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"

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

首頁 信箱 新聞 股市 氣象 運動 影音 名人娛樂 Flickr 購物中心 商城 拍賣 更多

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

推薦 1

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，透過指尖敲敲鍵盤，就能攻破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，這名學生平時就用家中電腦，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法使用函送法辦，最高可被判處三年以下刑期。

新聞相關影音

新聞搜尋 新聞搜尋

你可能還會想看

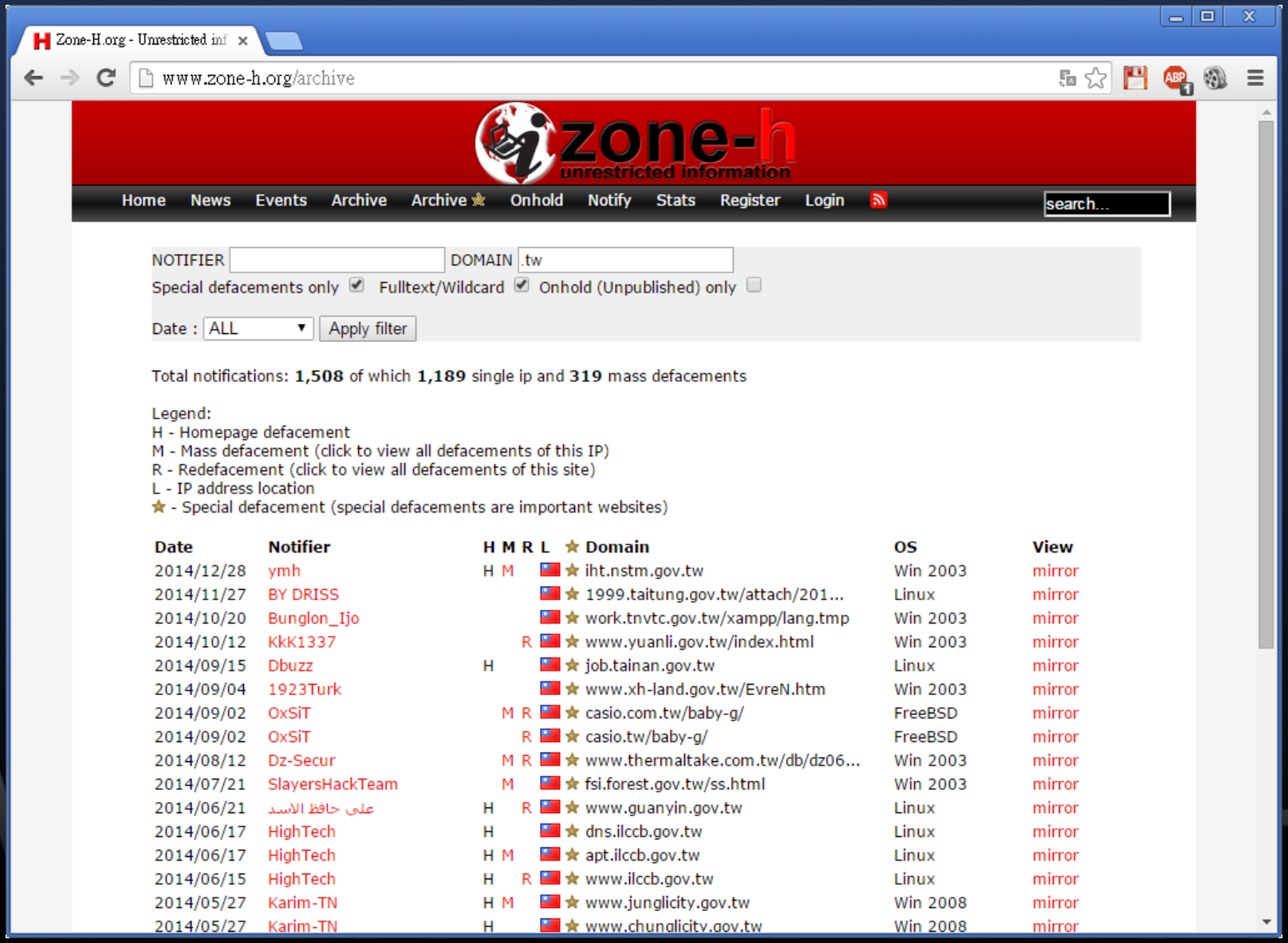
- 柯P上任前夕 趙少康閃辭富邦金獨董
- 中年大叔靠一枝眼線筆 負債3千萬翻身年營收3億
- NBA／湖人沒Kobe更強？ 史考特：這些人瘋了
- 女大生堅提告：給他教訓
- 台灣第一小生 魏少朋病逝
- 炒飯遭前夫捉姦 女星矢口真里驚：糟糕了
- 岳父貼心一句話 高山峰大鑼男兒淚
- 周刊：郭美珠爆白冰冰曾是性工作者？

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

正在等候 s.yimg.com...

zone-h



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.chunglicity.gov.tw	Win 2008	mirror

Underground Economy

The Black Market

$980-$4,900
Trojan program to steal online account information

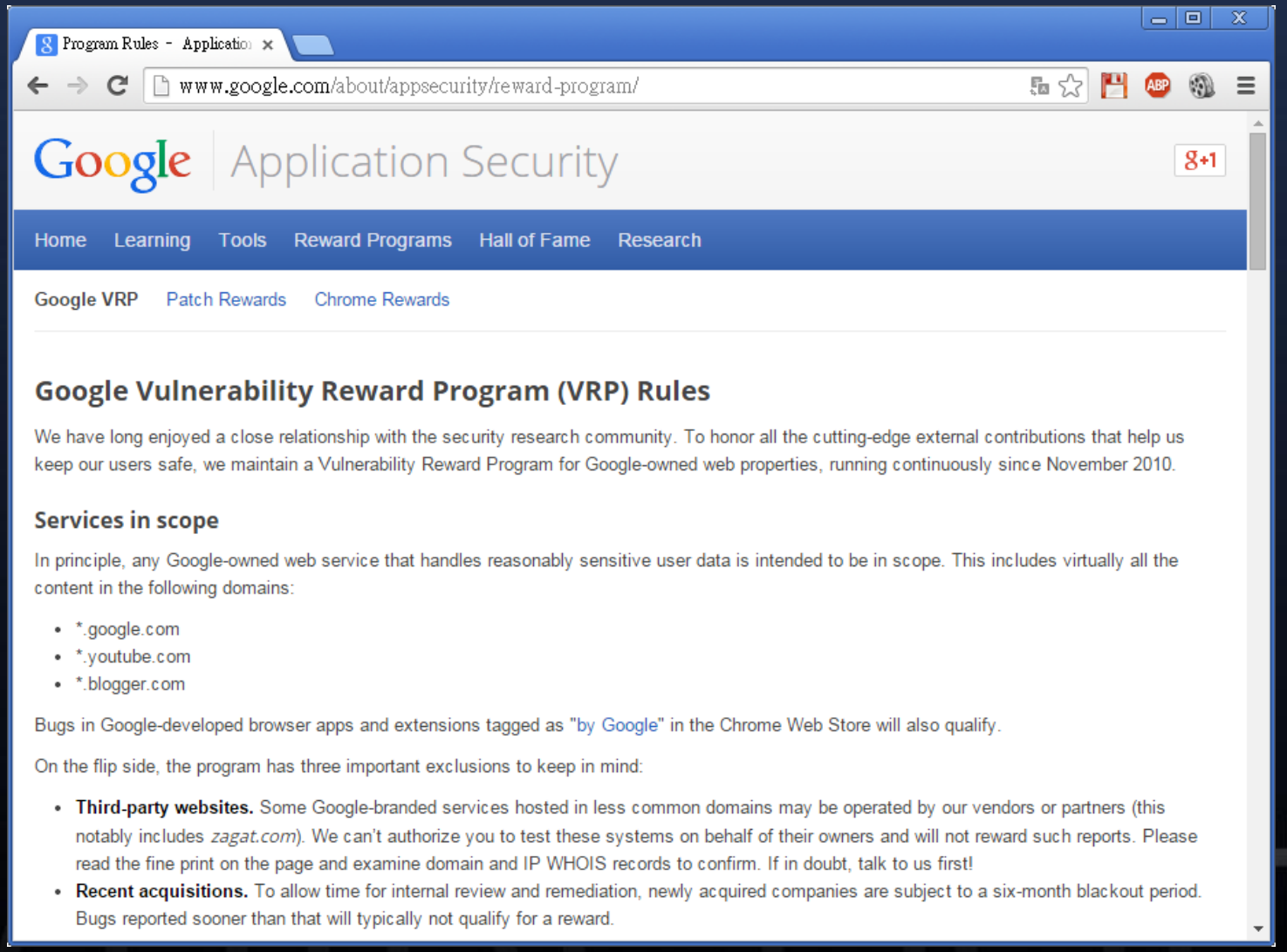
$490
Credit card number with PIN

$78-$294
Billing data, including account number, address, Social Security number, home address, and birth date

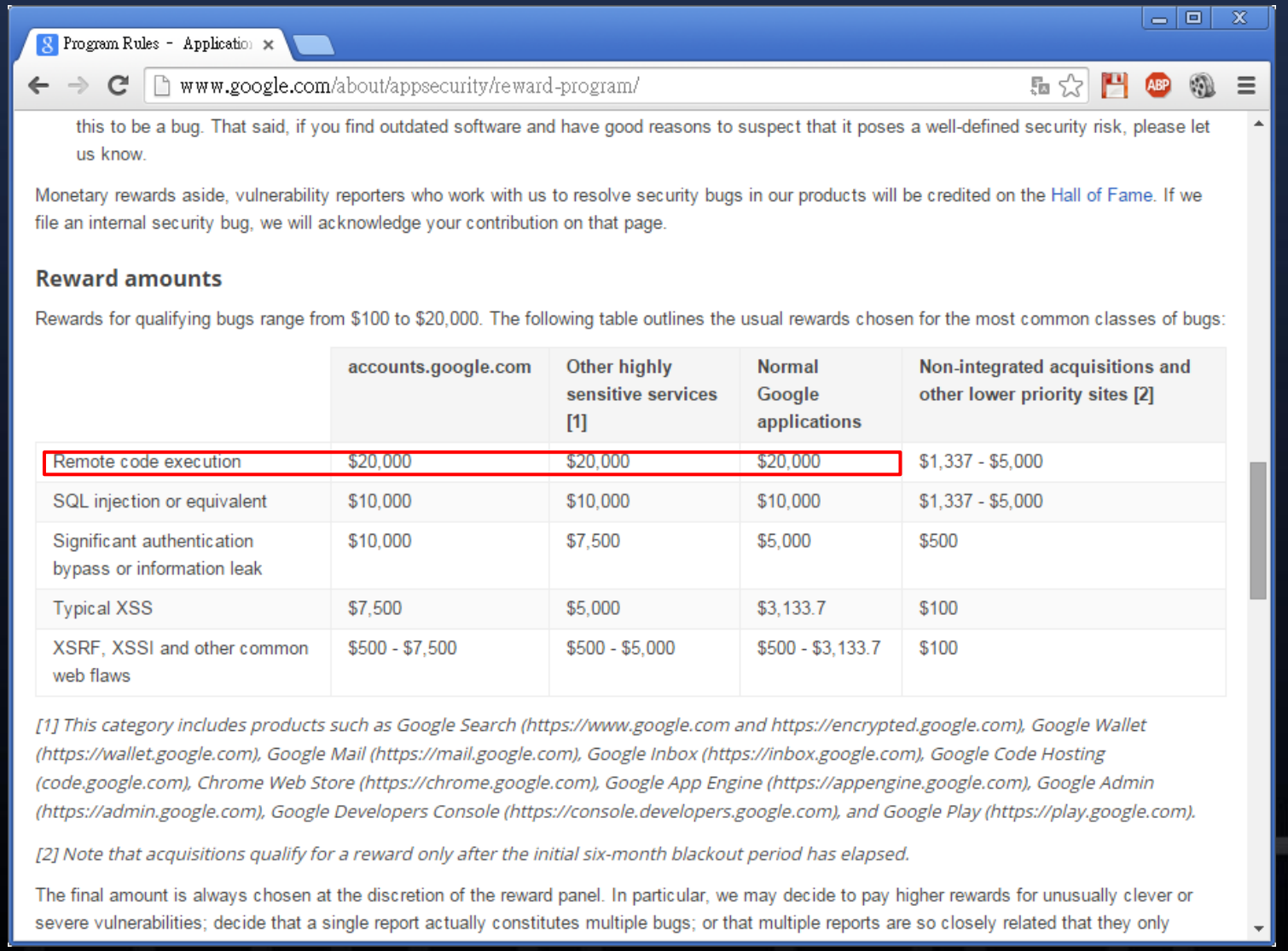
別讓駭客不開心

- 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

Google VRP - 1


Program Rules - Applicatio
www.google.com/about/appsecurity/reward-program/
Google Application Security
+1
Home Learning Tools Reward Programs Hall of Fame Research
Google VRP Patch Rewards Chrome Rewards
Google Vulnerability Reward Program (VRP) Rules
We have long enjoyed a close relationship with the security research community. To honor all the cutting-edge external contributions that help us keep our users safe, we maintain a Vulnerability Reward Program for Google-owned web properties, running continuously since November 2010.
Services in scope
In principle, any Google-owned web service that handles reasonably sensitive user data is intended to be in scope. This includes virtually all the content in the following domains:
*.google.com
*.youtube.com
*.blogger.com
Bugs in Google-developed browser apps and extensions tagged as "by Google" in the Chrome Web Store will also qualify.
On the flip side, the program has three important exclusions to keep in mind:
Third-party websites. Some Google-branded services hosted in less common domains may be operated by our vendors or partners (this notably includes zagat.com). We can't authorize you to test these systems on behalf of their owners and will not reward such reports. Please read the fine print on the page and examine domain and IP WHOIS records to confirm. If in doubt, talk to us first!
Recent acquisitions. To allow time for internal review and remediation, newly acquired companies are subject to a six-month blackout period. Bugs reported sooner than that will typically not qualify for a reward.

Google VRP - 2



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

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 讚 分享 201 g+1 6

文/ 林妍溱 | 2014-07-16 發表

iThome Weekly 電腦報
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

Google Project Zero - 2

Alibaba


阿里巴巴集团安全应急响
security.alibaba.com/announcement/notice_20.htm?spm=0.0.0.0.dvrQwO
Alibaba Group 阿里巴巴集团
安全应急响应中心
security.alibaba.com
首 页
公 告
报告漏洞
贡献榜
博 客
返回公告主页
我们希望能够借助集体的力量提升我们的
阿里500万安全赏金计划2014年8月奖励公告
公告编号：ASRC-2014-14
公告来源：阿里巴巴集团安全应急响应中心
公告日期：2014-8-6
公告内容：
为了更好的回馈白帽子们对阿里巴巴集团保护用户安全的帮助和支持，2014年2月，阿里巴巴集团安全应急响应中心(ASRC)正式推
出“阿里安全赏金计划”，拿出500万现金奖励有突出贡献的白帽子。凡发现阿里巴巴集团旗下产品或业务的安全漏洞，直接提交至A
平台并得到确认，除可获得原有的漏洞奖励计划积分礼品外，如对阿里巴巴集团安全提升价值较大，单个漏洞最高可获得10万元的现
励。
日前，来自零日信息的“EvilMoon”反馈了阿里巴巴集团系统的安全漏洞，并积极协助我们改进和加强系统安全，依据“阿里安
计划”阿里巴巴集团给予白帽子“EvilMoon”现金5万元（税后）的奖励，感谢白帽子“EvilMoon”对阿里巴巴集团安全作出的贡献
此我们也感谢广大白帽子对我们安全一如既往的帮助和支持。
欢迎广大用户继续来ASRC平台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
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，

乌云 - 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


搜索结果 | WooYun.org
www.wooyun.org/searchbug.php
WooYun.org
加关注
11.8万
首页
厂商列表
白帽子
乌云榜
团队
漏洞列表
提交漏洞
安全中心
乌云招聘
知识库
公告
当前位置：WooYun >> 搜索结果
搜索关键字： 台湾 (共 60 条记录)
将未公开漏洞纳入搜索结果
国立金门大学主站sql注入，且phpmyadmin外连
咱们台湾省的，你懂的...台湾省国立金门大学主站sql注入漏洞： http://www.nqu.edu.tw/cht/index.php?code=list&flag=detail&ids=12&article_id=23431 参数：ids 并且
联，嘿嘿 http://www.nqu.edu.tw/phpmyadmin/ 直接读取root密码：80427148 ...壮哉大台湾省。。 ...过滤神马的
提交日期：2014-12-04 作者：wps2015
台湾国立交通大学VPN泄露
台湾国立交通大学VPN泄露...code 区域账号:easonyeh@mail.nctu.edu.tw 密码:qazwsx1234 登陆地址:https://sslvpn.nctu.edu.tw/dana-na/auth/url_default/welcome.cg
更改密码
提交日期：2014-11-20 作者：miyachiki
台湾国立高雄师范大学内部邮箱泄露
台湾国立高雄师范大学内部邮箱泄露(可以连接学生HomePage FTP)...code 区域https://github.com/mn-works/miit/blob/d3534db612173f8e51f6671490d33b0f824219
est.php 登陆地址:http://stu99.nknu.edu.tw/cgi-bin/openwebmail/openwebmail.pl 登陆成功 code 区域學生HomePage使用方法說明 http://stu99.nknu.edu.tw/ 1.主機：
u.tw 2.帳號：與E-mail帳號相同 连接成功 ... ...删除gi...
提交日期：2014-11-19 作者：miyachiki

“台灣是全球殭屍網路第四大國”

DDoS 攻擊需要大量的殭屍

www.techbang.com/posts/18717-ddos

T客邦

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

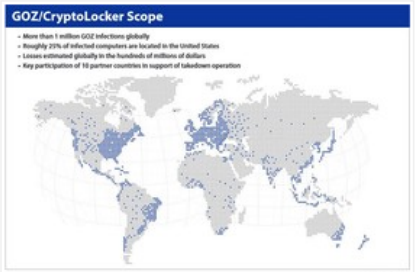
網路 手機 平板 筆電 零組件 網通 影音 電信 軟體 周邊 社會話題

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

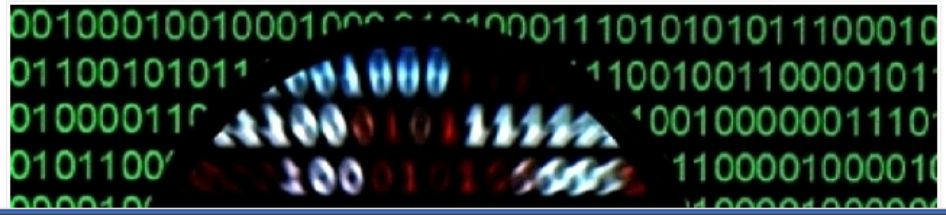
DDoS 攻擊需要大量的殭屍電腦，台灣是全球殭屍網路第 4 大國

老巴 發表於 2014年6月20日 10:02 | 收藏此文

g+1 60 讚 1,114



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 效能大提昇

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

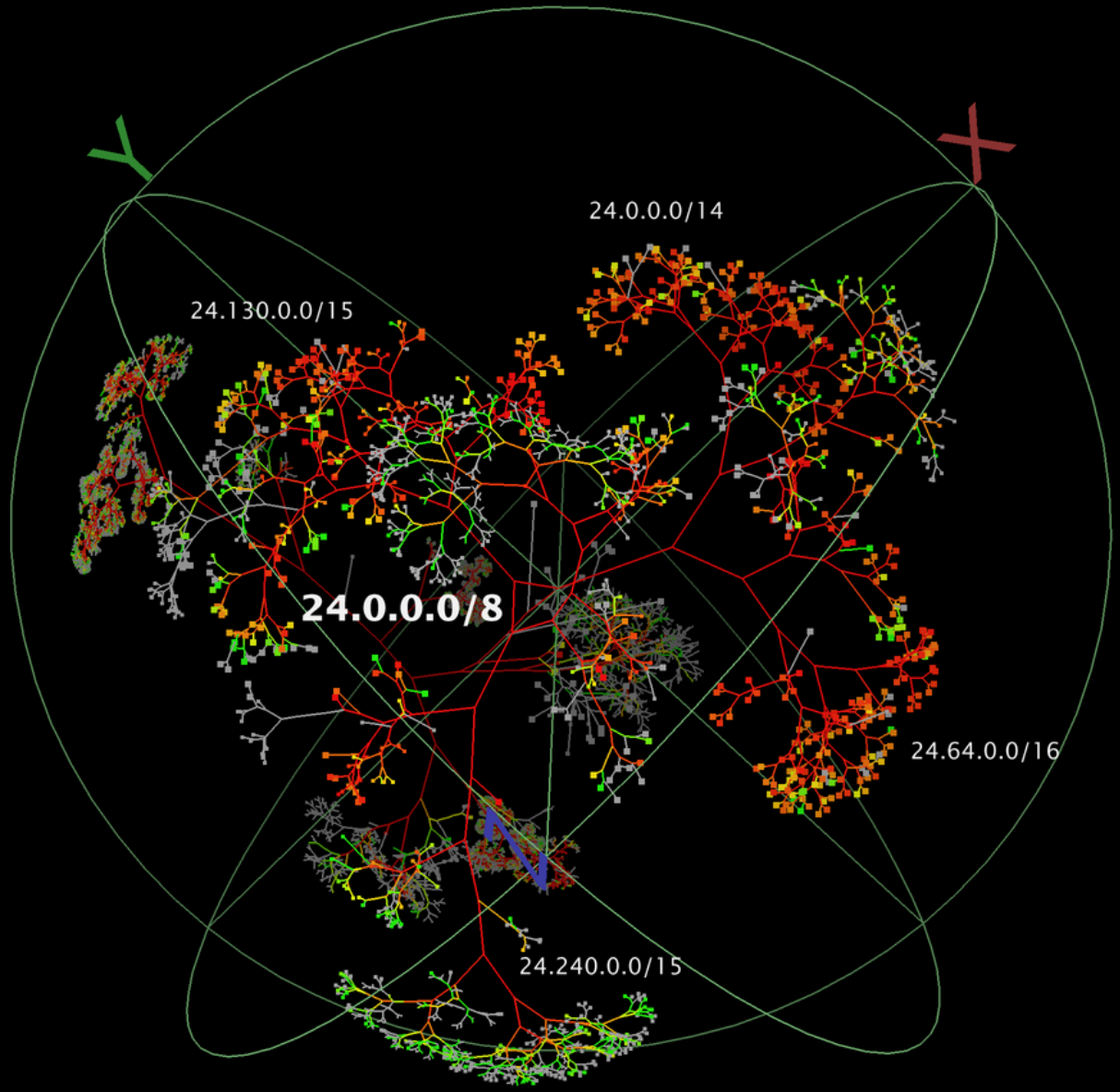
8/ Facebook 年度回顧，看看自己的 2013 年重要時刻

全民大亂鬥

李婧語 說：

全世界都留一手


美國國安局坦承不會公布所有漏洞資訊
www.ithome.com.tw/news/87299
iThome
美國國安局坦承不會公布所有漏洞資訊
美國總統特助暨美國白宮網路安全負責人Michael Daniel透過白宮部落格表示，他們會權衡是否揭露所發現安全漏洞的利弊得失，明白表示不一定會公布所有的漏洞訊息。
文/ 陳曉莉 | 2014-04-30 發表
9,687 按讚加入iThome粉絲團
分享 10
0
圖片來源: 維基共享資源；作者：NSA



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

VulReport

https://vulreport.net

VulReport

關於網站 積分排名 漏洞列表 新聞列表 聯絡我們 通報漏洞

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@8

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 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 第三六章 妨害電腦使用罪

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

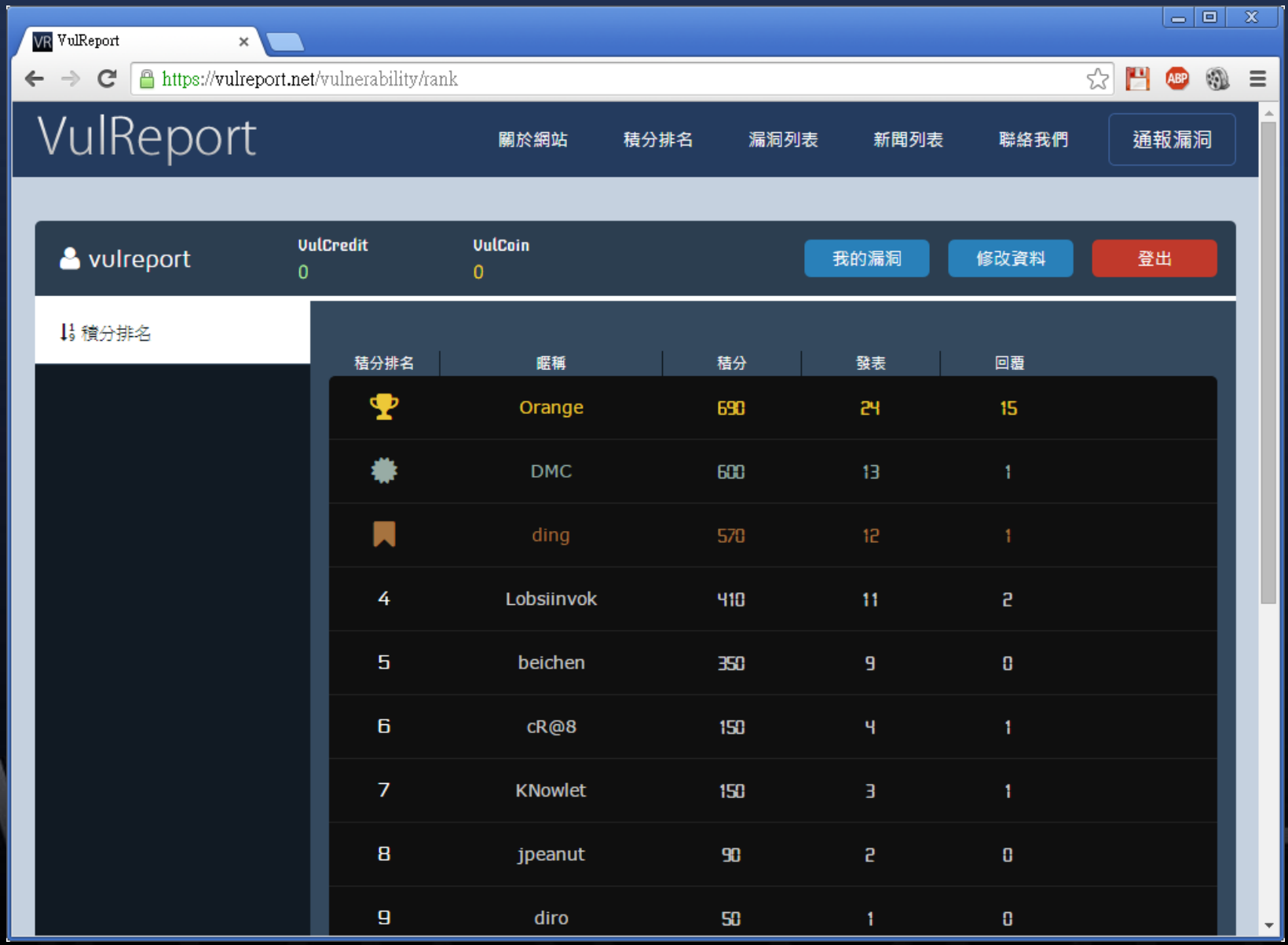
- 第 358 條
  無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
- 第 359 條
  無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。
- 第 360 條
  無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
- 第 361 條
  對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。
- 第 362 條
  製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

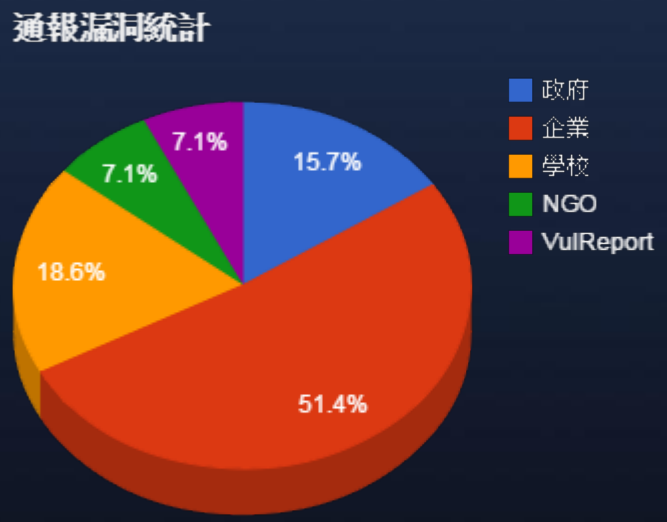
VulReport

漏洞積分排名 (2015⅛)



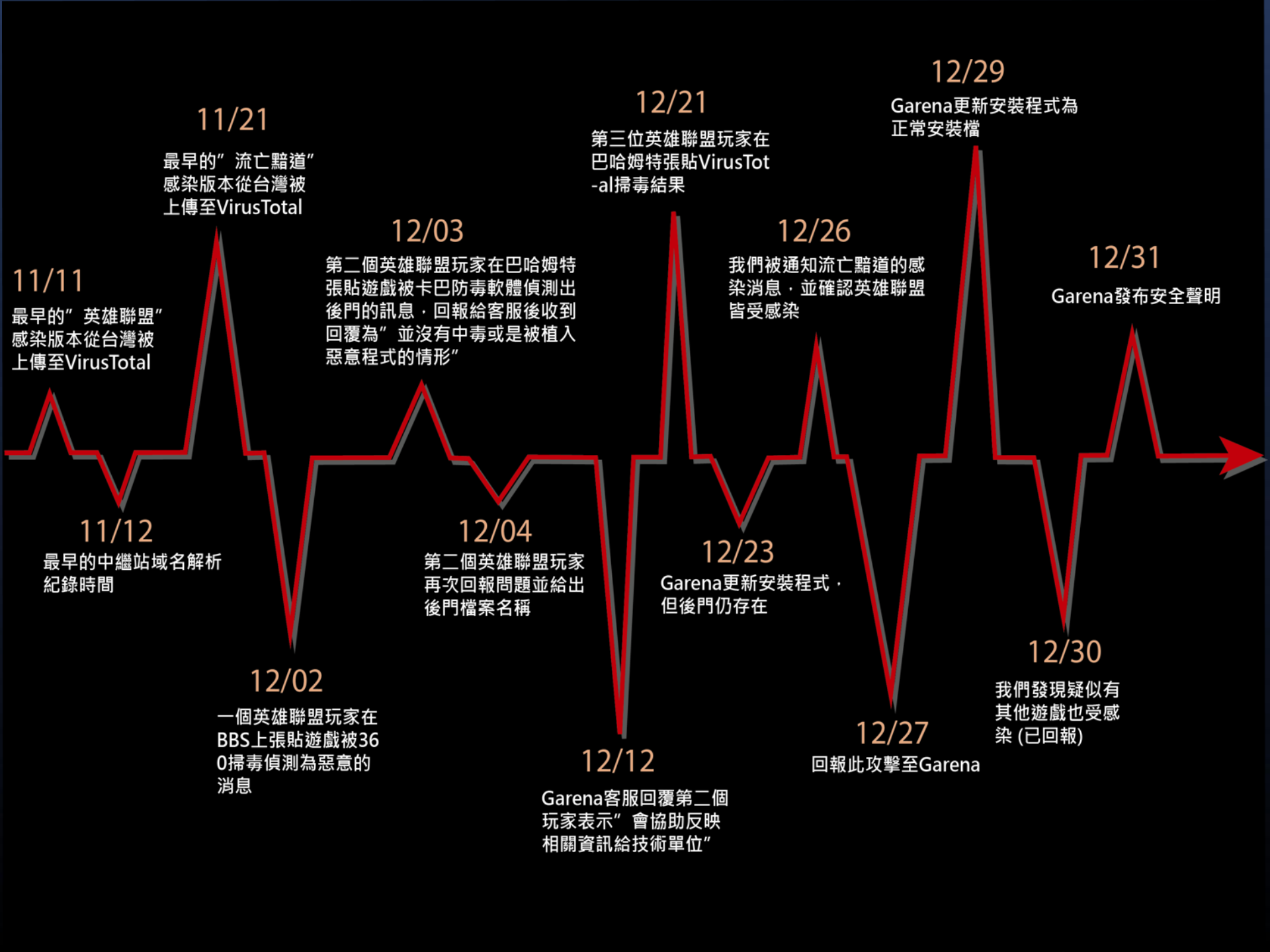
通報漏洞統計 (2015/1/8)

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

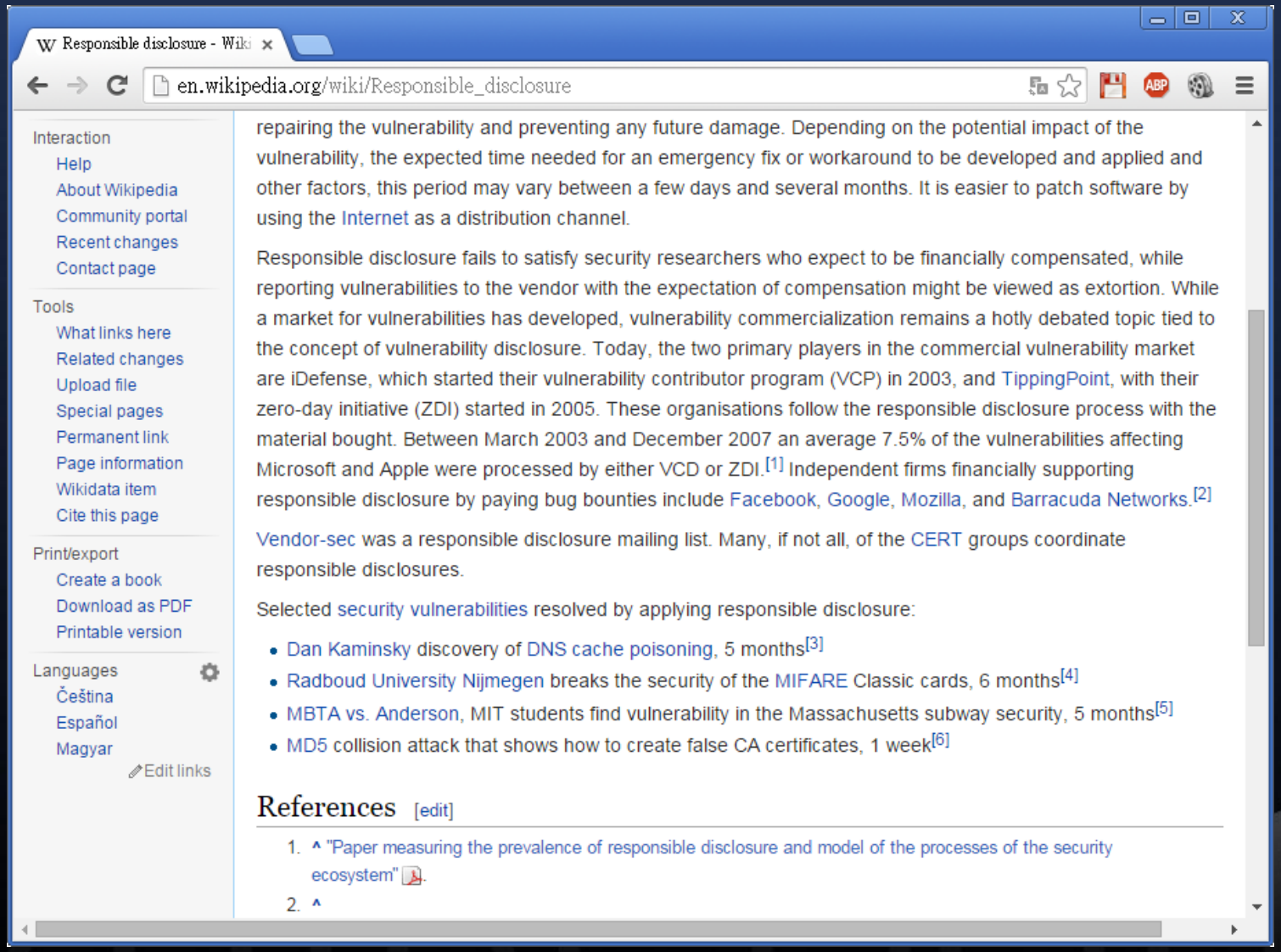


VulReport 企業帳號

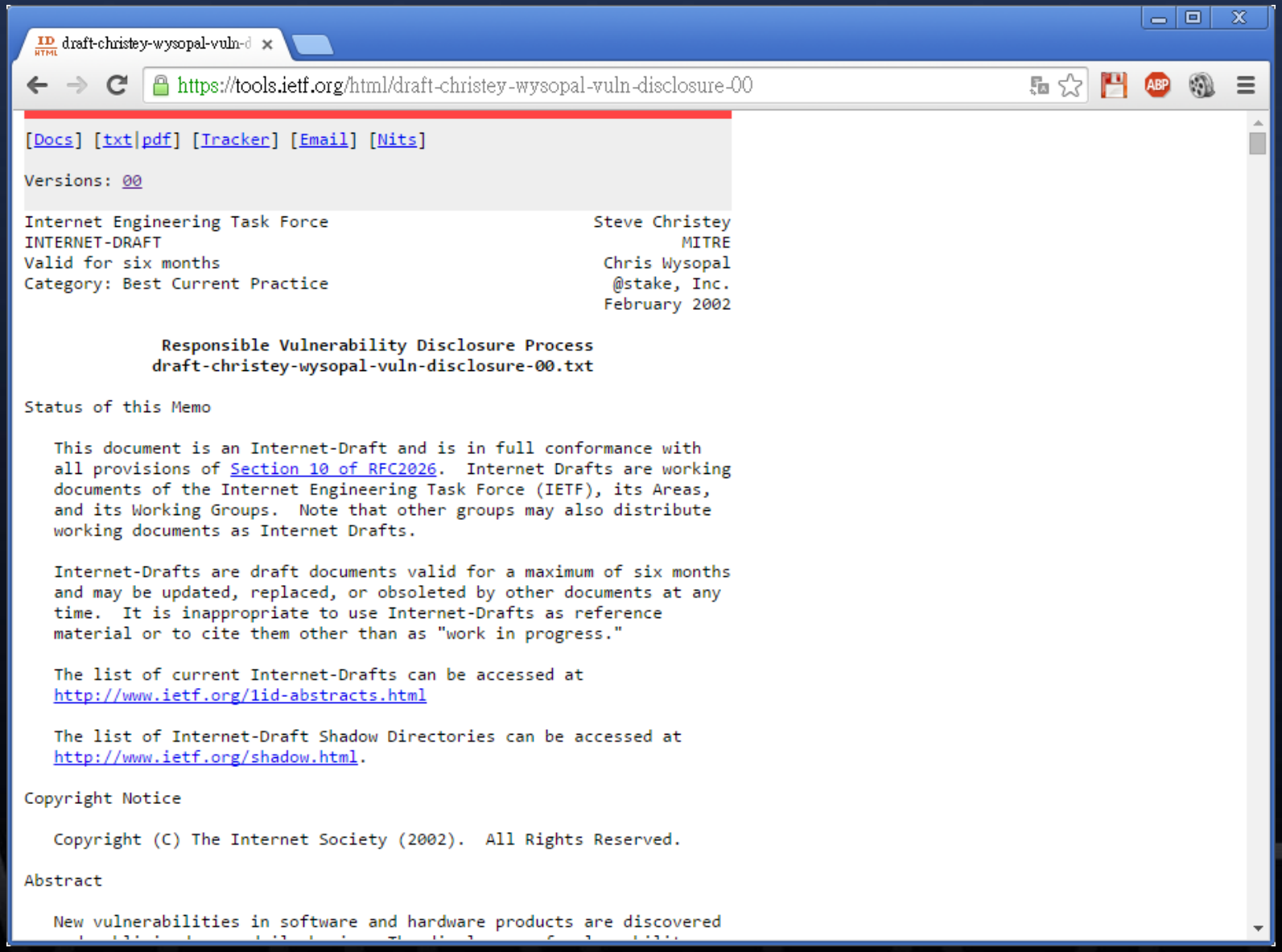
- 等級: 免費/正式/黃金/鑽石
- 優先通知漏洞通報
- 通報期限: 30/45/65/90
- 資安諮詢服務
- Logo連結
- 資安人才招聘
- 漏洞資訊提供研究
- 資安產品或服務推薦
- 對外服務檢測(研議中)
- 詳見: http://goo.gl/9cbFgN


11/11
最早的”英雄聯盟”感染版本從台灣被上傳至VirusTotal
11/12
最早的中繼站域名解析紀錄時間
11/21
最早的”流亡黯道”感染版本從台灣被上傳至VirusTotal
12/02
一個英雄聯盟玩家在BBS上張貼遊戲被360掃毒偵測為惡意的消息
12/03
第二個英雄聯盟玩家在巴哈姆特張貼遊戲被卡巴防毒軟體偵測出後門的訊息，回報給客服後收到回覆為”並沒有中毒或是被植入惡意程式的情形”
12/04
第二個英雄聯盟玩家再次回報問題並給出後門檔案名稱
12/12
Garena客服回覆第二個玩家表示”會協助反映相關資訊給技術單位”
12/21
第三位英雄聯盟玩家在巴哈姆特張貼VirusTot-al掃毒結果
12/23
Garena更新安裝程式，但後門仍存在
12/26
我們被通知流亡黯道的感染消息，並確認英雄聯盟皆受感染
12/27
回報此攻擊至Garena
12/29
Garena更新安裝程式為正常安裝檔
12/30
我們發現疑似有其他遊戲也受感染 (已回報)
12/31
Garena發布安全聲明

wiki - responsible disclosure



Responsible Vulnerability Disclosure Process

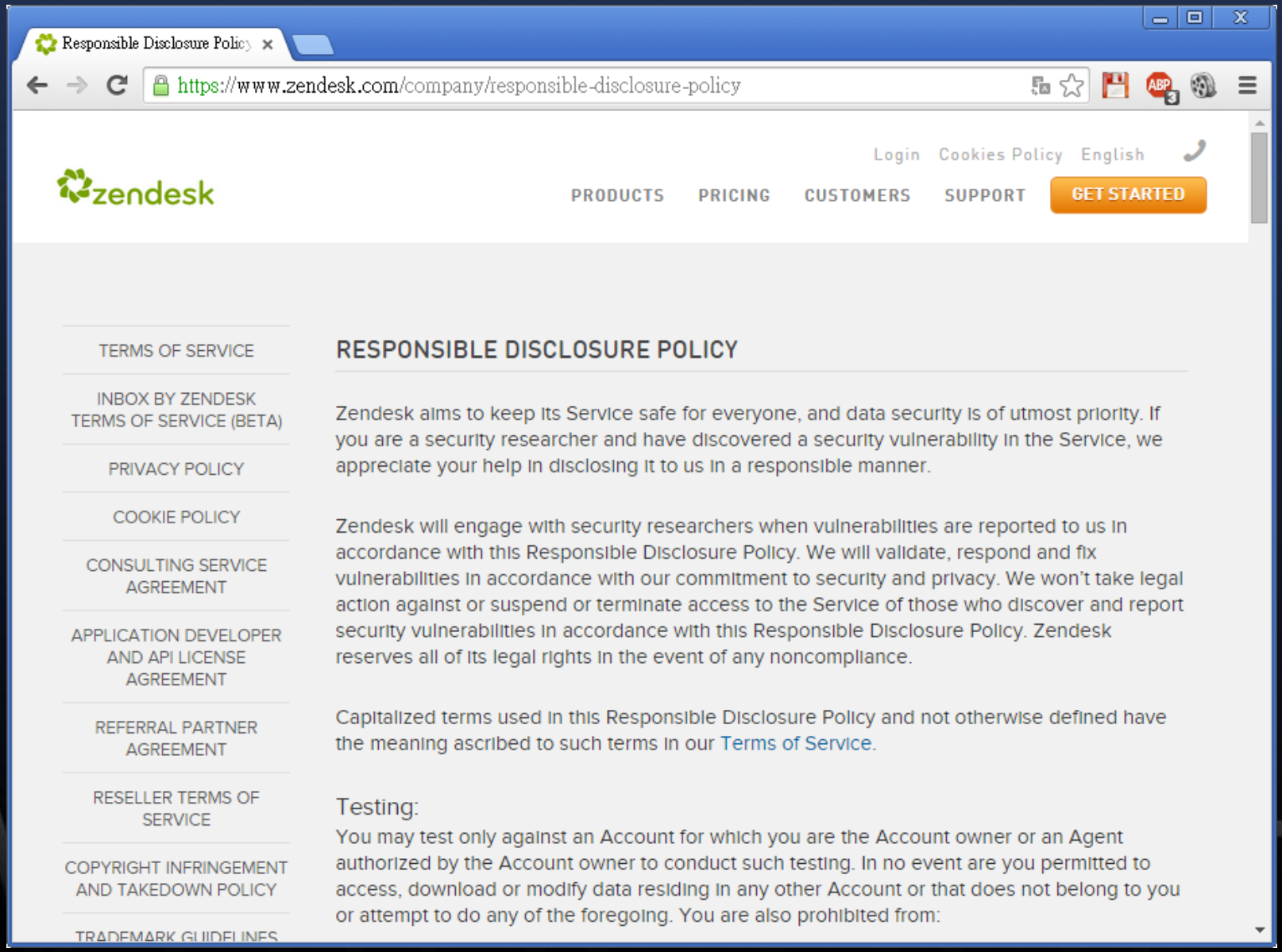


Security Response Center

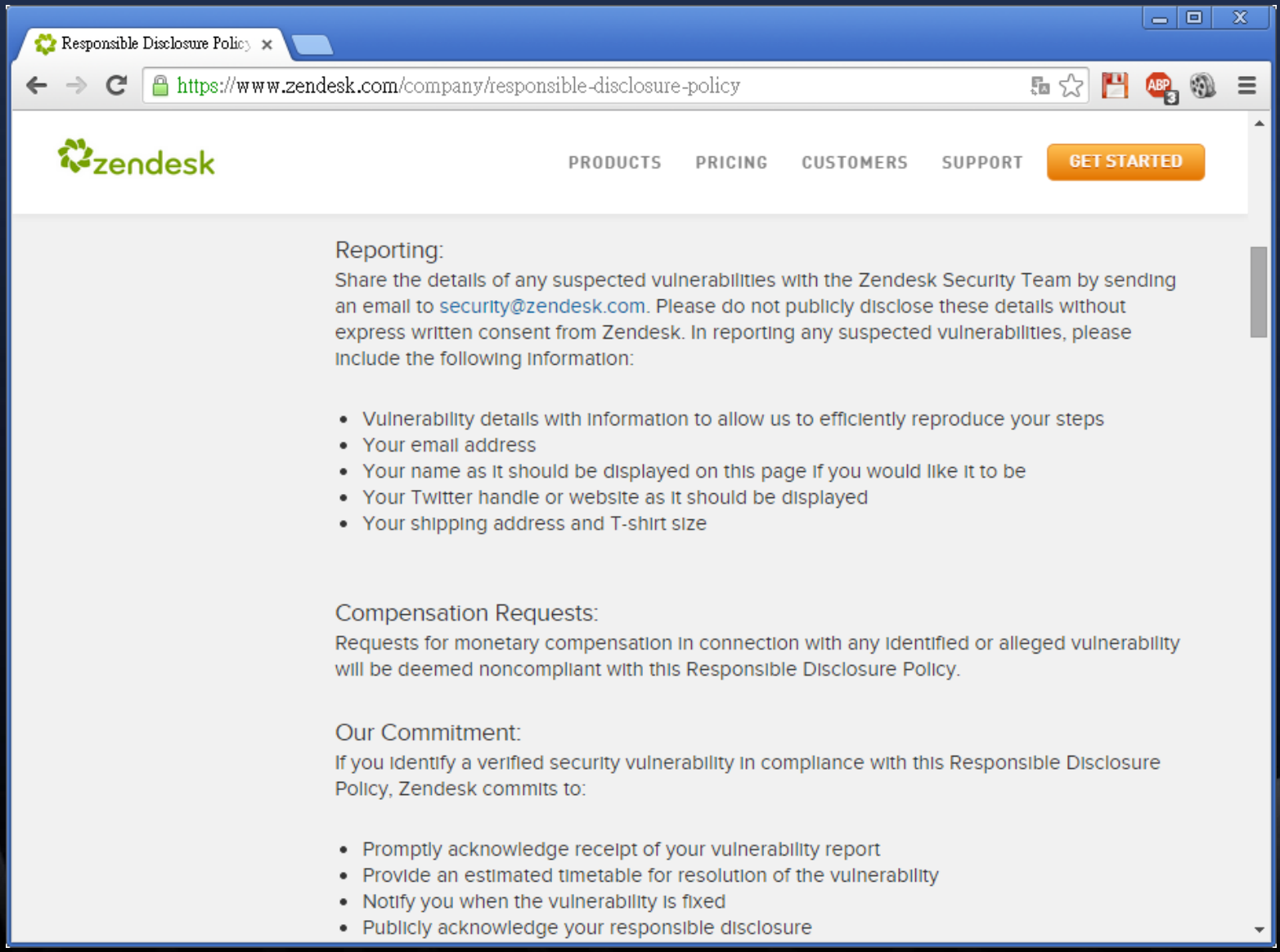
責任揭密政策 - Uber


Uber Security
https://www.uber.com/zh-TW/security
主選單
LEGAL
UBER
登入
註冊
使用者條款
隱私政策
版權
安全性政策
其他
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

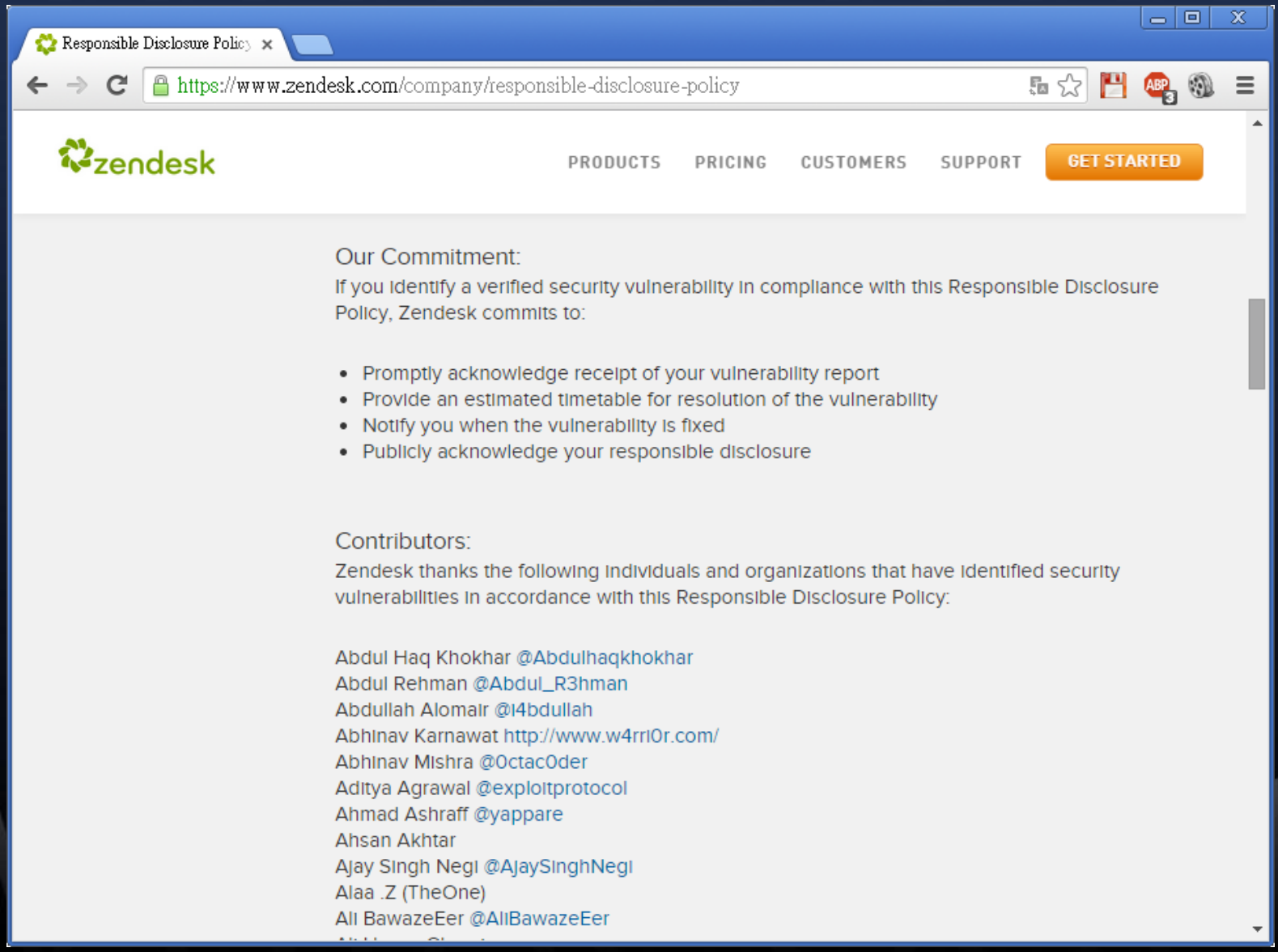
responsible disclosure policy -1



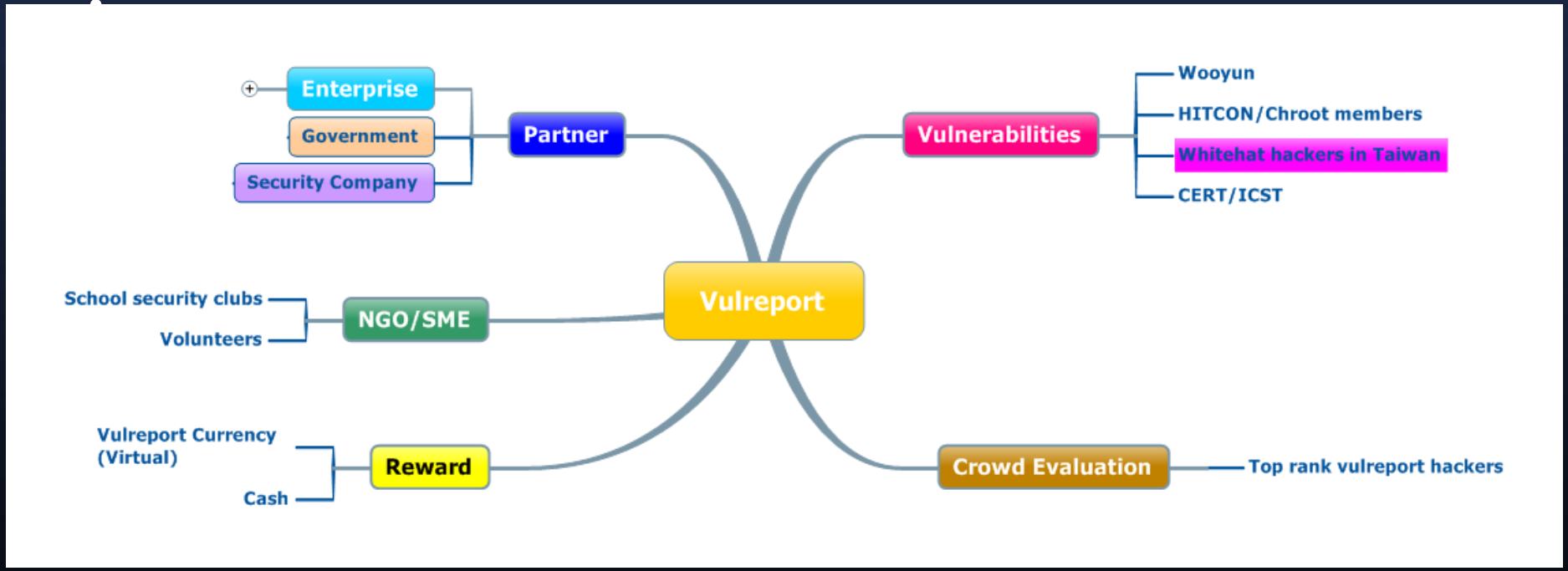
responsible disclosure policy -2



responsible disclosure policy - 3



VulReport 未來規劃




Happy Hackers ☺

VulReport

WEB: https://vulreport.net/
FB: facebook.com/vulreport

VulReport

Q&A