), '隱私政策' (Privacy Policy), '版權' (Copyright), '安全性政策' (Security Policy), and '其他' (Other). The '責任揭密政策' (Responsible Disclosure Policy) tab is selected and highlighted in blue.

責任揭密政策

維護您與 Uber 之間的資料安全與隱私，就是 Uber 工程團隊的最高目標之一。如果您是安全性研究人員（或是其他敏銳的使用者）並且在我們其中一項產品中發現安全性漏洞，請聯繫 SECURITY-ABUSE@UBER.COM. 針對某些 特別敏感的回報，您可以使用 [UBER 產品安全 PGP/GPG 金鑰](#) 將您的電子信箱加密。我們會優先處理寄至此地址的回報，並盡快進行調查。

任何依照此揭露政策向我們回報的漏洞，Uber 承諾將立即驗證、回應及修正這些漏洞，且不會對負責任的回報者採取任何法律行動或行政措施。Uber 保留對於所有未遵循法規之事件的合法權利。

提交的安全問題應包含下列資訊：

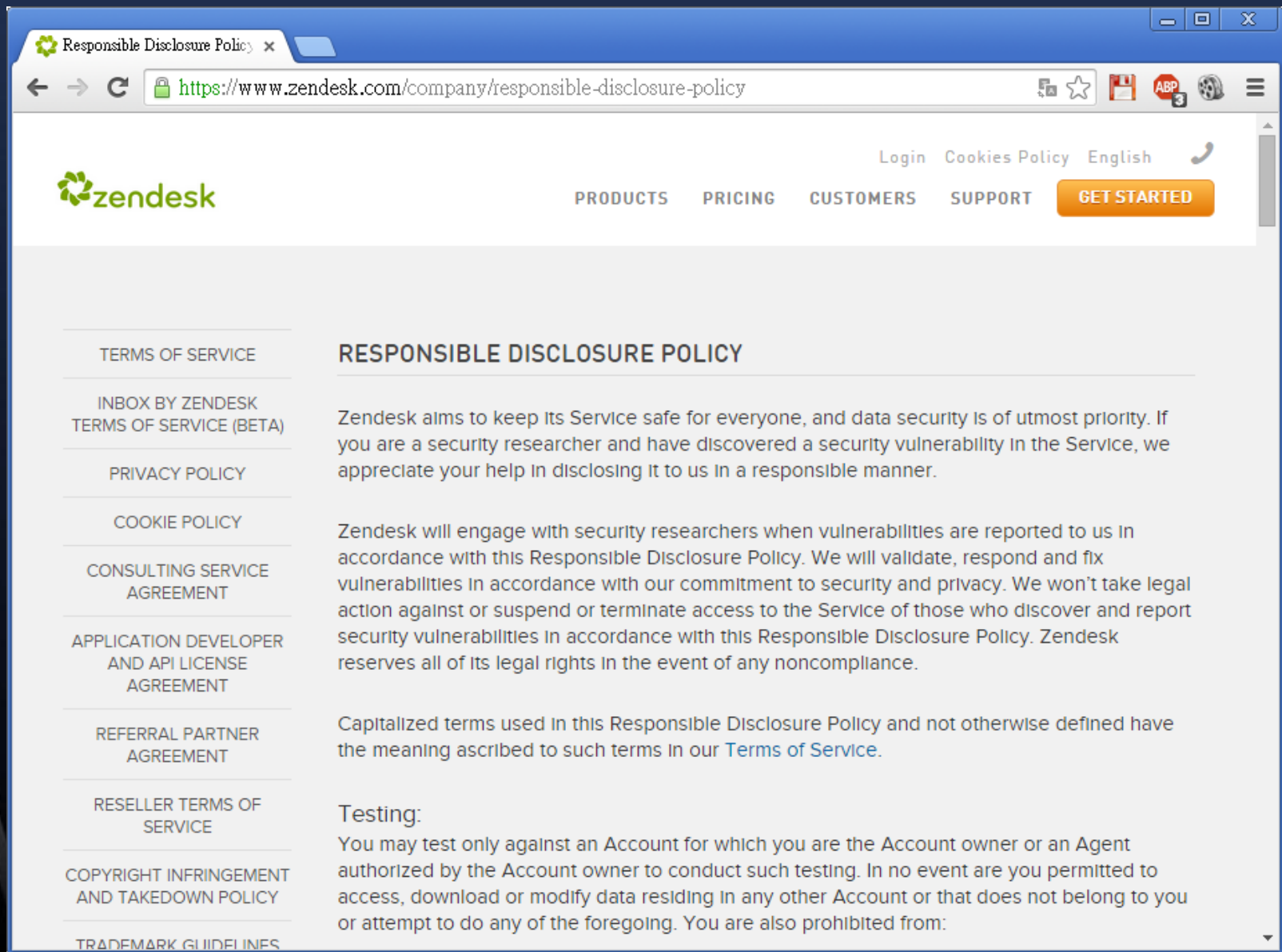
- 您的電子信箱
- 您的全名
- 問題摘要（例如，Foo 頁面上的 XSS、Bar 頁面上的 CSRF、App Baz 中的 SQLi）
- 回報問題的步驟

部分使用者會向我們回報之前未發現的高度或重大安全漏洞，為了表達誠摯的謝意，Uber 將會在此頁面維護一份回報者清單。

確認

- [RAFAEL PABLOS](#)
- [ARVIND SINGH SHEKHAWAT](#)
- [CHETAN GULHANE](#)
- [NITIN GOPLANI & JATINDER PAL SINGH](#)
- [MANISH BHATTACHARYA](#)
- [DYLAN S HAILEY](#)
- [YUJI KOSUGA, PHD](#)
- [TONY TRUMMER & TUSHAR DALVI](#)

responsible disclosure policy -1



The screenshot shows a web browser window with the URL <https://www.zendesk.com/company/responsible-disclosure-policy>. The page features the Zendesk logo and a navigation menu with links to PRODUCTS, PRICING, CUSTOMERS, SUPPORT, and a GET STARTED button. A sidebar on the left contains links to various legal documents, including the Responsible Disclosure Policy. The main content area is titled 'RESPONSIBLE DISCLOSURE POLICY' and contains three paragraphs of text. The first paragraph states that Zendesk aims to keep its Service safe and that it appreciates security researchers who report vulnerabilities in a responsible manner. The second paragraph explains that Zendesk will engage with security researchers when vulnerabilities are reported, validate them, and fix them in accordance with its commitment to security and privacy. The third paragraph states that Zendesk reserves all of its legal rights in the event of noncompliance. Below this, a section titled 'Testing:' explains that users may test only against an Account for which they are the Account owner or an Agent authorized by the Account owner to conduct such testing. It also states that users are prohibited from accessing, downloading, or modifying data residing in any other Account or that does not belong to them.

Responsible Disclosure Policy

<https://www.zendesk.com/company/responsible-disclosure-policy>

Login Cookies Policy English

PRODUCTS PRICING CUSTOMERS SUPPORT GET STARTED

TERMS OF SERVICE

INBOX BY ZENDESK
TERMS OF SERVICE (BETA)

PRIVACY POLICY

COOKIE POLICY

CONSULTING SERVICE
AGREEMENT

APPLICATION DEVELOPER
AND API LICENSE
AGREEMENT

REFERRAL PARTNER
AGREEMENT

RESELLER TERMS OF
SERVICE

COPYRIGHT INFRINGEMENT
AND TAKEDOWN POLICY

TRADEMARK GUIDELINES

RESPONSIBLE DISCLOSURE POLICY

Zendesk aims to keep its Service safe for everyone, and data security is of utmost priority. If you are a security researcher and have discovered a security vulnerability in the Service, we appreciate your help in disclosing it to us in a responsible manner.

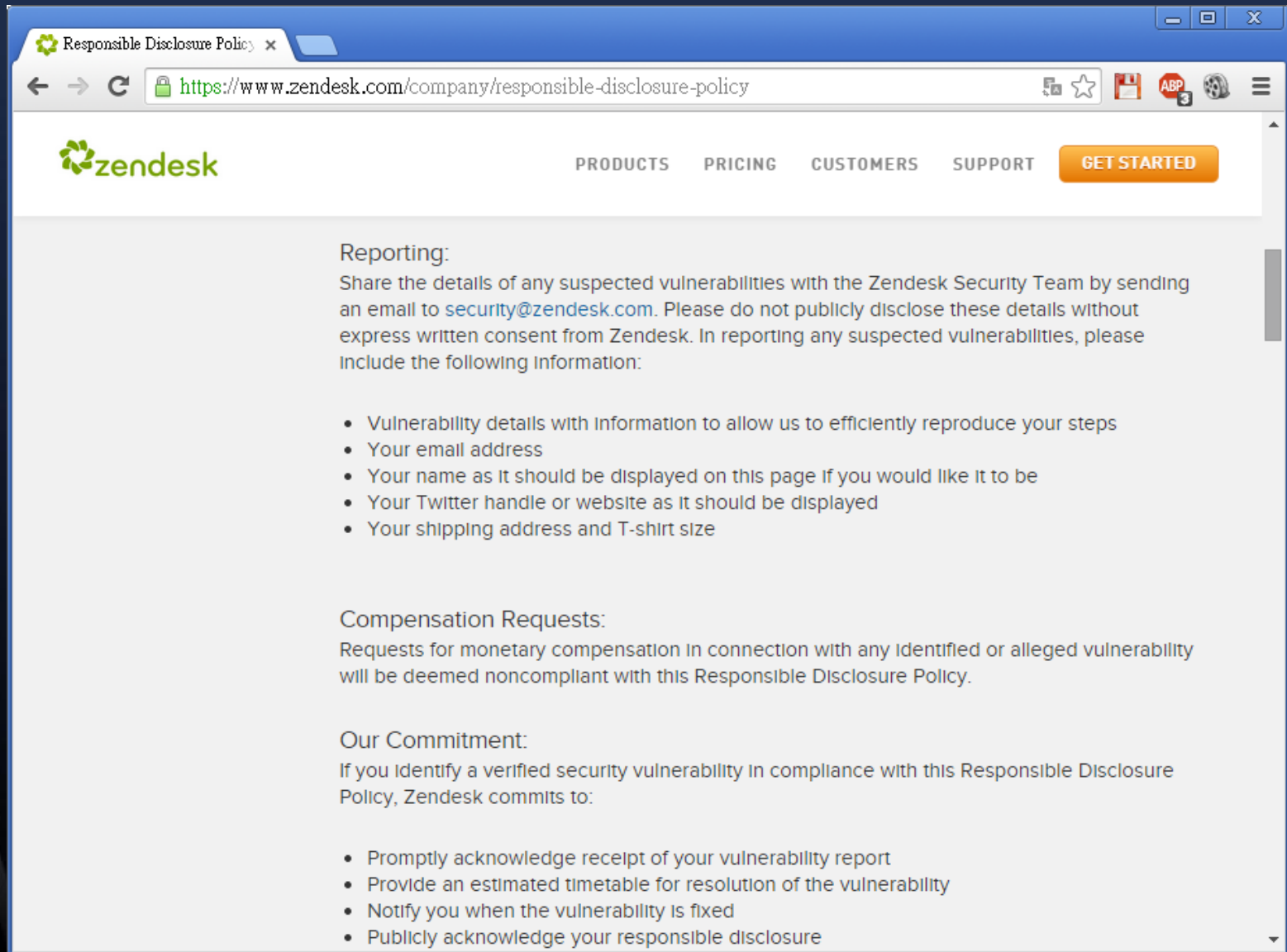
Zendesk will engage with security researchers when vulnerabilities are reported to us in accordance with this Responsible Disclosure Policy. We will validate, respond and fix vulnerabilities in accordance with our commitment to security and privacy. We won't take legal action against or suspend or terminate access to the Service of those who discover and report security vulnerabilities in accordance with this Responsible Disclosure Policy. Zendesk reserves all of its legal rights in the event of any noncompliance.

Capitalized terms used in this Responsible Disclosure Policy and not otherwise defined have the meaning ascribed to such terms in our [Terms of Service](#).

Testing:

You may test only against an Account for which you are the Account owner or an Agent authorized by the Account owner to conduct such testing. In no event are you permitted to access, download or modify data residing in any other Account or that does not belong to you or attempt to do any of the foregoing. You are also prohibited from:

responsible disclosure policy -2



The screenshot shows a web browser window with the title 'Responsible Disclosure Policy' and the URL 'https://www.zendesk.com/company/responsible-disclosure-policy'. The page features the Zendesk logo and a navigation bar with links for PRODUCTS, PRICING, CUSTOMERS, SUPPORT, and a GET STARTED button. The main content is divided into three sections: Reporting, Compensation Requests, and Our Commitment, each with a list of bullet points.

Reporting:
Share the details of any suspected vulnerabilities with the Zendesk Security Team by sending an email to security@zendesk.com. Please do not publicly disclose these details without express written consent from Zendesk. In reporting any suspected vulnerabilities, please include the following information:

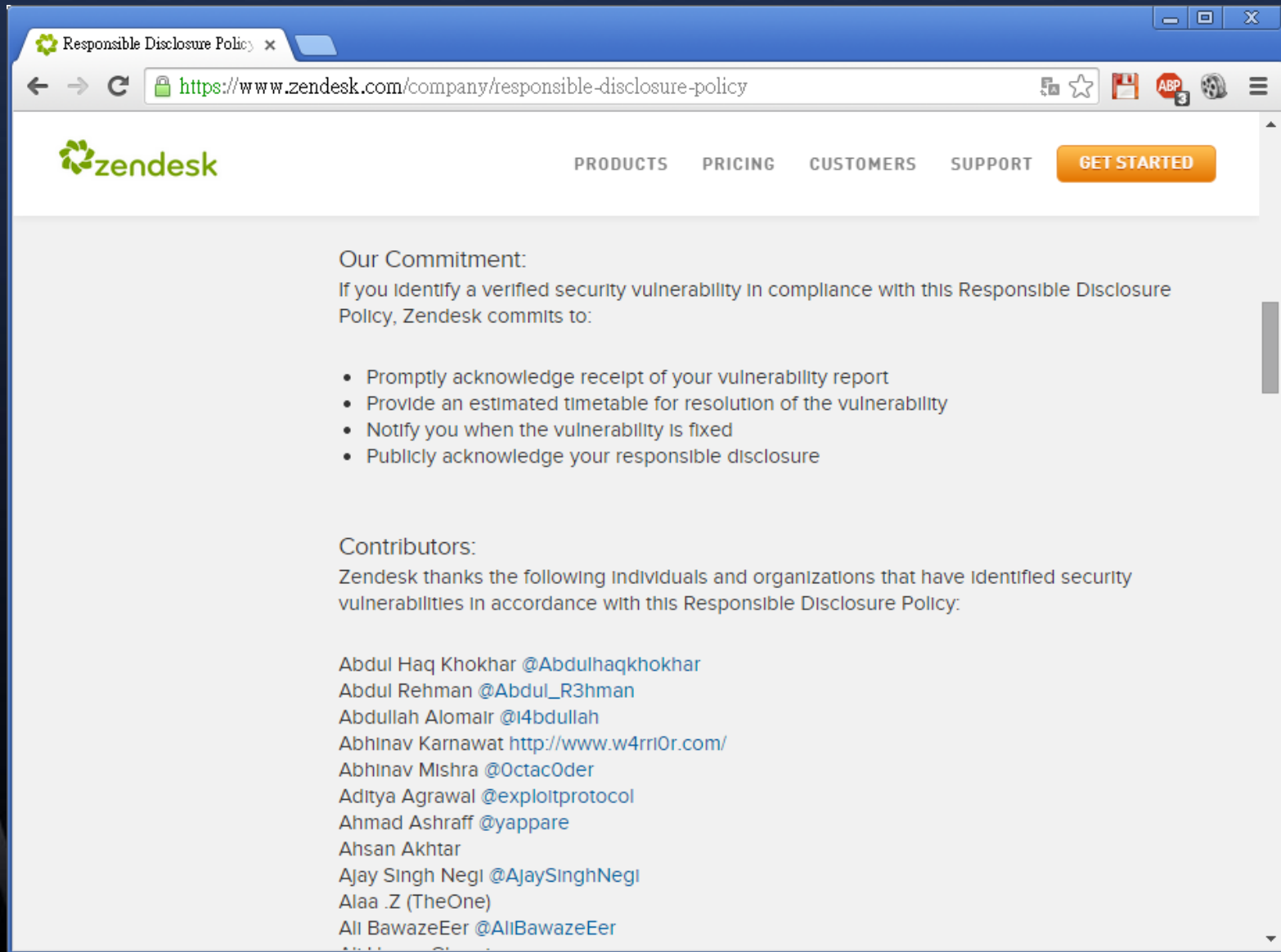
- Vulnerability details with information to allow us to efficiently reproduce your steps
- Your email address
- Your name as it should be displayed on this page if you would like it to be
- Your Twitter handle or website as it should be displayed
- Your shipping address and T-shirt size

Compensation Requests:
Requests for monetary compensation in connection with any identified or alleged vulnerability will be deemed noncompliant with this Responsible Disclosure Policy.

Our Commitment:
If you identify a verified security vulnerability in compliance with this Responsible Disclosure Policy, Zendesk commits to:

- Promptly acknowledge receipt of your vulnerability report
- Provide an estimated timetable for resolution of the vulnerability
- Notify you when the vulnerability is fixed
- Publicly acknowledge your responsible disclosure

responsible disclosure policy - 3



The screenshot shows a web browser window with the title "Responsible Disclosure Policy" and the URL "https://www.zendesk.com/company/responsible-disclosure-policy". The Zendesk logo is in the top left, and navigation links for "PRODUCTS", "PRICING", "CUSTOMERS", "SUPPORT", and a "GET STARTED" button are in the top right. The main content area is titled "Our Commitment:" and describes the company's commitment to handling security vulnerabilities. It includes a bulleted list of commitments: promptly acknowledging reports, providing a timetable for resolution, notifying when fixed, and publicly acknowledging disclosures. Below this, the "Contributors:" section thanks individuals and organizations for identifying vulnerabilities, listing names and their social media or website handles.

Responsible Disclosure Policy x

← → ↻ <https://www.zendesk.com/company/responsible-disclosure-policy> ☆ 📄 ABP 3 🎬 ☰

 [PRODUCTS](#) [PRICING](#) [CUSTOMERS](#) [SUPPORT](#) [GET STARTED](#)

Our Commitment:

If you identify a verified security vulnerability in compliance with this Responsible Disclosure Policy, Zendesk commits to:

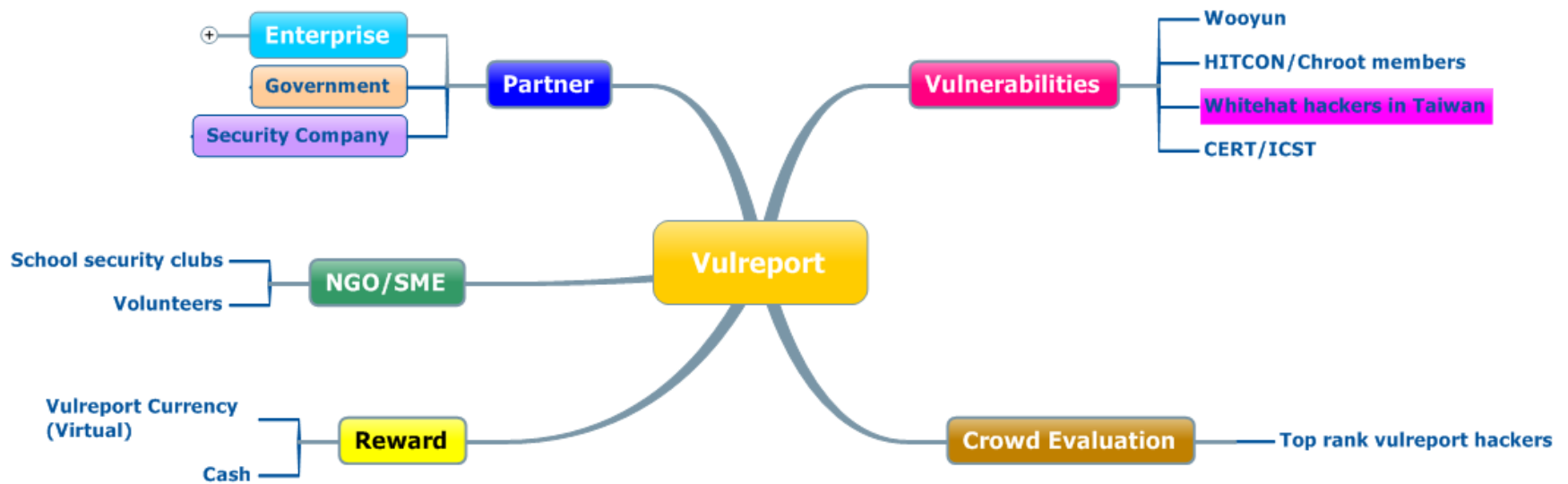
- Promptly acknowledge receipt of your vulnerability report
- Provide an estimated timetable for resolution of the vulnerability
- Notify you when the vulnerability is fixed
- Publicly acknowledge your responsible disclosure

Contributors:

Zendesk thanks the following individuals and organizations that have identified security vulnerabilities in accordance with this Responsible Disclosure Policy:

Abdul Haq Khokhar @Abdulhaqkhokhar
Abdul Rehman @Abdul_R3hman
Abdullah Alomair @i4bdullah
Abhinav Karnawat <http://www.w4rri0r.com/>
Abhinav Mishra @OctacOder
Aditya Agrawal @exploitprotocol
Ahmad Ashraff @yappare
Ahsan Akhtar
Ajay Singh Negi @AjaySinghNegi
Alaa .Z (TheOne)
Ali BawazeEer @AliBawazeEer

VulReport 未來規劃



VulReport

Happy Hackers ☺



VulReport

WEB: <https://vulreport.net/>

FB: facebook.com/vulreport

VulReport

Q&A

