

# HITCON ZeroDay

## 年度報告

台灣駭客協會 HITCON ZeroDay

<https://zeroday.hitcon.org>

2018.07.27 HITCON Community

allenown@hitcon.org



# 講者簡介

翁浩正 (Allen Own)

[allenown@hitcon.org](mailto:allenown@hitcon.org)

戴夫寇爾 DEVCORE 執行長

台灣駭客協會 HITCON 常務理事





# ZeroDay

值得信賴的漏洞通報平台

## 最新消息

- 複測流程調整公告
- HITCON Community 2017 - ZeroDay 發表會
- 通報者修改漏洞通報功能上線
- Struts2 S2-045 漏洞預警 (CVE-2017-5638)
- 漏洞接受標準說明及改善建議

[更多...](#)

## 最新公開

- 演色印刷事業有限公司 任意檔案下載&弱密碼
- 無我茶會存在資料庫注入漏洞
- 國立臺灣大學圖書館電子期刊後台登入網站存在弱密碼
- 屏榮信鴿聯誼會存在MySQL注入漏洞
- 台中市建築人聯誼會存在資訊洩漏及目錄遍歷且可操作編輯器

[更多...](#)

# HITCON ZeroDay 介紹

- <https://zeroday.hitcon.org>
- HITCON ZeroDay 為社團法人台灣駭客協會所成立的公益計畫。宗旨在於協助資安專家與企業溝通互利，讓資安專家與企業站在同一陣線，共創資安環境的良好正循環。
- HITCON ZeroDay 於 2015 年底推出。透過可靠的漏洞通報平台，幫助企業有效處理和修補漏洞，亦令通報者得以即時獲知相關進度，打造彼此之間互信合作的溝通管道。



我們兩歲了！

感謝研發組、審核組、通報組志工們  
一起持續為台灣努力奮鬥！



讓漏洞成為你的助力



schneier.com

# Schneier on Security

Blog Newsletter Books **Essays** News Speaking Crypto About Me

[← MySpace Passwords Aren't So Dumb](#)     [Information Security and Externalities →](#)

## Schneier: Full Disclosure of Security Vulnerabilities a 'Damned Good Idea'

Bruce Schneier  
*CSO Online*  
January 2007

Full disclosure -- the practice of making the details of security vulnerabilities public -- is a damned good idea. Public scrutiny is the only reliable way to improve security, while secrecy only makes us less secure.

Unfortunately, secrecy *sounds* like a good idea. Keeping software vulnerabilities secret, the argument goes, keeps them out of the hands of the hackers (See [The Vulnerability Disclosure Game: Are We More Secure?](#)). The problem, according to this position, is less the vulnerability itself and more the information about the vulnerability.

But that assumes that hackers can't discover vulnerabilities on their own, and that software companies will spend time and money fixing secret vulnerabilities. Both of those assumptions are false. Hackers have proven to be quite adept at discovering secret vulnerabilities, and full disclosure is the only reason vendors routinely patch their systems.

To understand why the second assumption isn't true, you need to understand the underlying economics. To a software company, vulnerabilities are largely an externality. That is, they affect you -- the user -- much more than they affect it. A smart vendor treats vulnerabilities less as a software problem, and more as a PR problem. So if we, the user

### Search

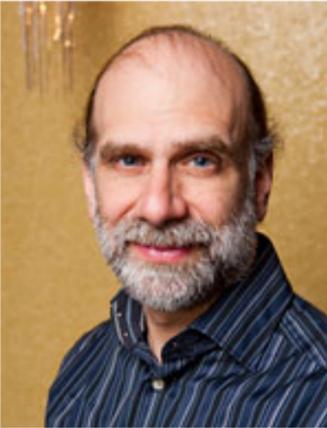
Powered by *DuckDuckGo*

blog  essays  whole site

### Subscribe



### About Bruce Schneier



I've been writing about security issues on my [blog](#) since 2004, and in my monthly [newsletter](#) since 1998. I write [books](#), [articles](#), and [academic papers](#). Currently, I'm the Chief Technology Officer of [Palo Alto Networks](#).

# HITCON ZeroDay 介紹



# 通報平台的任務

- 確認企業、通報者雙方溝通順暢
- 驗證漏洞確實存在
- 避免通報者將漏洞惡意利用
- 避免企業卸責不修正漏洞
- 給予通報者獎勵（credit、獎金）
- 給予企業尋才的管道
- 企業與資安廠商的媒合



# 功能特色 (通報者)

- 通報漏洞給企業
- 漏洞細節支援 Markdown 寫作
- 即時得知漏洞更新狀態
- 與企業私密訊息溝通
- 公開留言板討論
- 積分排行榜顯示貢獻程度



# 功能特色 (企業)

- 專屬企業帳號後台
- 即時得到最新漏洞
- 即時更新漏洞狀態
- 與 ZD 團隊或通報者私密訊息溝通
- 給予通報者獎勵
- (未來) 媒合資安廠商及資安人才



# 功能特色 (Open Data)

- RSS Feed 提供各種最新漏洞資訊訂閱
- API Interface 給予合作廠商串接資料



# News Feed

- 最新公開漏洞：

[https://zeroday.hitcon.org/rss/new\\_publish\\_vul](https://zeroday.hitcon.org/rss/new_publish_vul)

- 最新提交漏洞：

[https://zeroday.hitcon.org/rss/new\\_submit\\_vul](https://zeroday.hitcon.org/rss/new_submit_vul)

- 最新消息：

[https://zeroday.hitcon.org/rss/new\\_info](https://zeroday.hitcon.org/rss/new_info)



# 新功能！

- 更完善的企業後台
- 通報者協助企業複測
- 通報排行榜
- 漏洞獎勵計畫 (Bug Bounty Program)
- 私人訊息 (對個人、對企業)



- 漏洞列表
- 訊息
- 修改企業帳號使用者
- 修改企業資料
- 操作記錄

ZD-2017-00962 風險：低

# HITCON ZeroDay Reflected XSS

Reflected XSS

## 公開倒數

已公開

## 公開網址

倒數結束或將狀態設定為「公開」後，此漏洞通報的詳細資訊將會在這個網址被公開：  
<https://zeroday.hitcon.org/vulnerability/ZD-2017-00962>

## 漏洞狀態

公開

Last Update : 2017/11/05



## 處理歷程

- 2017/10/31 新提交 (由 Walter 設定)
- 2017/10/31 新提交 (由 Walter 設定)
- 2017/10/31 新提交 (由 Walter 設定)
- 2017/11/01 審核完成 (由 HITCON ZeroDay 服務團隊 設定)
- 2017/11/01 修補中 (由 HITCON ZeroDay 服務團隊 設定)
- 2017/11/01 已修補 (由 HITCON ZeroDay 服務團隊 設定)
- 2017/11/01 確認已修補 (由 HITCON ZeroDay 服務團隊 設定)
- 2017/11/05 公開 (由 HITCON ZeroDay 服務團隊 設定)



# ZeroDay

值得信賴的漏洞通報平台

## 最新消息及最新漏洞

### 最新消息

- HITCON Community 2017 - ZeroDay 發表會
- 通報者修改漏洞通報功能上線
- Struts2 S2-045 漏洞預警 (CVE-2017-5638)
- 漏洞接受標準說明及改善建議
- 暫停接受台灣以外地區漏洞通報

[更多...](#)

### 最新公開

- 台灣證券交易所 網頁標籤未過濾
- 國立臺灣大學圖書館電子期刊後台登入網站存在弱密碼
- 屏榮信鴿聯誼會存在MySQL注入漏洞
- 台中市建築人聯誼會存在資訊洩漏及目錄遍歷且可操作編輯器
- 四季百貨手機板存在資料庫注入漏洞

[更多...](#)



漏洞

消息

排行榜

企業

註冊 or

登入

# 排行榜

最新

歷史排行

總排行

## 歷史積分排行榜

所有通報者的漏洞通報積分排行

[2017](#) [[2018](#)]

[年度] [01](#) [02](#) [03](#)

1 **Nothattack**  
Anonymous Pingtung

2 **Elijia**  
VA

3 **taroballz**  
My github: <https://github.com/curtis992250>

4 **癡情法王**

5 **Mujihad**

6 **Sibe**  
春天的寂靜簡約日式雅房 與最親密好友共度安靜休閒氛圍



讓企業可以公告修復狀況，民眾也可以針對漏洞進行討論

## 留言討論

### 企業帳號

有關ZD-2017-01169的漏洞, 本公司評估內容如下:1. 依據證交所規劃, app.twse.com.tw預計於107年2月1日改版, 程式架構由PHP更動為Java, 舊版APP停止服務訊息已於106年12月底公告。2. 經本公司評估: 1)相關開發資源均專注於新版系統開發專案; 2)ZD-2017-01169漏洞相關資安風險評估為低; 3)ZD-2017-01169漏洞將隨舊版停止服務後消滅; 4)彙整以上資訊, 討論後決定暫不修補此漏洞。3. 在此感謝各位協助改善本公司網站資安漏洞, 降低遭駭風險, 亦請於新版系統上線後, 能持續協助本公司改善相關風險。

2018-02-01 12:12:35

[登入後留言](#)

聯絡廠商

向受通報的廠商取得聯繫，提供漏洞更詳細的資訊，或向廠商建議修復方式。

聯絡 ZeroDay

聯絡 ZeroDay 的管理人員，以尋求與此通報相關的協助。

## 通報者協助企業進行漏洞複測

### 複測結果回報

複測成功 ▼ 確認已修復！

請於此處選擇複測結果通知廠商。

[回報複測結果](#)

### 留言討論

Manager ▼

此處留言討論為公開區域，請避免洩漏個資、系統機敏資料、帳號密碼等。若要溝通通報細節請利用「訊息」功能。

[送出](#)

企業帳號是『免費』的！  
歡迎大家趕快註冊功能更完整～



# 合作對象

- HITCON
- TWCERT/CC
- TACERT
- 民間企業



zeroday.hitcon.org

漏洞 消息 企業 註冊 or 登入

### 漏洞

- 全部
- 活動中
- 修補中
- 公開
- WooYun

### 漏洞列表

用戶所提交的漏洞列表。

搜尋漏洞 通報漏洞

#### 活動中

ZD-2017-00694	審核完成	2017/08/25	Yovics
某單位 已遭改首頁 多處SQL Injection 多處XSS			
ZD-2017-00693	審核完成	2017/08/25	Yovics
某單位 多處SQL injection 多處XSS			
ZD-2017-00692	審核完成	2017/08/25	taroballz
某單位 公司存在MySQL時間延遲注入漏洞可登錄後台			
ZD-2017-00691	審核完成	2017/08/25	Mico
某單位 多個大學 商品購物合作網站(總主站) 檔案引入漏洞			
ZD-2017-00690	審核完成	2017/08/24	Bojack
某單位 教育單位 DNS 資訊洩漏			
ZD-2017-00472	已修補	2017/06/03	nacopark
某些學校 某單位 Broken Access Control			
ZD-2017-00601	已修補	2017/08/05	Racter
某單位 SQL錯誤訊息未攔截			
ZD-2017-00688	新提交	2017/08/24	

# 漏洞列表





漏洞

消息

企業

註冊 or

登入

漏洞

全部

活動中

修補中

公開

WooYun

ZD-2017-00533

財政部賦稅署

# 財政部賦稅署 任意下載檔案漏洞

任意下載檔案

## 處理狀態

公開

Last Update : 2017/08/06



新提交

已審核

已通報

已修補

公開

# 漏洞處理階段

收合完整歷程 ▲

2017/07/10 新提交 (由 鄉民 修改)

2017/07/10 新提交 (由 鄉民 修改)

2017/07/10 新提交 (由 鄉民 修改)

2017/07/10 審核完成 (由 HITCON ZeroDay 服務團隊 修改)

2017/07/10 修補中 (由 HITCON ZeroDay 服務團隊 修改)

2017/07/10 審核完成 (由 HITCON ZeroDay 服務團隊 修改)

# 漏洞詳細資訊



zeroday.hitcon.org

漏洞 消息 allenown

## 漏洞

全部  
活動中  
修補中  
公開

## 通報漏洞

告訴我們您所知道的漏洞

---

### 標題

簡述單位、漏洞名稱，如「OO 公司資料庫注入漏洞」

---

### 廠商

該漏洞單位的名稱

---

### 介紹

一句話簡述本漏洞為何

---

### 類型

選擇一個漏洞類型

▼

---

### 風險

該漏洞風險等級，嚴重、高、中、低、無風險

zeroday.hitcon.org/user/

漏洞 消息 企業 註冊 or 登入

### 使用者面板

通報漏洞列表

## 漏洞列表

用戶所提交的漏洞列表。

# 使用者提報漏洞列表

ZD-2017-00738	公開	電週文化事業股份有限公司(iThome)	2017/09/05
iThome 配置錯誤導致任意下載			
ZD-2017-00466	公開	台灣智慧服務股份有限公司	2017/07/16
Family Asyst IoT設備及伺服器弱點導致可控制任意設備			
ZD-2016-00311	公開	kktown	2017/02/23
kktown XSS			
ZD-2016-00062	公開	Openfind 網擎資訊	2016/09/20
Openfind 知名信箱儲存型XSS漏洞			
ZD-2016-00059	公開	pqi	2017/02/02
PQI無線Wi-Fi行動硬碟漏洞			
ZD-2016-00031	公開	openfind	2016/11/09
知名openfind信箱任意重置密碼漏洞			



漏洞列表

修改廠商資料

低 ZD-2017-00017 2017/03/18  
資訊洩漏  
新提交 公開：59天2小時

嚴重 ZD-2017-00001 2017/01/18  
測試公司遠端命令執行  
通報未回應 公開：30天0小時

# 企業後台：漏洞總覽

## 漏洞狀態

### 通報未回應

Last Update : 2017/03/18



漏洞狀態

✓ 修補中  
已修補  
公開

更新

### 處理歷程

2017/01/18 新提交 (由 HITCON ZeroDay 服務團隊 設定)

2017/01/19 審核完成 (由 HITCON ZeroDay 服務團隊 設定)

2017/01/19 審核中 (由 HITCON ZeroDay 服務團隊 設定)

2017/03/18 通報未回應 (由 HITCON ZeroDay 服務團隊 設定)

# 企業後台：漏洞狀態變更

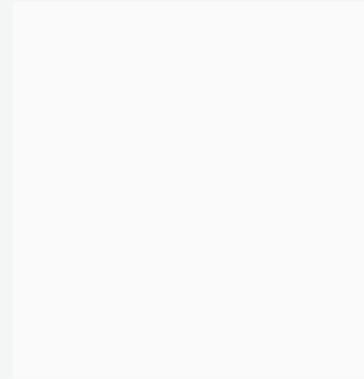


漏洞列表

修改廠商資料

於 xxx.com/login 處可直接執行系統指令，取得系統權限。

截圖



處理說明

**admin**

感謝通報，敝公司正修復該漏洞中。

2017-03-18 22:48:49

目前已修復完畢！

Comment

# 企業後台：漏洞處理說明留言



漏洞列表

訊息

修改企業帳號使用者

修改企業資料

ZD-2017-00001 風險：critical

## 測試公司遠端命令執行

[前往漏洞頁面](#)

我有一個問題想問 ZeroDay 團隊，本漏洞修復的方式可以如何進行？

2017-04-09 9:39:10

**HITCON ZeroDay**

您好，請您更新 framework 版本至 2.3.32 即可。

2017-04-10 23:41:22

我瞭解了，感謝貴單位的協助！

2017-04-11 10:57:39

發送

# 企業後台：與通報者聯繫





Admin



[發送私人訊息](#)



[以企業身份發送私人訊息](#)



[通報漏洞列表](#)

[排行榜](#)

[最新](#)

[歷史排行](#)

[資源](#)

[FAQ 常見問題](#)

[通報流程](#)

[ZeroDay](#)

[關於我們](#)

[服務條款](#)

# 私人訊息





Service

to me

11:23 PM (11 minutes ago)



您好，

我們是 HITCON ZeroDay 漏洞通報平台，為社團法人台灣駭客協會所籌組之公益計畫，協助企業進行資安漏洞之通報。

以下為貴單位之漏洞詳細內容如下，該系統存在遠端命令執行漏洞，攻擊者可直接取得系統權限，煩請協助處理。

漏洞編號：ZD-2017-00001

公開頁面：<https://zeroday.hitcon.org/vulnerability/ZD-2017-00001>

漏洞詳情：<https://zeroday.hitcon.org/private/XXXXXXXXXX>

查看密碼：iwucnkyo

問題網址：<http://xxx.com/login>

此外請容我們再次提醒您，基於平台之規範，一定時間後漏洞詳細內容便會公開，還請貴單位盡快修補，若有漏洞修復上之疑問，亦歡迎與我們連繫。

漏洞公開時間：2017-06-01

完成漏洞修補後，也麻煩您前往企業後台更新狀態，以利進行漏洞修補的複檢，感謝您的協助與配合。

--

Regards,

HITCON ZeroDay 計畫

HITCON ZeroDay 漏洞通報平台

社團法人台灣駭客協會公益計畫

# 漏洞通報信



# 企業帳號特點

- 漏洞及狀態自動通知

- 接獲貴企業之漏洞通報或漏洞狀態有所變更，系統皆將自動於第一時間寄信通知您所指定的聯繫窗口，節省原先等待人工作業的時間。

- 私密訊息對話視窗

- 由安全私密的對話視窗直接與漏洞通報者、ZeroDay 團隊溝通，更快地解決您在處理漏洞或使用平台上所遭遇的疑問。

- 更便利的漏洞管理

- 輕鬆切換漏洞修復狀態，亦能一目瞭然地追蹤貴企業相關漏洞之複審情形，為您省去與 ZeroDay 團隊信件往來所需的時間心力。

- 企業窗口變更

- 企業需調整聯繫窗口時，將可自行至企業帳號後台修改，無須另行寄信申請或認證，大幅提升便利性及安全性。



# 漏洞通報流程



# 2017 & 2018 年統計數據

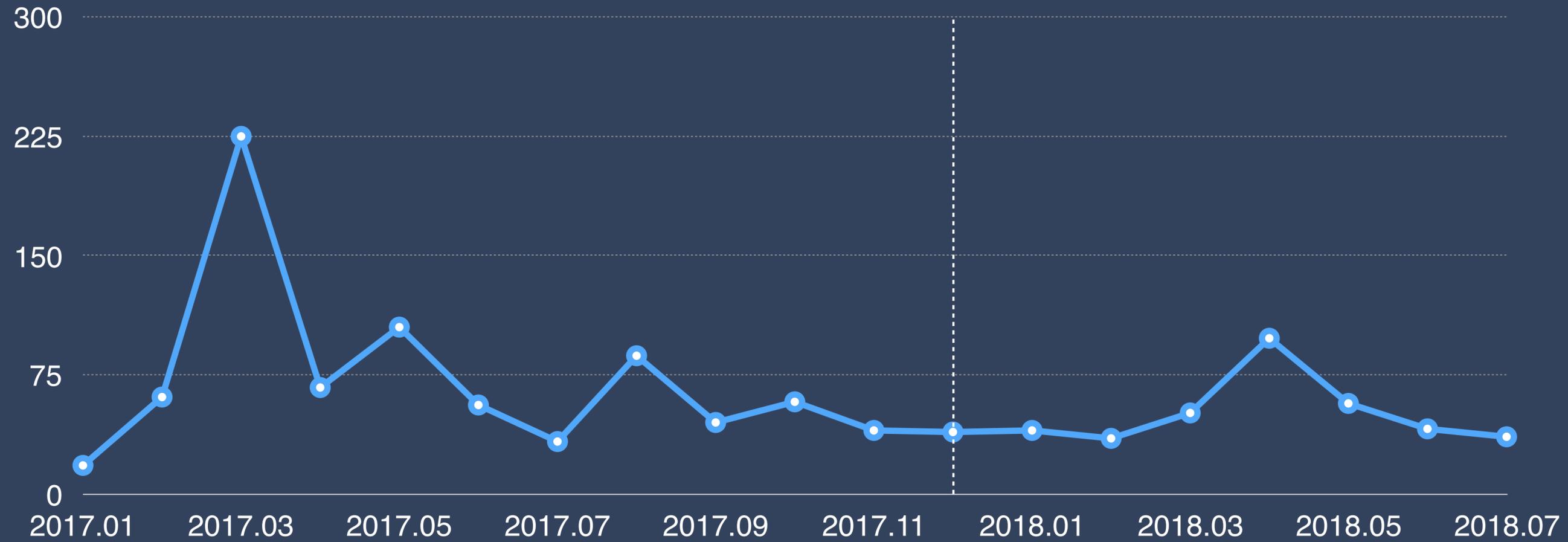


# 使用者、企業數量

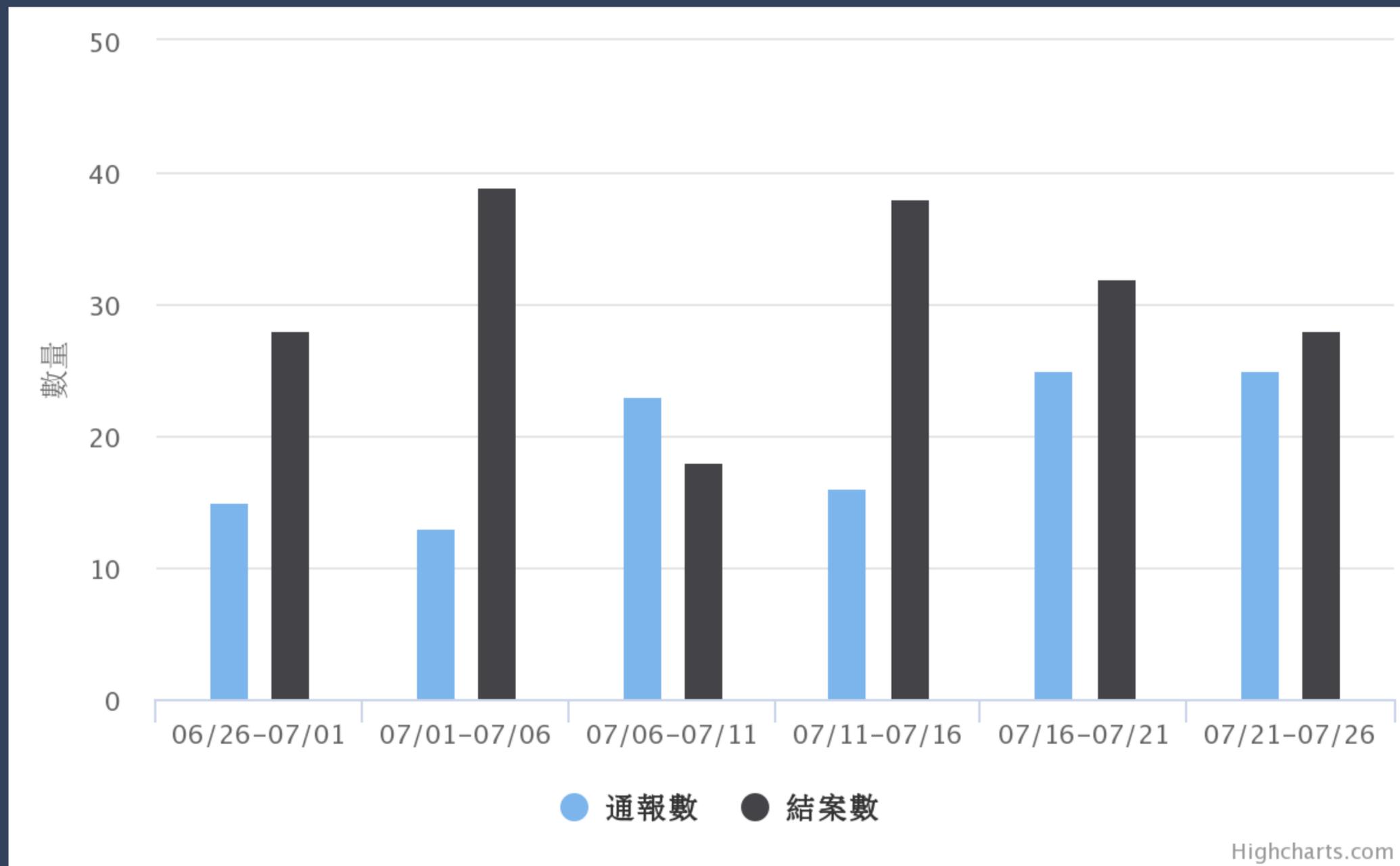
- 使用者數量：約 1,500 人
- 企業帳號數量：約 300 家
- 通報企業數量：約 2,300 家



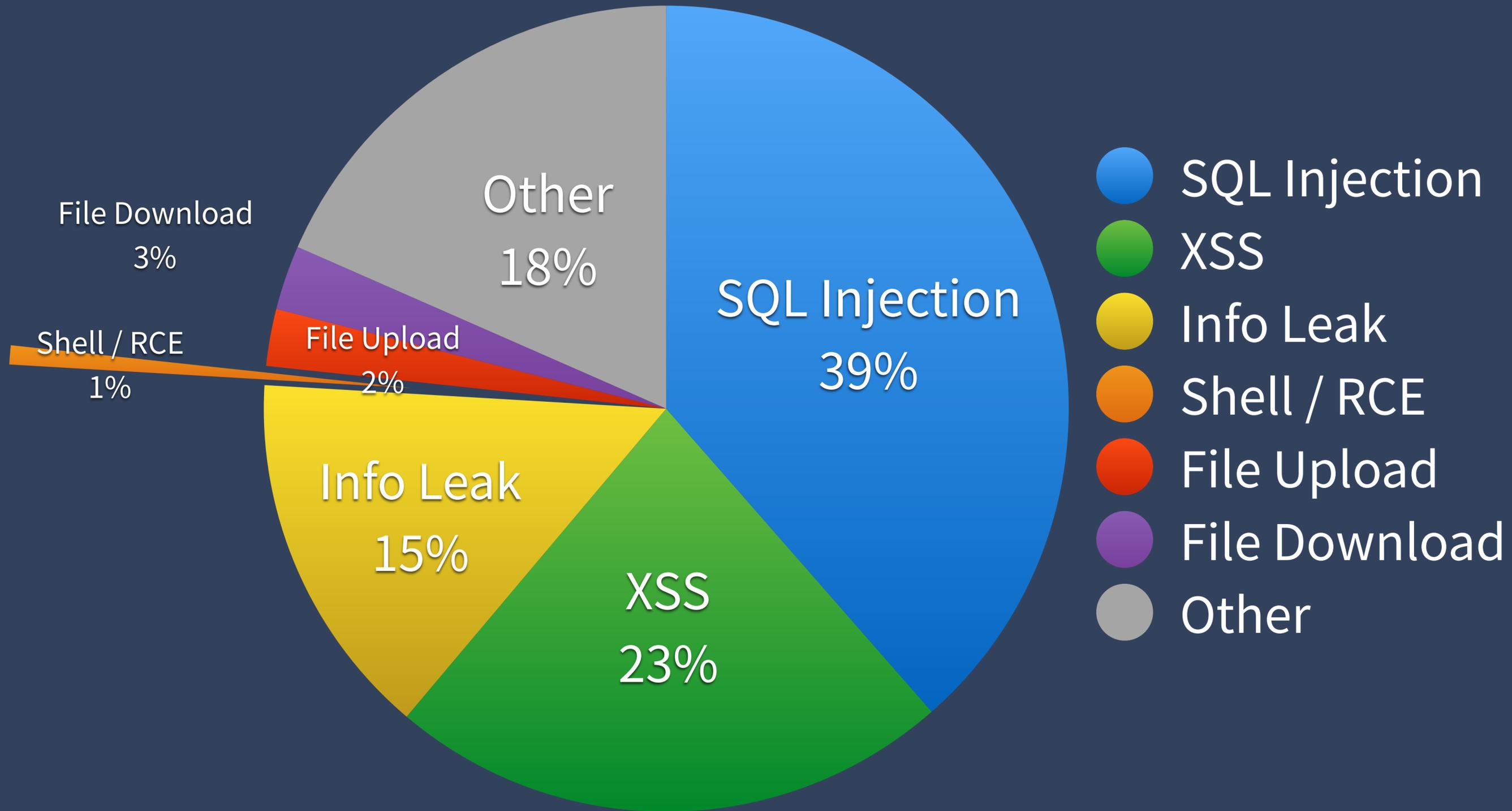
# 註冊人數



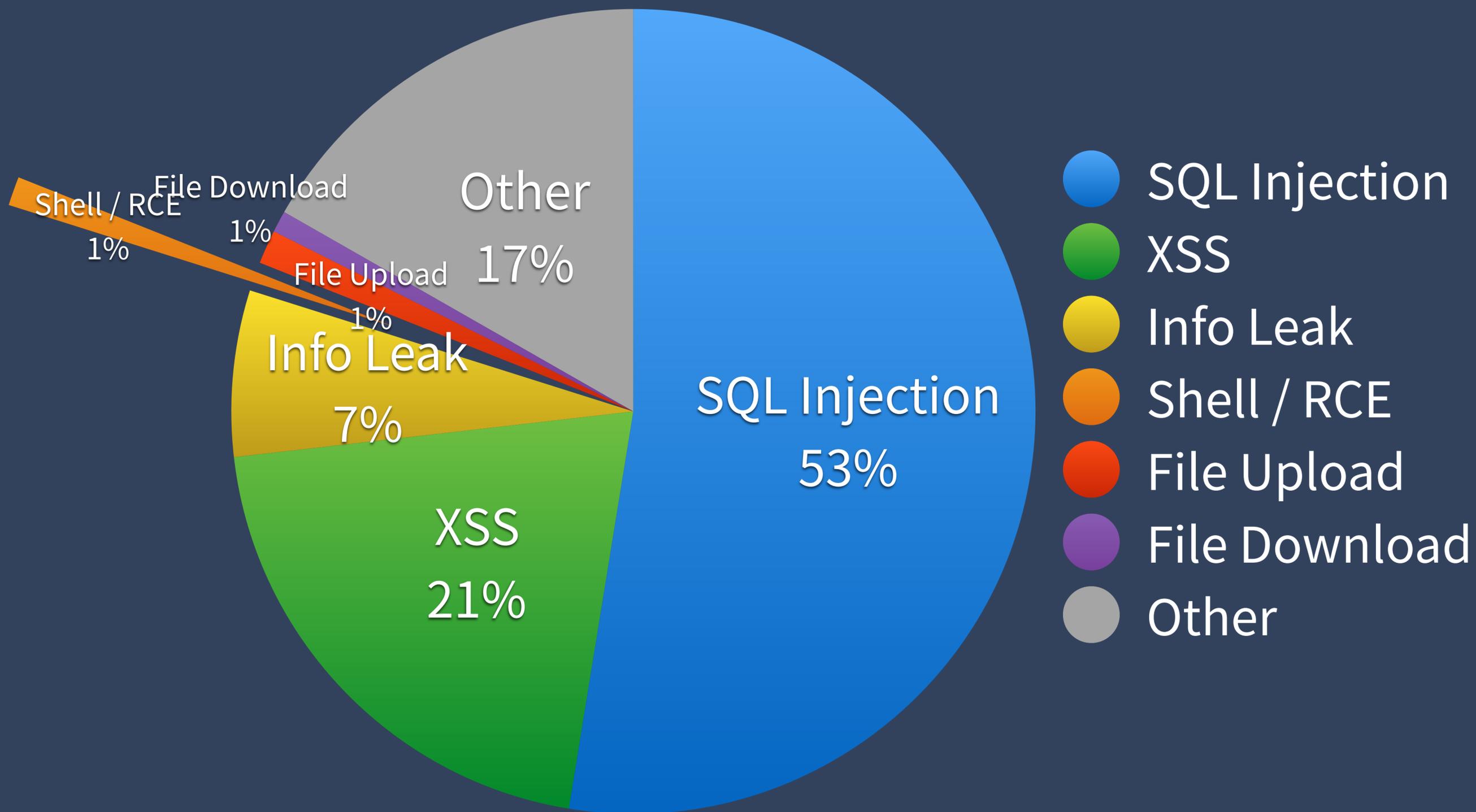
# 通報概況



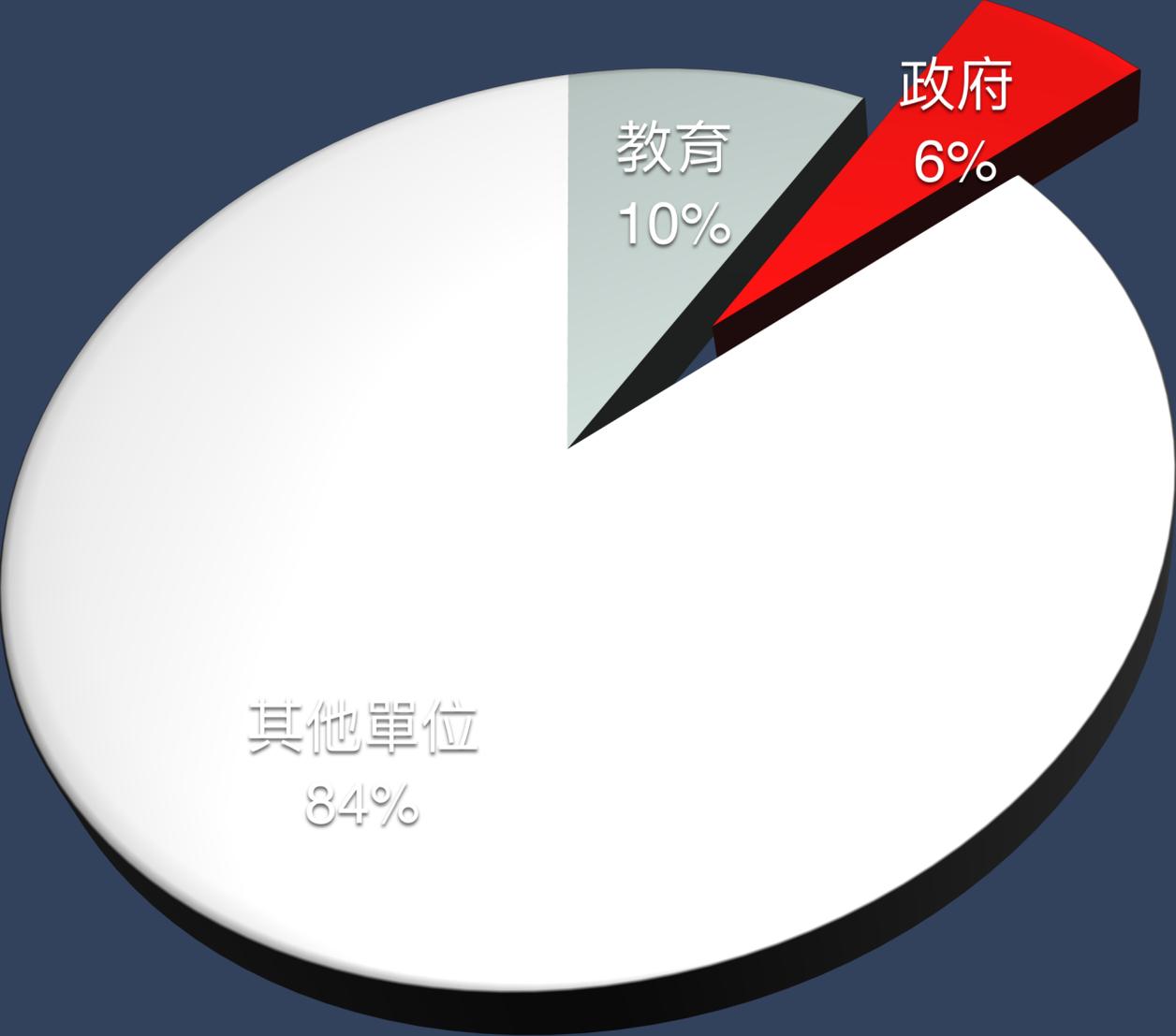
# 漏洞分類比例 (2017)



# 漏洞分類比例 (2018.01~now)



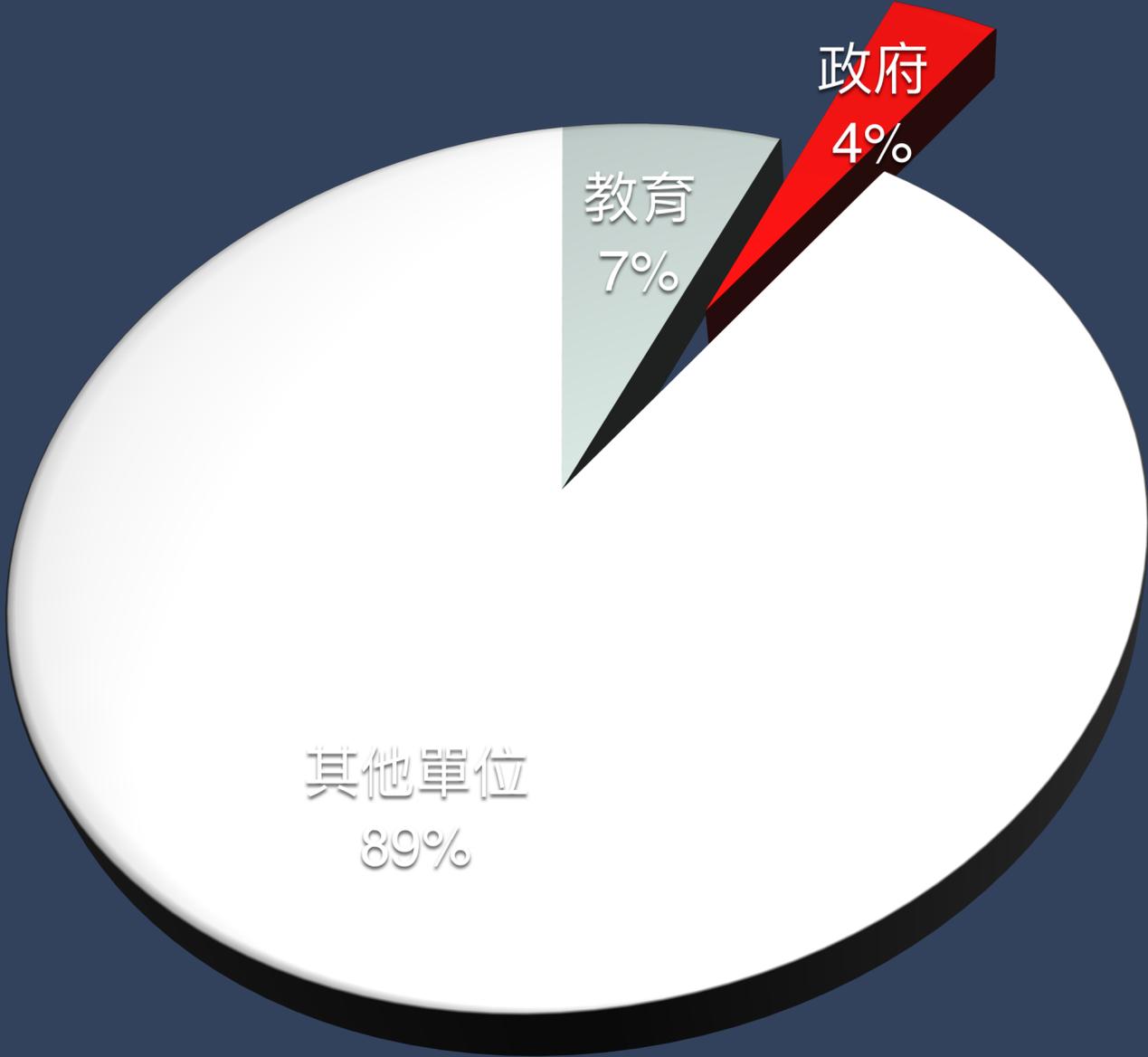
# 通報漏洞單位別 (2017)



資料來源: HITCON ZeroDay 2018.03.11



# 通報漏洞單位別 (2018)



資料來源: HITCON ZeroDay 2018.07.26



# 合作通報數據

- TWCERT/CC: 6 % (政府相關單位漏洞)
- TACERT: 10 % (部分教育單位)



# 其他數據

- 已修復後公開的漏洞數量：24.3%
- 漏洞數量 2016 -> 2017 成長 **245%**



# 2017 年通報漏洞趨勢分析



# 漏洞趨勢分析

- 多數網站仍完全沒有安全防護及安全程式碼開發，一攻就破
- SQL Injection , XSS 仍可一招打天下
- 企業修復漏洞過度依賴 WAF 等設備，沒有修復程式人員
- 依舊存在大量預設帳號密碼網站及設備
- 企業對於漏洞通報態度趨於積極，但仍大量企業沒有回應
- 企業修復漏洞僅修復單一點，其他地方仍存在漏洞
- 委外開發的團隊品質不佳，所有旗下專案皆有大量相同漏洞



# 沒有防護及安全開發，一攻就破

- `http://example.com/news.php?id=1`
- `http://example.com/news.php?id=1'` => 出錯
- `http://example.com/news.php?id=1<><script>alert(1)</script>`



# 過度依賴 WAF 等設備

- `news.php?id=1 or 1=1 %23`
- WAF 阻擋 `or 1=1`
- `news.php?id=1><script>alert(1)</script>`
- WAF 阻擋 `alert()`



# 依舊存在大量預設帳號密碼網站及設備



The screenshot shows a web browser window displaying a vulnerability report on the ZeroDay website. The URL in the address bar is [zeroday.hitcon.org/vulnerability/ZD-2018-00022](https://zeroday.hitcon.org/vulnerability/ZD-2018-00022). The page title is "ZD-2018-00022 中華電信轉通報窗口(HiNet)". The main heading is "中華電信 數據機設備無線網路可登入數據機管理端". Below the heading, a subtitle reads "嚴重者將SLID認證資訊清空將導致無法註冊網路(含PPPOE也會掛掉)". The "處理狀態" (Processing Status) section shows a vertical progress bar with four stages: "公開" (Public), "新提交" (New Submission), "已審核" (Reviewed), and "已修補" (Fixed). The "公開" stage is currently active, with a "Last Update : 2018/03/06" timestamp.

· <https://zeroday.hitcon.org/vulnerability/ZD-2018-00022>



# 企業對於漏洞通報態度趨於積極，但仍大量企業沒有回應

- 多數的通報還是遭遇石沈大海的結局...

## 處理狀態

公開

Last Update : 2018/03/12



# 企業修復漏洞僅修復單一點，其他地方仍存在漏洞

- <https://zeroday.hitcon.org/vulnerability/ZD-2017-01212>



# 開發團隊品質不佳，所有專案皆有相同漏洞

- <https://zeroday.hitcon.org/vulnerability/ZD-2017-00527>



The screenshot shows a web browser window with the URL [zeroday.hitcon.org/vulnerability/ZD-2017-00527](https://zeroday.hitcon.org/vulnerability/ZD-2017-00527). The page features a dark navigation bar with the site logo and menu items: 漏洞, 消息, 排行榜, 企業, 獎勵計劃, and a user profile for allenown. The main content area is white and displays the following information:

- 漏洞** (Vulnerability)
- 全部 (All)
- 活動中 (Active)
- 修補中 (Being Fixed)
- 公開 (Public)
- WooYun

The specific vulnerability details are:

- ZD-2017-00527** (linked)
- 易透網科技開發股份有限公司 (E透網科技開發股份有限公司)
- 易透網科技開發的所有網站資料庫注入漏洞 (SQL injection vulnerability in all websites developed by E透網科技開發股份有限公司)
- SQL injection

The **處理狀態** (Processing Status) section shows a vertical timeline with four stages:

- 公開** (Public) - Last Update : 2017/09/08
- 新提交 (New Submission)
- 已審核 (Reviewed)
- 已通報 (Reported)
- 未回報修補狀況 (No repair status reported)



# 開發團隊品質不佳，所有專案皆有相同漏洞

- <https://zeroday.hitcon.org/vulnerability/ZD-2017-00309>



The screenshot shows a web browser window with the URL [zeroday.hitcon.org/vulnerability/ZD-2017-00309](https://zeroday.hitcon.org/vulnerability/ZD-2017-00309). The page features a dark green navigation bar with a logo and menu items: 漏洞, 消息, 排行榜, 企業, 獎勵計劃, and allenown. The main content area is white and displays the following information:

- 漏洞** (Vulnerability)
- 全部 (All)
- 活動中 (Active)
- 修補中 (Being Fixed)
- 公開 (Public)
- WooYun

The main content area displays the vulnerability ID **ZD-2017-00309** and the source **雅普資訊社** (Yapuzhixun). The title is **OO 公司所製作的許多網站存在資料庫注入漏洞** (Many websites created by OO company have database injection vulnerabilities). The description is **該漏洞能爆出後台管理員帳號密碼** (This vulnerability can expose the administrator account and password).

The **處理狀態** (Processing Status) section shows a vertical red progress bar with four white circles. The status is **公開** (Public) in green text, with a last update date of **Last Update : 2017/05/11**. The progress bar is currently at the top, indicating the status is 'Newly Submitted' (新提交).

The progress bar has four stages:

- 新提交 (Newly Submitted)
- 已審核 (Reviewed)
- 已通報 (Reported)
- 已修補 (Fixed)



# 預設帳號密碼

- <https://zeroday.hitcon.org/vulnerability/ZD-2018-00022>



The screenshot shows a web browser window with the URL [zeroday.hitcon.org/vulnerability/ZD-2018-00022](https://zeroday.hitcon.org/vulnerability/ZD-2018-00022). The page features a dark navigation bar with the site logo and menu items: 漏洞 (Vulnerabilities), 消息 (Messages), 排行榜 (Ranking), and 企業 (Companies). The main content area is white and displays the following information:

- 漏洞 (Vulnerability):** A sidebar menu on the left lists categories: 全部 (All), 活動中 (Active), 修補中 (Patched), 公開 (Public), and WooYun.
- Header:** The vulnerability ID [ZD-2018-00022](#) and the target **中華電信轉通報窗口(HiNet)** are shown.
- Title:** **中華電信 數據機設備無線網路可登入數據機管理端**
- Description:** 嚴重者將SLID認證資訊清空將導致無法註冊網路(含PPPOE也會掛掉)
- 處理狀態 (Processing Status):** A vertical timeline shows the status progression:
  - 公開 (Public):** Last Update : 2018/03/06
  - 新提交 (New Submission)**
  - 已審核 (Reviewed)**
  - 已通報 (Reported)**
  - 已修補 (Patched)**



給企業的建議？



# 達成最低程度資安需求，找出問題

- 大型網站：滲透測試、紅隊演練
- 中小型網站：若無預算，僅安排弱點掃描、網頁安全掃描工具



做資安一定要花大錢嗎？

不一定，重點是戰略。

要瞭解不同的選擇，可以解決的問題是什麼。

別想著花弱點掃描的預算，就買到滲透測試的品質。



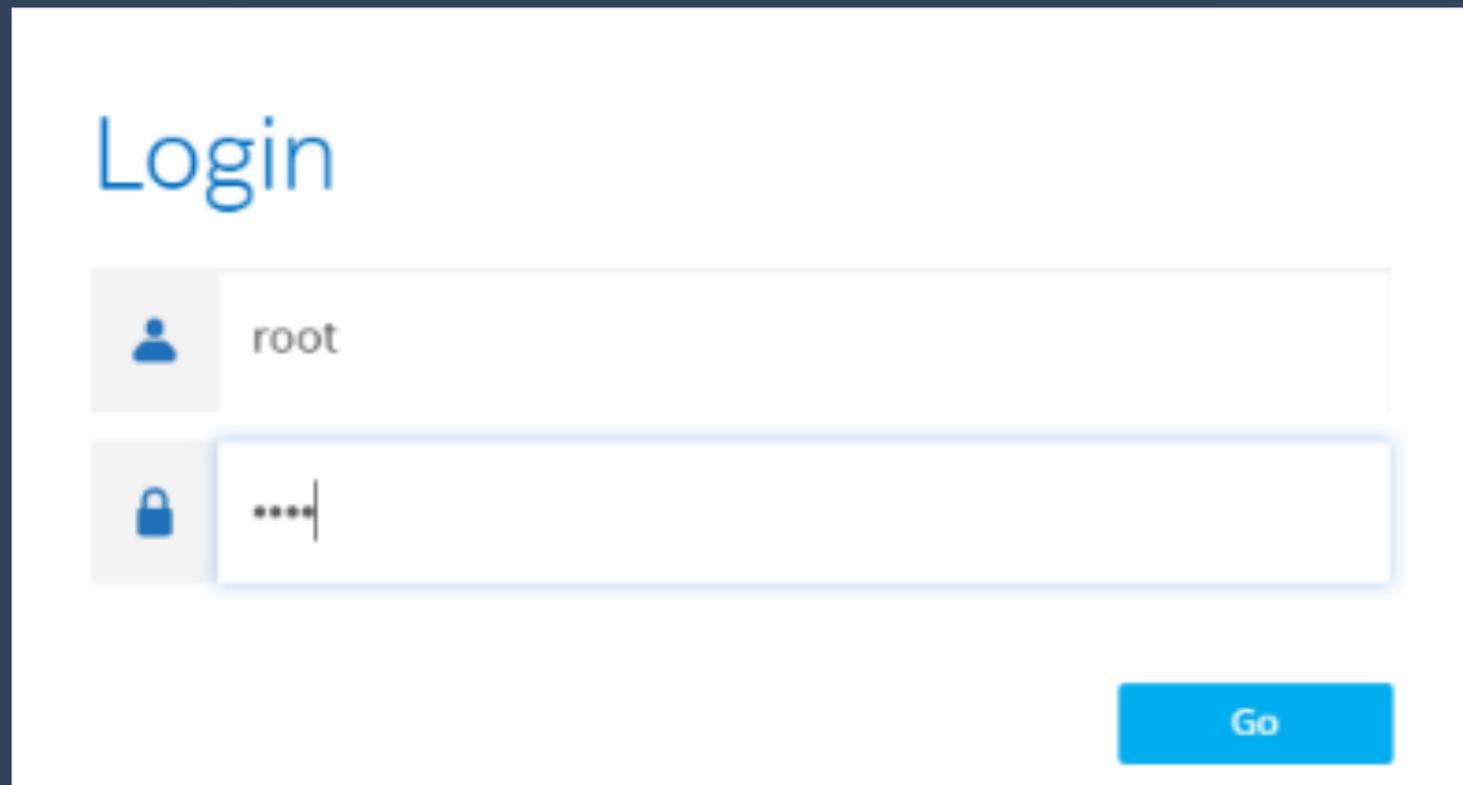
# 謹慎使用 WAF 等防禦設備

- 防禦設備並非萬能，不要被廠商的話術誘導了！
- 網站修補漏洞的時間差，可用 WAF 等設備暫時擋下前幾波攻擊
- 記住攻擊者仍擁有各種繞過防禦偵測的手法！



# 修改預設密碼

- 網頁套件、伺服器、各類設備，務必修改預設密碼
- 攻擊思維第一步就會嘗試預設密碼，登入管理介面



Login

Go

No more admin / admin!



# 慎選委外團隊

1. 委外開發的合約中明訂驗收項目包含資安檢測，並且限制開發團隊必須制訂資安漏洞修補計畫。
2. 委外團隊如有不良記錄，例如大量相同漏洞不斷被發現，且修補態度不佳，應另擇團隊。
3. 在驗收時以及定期進行安全檢測掃描，確認網站不會因淺而易見的漏洞而被入侵。



# 漏洞通報並非完整檢測，防護要靠自己

- 收到漏洞通報時，不少企業僅會修復通報點，而不會全盤檢
- 通報者不是檢測單位，不會幫你檢測整個網站！
  
- 相同的程式撰寫邏輯缺陷，在其他地方也會發生！  
接到通報後，建議針對整個網站相同處進行全盤檢視。



# 利用平台與通報者密切溝通

- 通報者最瞭解漏洞，可以多利用平台功能跟通報者溝通



The screenshot displays a web interface for a company named "測試股份有限公司" (Test Co., Ltd.). The top navigation bar includes the company name and an "Admin" user profile. A sidebar on the left lists navigation options: "漏洞列表" (Vulnerability List), "訊息" (Messages), "修改企業帳號使用者" (Modify Enterprise Account User), and "修改企業資料" (Modify Enterprise Information). The main content area shows a specific vulnerability entry with ID "ZD-2017-00001" and a risk level of "critical". The title of the entry is "測試公司遠端命令執行" (Test Co. Remote Command Execution). Below the title, there is a chat interface with three messages:

- Message 1 (User): "我有一個問題想問 ZeroDay 團隊，本漏洞修復的方式可以如何進行?" (I have a question for the ZeroDay team, how can the way of fixing this vulnerability be carried out?) - 2017-04-09 9:39:10
- Message 2 (HITCON ZeroDay): "您好，請您更新 framework 版本至 2.3.32 即可。" (Hello, please update the framework version to 2.3.32.) - 2017-04-10 23:41:22
- Message 3 (User): "我瞭解了，感謝貴單位的協助!" (I understand, thank you for your assistance!) - 2017-04-11 10:57:39

A "發送" (Send) button is visible at the bottom right of the chat area.



# 建立讓通報更順暢的環境

- 配置專門資安聯繫窗口，並明列於網站上。
- 檢查 whois、官網聯絡信箱及電話是否正常。
- 針對漏洞即時應變，建立 SOP。
- 修補完成即時回報通報平台，以完成通報流程。



給通報者的建議？



# 清楚的說明漏洞所在

- 清楚的說明、相關網址、攻擊 Payload、截圖缺一不可
- <https://zeroday.hitcon.org/vulnerability/ZD-2017-00716>
- <https://zeroday.hitcon.org/vulnerability/ZD-2018-00015>
- <https://zeroday.hitcon.org/vulnerability/ZD-2018-00034>



# 清楚的漏洞描述

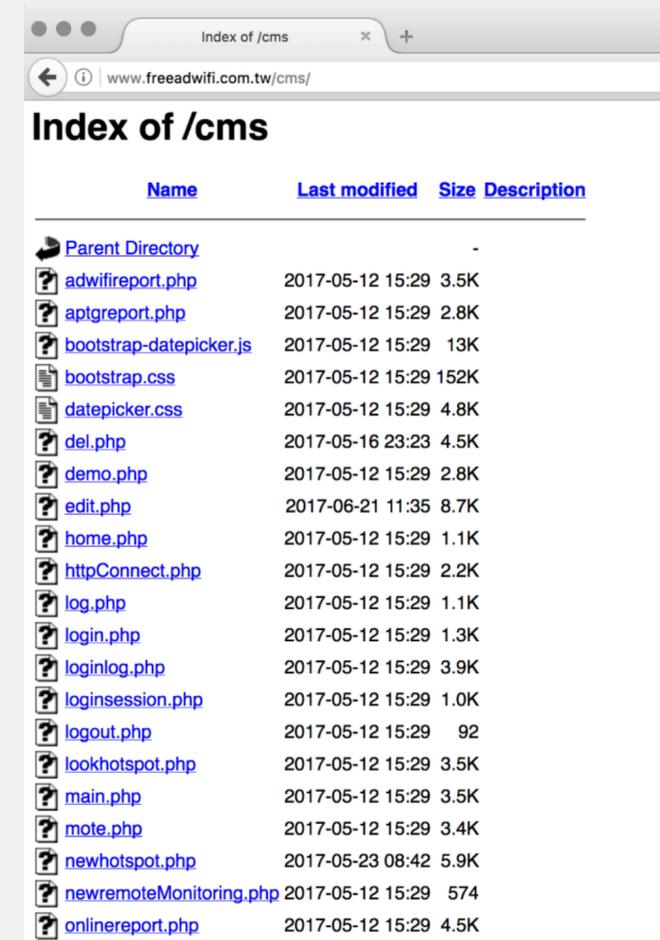
## 相關網址

```
http://www.freedwifi.com.tw/  
http://www.freedwifi.com.tw/cms/  
http://www.freedwifi.com.tw/runtime/  
http://www.freedwifi.com.tw/runtime/output/look.php  
http://210.200.141.50/monitoring/look.php
```

## 敘述

最近常常帶著沒關機的 macbook 搭捷運，回到家發現瀏覽器都是捷運 WiFi 的登入頁面且在沒有連接捷運 WiFi 時，仍可存取 <http://www.freedwifi.com.tw/> 因此做了些簡單測試，並發現多個 WiFi 系統漏洞

- 未關閉 Directory Listing  
管理系統:  
<http://www.freedwifi.com.tw/cms/>



Name	Last modified	Size	Description
Parent Directory	-	-	-
adwifireport.php	2017-05-12 15:29	3.5K	
aptgreport.php	2017-05-12 15:29	2.8K	
bootstrap-datepicker.js	2017-05-12 15:29	13K	
bootstrap.css	2017-05-12 15:29	152K	
datepicker.css	2017-05-12 15:29	4.8K	
del.php	2017-05-16 23:23	4.5K	
demo.php	2017-05-12 15:29	2.8K	
edit.php	2017-06-21 11:35	8.7K	
home.php	2017-05-12 15:29	1.1K	
httpConnect.php	2017-05-12 15:29	2.2K	
log.php	2017-05-12 15:29	1.1K	
login.php	2017-05-12 15:29	1.3K	
loginlog.php	2017-05-12 15:29	3.9K	
loginsession.php	2017-05-12 15:29	1.0K	
logout.php	2017-05-12 15:29	92	
lookhotspot.php	2017-05-12 15:29	3.5K	
main.php	2017-05-12 15:29	3.5K	
mote.php	2017-05-12 15:29	3.4K	
newhotspot.php	2017-05-23 08:42	5.9K	
newremoteMonitoring.php	2017-05-12 15:29	574	
onlinereport.php	2017-05-12 15:29	4.5K	

連線報表記錄:  
<http://www.freedwifi.com.tw/runtime/>

ZD-2017-00716 臺北大眾捷運股份有限公司  
台北捷運 WiFi 管理系統多個漏洞

Directory Listing, Login Bypass, Directory Traversal, XSS 等多個漏洞

## 處理狀態

公開

Last Update : 2017/10/08



[點此顯示完整的處理歷程](#) ▼

<https://zeroday.hitcon.org/vulnerability/ZD-2017-00716>



# 不好的示範

- 審核組及企業難以知道想表達什麼意思

## 相關網址

http://[REDACTED]

## 敘述

HTTP GET

## 留言討論

Manager

此處留言討論為公開區域，請避免洩漏個資、系統機敏資料、帳號密碼等。若要溝通通報細節請利用「訊息」功能。

送出



# 修補建議

- 給予企業的建議非常重要，可以讓企業往正確的方向修補漏洞

## 敘述

[http://www.nippon-paint.com.tw/product.php?id=50'](http://www.nippon-paint.com.tw/product.php?id=50)

測試在變數後面加上單引號，會出現 MySQL error message，如圖一，有使用 `mysql_real_escape_string()`

<http://www.nippon-paint.com.tw/product.php?id=50> union select 1,2,3,4,5,6,7,8 --

圖二、圖三，測試出此 table 有幾個欄位

<http://www.nippon-paint.com.tw/product.php?id=0> union select 1,@@version,3,4,5,6,user(),@@datadir--

在某些可見欄位上插入想取得的資訊，例如：MySQL version、檔案位置等，如圖四

`sqlmap -u "http://www.nippon-paint.com.tw/product.php?id=50" --tables`

用 sqlmap 可以掃出他的 db 及 table，如圖五

## 修補建議

由於已有使用 `mysql_real_escape_string()`，建議再將變數做轉型，變數可以以 string 接收，再轉型為 integer，最後再丟入 sql 語句進入資料庫。



# 複測漏洞

- 當企業提出需求，可幫助企業瞭解漏洞是否正確的修復完畢

聯絡廠商

向受通報的廠商取得聯繫，提供漏洞更詳細的資訊，或向廠商建議修復方式。

聯絡 ZeroDay

聯絡 ZeroDay 的管理人員，以尋求與此通報相關的協助。

## 複測結果回報

複測成功



確認已修復！

請於此處選擇複測結果通知廠商。

回報複測結果



# 年度最佳貢獻



1   路西菲爾  
>< Coding

2   Mujihad

3   癡情法王

4  Elija  
Vulnerability Assesment

5  IForgetMyName  
MyNameIsLee(我覺得應該可能是吧?)

6  faded

7  (就只知道抄襲，還會什麼!)By Sibe  
<http://bluesnow.strikingly.com/> 我是一個永遠不曾被感謝的黑客

8  Amos

9  Hzlaga

10  cra5h  
漏洞水准过低啥也没学到



# Bug Bounty Program

## 漏洞獎勵計畫！





# 漏洞獎勵計畫

讓漏洞成為您的助力



企業在面對不斷出現的資安威脅時，往往是很辛苦的歷程。若能夠在被攻擊前，先一步修補該漏洞，將可以避免不必要的損失。我們很清楚企業的困境，更知道資安專家需要的是什麼，「漏洞獎勵計畫 Bug Bounty Program」因而成立。

企業用戶可以根據每則漏洞通報的嚴重性、對企業的幫助，給予通報者適度的獎勵，如獎金、感謝函、公開表揚等。除了彰顯企業對於資安的重視之外，更能讓資安專家感到被重視，進而持續為企業回報，避免漏洞流至黑色產業。若企業想要擴大漏洞獎勵計畫，更可以自行在獨立頁面舉辦，主動招募資安專家進行測試，讓企業更早獲得第一手漏洞情資。

- 漏洞列表
- 訊息
- 修改企業帳號使用者
- 修改企業資料
- 設定獎勵計畫
- 操作記錄

## 獎勵

您現在可以向通報者提出獎勵，除回饋通報者的努力外，更能鼓勵通報者繼續積極發現並通報漏洞，一齊共同改善資安環境。請在此選擇您將提供給通報者的獎勵方式，您可以同時選擇多種方式。



**獎勵金 Reward**  
提供現金獎勵金予通報者



**感謝函 Thank**  
寄發感謝信函向通報者致謝



**風雲榜 Hall of Fame**  
在企業網站公開表揚通報者的貢獻

### 獎勵金額

新台幣  元

### 風雲榜

公開網址

**向通報者提出獎勵**

當您按下「向通報者提出獎勵」後，通報者將會在「訊息聯絡」中收到一封通知訊息。您可以繼續在訊息中與通報者聯絡及討論相關事宜。

## 詳細資料

ZDID: ZD-2018-00015  
Risk: 低  
Type: 資料庫注入攻擊 (SQL Injection)  
Author: test\_user

[漏洞](#)[消息](#)[排行榜](#)[企業](#)[獎勵計劃](#)[Admin](#)

## Bug Bounty

[提供獎勵計畫](#)

## 提供獎勵計畫

所有現正提供 Bug Bounty 獎勵計畫的企業

社團法人台灣駭客協會

發出率：100%

NT\$2,147,483,647

我是一個好企業股份有限公司

發出率：33.33%



1 / 1

# 測試漏洞

[前往漏洞頁面](#)

企業為了感謝您的通報，願意提供下列獎勵。您可以根據您的意願自由選擇接受與否，相關細節您可以透過訊息功能與企業聯絡。當您做出選擇，請於下方點選接受或不接受，系統將會通知企業進行後續流程。

-  獎勵金 Reward  
NT\$50,000
-  感謝函 Thank
-  風雲榜 Hall of Fame

特別提醒您，若您接受漏洞獎勵，企業有可能會希望得知您的真實身份，若您有身份上的顧慮，請鄭重考慮後再行決定。

HITCON ZeroDay 僅作為企業與通報者之間溝通的平台，其過程完全透明，我們不會向企業或使用者收取任何費用，也不會對企業的獎勵承諾負責。若計畫中雙方有任何的爭議，請直接向該企業協調。

有關 Bug Bounty 計畫，您可至 [這裡](#) 詳細瞭解。

接受提議

不接受提議

# 對企業的幫助

- 針對漏洞給予專家獎勵
  - 企業在確認漏洞通報無誤時，若認為通報者對於企業是有幫助的，可與通報者溝通給予獎勵。獎勵的機制及方式企業可自由設定。
- 獨立頁面主動招募漏洞
  - 除了被動通報之外，企業可主動設立漏洞獎勵計畫頁面，主動招募資安專家針對目標進行測試，彰顯企業對於資安的重視及成熟度。
- 透過計畫尋找合適人才
  - 透過此計畫可以找到優良的資安人才，若互動良好可以進一步成為企業尋找資安人才的媒合管道。



# 對通報者的好處

- 幫助企業改善現存漏洞
  - 企業面對未知漏洞的威脅，必須靠民間的力量才能更進一步加速改善。通報除了改善企業體質，更可以藉由企業的表揚作為個人技術能力的履歷。
- 挑戰自我資安技術能力
  - 除了協助尋找企業漏洞之外，更可以挑戰企業公開的計畫，找出更完善的系統中有無漏洞存在的可能性。
- 透過計畫媒合良好企業
  - 若民間專家想要尋找重視資安的企業，可以藉由尋找參與計畫的企業，並與該企業互動溝通，瞭解企業的態度及需求，成為求職的一個選擇。



# 下一步？

- 漏洞獎勵計畫 Bug Bounty Program
- 企業人才招聘
- 資安專家求職
- 歡迎大家多多推廣多多使用，多多給予意見
- [service@zeroday.hitcon.org](mailto:service@zeroday.hitcon.org)



讓漏洞成為我們的助力！

<https://zeroday.hitcon.org>

