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，才會

然而對我而言，使用

很抱歉的，POPO只

你的後台，做盡你能做的任何

然而這入侵的方式和

但官方與使用者卻不重視也不

『墨菲定律：有可能

有0.1%，那麼這個網站一定會

然而因為4.9%的人

惶，這整個決定是非常非常

我只希望這事件從這

你們幫我發一封Mail，告訴P

我想，還是一次打酣

很抱歉在這整個過程

，但，請相信我這是善意的，

也很抱歉被植入的程

其實我是喜愛這邊的

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，而

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

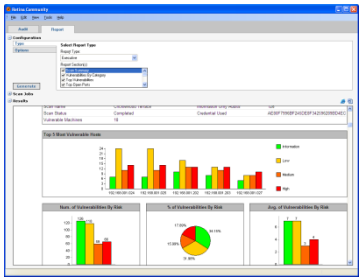
Okay，以上，感謝您和我一起站在這歷史性的一刻上:)，而點下面原來的留言框處，就是那個說這邊被入侵的貓咪，還可以再看一次我的廢話

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	

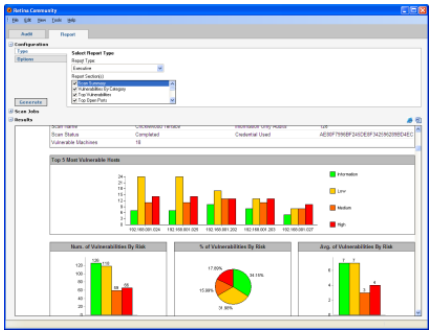
資安檢測類型

- 資安檢測
  - 資安稽核
  - 弱點掃描
  - 滲透測試



弱點掃描(Vulnerability Assessment, VA)

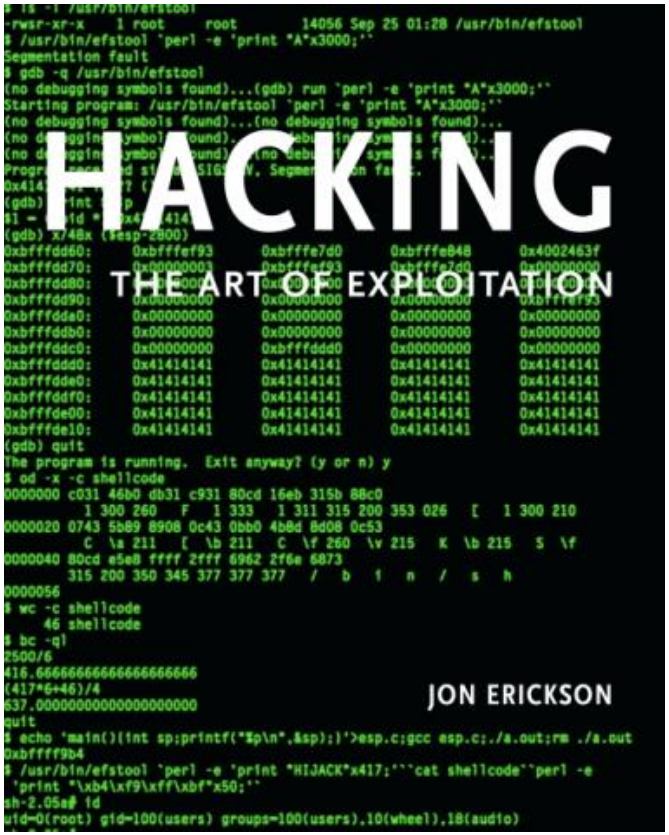
- 使用自動化的弱點掃描工具，發現系統及應用程式已知的安全弱點
- 弱點掃描包含了：探測主機狀態、網路埠的狀態、作業系統類型、系統服務及應用程式類型、弱點檢測等



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



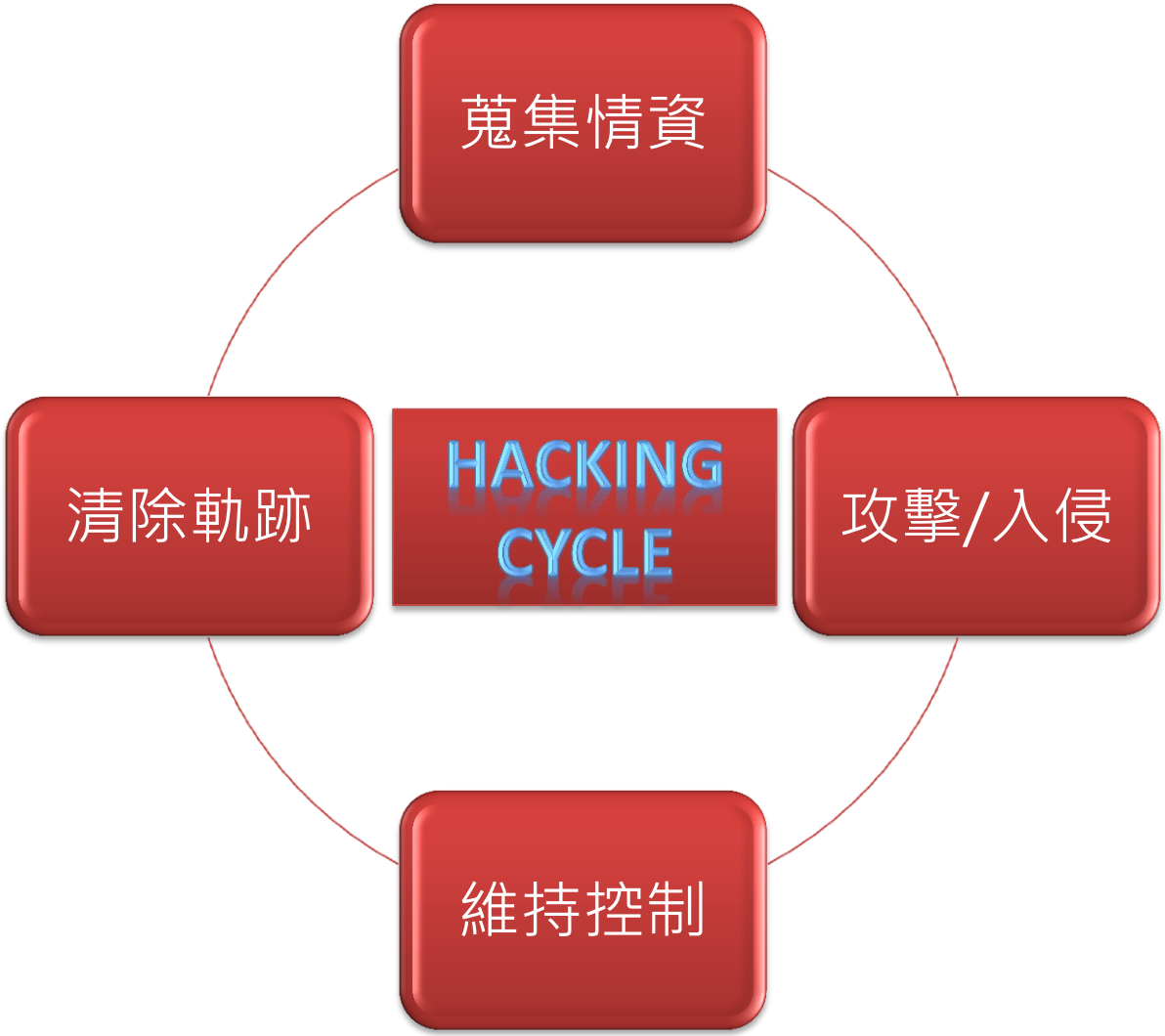
滲透測試(Penetration Testing, PT)

- 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

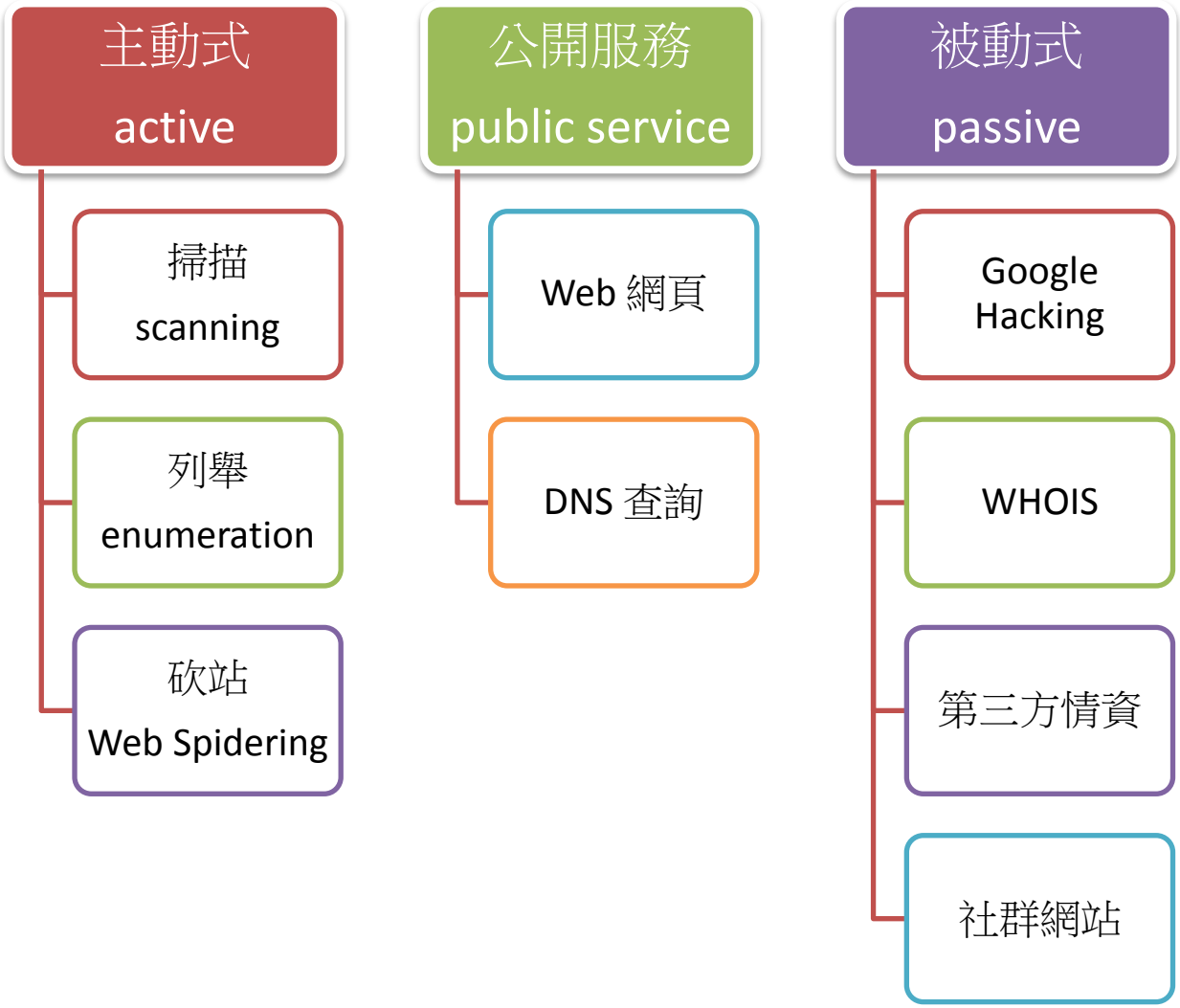
課程大綱

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

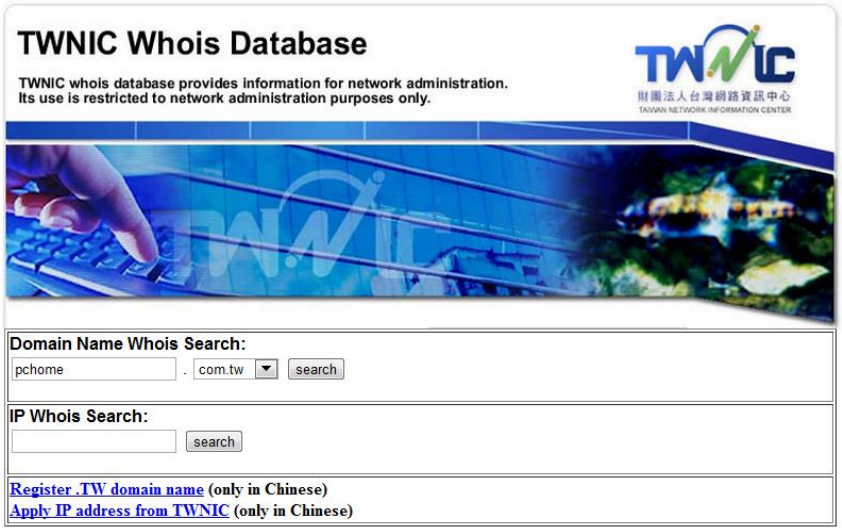


蒐集目標情資


主動式
active
掃描
scanning
列舉
enumeration
砍站
Web Spidering
公開服務
public service
Web 網頁
DNS 查詢
被動式
passive
Google
Hacking
WHOIS
第三方情資
社群網站

WHOIS 查詢工具

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

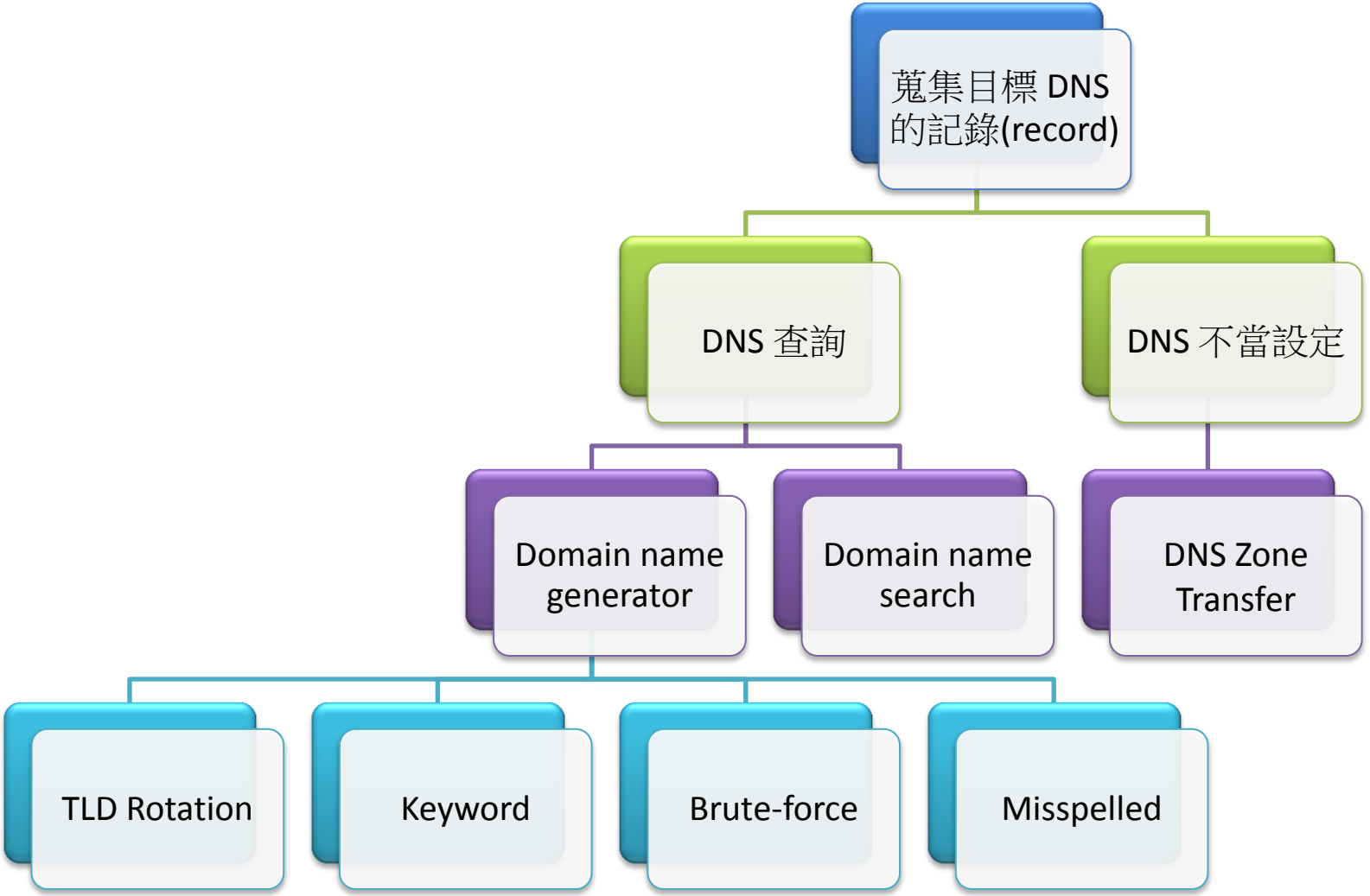



```
Domain Name: pchome.com.tw
Registrant:
網路家庭國際資訊股份有限公司
PC home online
12F No.105, Sec.2 Tun-Hwa South Road. Taipei,Taiwan, R.O.C

   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
```

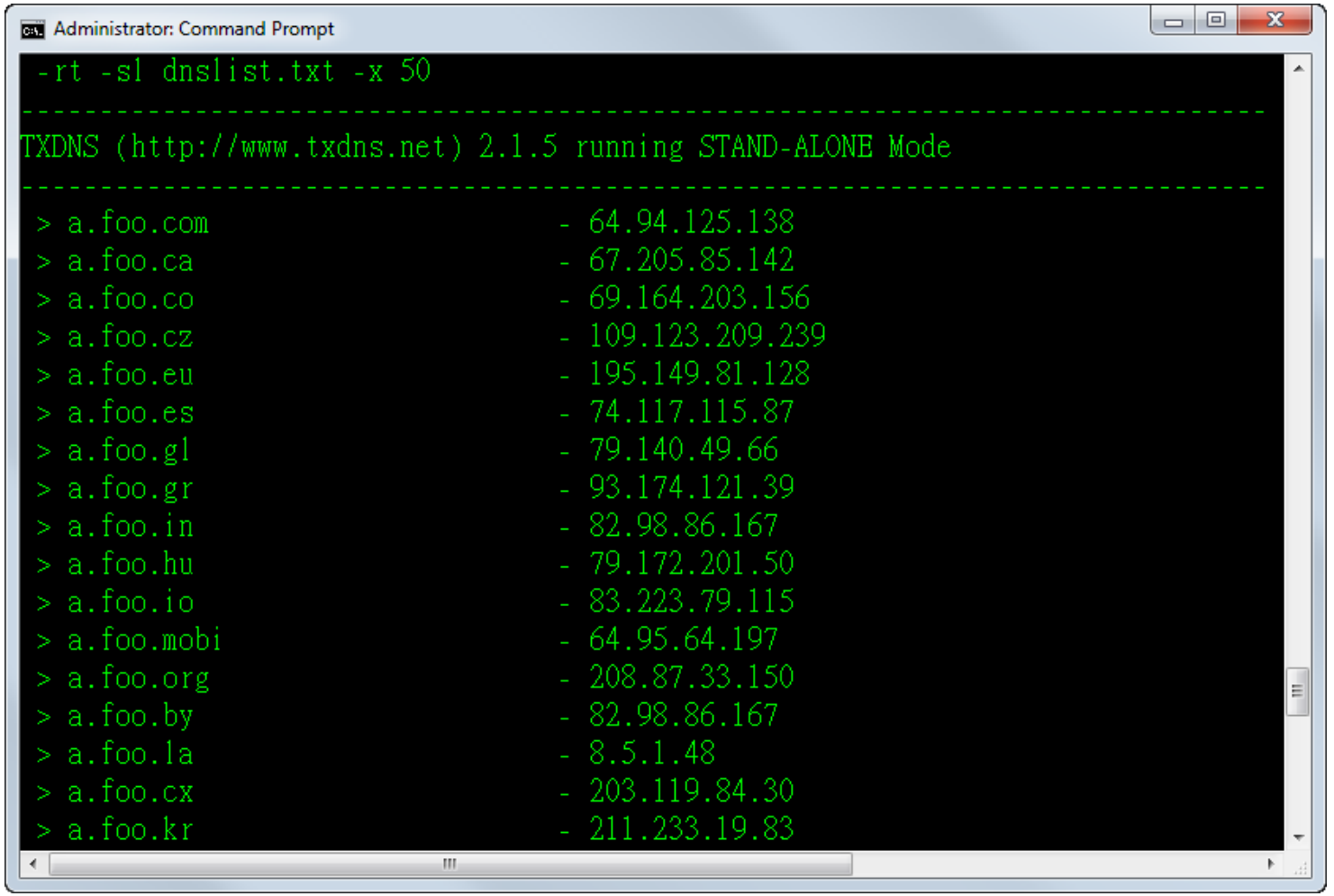
第三方 WHOIS 查詢工具

- 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


蒐集目標 DNS 的記錄(record)
DNS 查詢
DNS 不當設定
Domain name generator
Domain name search
DNS Zone Transfer
TLD Rotation
Keyword
Brute-force
Misspelled

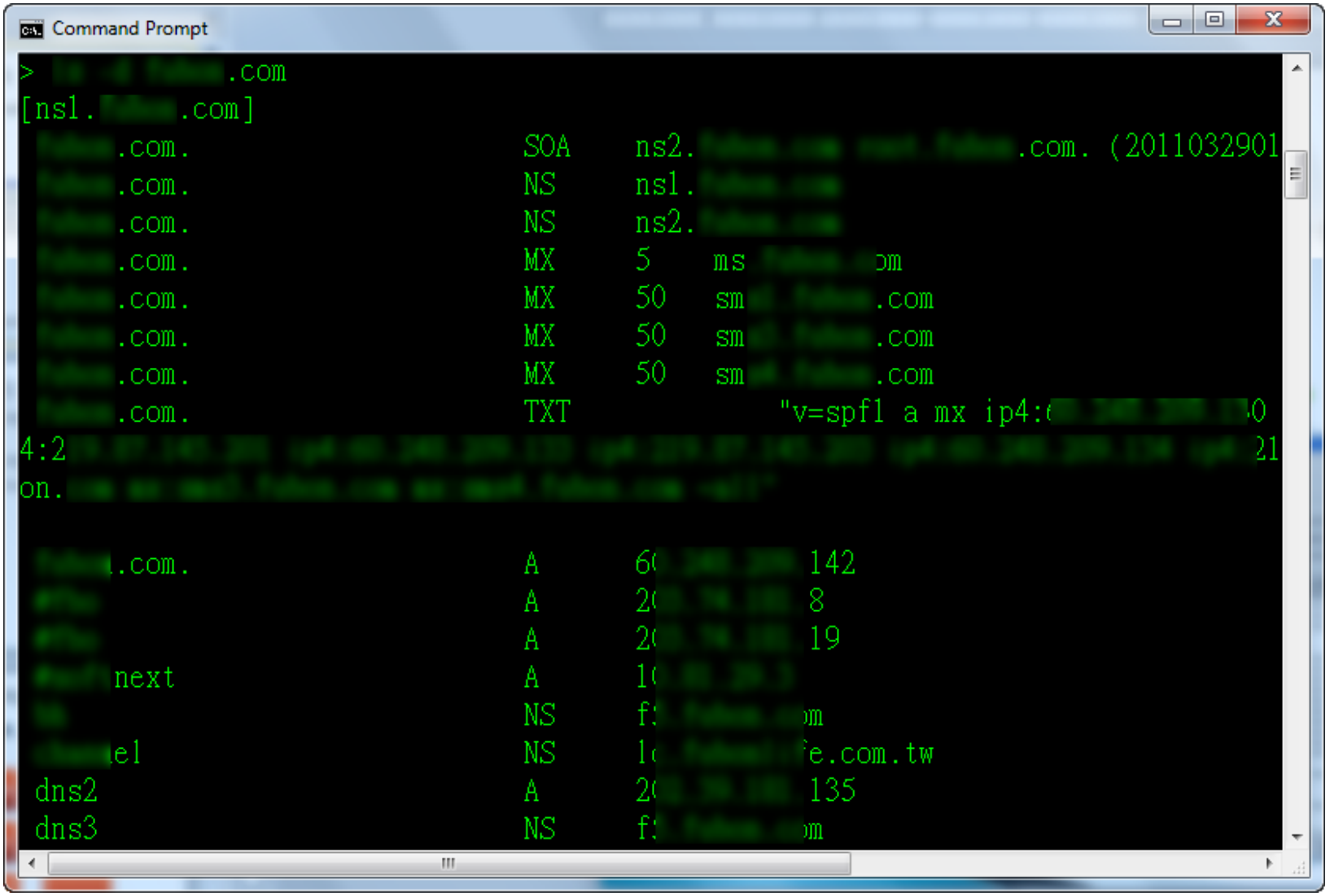
DNS 暴力查詢


Administrator: Command Prompt
-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



Google Hacking

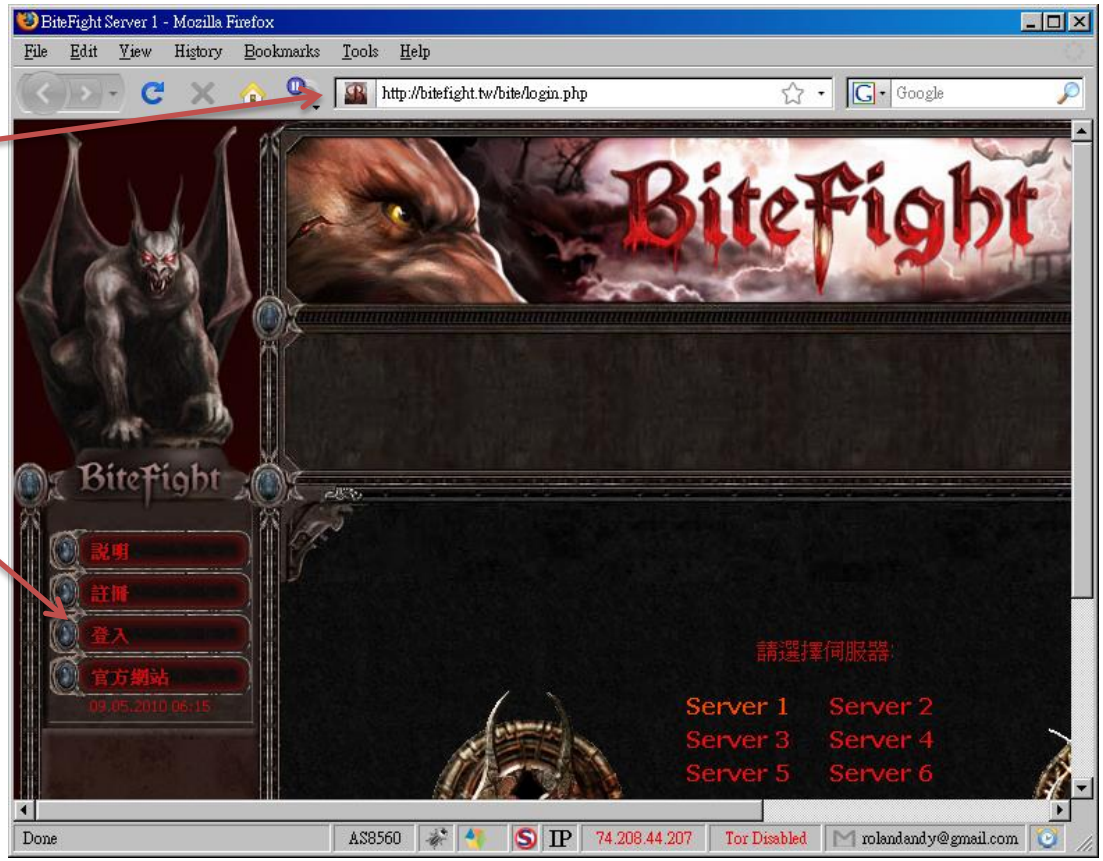
- "Google hacking is a computer hacking technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites use." -Wikepedia
- Keyword(關鍵字)
  - 搜尋相關內容
  - 相關度(relevance)
- Operator
  - 有效鎖定範圍
  - 精準過濾資訊

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

- intitle
- inurl
- intext
- site
- filetype/ext
- -
- -
- OR, |
- “”

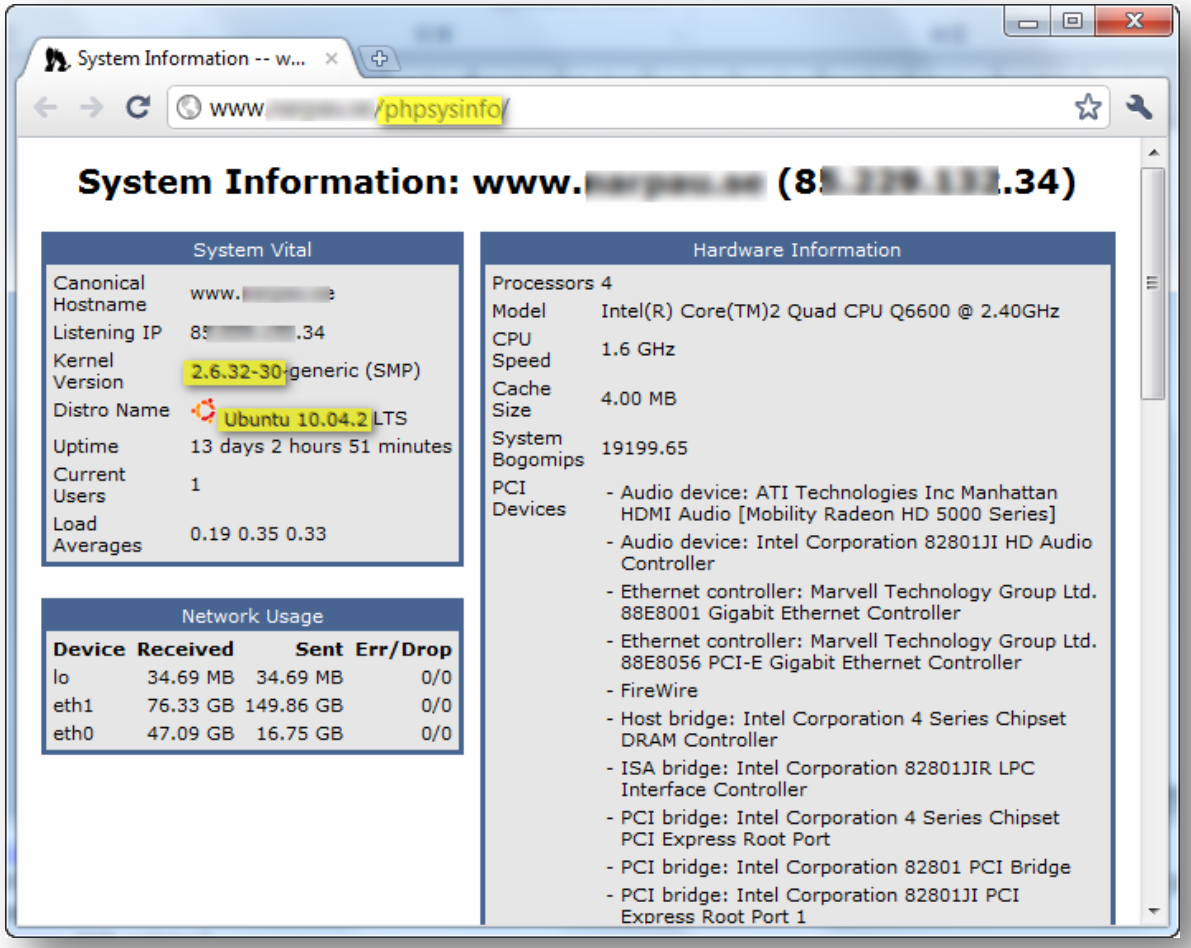


Google Hacking Database

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

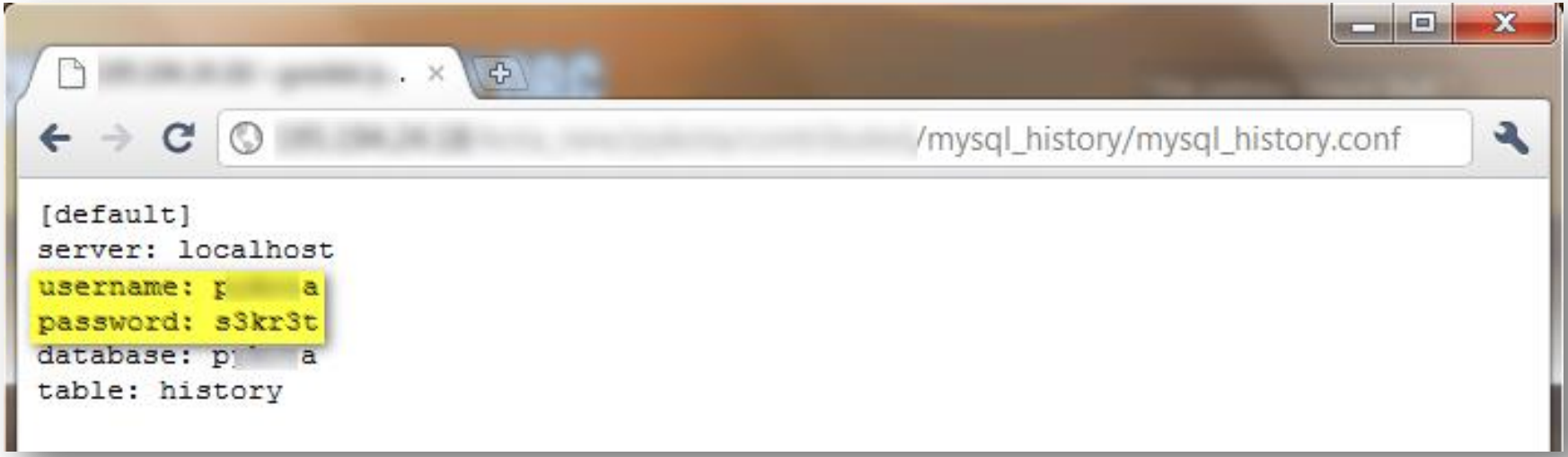
搜尋網站作業系統

- inurl:phpSysInfo/ "created by phpsysinfo"



搜尋含密碼的檔案

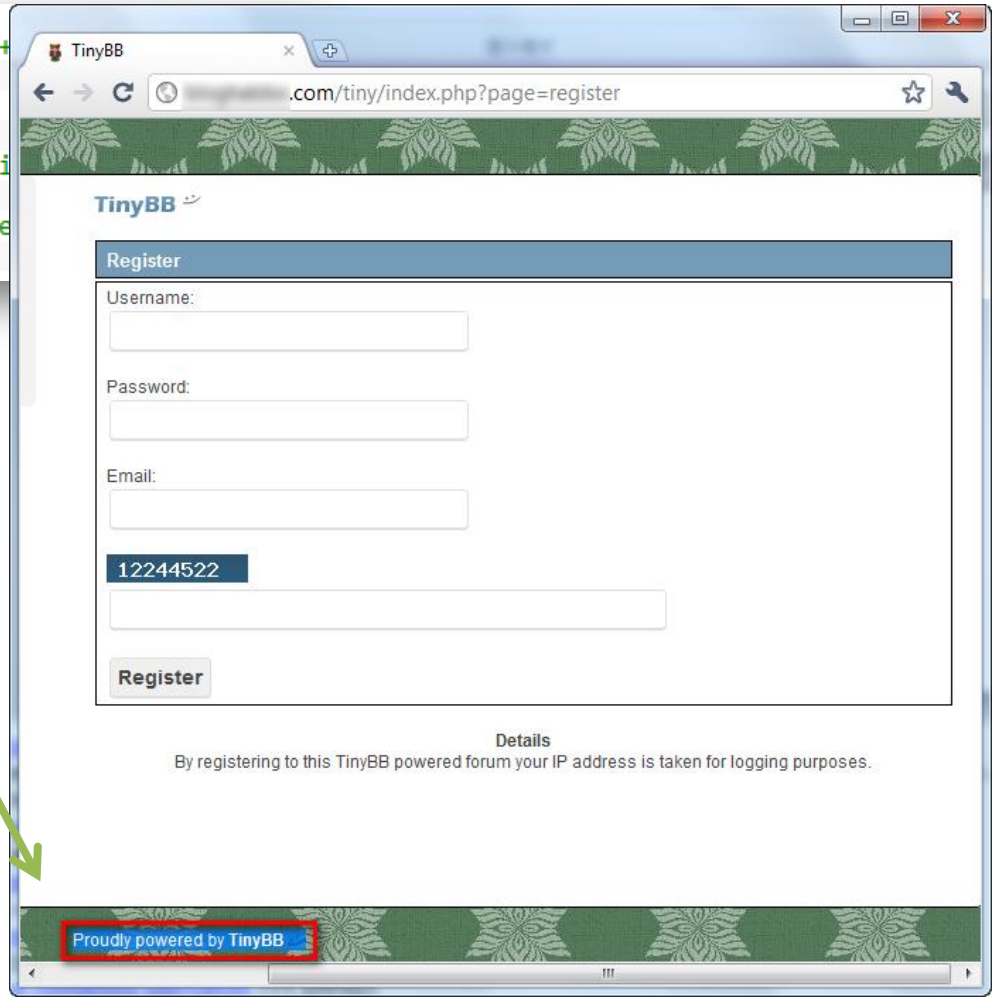
- intitle:”Index of” .mysql_history

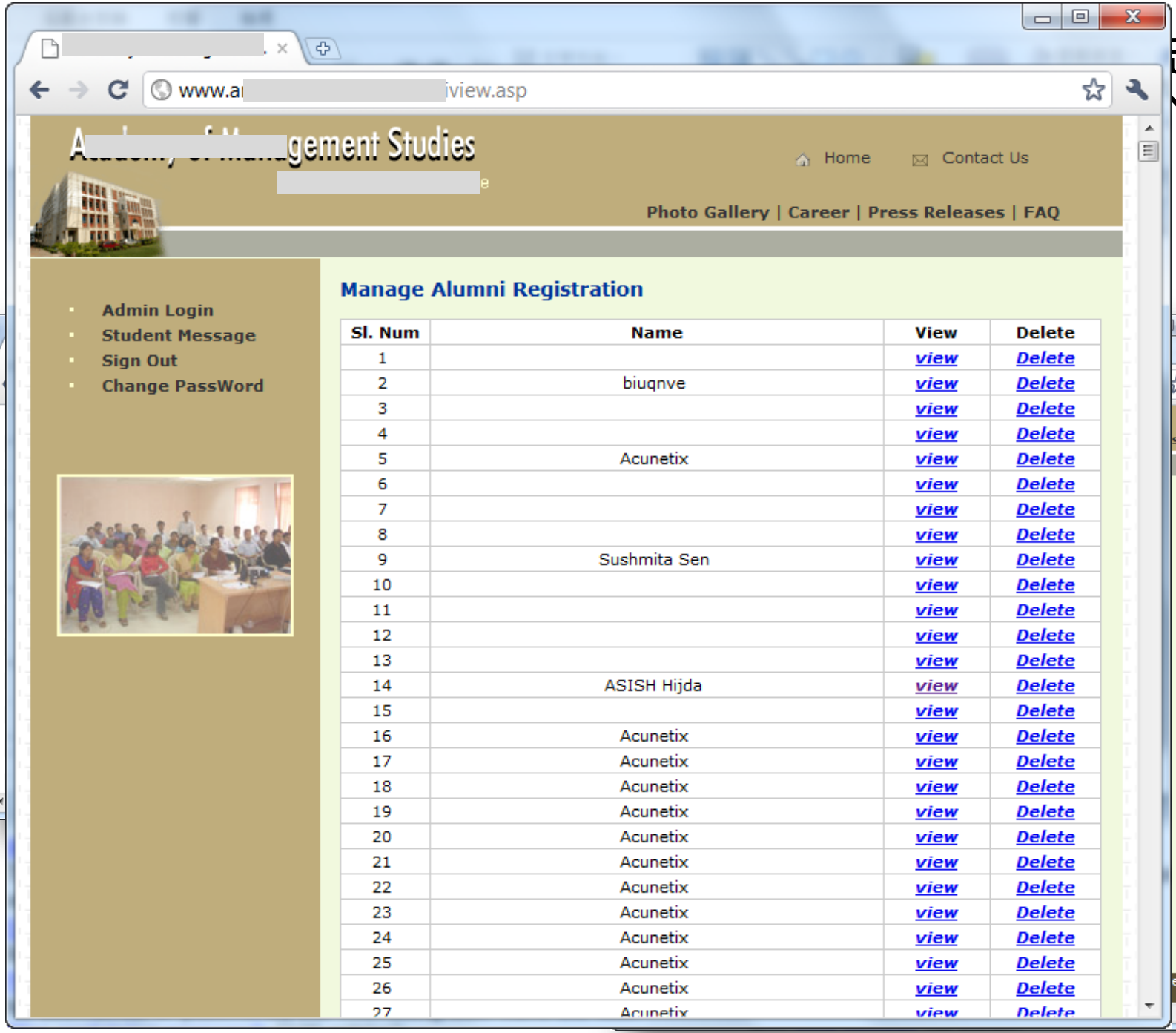


搜尋弱點

- 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]gmai
# Version           : 1.4
# Tested on        : Centos 5.5 with magic_quote
# Thanks to       : ptrace.net
```




www.a iview.asp
gement Studies
Home
Contact Us
Photo Gallery | Career | Press Releases | FAQ
Admin Login
Student Message
Sign Out
Change PassWord
Manage Alumni Registration
Sl. Num
Name
View
Delete
1 view Delete
2 biuqnve view Delete
3 view Delete
4 view Delete
5 Acunetix view Delete
6 view Delete
7 view Delete
8 view Delete
9 Sushmita Sen view Delete
10 view Delete
11 view Delete
12 view Delete
13 view Delete
14 ASISH Hijda view Delete
15 view Delete
16 Acunetix view Delete
17 Acunetix view Delete
18 Acunetix view Delete
19 Acunetix view Delete
20 Acunetix view Delete
21 Acunetix view Delete
22 Acunetix view Delete
23 Acunetix view Delete
24 Acunetix view Delete
25 Acunetix view Delete
26 Acunetix view Delete
27 Acunetix view Delete

搜尋 metadata

IP代理發放單位網段:2 0-2 255	
Chinese Name	
Netname	-NET
Organization Name	The
Street Address	. Rd.
Admin. Contact	.tw
Tech. Contact	.tw
Spam. Contact	.tw
用戶單位:2 72.0/24	
Netname	2-NET
Registered Date	1995-01-23
Admin. Contact	
Tech. Contact	

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?

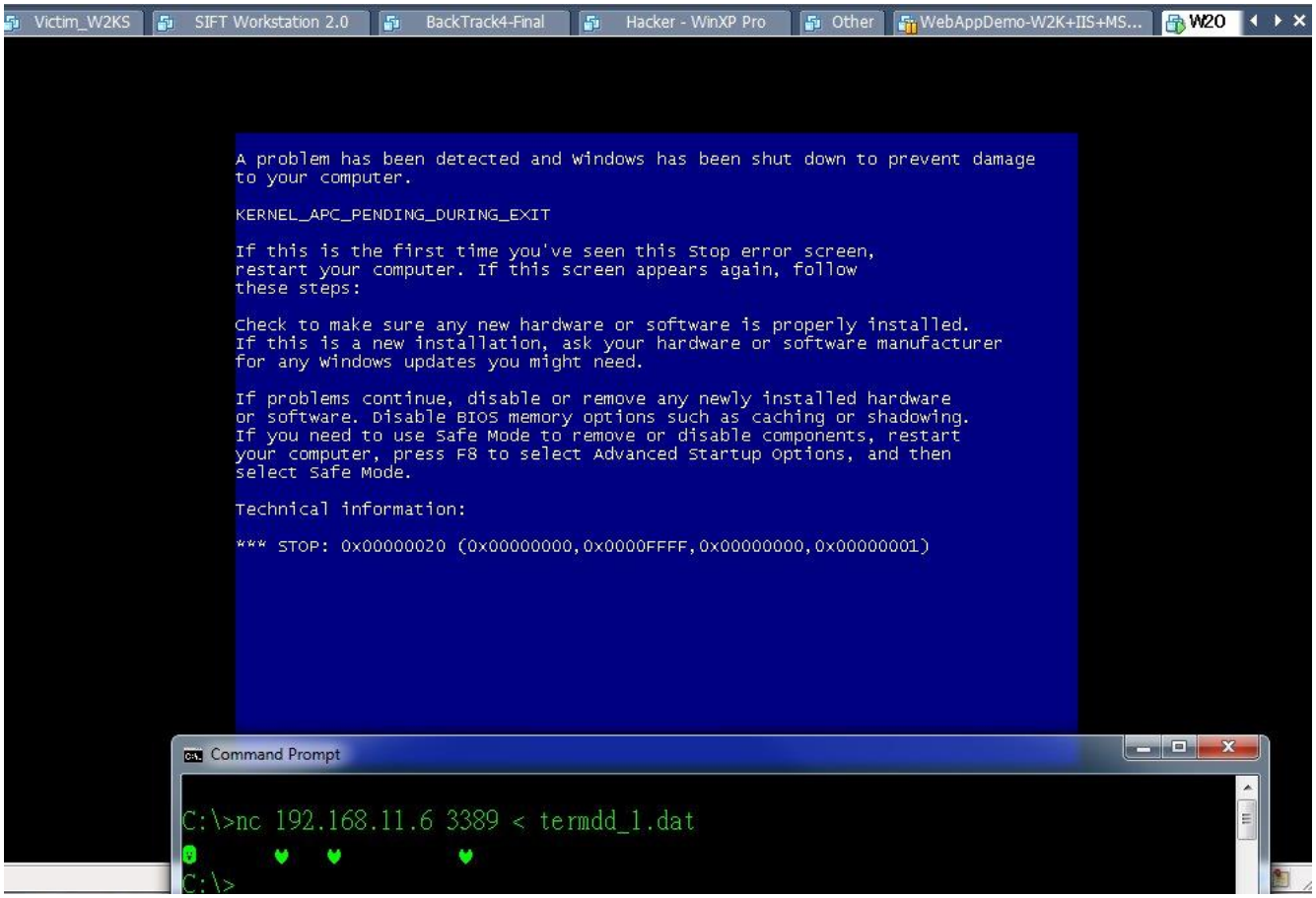
2. 台灣的教育類網站上含有密碼的 Excel 檔案

3. 有登入功能的網頁

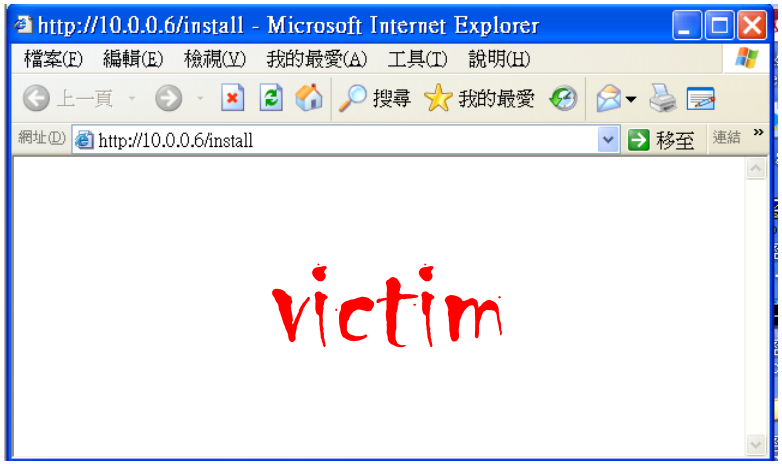
攻擊及入侵目標

	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



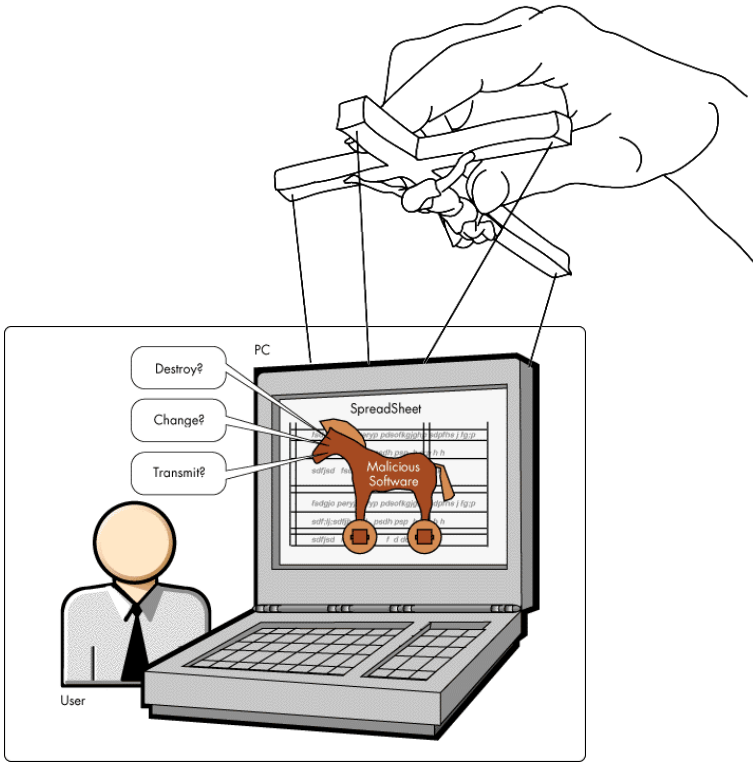
MS .LNK Vulnerability




```
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 reverse shellESTABLISHED
```

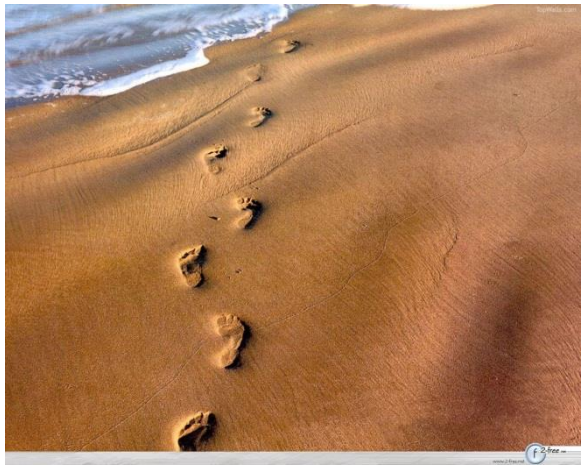
維持控制權

- 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



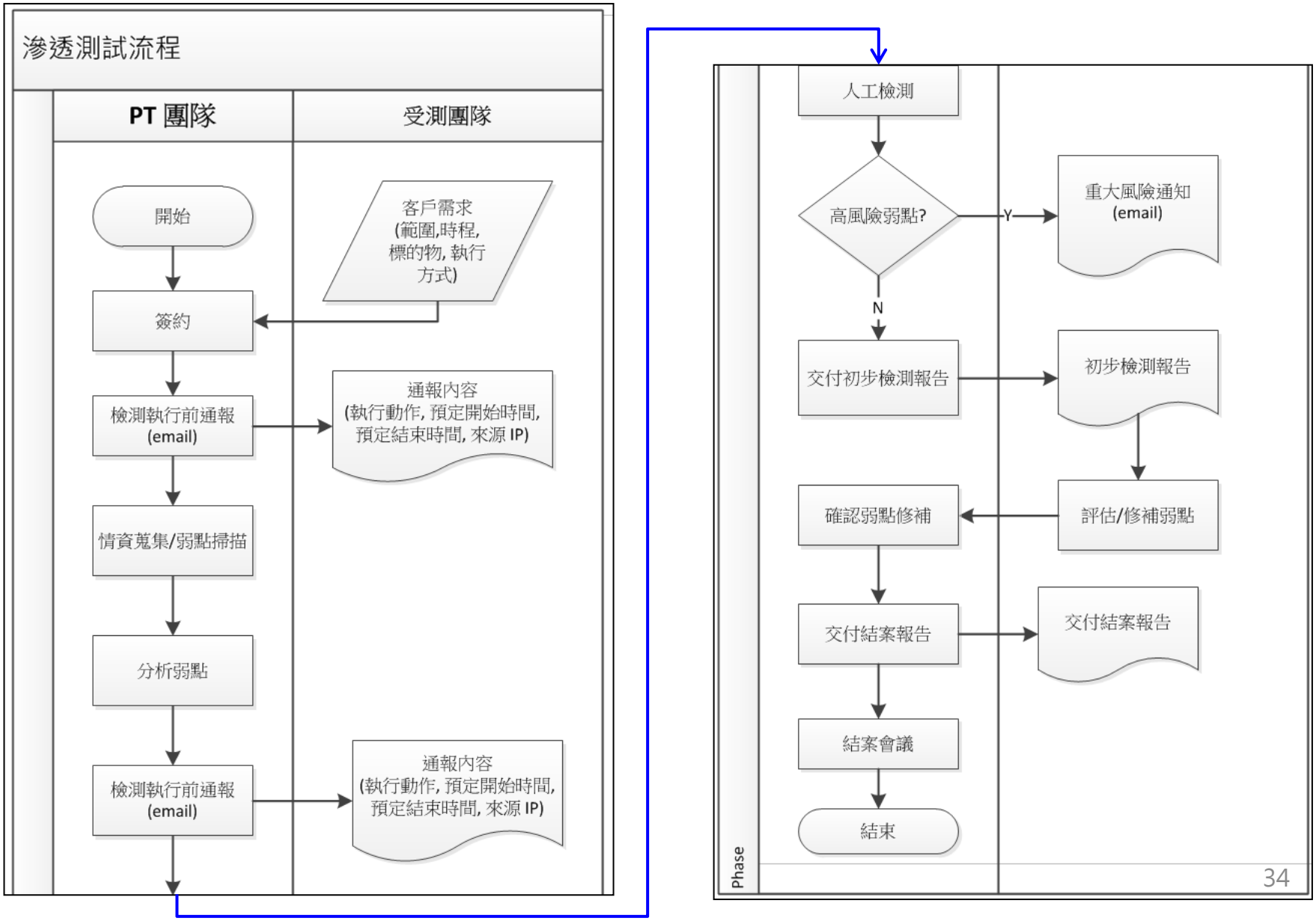
匿蹤及滅跡

- 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


滲透測試流程
PT 團隊
受測團隊
開始
客戶需求
(範圍,時程,
標的物, 執行
方式)
簽約
檢測執行前通報
(email)
通報內容
(執行動作, 預定開始時間,
預定結束時間, 來源 IP)
情資蒐集/弱點掃描
分析弱點
檢測執行前通報
(email)
通報內容
(執行動作, 預定開始時間,
預定結束時間, 來源 IP)
人工檢測
高風險弱點?
Y
重大風險通知
(email)
N
交付初步檢測報告
初步檢測報告
確認弱點修補
評估/修補弱點
交付結案報告
交付結案報告
結案會議
結束
Phase

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

手動檢測

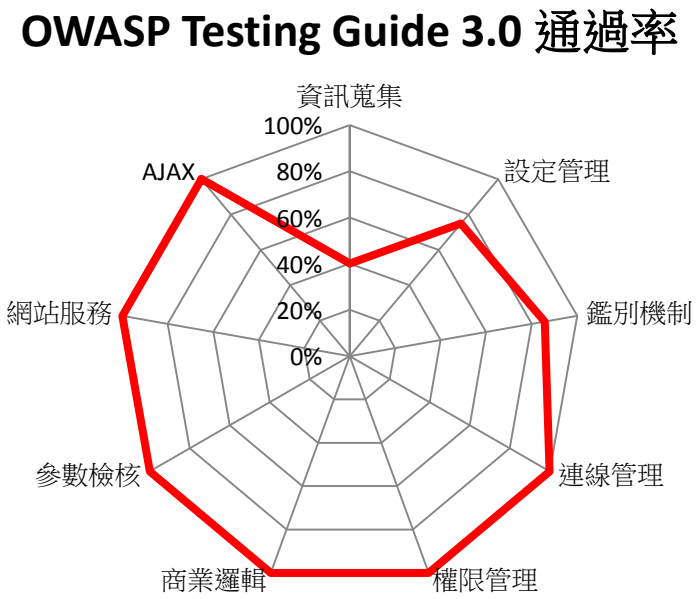
- 驗證弱點
  - 以手動方式驗證識別出的弱點，透過模擬駭客手法「利用」(exploit)弱點，並嚐試在不影響待測目標的運作下入侵系統。例如：猜測密碼、獲得作業系統的權限或透過網站應用程式弱點入侵資料庫等。

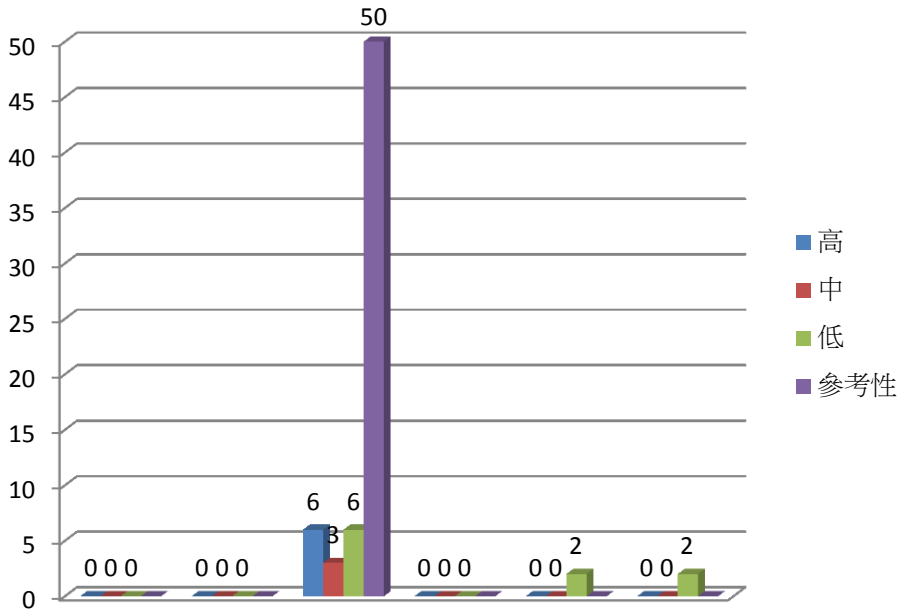
- 蒐集證據
  - 在檢測的所有階段，驗證的重要發現均會被記錄並保存，包含：入侵途徑、影響評估及弱點利用驗證(Proof of Concept, PoC)。

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

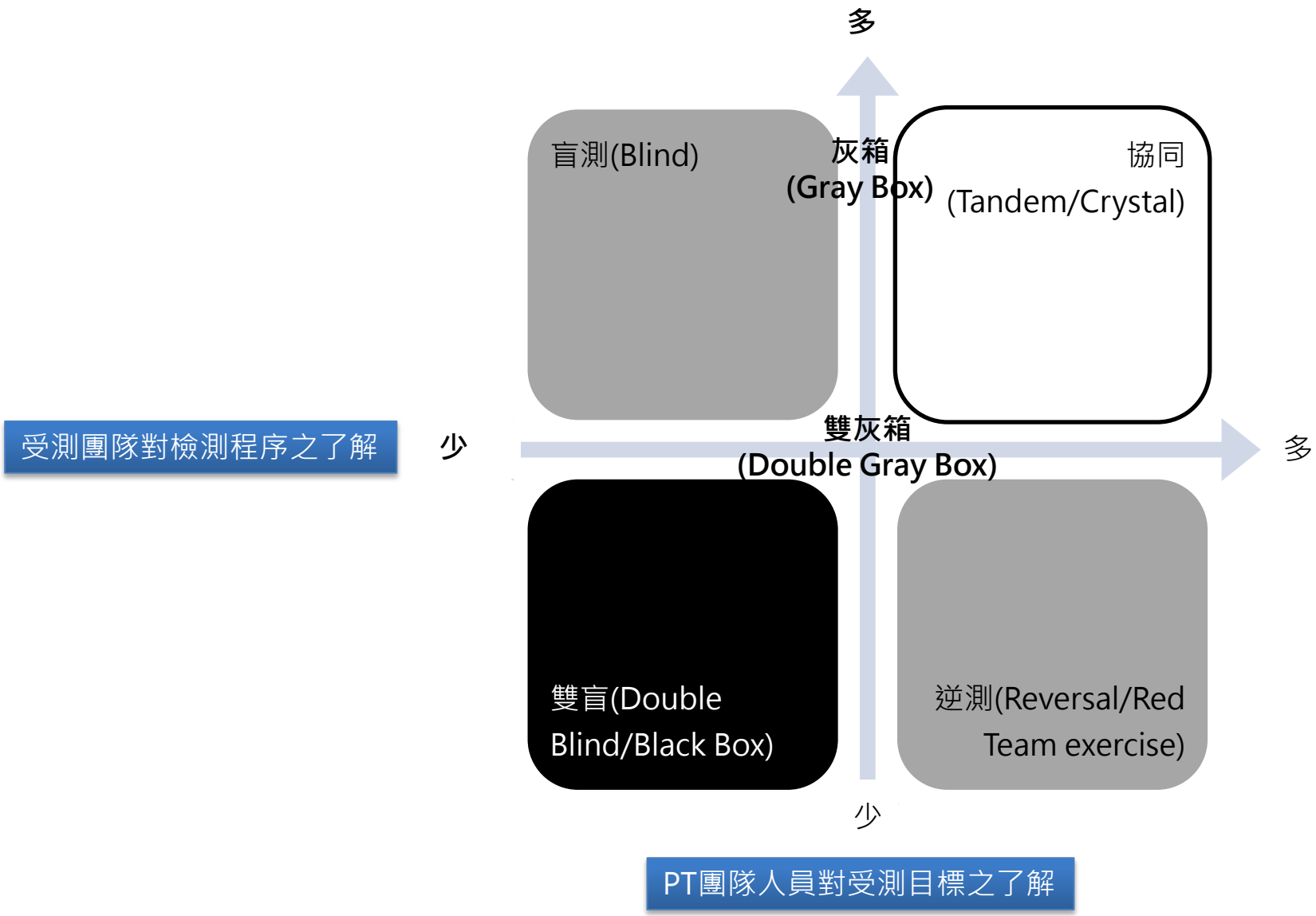
Report Visualization



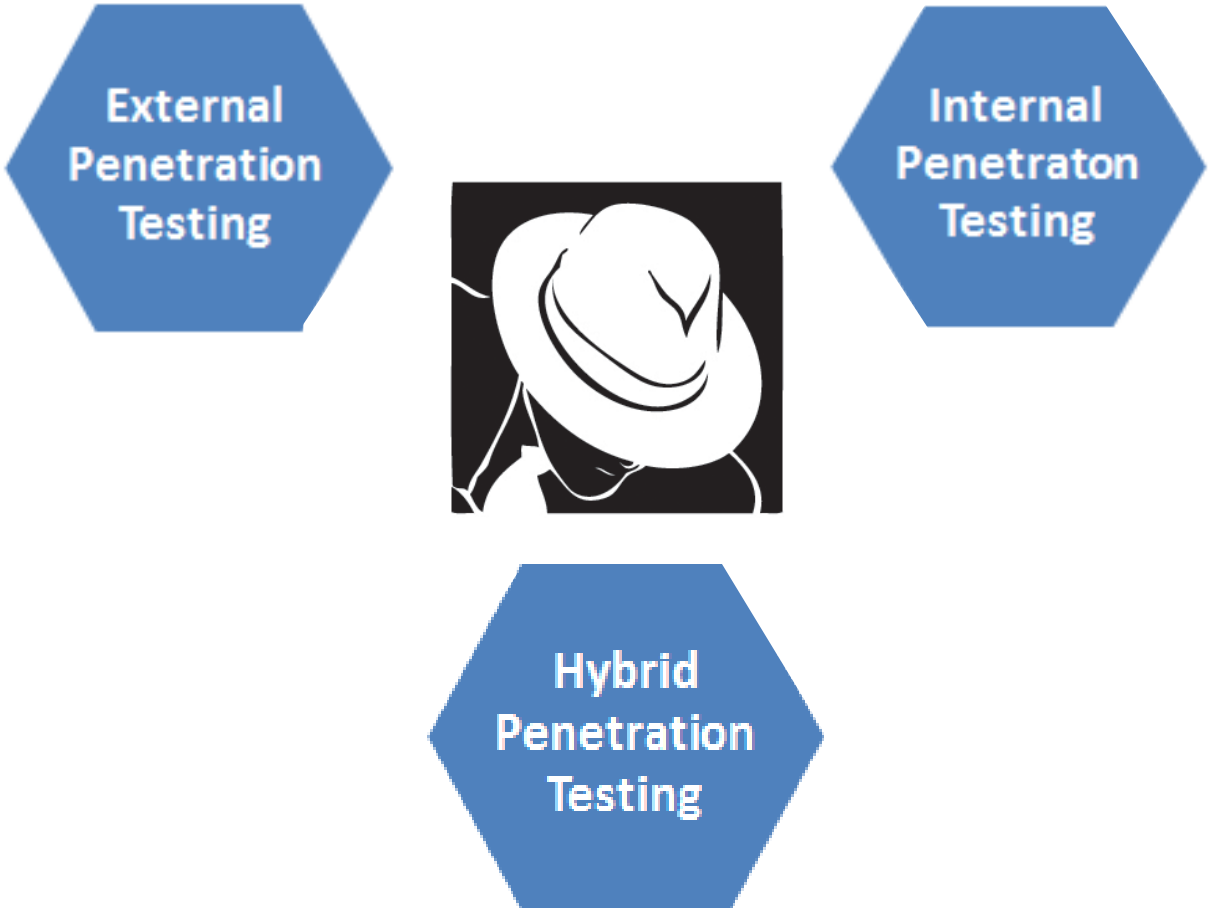


風險等級 / 檢測目標	重大風險	高	中	低
www.xxx.com	0	0	1	1
小計	0	0	1	1

滲透測試方法-by knowledge



滲透測試方法-by location



https://www.htbridge.com/pages/services/hybrid_penetration_testing.html

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	

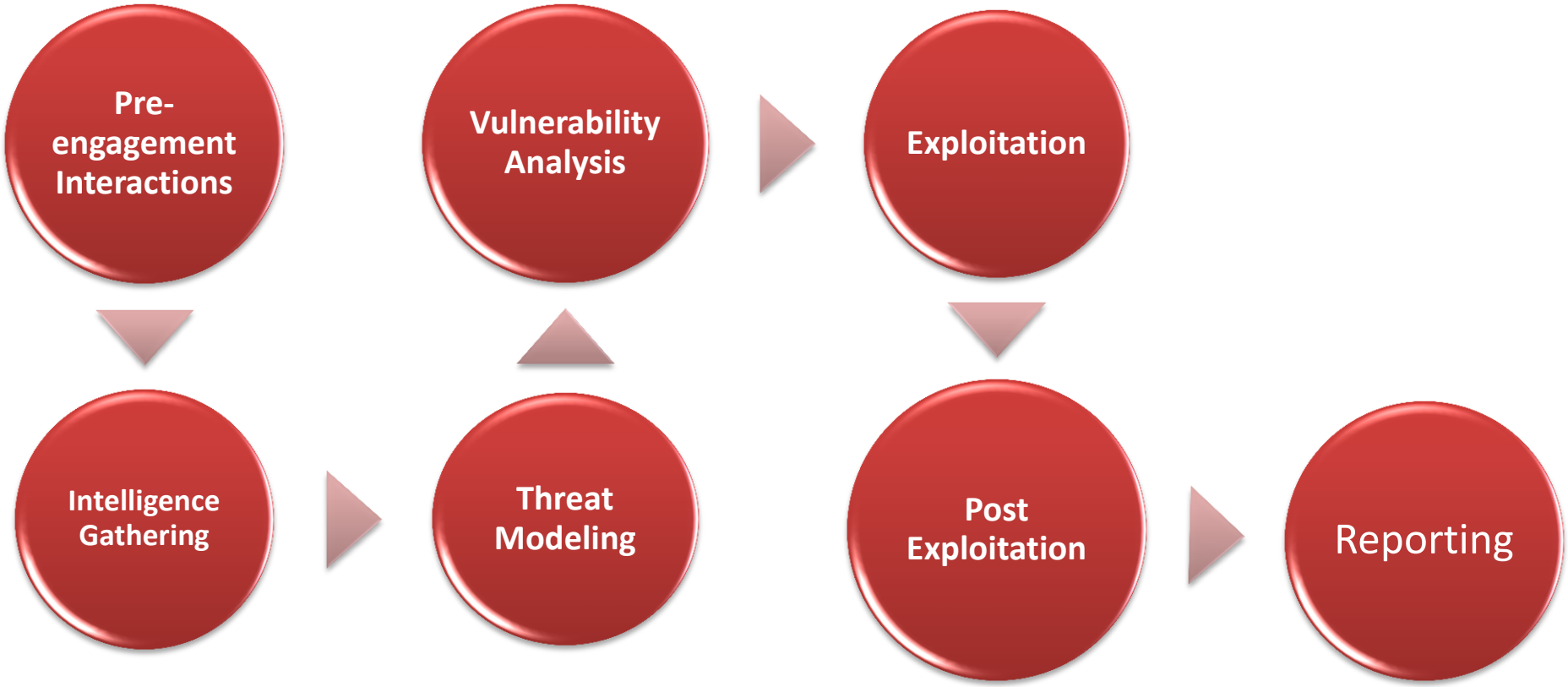
PT Guidelines

- 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


人員
網路
實體
OSSTMM 3
The Open Source Security Testing Methodology Manual
電信
無線

PT Phases of the PTES



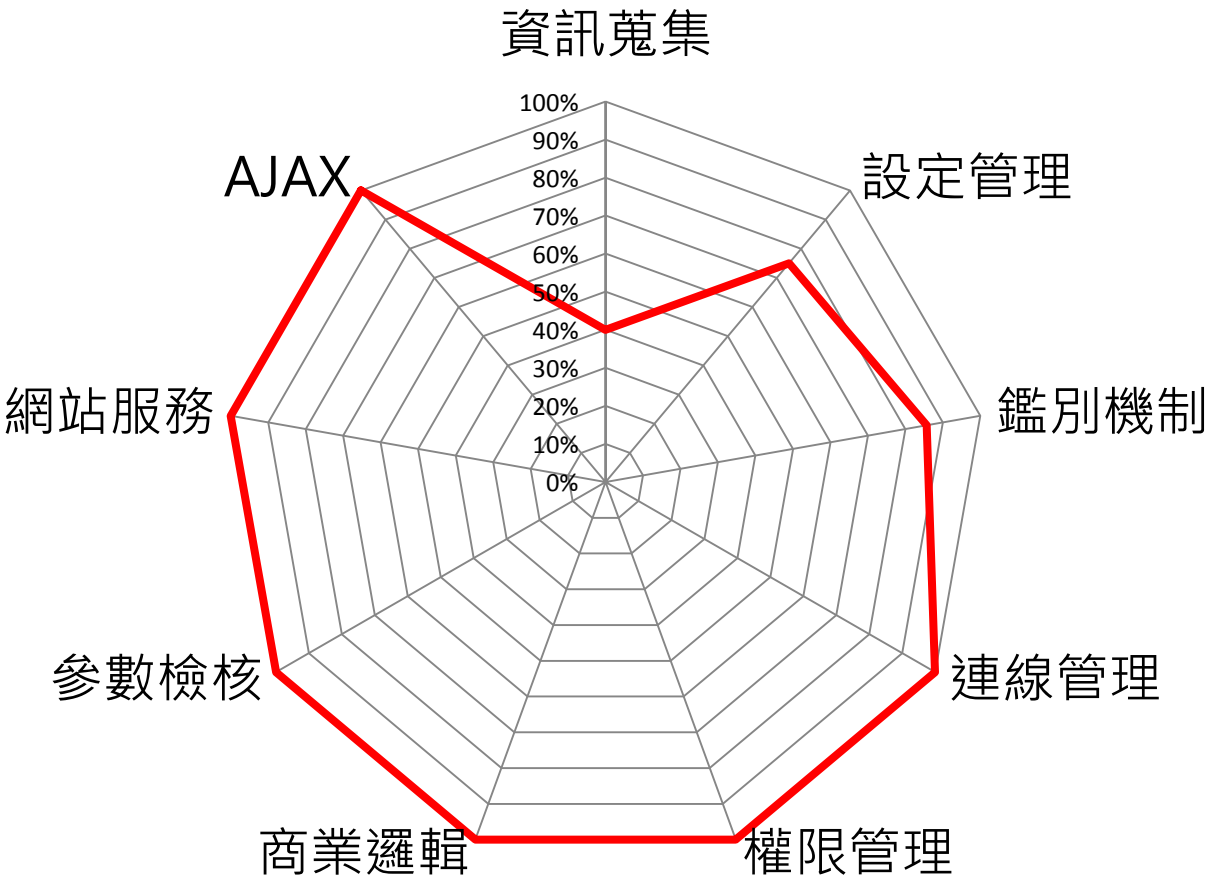
OWASP Top 10

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

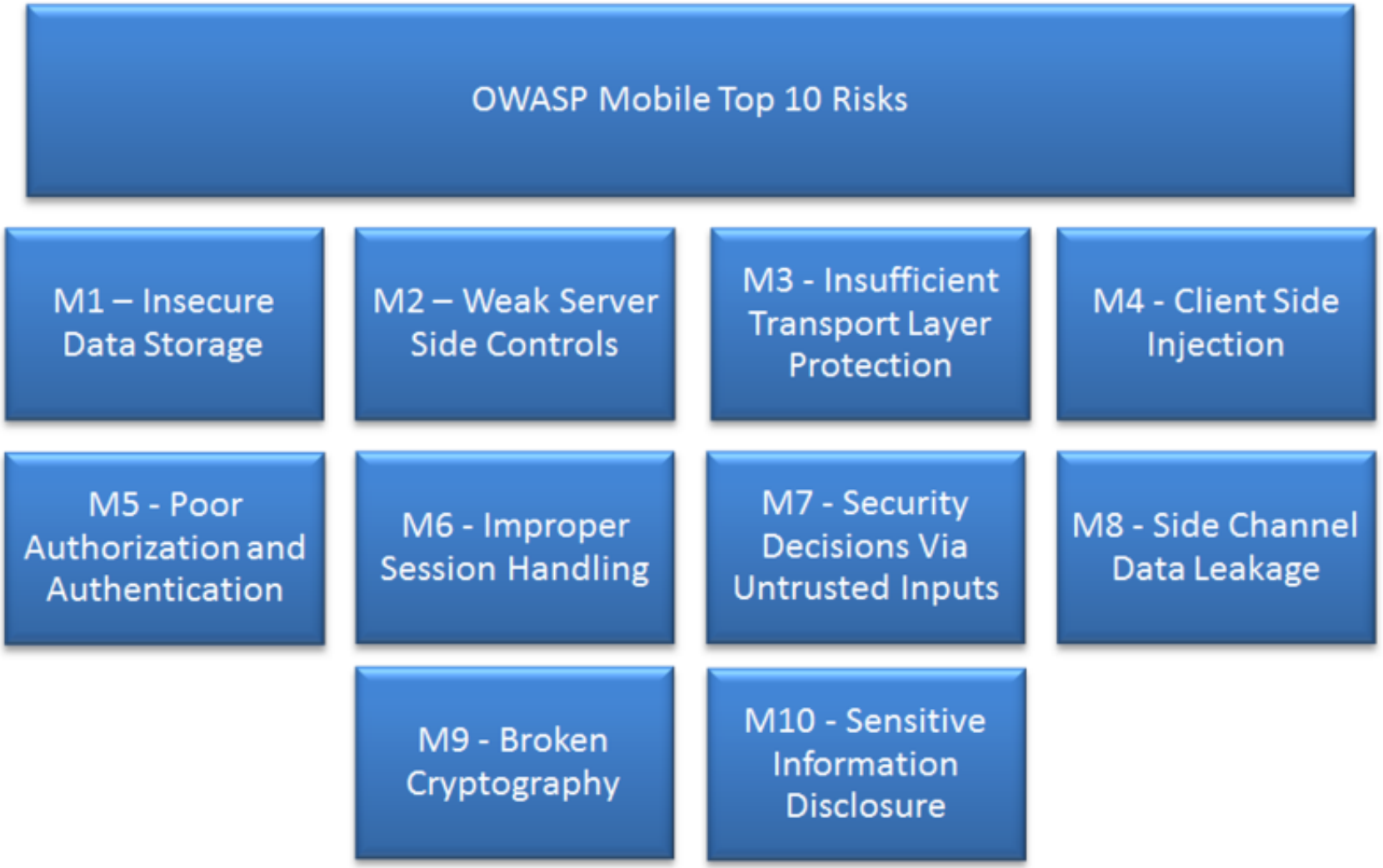
http://security-sh3ll.blogspot.tw/2013/02/owasp-top-10-application-security-risks.html

OWASP Testing Guide

OWASP Testing Guide 3.0 通過率



Mobile Top 10



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	

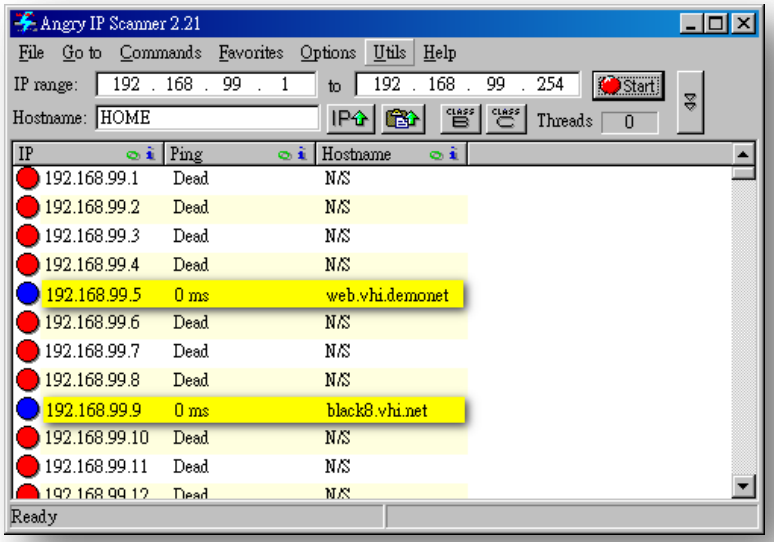
掃描(scan)的類型

- 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

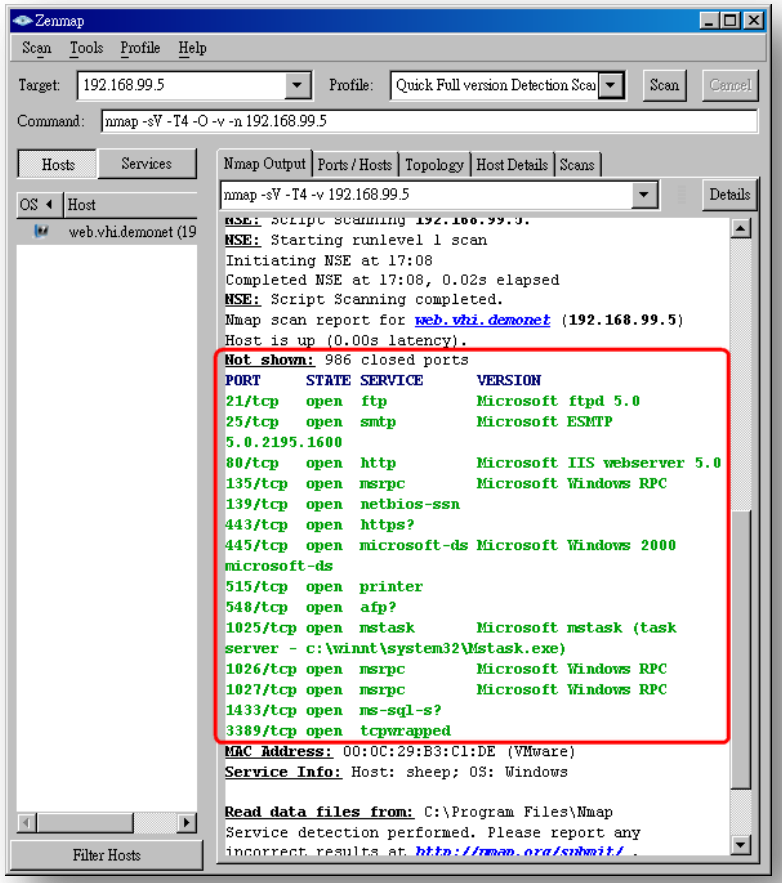
- Port 掃描發送訊息至目標主機的每個 port，由目標主機的回應推斷該 port 是否開啟，進一步探測其運行的服務或應用程式及漏洞

- 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)

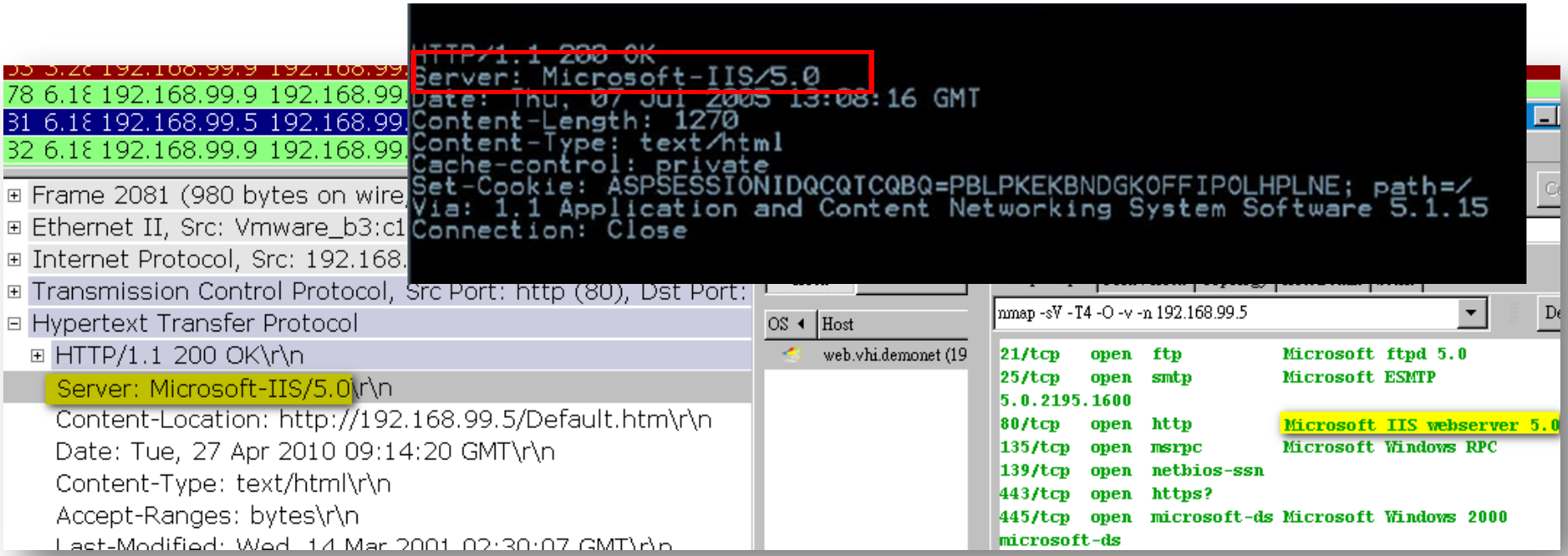


掃描 port 的工具

- 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 –s**T** –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 –s**S** –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

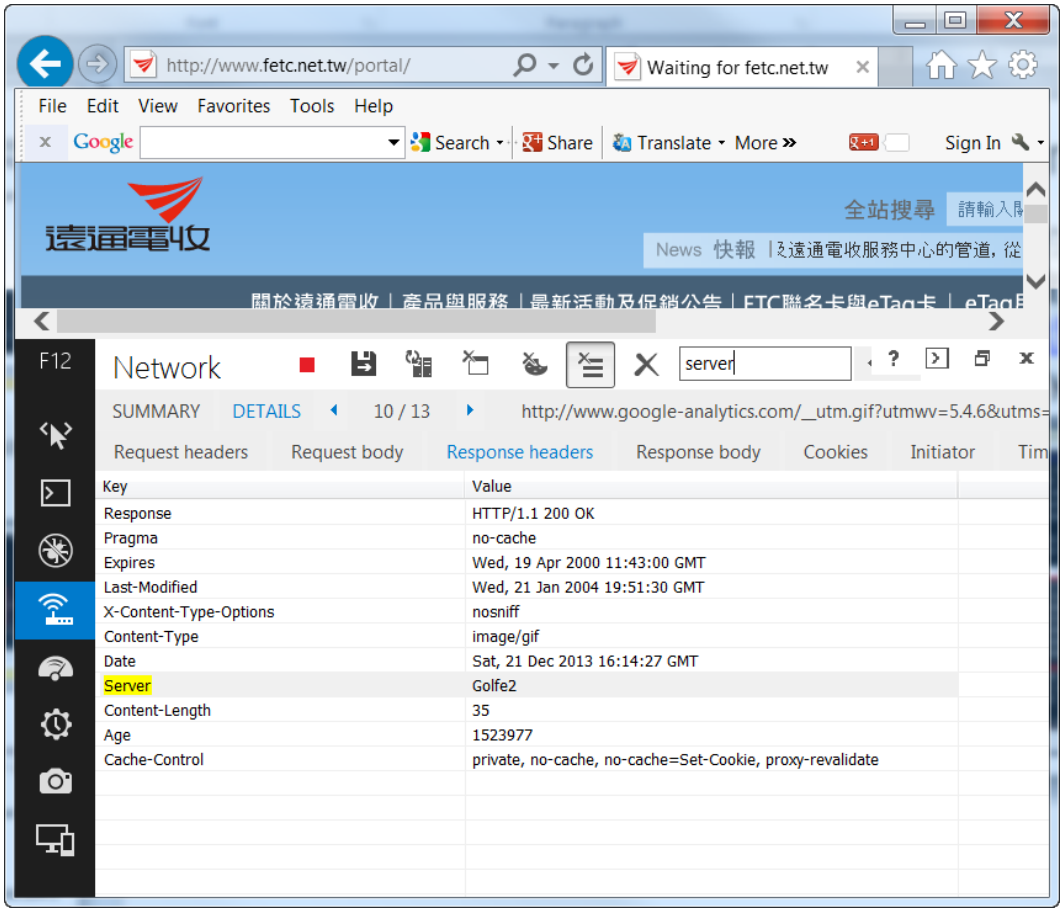


Banner Grabbing

- 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)

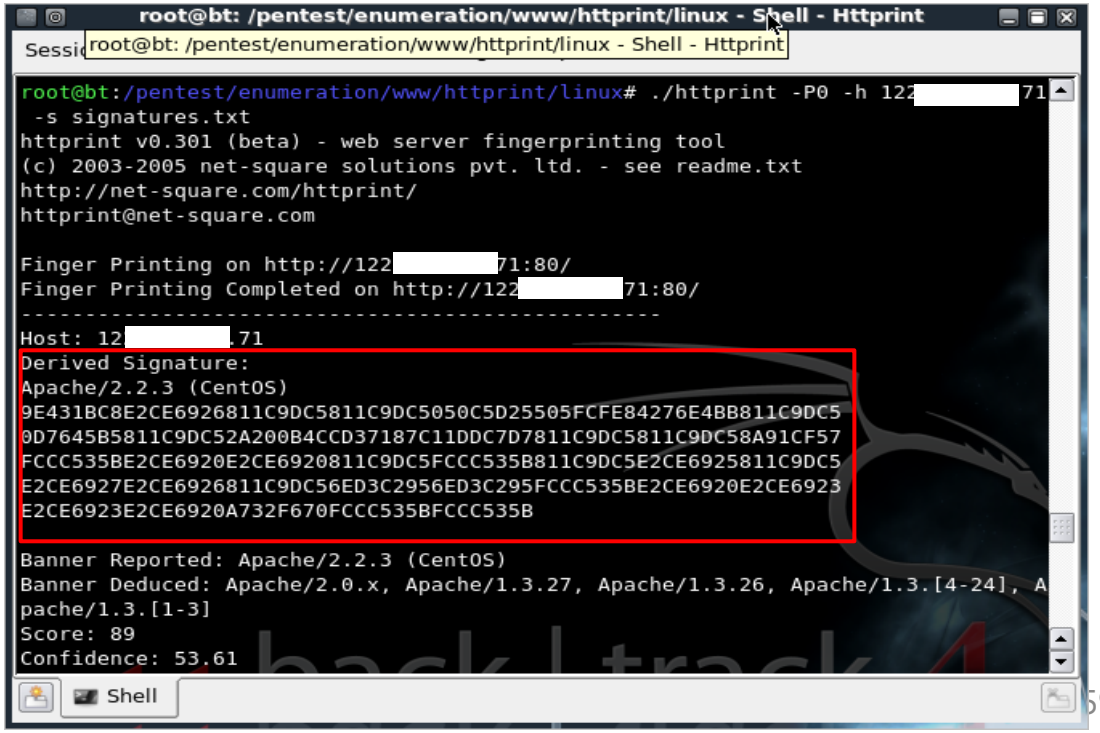
Lab. Web Server Banner

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
  - httprint
  - amap
  - nmap -sV

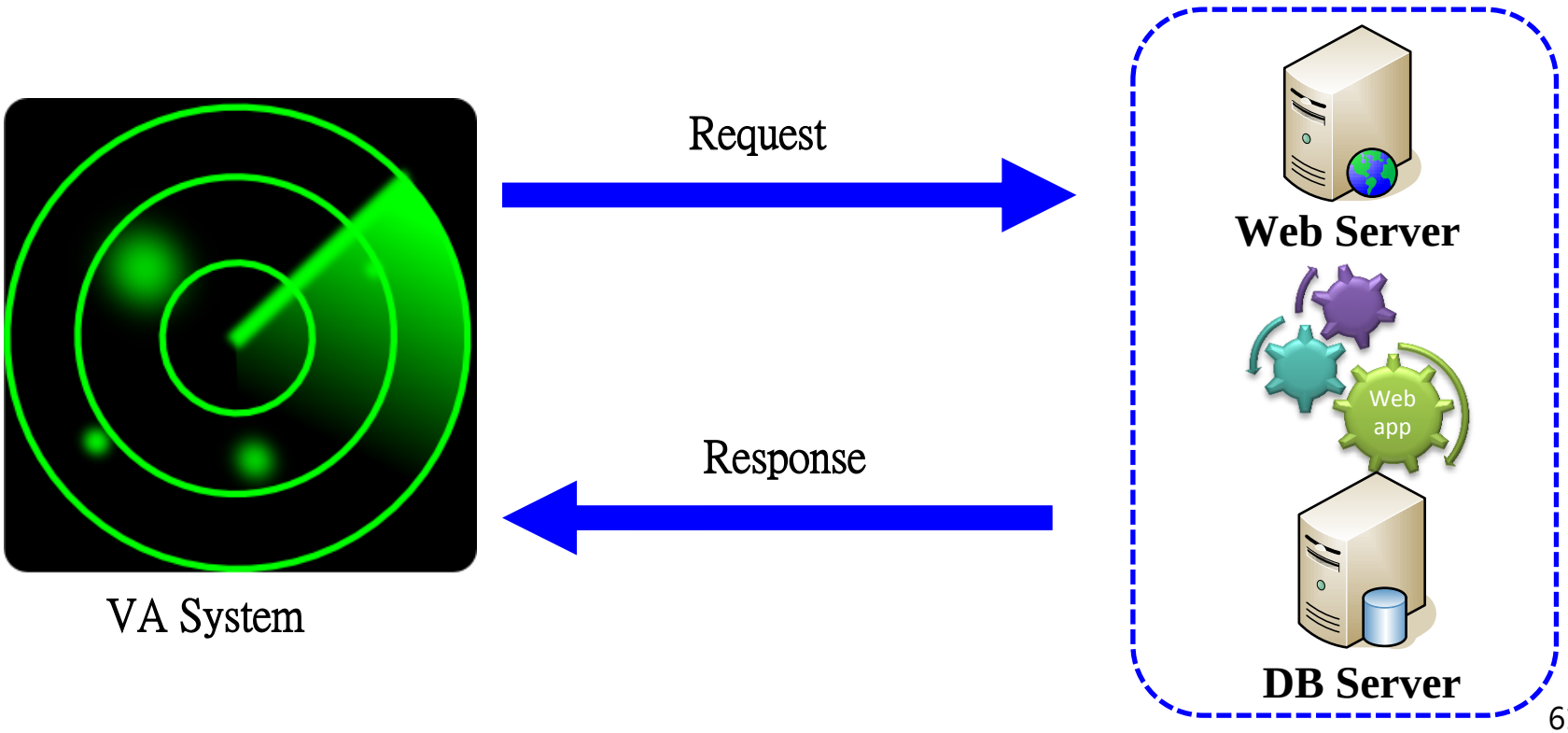


作業系統識別

- 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

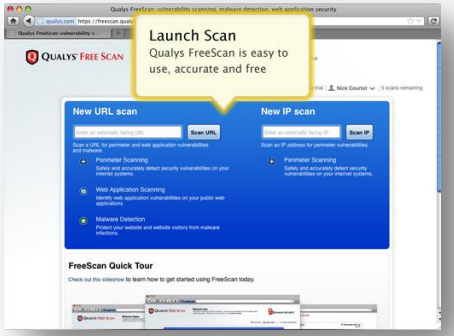
弱點掃描工具

- 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

Graph:http://icons.iconarchive.com

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__

64

VA Process

Configuring

Detect Live Hosts

Identify Live Hosts

Port Scanning

Identify Services

Identify Applications

Identify Vulnerabilities

Reporting

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 Netw ork Security					x
Trustw ave		x			

As of 10 August 2012

Nessus 5

- Tenable Network Security
- No more open source!
- Brower-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)*

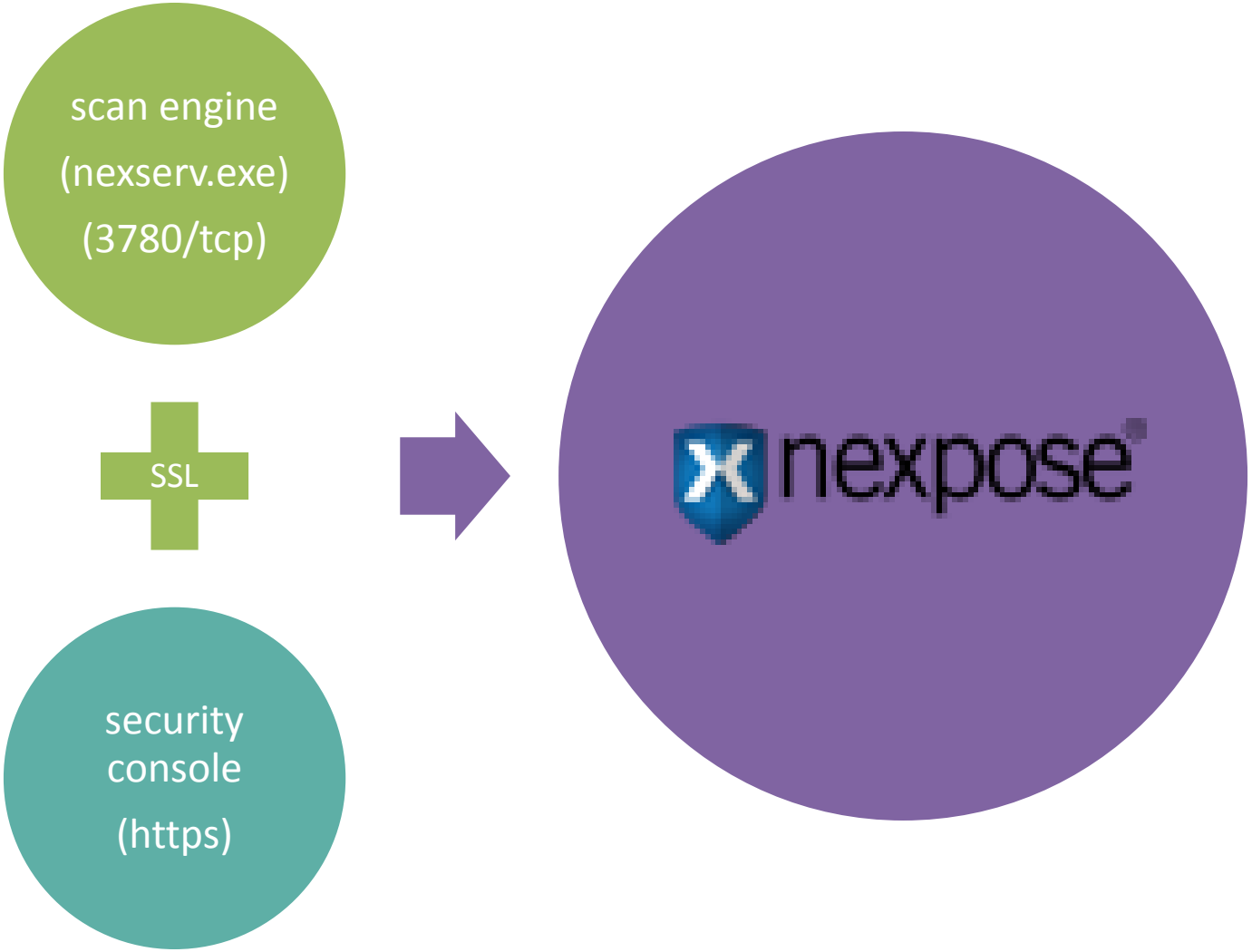
Community Edition

- 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 Netw ork Security					x
Trustw ave		x			

As of 10 August 2012

key components

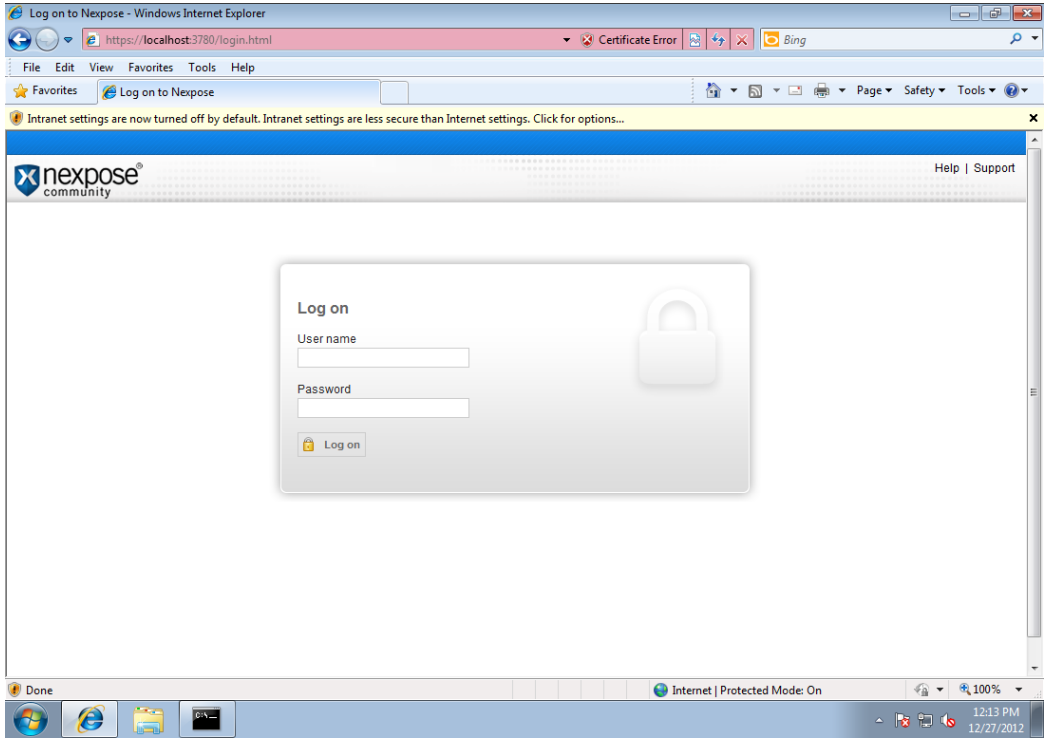


version comparison

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

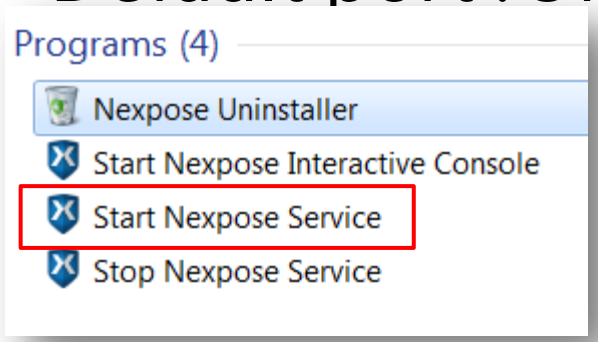
logging on and start to use

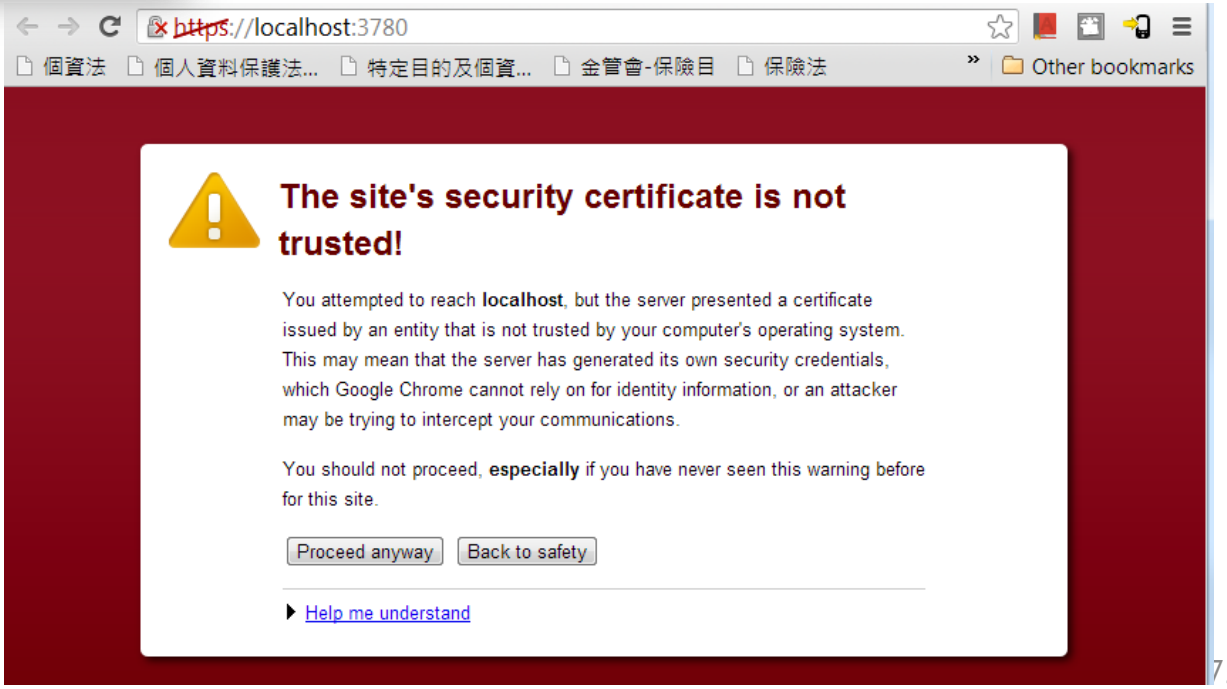
- supported browsers
  - Internet Explorer 7.0.x, 8.0.x, and 9.0
  - Mozilla Firefox 10.0.x and 17.0.x
  - Google Chrome



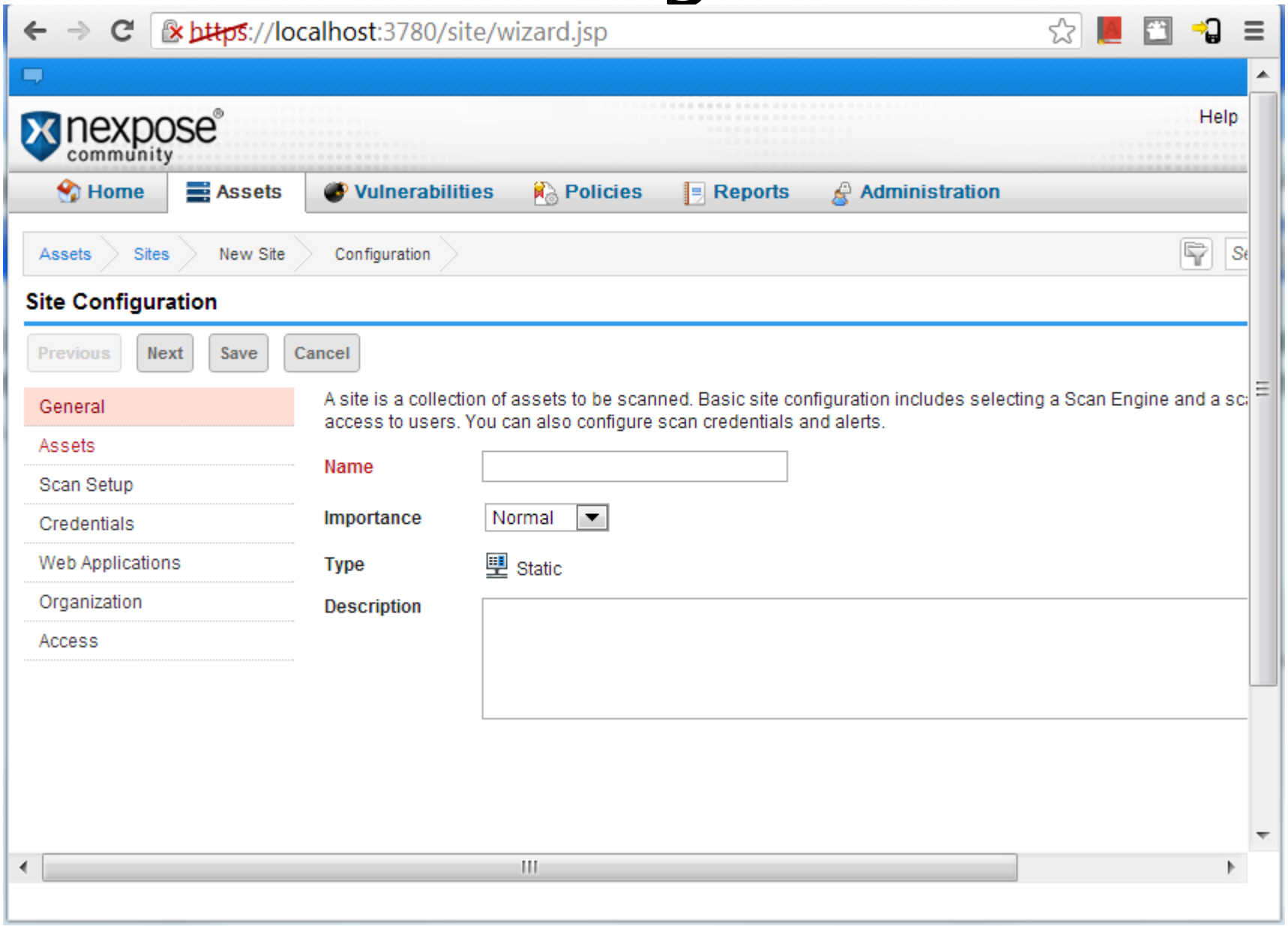
Connect nexpose Service

- Default port : 3780/tcp

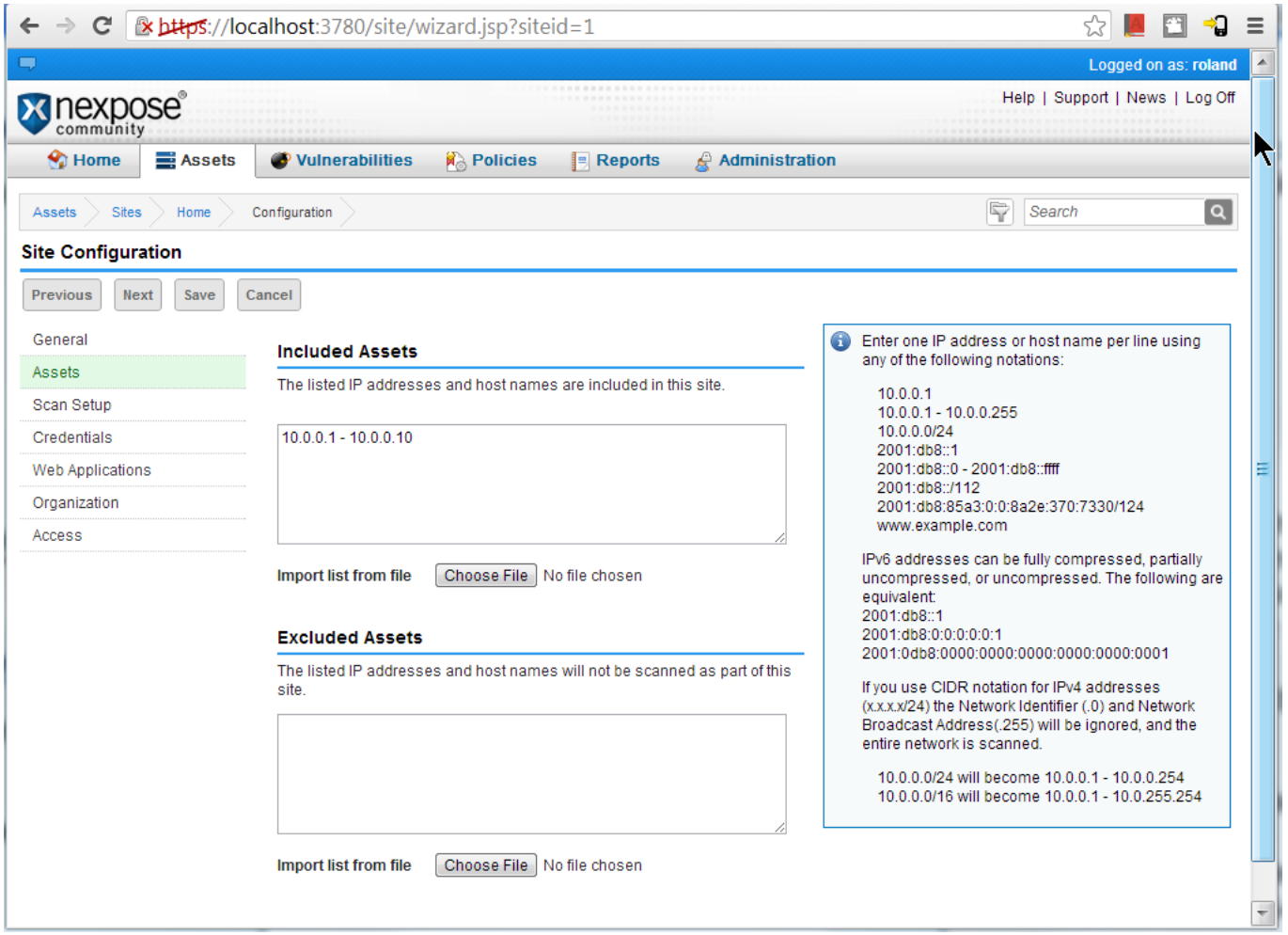




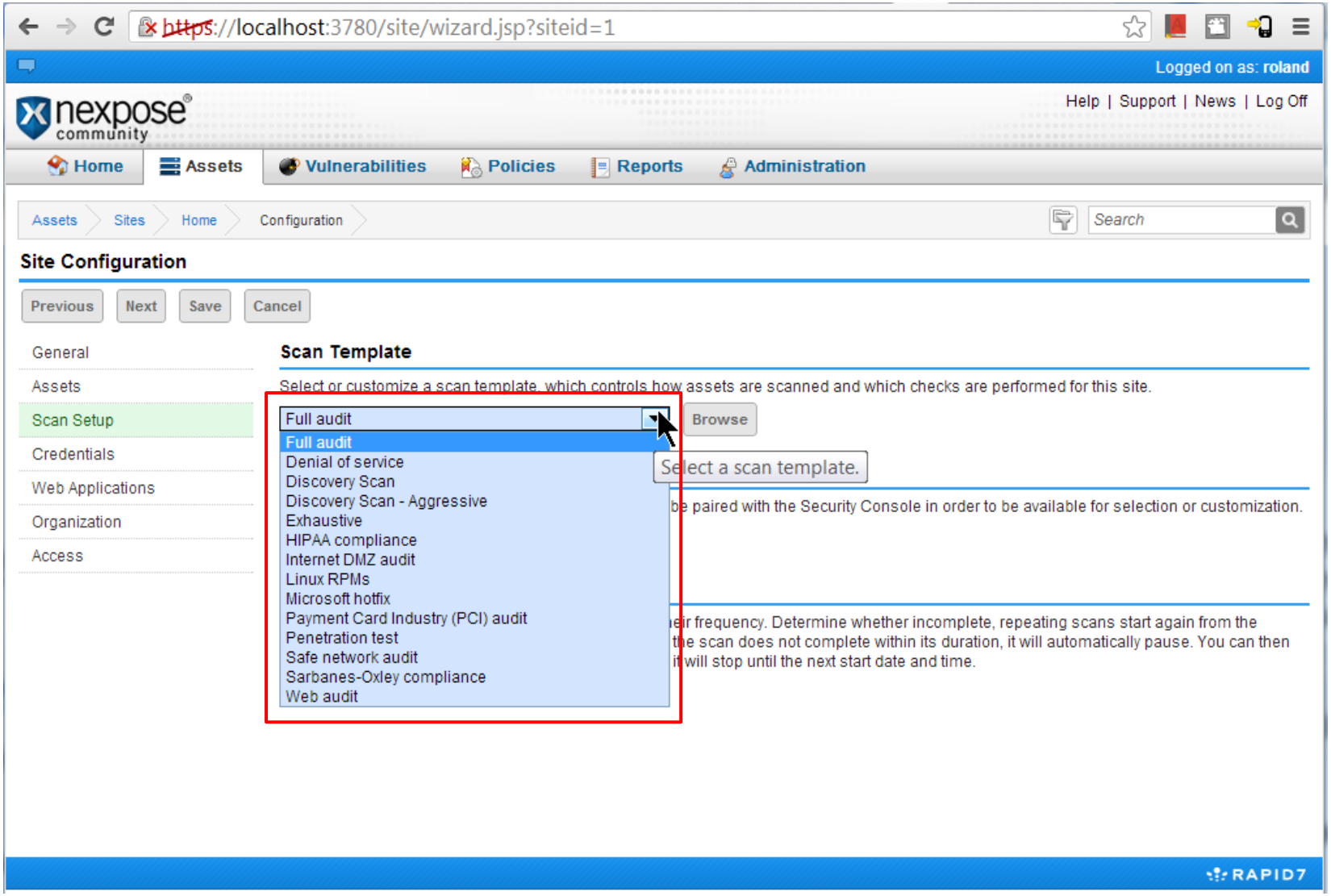
Site Configuration



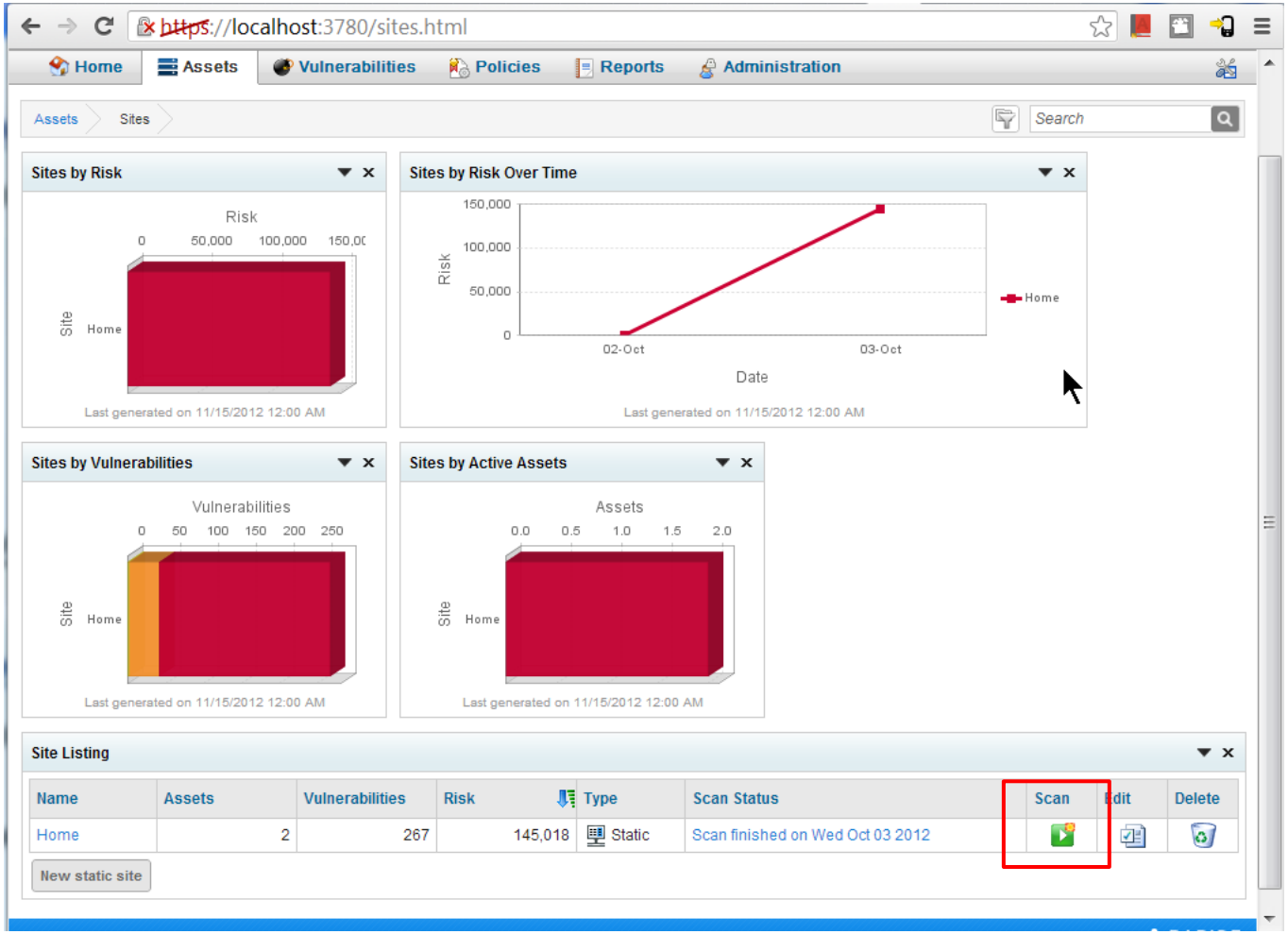
Assets Configuration



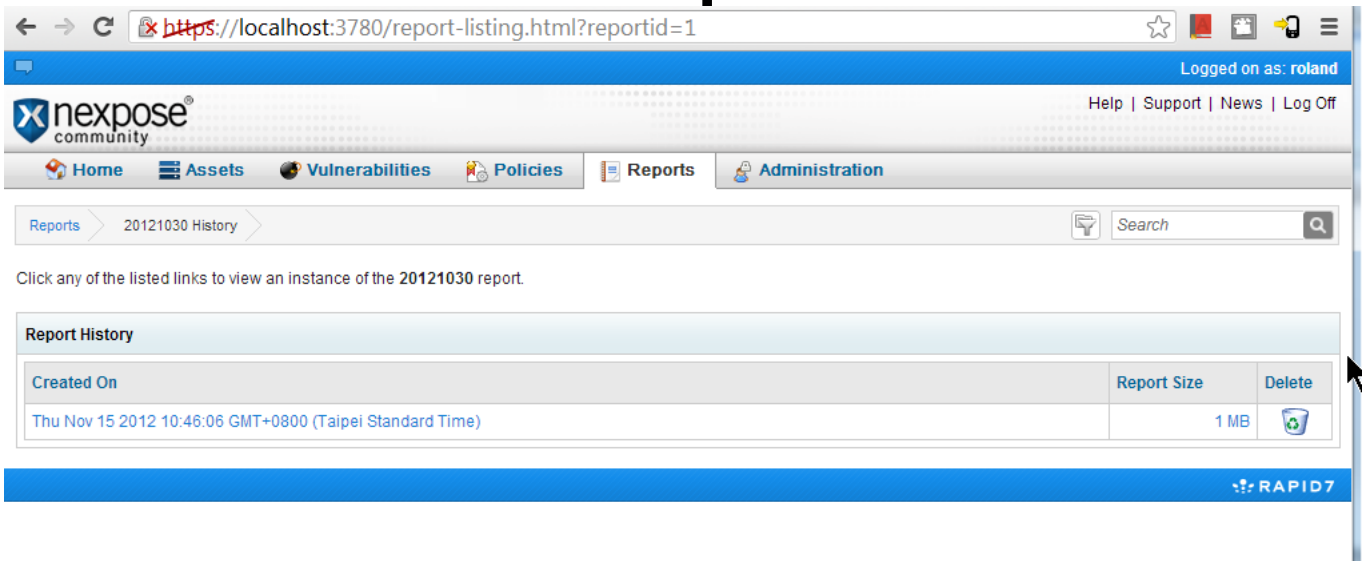
Scan Setup


https://localhost:3780/site/wizard.jsp?siteid=1
Logged on as: roland
nexpose community
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
Browse
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
Select a scan template.
be paired with the Security Console in order to be available for selection or customization.
eir 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


https://localhost:3780/sites.html
Home
Assets
Vulnerabilities
Policies
Reports
Administration
Assets
Sites
Search
Sites by Risk
Risk
0
50,000
100,000
150,00
Site
Home
Last generated on 11/15/2012 12:00 AM
Sites by Risk Over Time
150,000
100,000
50,000
0
Risk
02-Oct
03-Oct
Date
Home
Last generated on 11/15/2012 12:00 AM
Sites by Vulnerabilities
Vulnerabilities
0
50
100
150
200
250
Site
Home
Last generated on 11/15/2012 12:00 AM
Sites by Active Assets
Assets
0.0
0.5
1.0
1.5
2.0
Site
Home
Last generated on 11/15/2012 12:00 AM
Site Listing
Name
Assets
Vulnerabilities
Risk
Type
Scan Status
Scan
Edit
Delete
Home
2
267
145,018
Static
Scan finished on Wed Oct 03 2012
New static site

Report

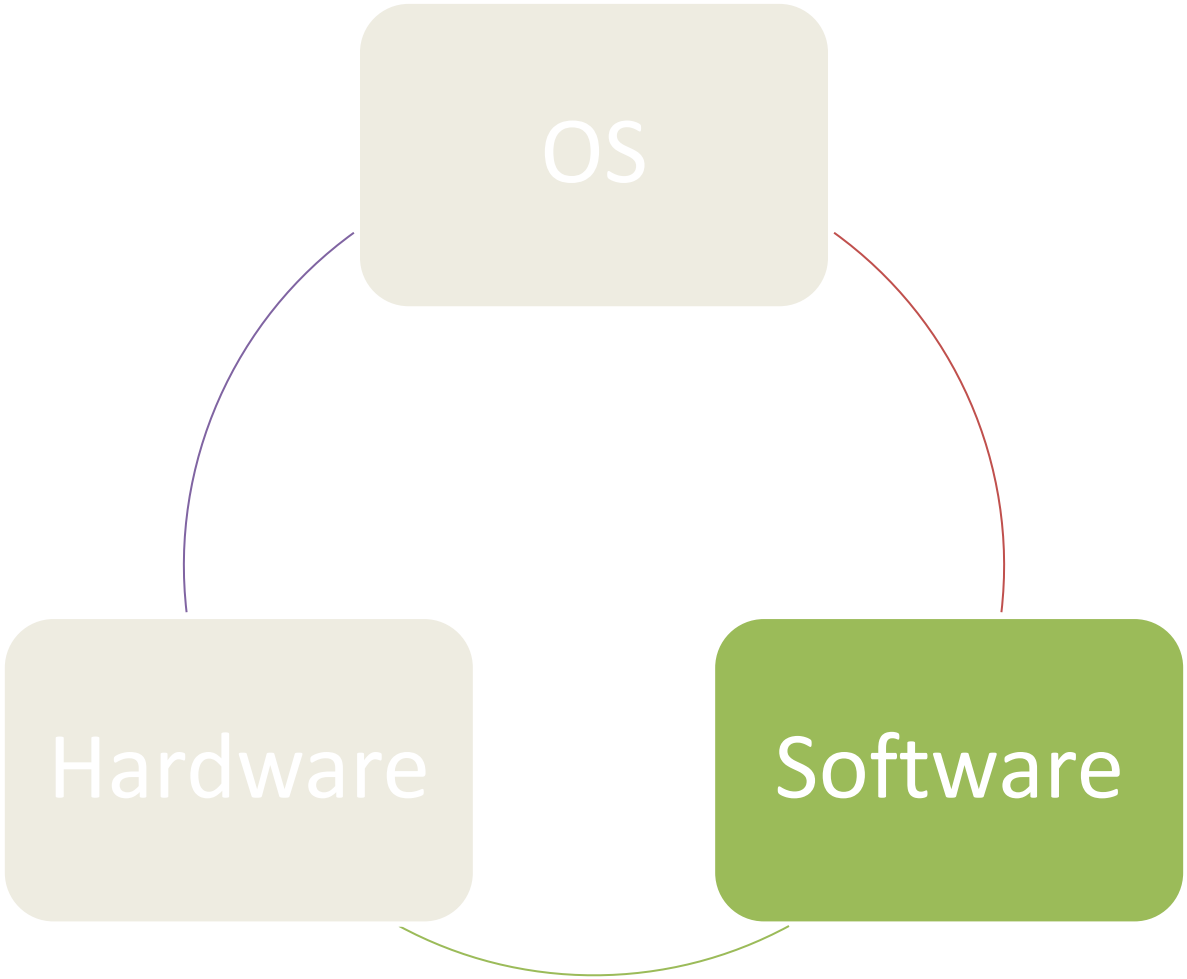

https://localhost:3780/report-listing.html?reportid=1
Logged on as: roland
nexpose community
Help | Support | News | Log Off
Home
Assets
Vulnerabilities
Policies
Reports
Administration
Reports
20121030 History
Search
Click any of the listed links to view an instance of the 20121030 report.
Report History
Created On
Report Size
Delete
Thu Nov 15 2012 10:46:06 GMT+0800 (Taipei Standard Time)
1 MB
RAPID7


Site Name
Start Time
End Time
Total Time
Status
Home
October 03, 2012 08:46, CST
October 03, 2012 08:52, CST
4 minutes
Success
Overall Risk Trend
Total Risk
Average Risk
Assets
Total Risk
Average Risk
Highest-Risk Site
Highest-Risk Asset
2 (was 0)
145,018 (was 0.0)
72,509 (was 0.0)
Home
145,018 (was 0.0)
002314AD7F54
144,030 (was 0.0)
The audit was performed on 2 systems, 2 of which were found to be active and were scanned.
Vulnerabilities by Severity
Critical
Severe
Moderate
Nodes by Vulnerability Severity
Critical
Severe
Moderate
Clean
There were 267 vulnerabilities found during this scan. Of these, 225 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 39 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 3 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities.
Critical vulnerabilities were found to exist on 1 of the systems, making them most susceptible to attack. 2 systems were found to have severe vulnerabilities. Moderate vulnerabilities were found on 2 systems. No systems were free of vulnerabilities.
Most Common Vulnerabilities
Most Common Vulnerability Categories
Remote Execution - 22.048%
Adobe - 20.063%
Adobe AcrobatReader - 14.734%
Denial of Service - 14.42%
Browsers - 7.001%
Mozilla - 6.897%
Mozilla Firefox - 6.897%
Adobe AIR - 5.329%
Web - 1.881%
XSS - 0.731%
There were 1 occurrences of the adobe-air-ove-2011-2130, adobe-air-ove-2011-2134, adobe-air-ove-2011-2135, adobe-air-ove-2011-2136, adobe-air-ove-2011-2137, adobe-air-ove-2011-2425, adobe-air-ove-2011-2445, adobe-air-ove-2011-2450, adobe-air-ove-2011-2451 and adobe-air-ove-2011-2452 vulnerabilities, making them the most common vulnerabilities. There were 211 vulnerabilities in the Remote Execution category, making it the most common vulnerability category.

課程大綱

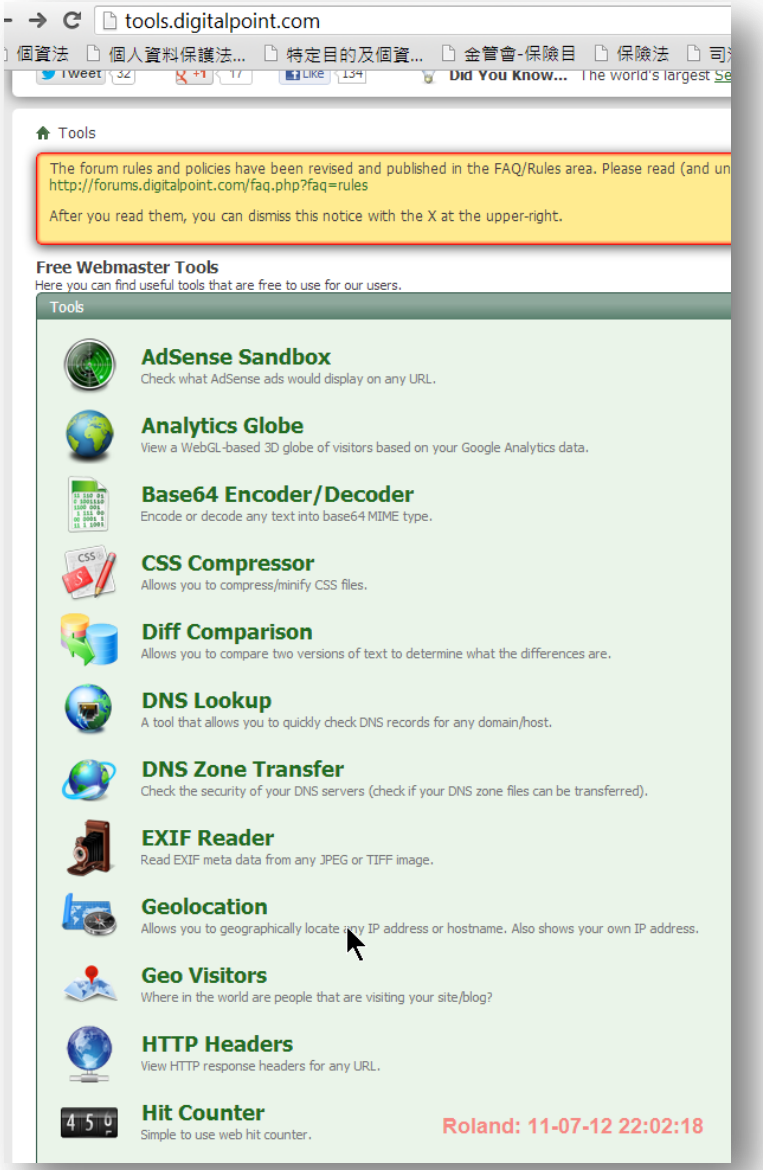
大綱	內容	時間
資訊安全檢測類型	1. 資安稽核 2. 弱點掃描 3. 滲透測試	6 小時 9:00~12:00 13:30~16:30 (每 50 分鐘休息 10 分鐘)
駭客思維與滲透測試	1. 駭客攻擊程序 2. 滲透測試程序 3. 滲透測試方法	
滲透測試相關規範與指引	1. OSSTMM 2. PTES 3. OWASP Testing Guide 4. SANS Top 20 5. OWASP Top 10	
滲透測試工具	1. 弱點掃描軟體 2. 滲透測試工具	
網頁應用程式滲透測試	1. SQL injection 2. XSS	
實務案例	實務案例解析	

PT Environment



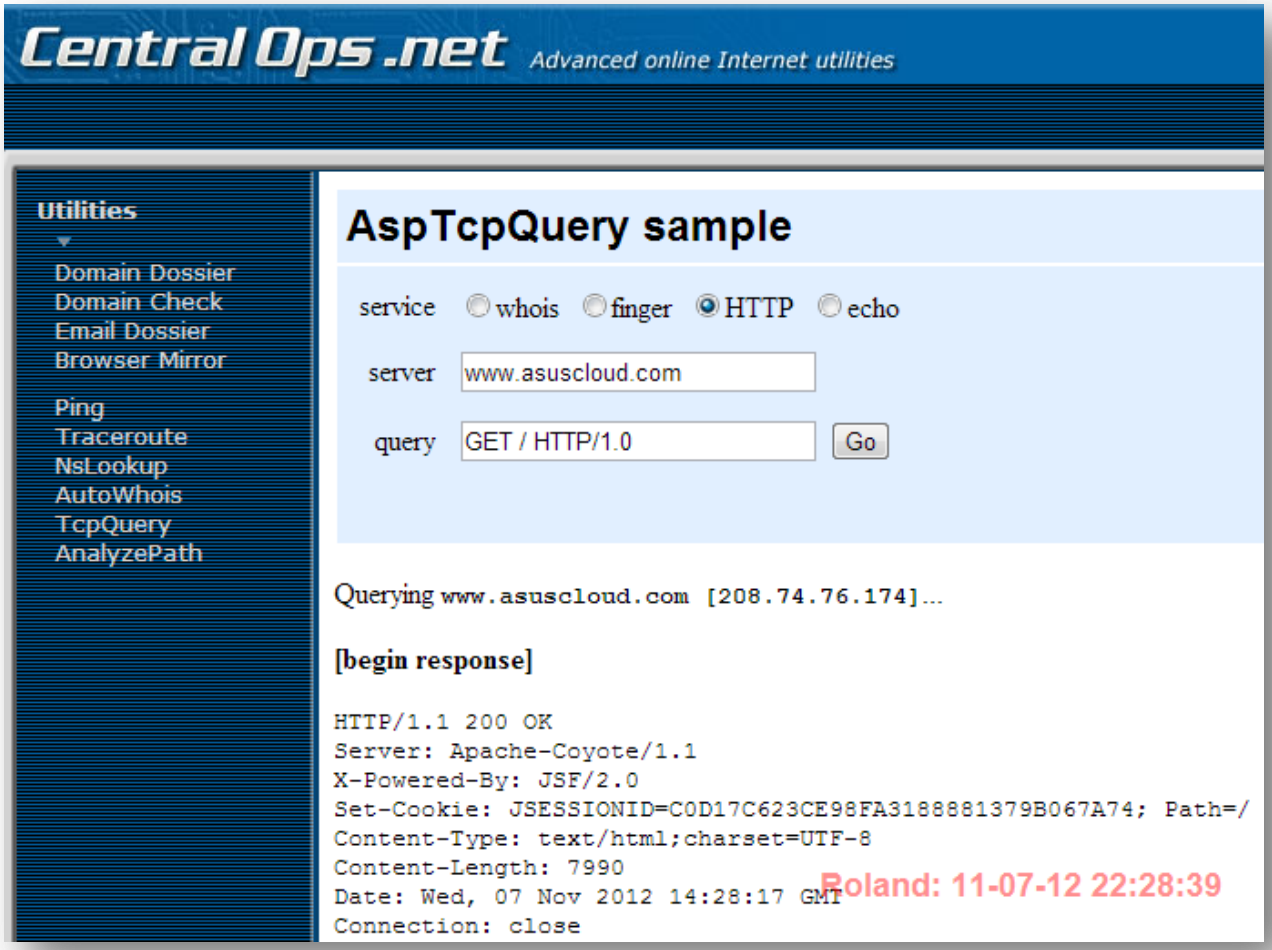
Web-based Recon Tools

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



Web-based Recon Tools

- http://centralops.net/co



Cloud-based Tools

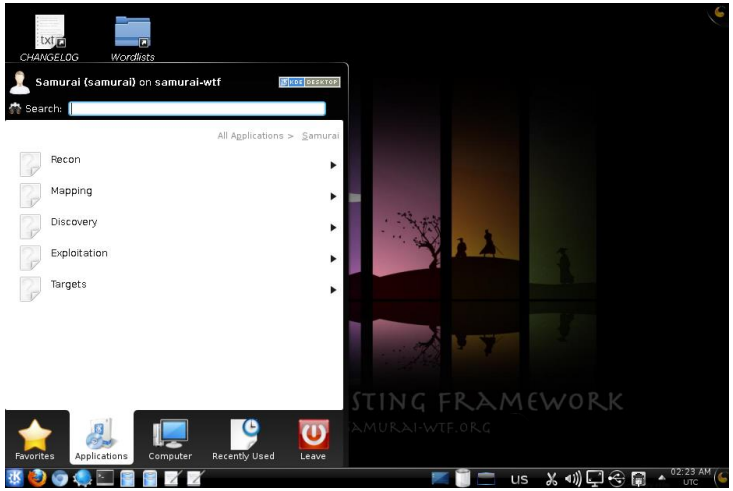
- CloudShark
- SHODAN
- PunkSpider
- WebSecurity ($)

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

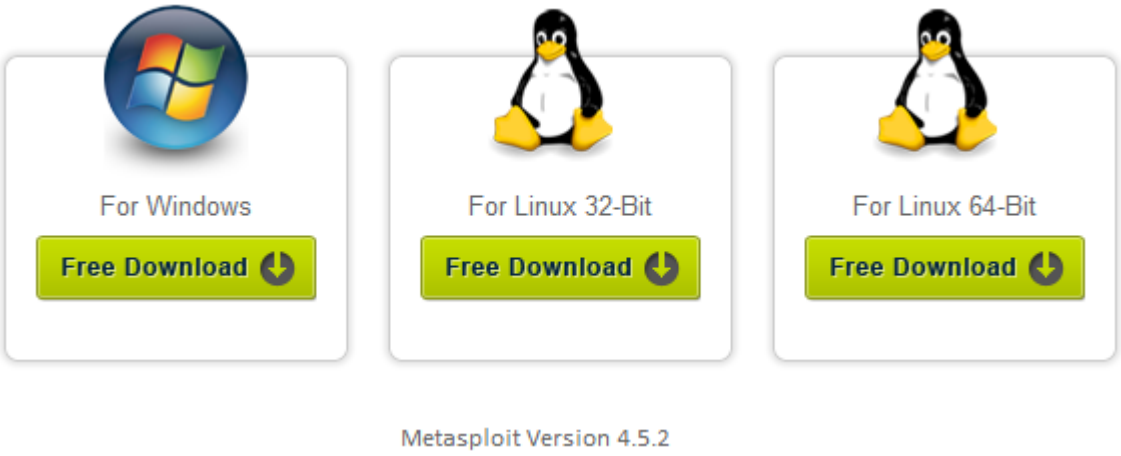
- OWASP Live CD (2008)
- Samurai WTF (2012)
- Web Security Dojo (2013)



What's Metasploit?

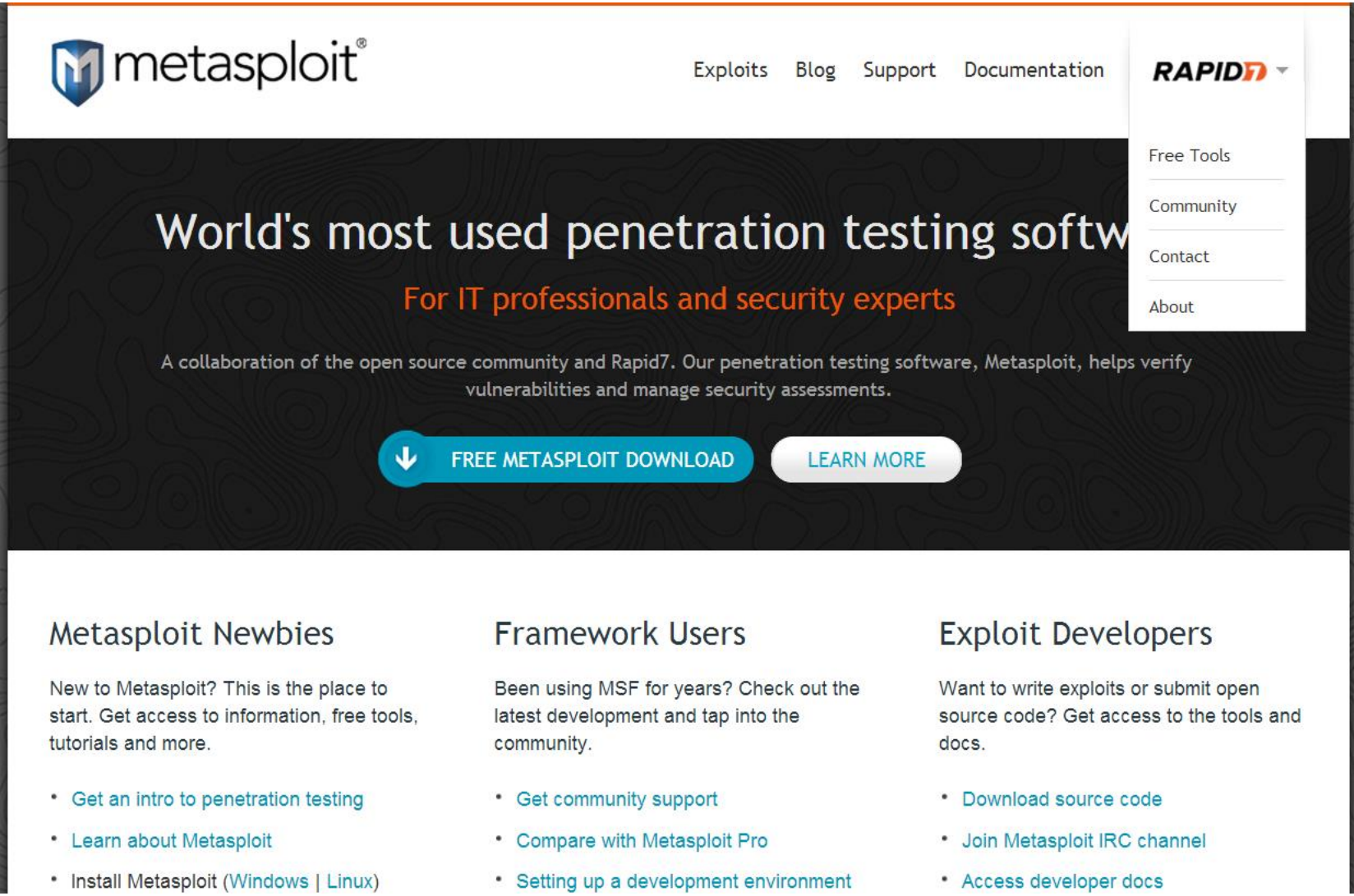
- Live framework for penetration testing
- From basic to advanced exploitation
- From manual to automatic exploiting
- From one-time to comprehensive
- Integrate with 3-rd party tools
- Designed by HD Moore
- COTS based on msf(metasploit framework)
  - Metasploit Express
  - Metasploit Pro

Supported OS



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

Who Made It?

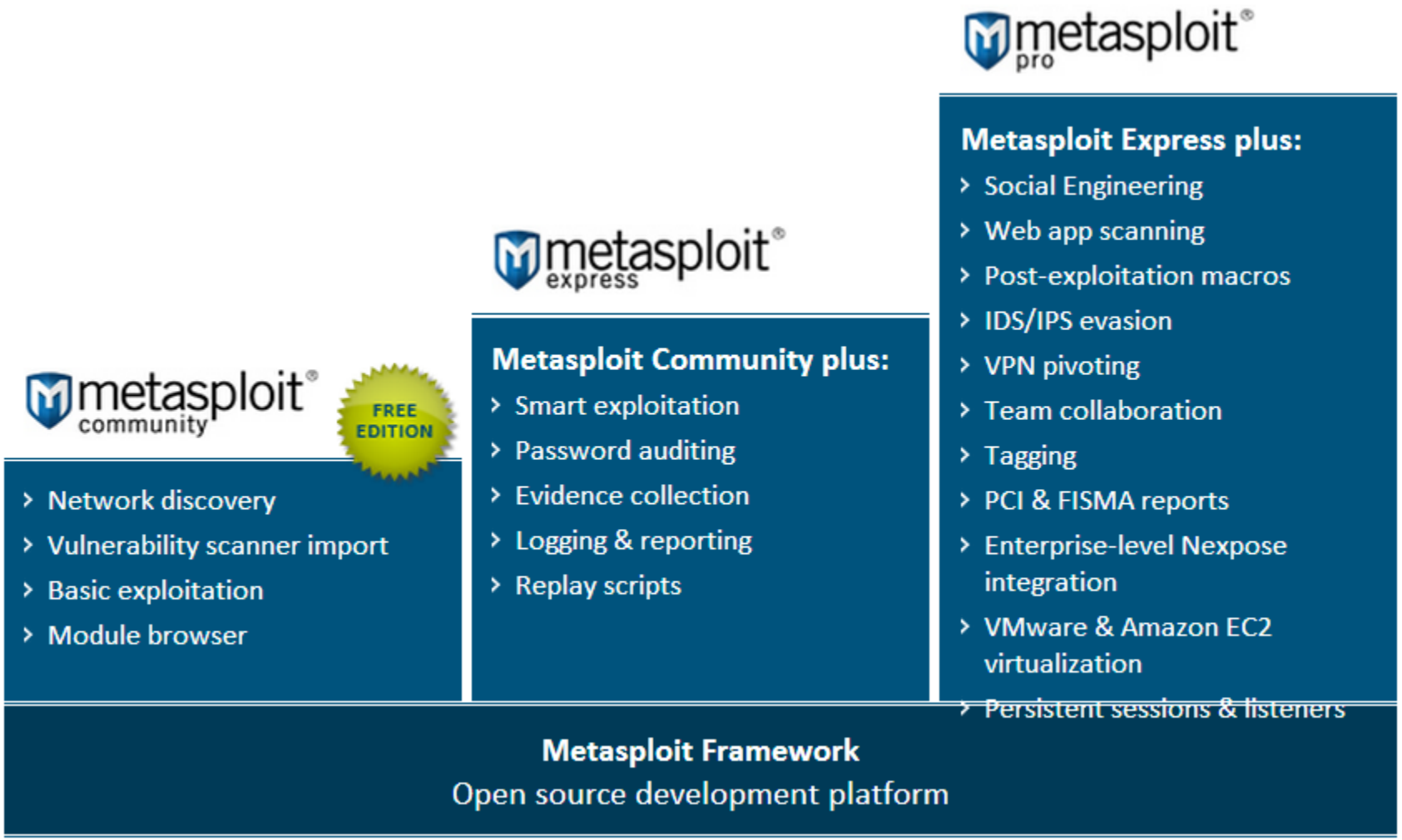

metasploit
Exploits
Blog
Support
Documentation
RAPID7
Free Tools
Community
Contact
About
World's most used penetration testing softw
For IT professionals and security experts
A collaboration of the open source community and Rapid7. Our penetration testing software, Metasploit, helps verify vulnerabilities and manage security assessments.
FREE METASPLOIT DOWNLOAD
LEARN MORE
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?

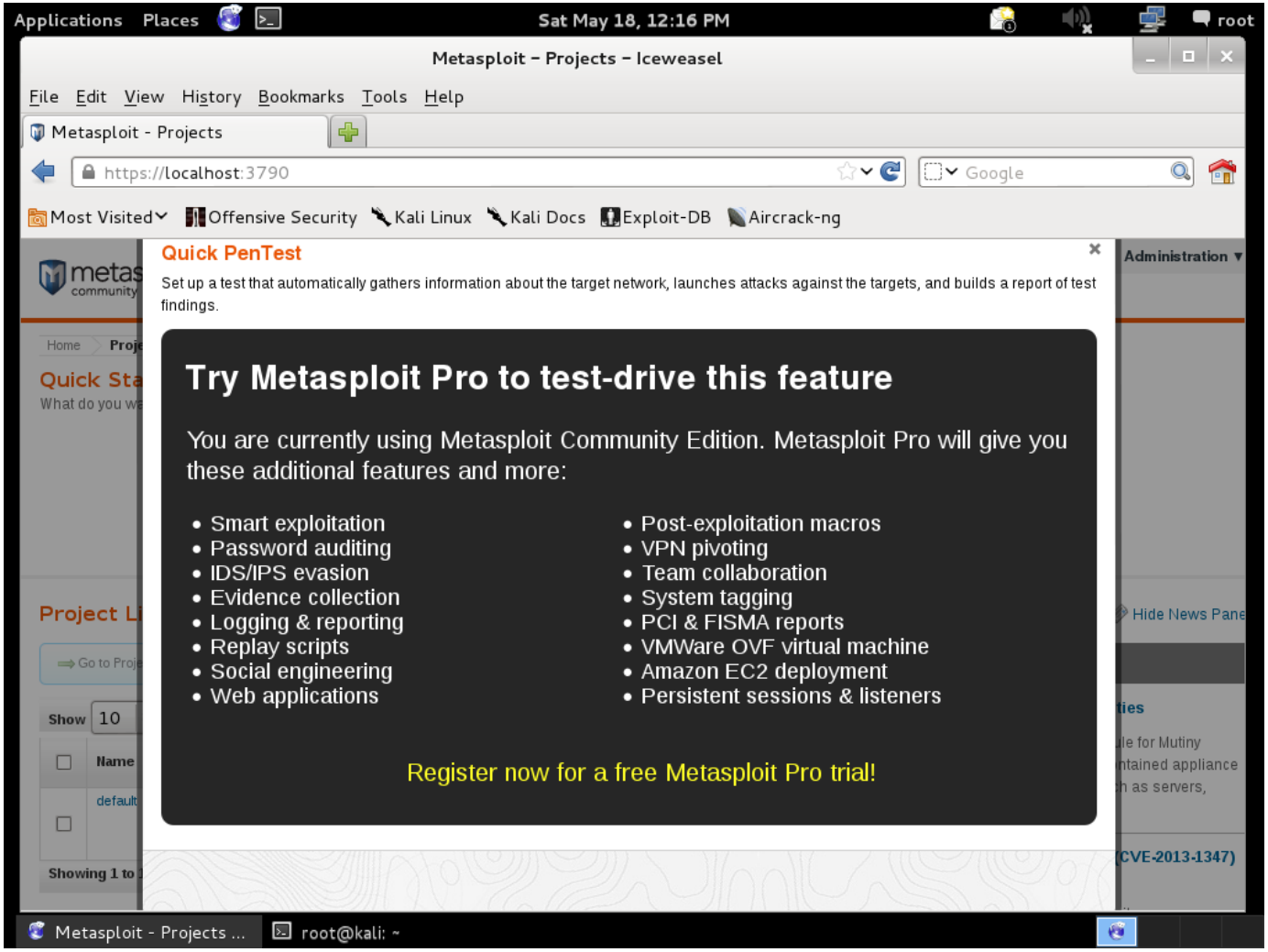
VA

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

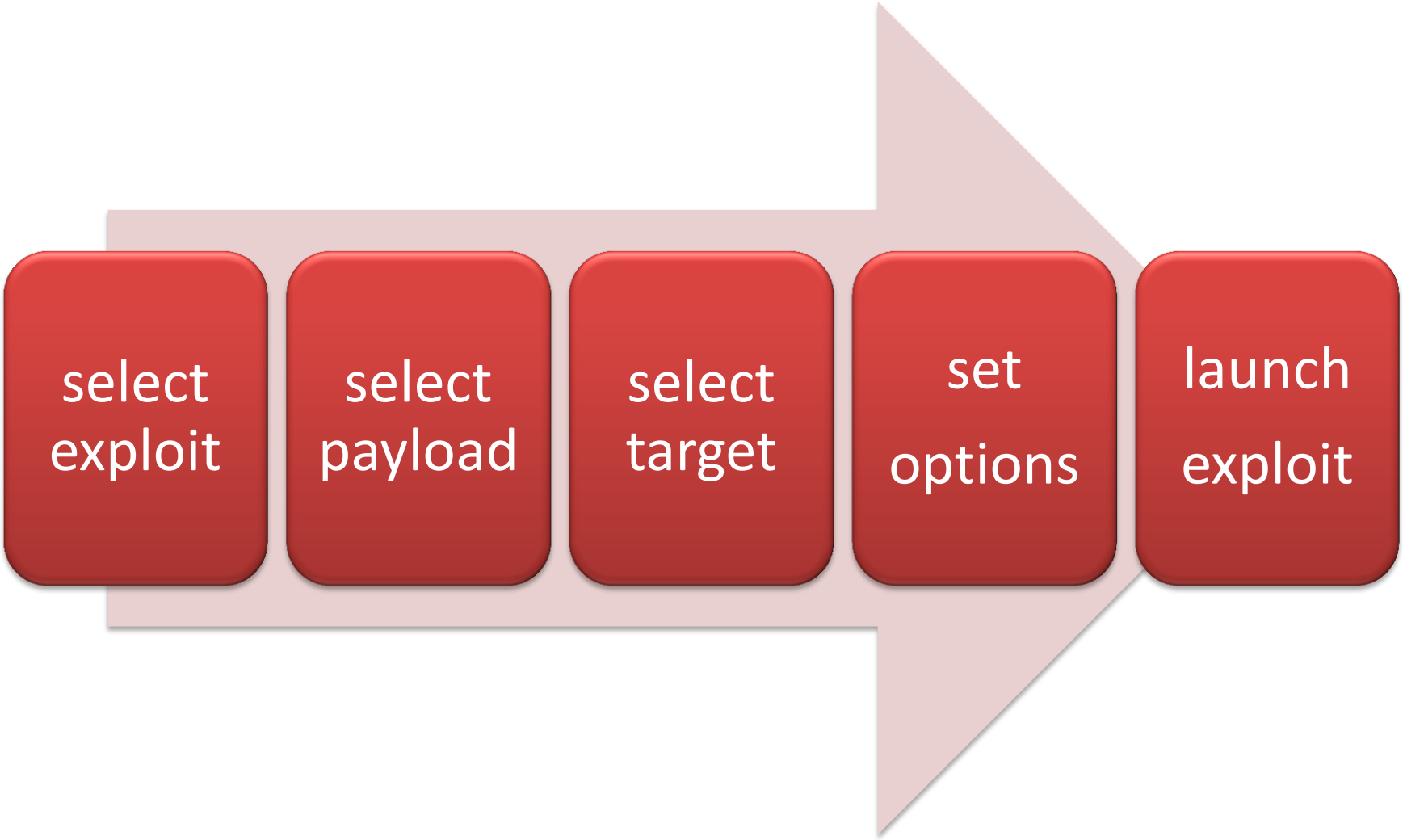
msf versions



Metasploit Pro



steps of exploitation in msf



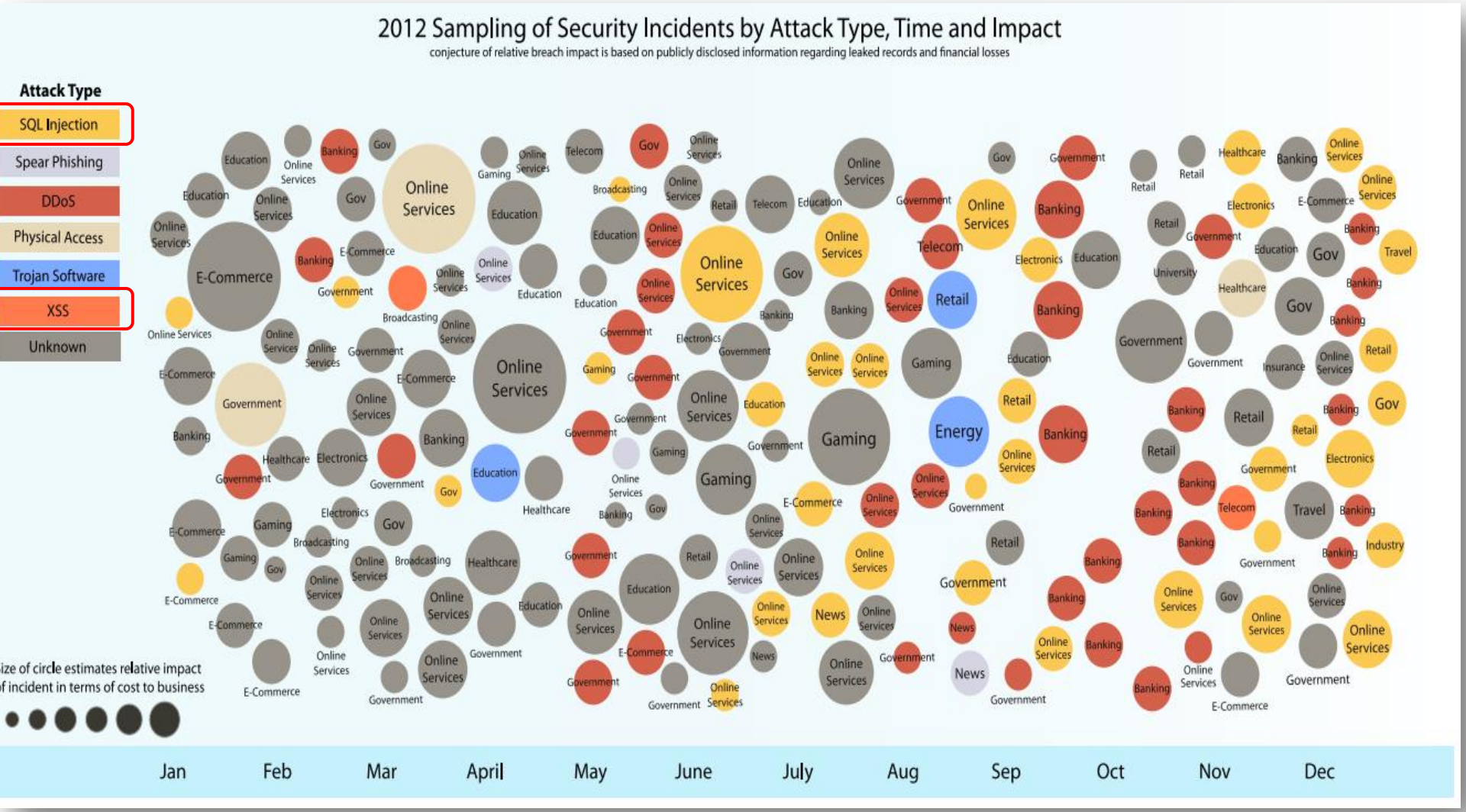
metasploit demo

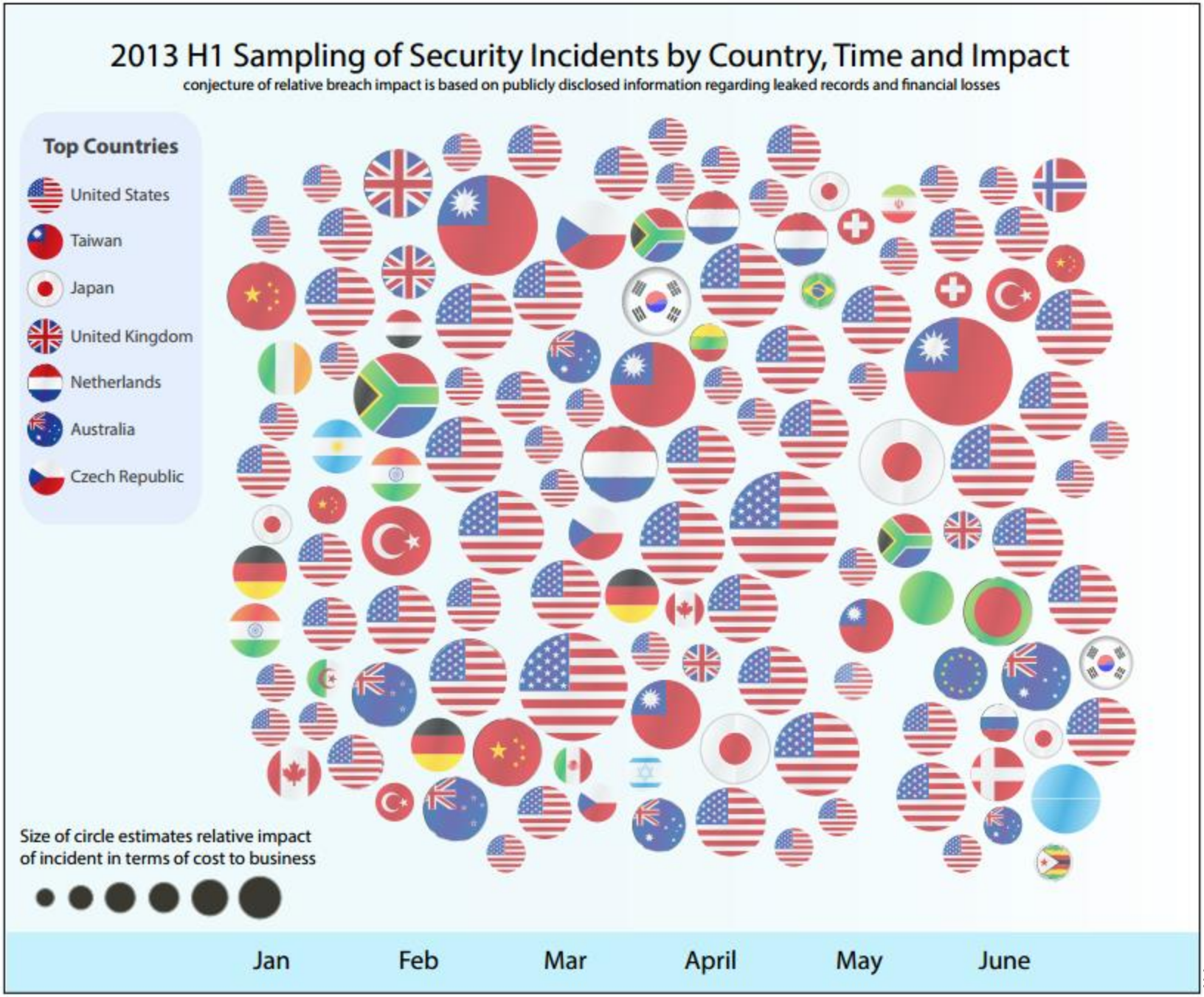
1. 社交工程攻擊瀏覽器弱點，入侵系統
2. 利用系統弱點，將步驟 1 獲得的一般權限，提昇為系統權限

課程大綱

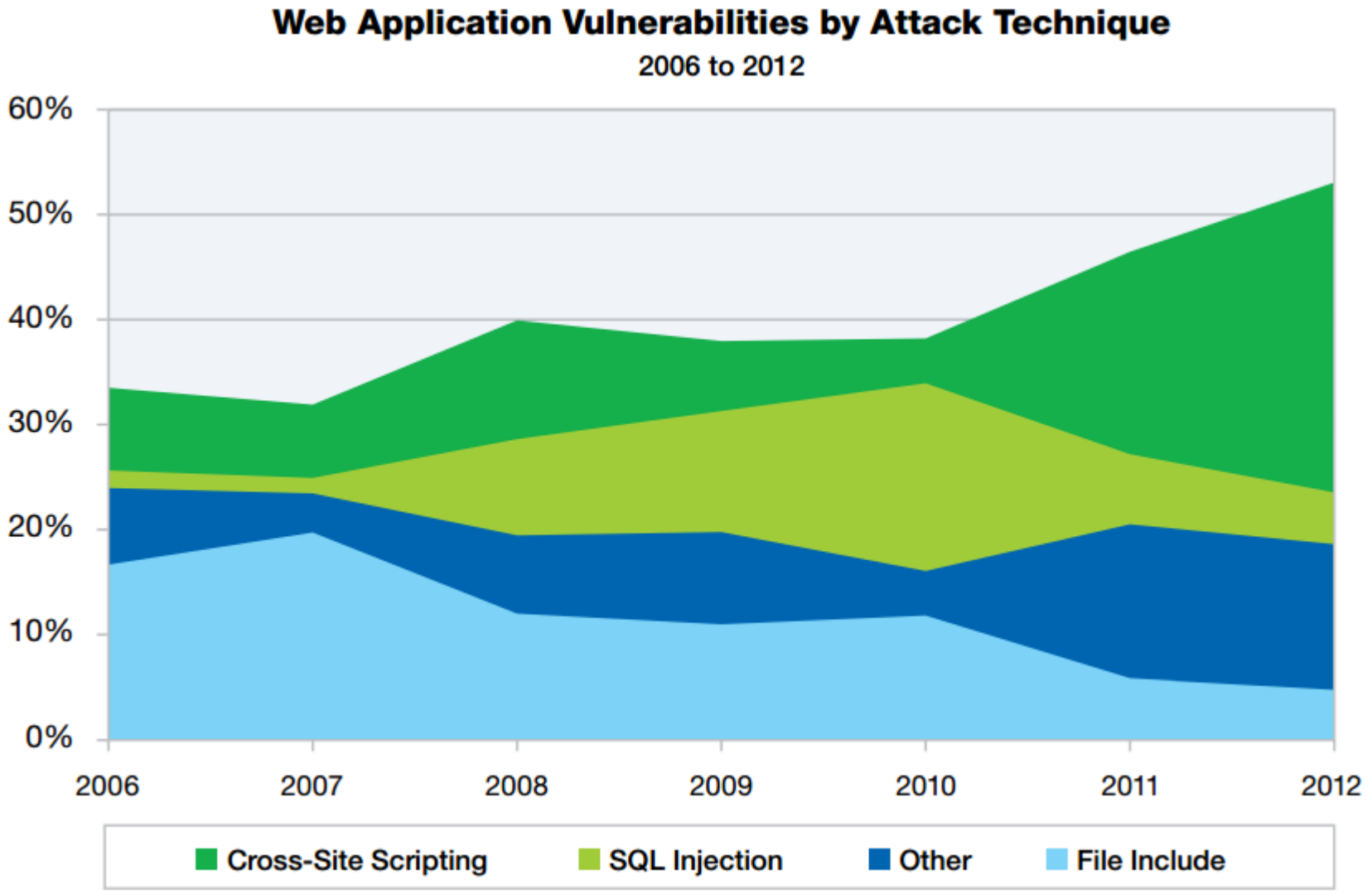
大綱	內容	時間
資訊安全檢測類型	1. 資安稽核 2. 弱點掃描 3. 滲透測試	6 小時 9:00~12:00 13:30~16:30 (每 50 分鐘休息 10 分鐘)
駭客思維與滲透測試	1. 駭客攻擊程序 2. 滲透測試程序 3. 滲透測試方法	
滲透測試相關規範與指引	1. OSSTMM 2. PTES 3. OWASP Testing Guide 4. SANS Top 20 5. OWASP Top 10	
滲透測試工具	1. 弱點掃描軟體 2. 滲透測試工具	
網頁應用程式滲透測試	1. SQL injection 2. XSS	
實務案例	實務案例解析	

Total Threat Trend



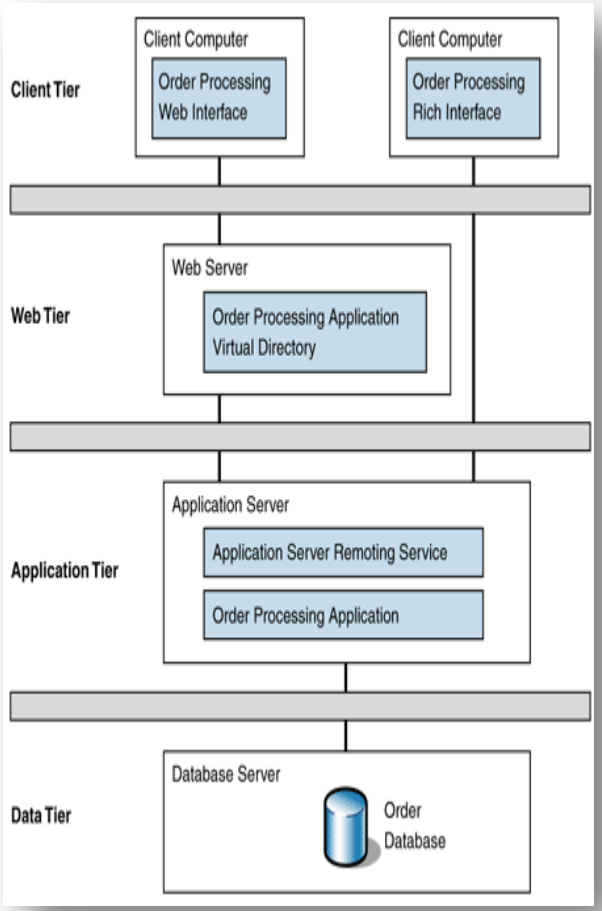

2013 H1 Sampling of Security Incidents by Country, Time and Impact
conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses
Top Countries
United States
Taiwan
Japan
United Kingdom
Netherlands
Australia
Czech Republic
Size of circle estimates relative impact of incident in terms of cost to business
Jan
Feb
Mar
April
May
June

Web Application Attack Trend



source：IBM xforce report 2012

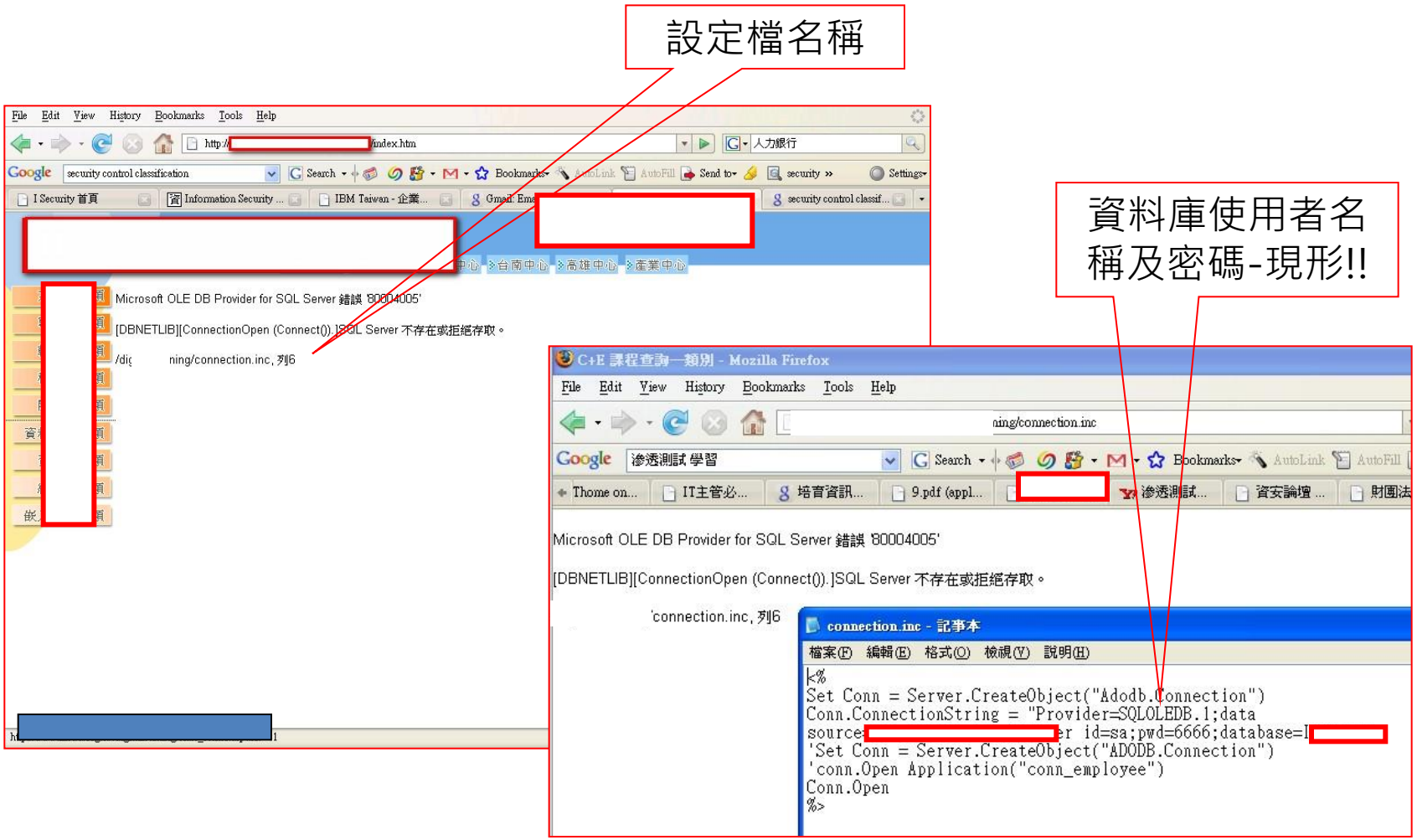
應用程式安全全景



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

左圖: http://msdn.microsoft.com/en-us/library/ff647195.aspx

案例：網頁設計不當洩露機密資訊



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 'i1pjf3tcxy22zuhaszs0ugjf' 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狀況。請檢閱堆疊追蹤以取得錯誤的詳細資訊，以及在程式碼中產生的位置。

例外詳細資訊: System.Data.SqlClient.SqlException: 接近 'i1pjf3tcxy22zuhaszs0ugjf' 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 'i1pjf3tcxy22zuhaszs0ugjf' 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.[redacted].ClsDBIO.Exc(List`1 iaSql) in C:\Office\TWPWeb\OmegaLib4\ClsDBIO.vb:466

[Exception: 接近 'i1pjf3tcxy22zuhaszs0ugjf' 之處的語法不正確。
遺漏字元字串 ')' 後面的引號。
Data Source=[redacted].205;Initial Catalog=CloudDB;User ID=CloudDBUser;Password=clouduser[redacted]]
   tw.com.[redacted].ClsDBIO.HandleEx(Exception ex) in C:\Office\TWPWeb\OmegaLib4\ClsDBIO.vb:841
   tw.com.[redacted].ClsDBIO.Exc(List`1 iaSql) in C:\Office\TWPWeb\OmegaLib4\ClsDBIO.vb:474

[Exception: 接近 'i1pjf3tcxy22zuhaszs0ugjf' 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.[redacted].ClsDBIO.HandleEx(Exception ex) in C:\Office\TWPWeb\OmegaLib4\ClsDBIO.vb:841
   tw.com.[redacted].ClsDBIO.Exc(List`1 iaSql) in C:\Office\TWPWeb\OmegaLib4\ClsDBIO.vb:480
   tw.com.[redacted].ClsDataUtil.SaveRec(Int32& idx, String iAgentId, String iFuncName, String iRtnMsg, String iSessionId) in C:\Office\TWPWeb\TWPWebLib\ClsDataUtil.vb:416
   tw.com.[redacted].ClsCloudUtil.RecRtn(Int32& idx, String iAgentId, String iMsg, String iSessionId, Boolean iRec) in C:\Office\TWPWeb\TWPWebLib\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

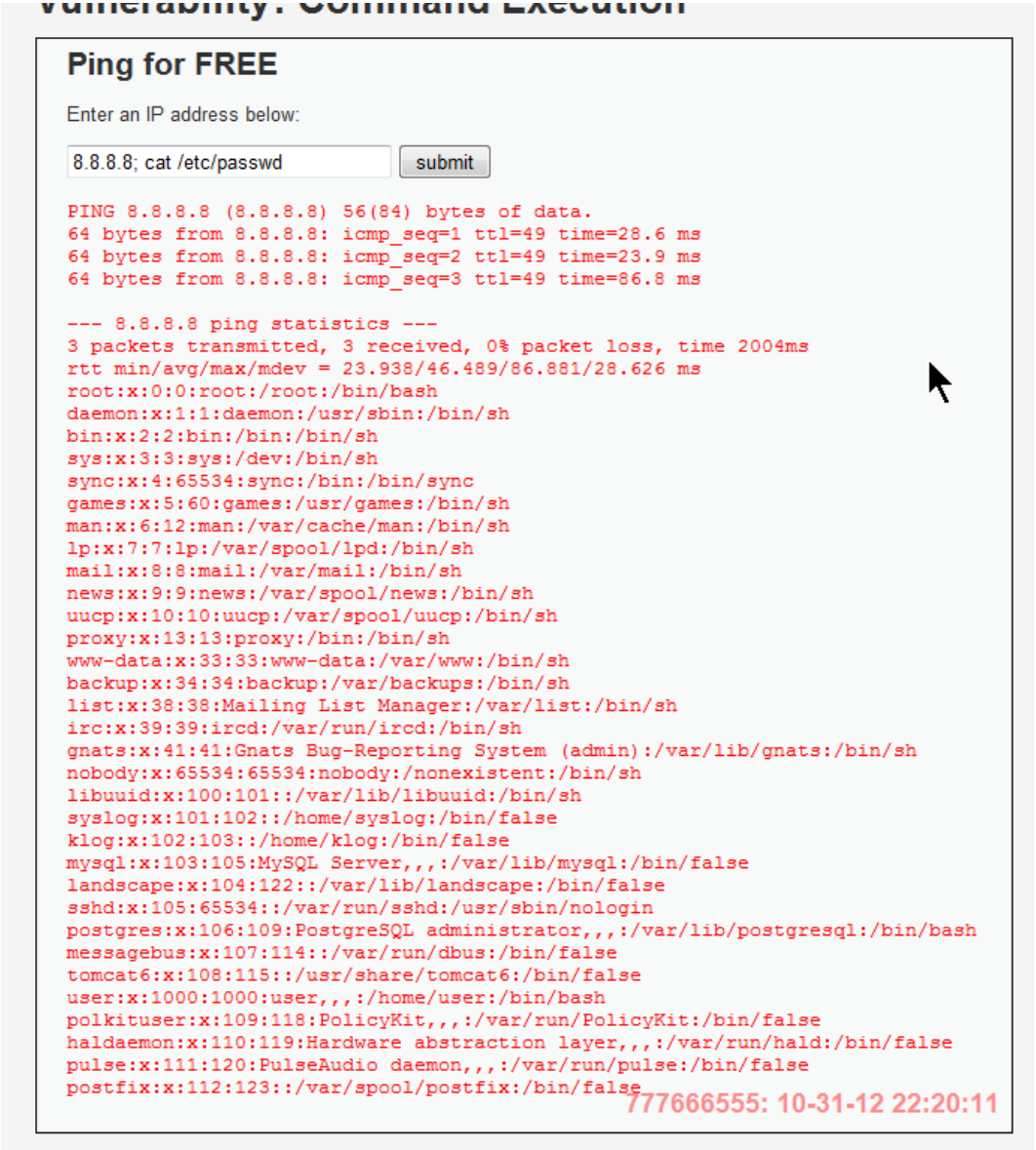
OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure 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

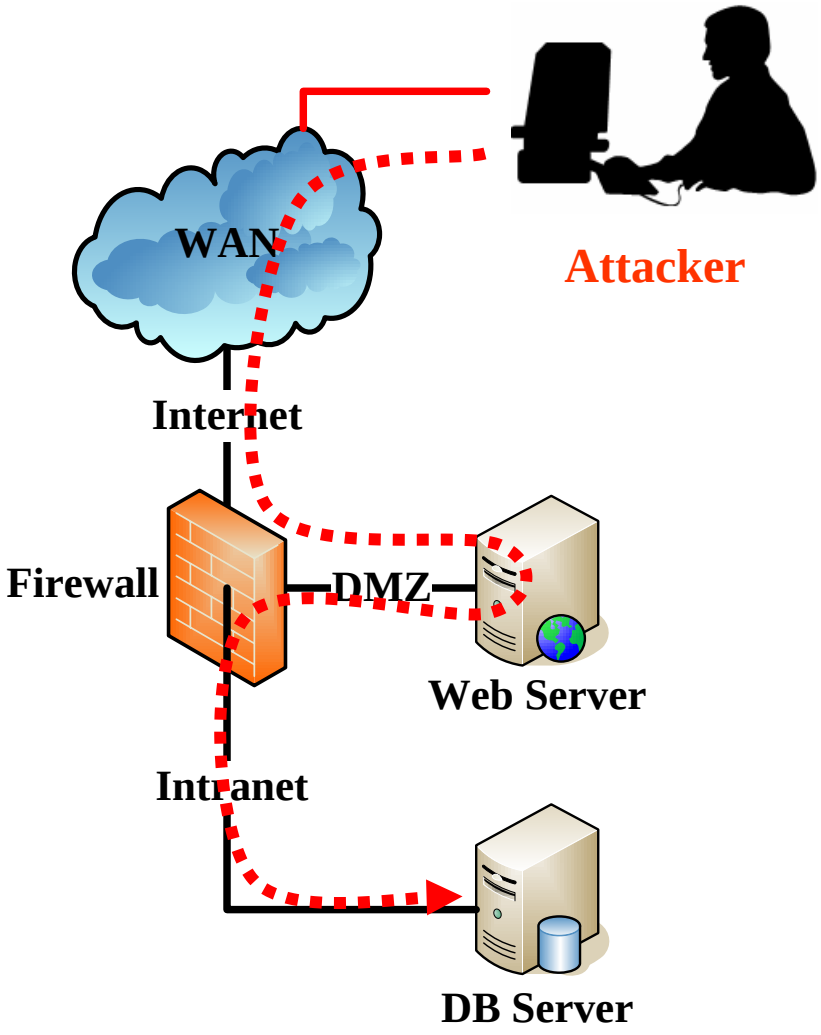
- Definition
  - Turns data(parameter) into "command"(OS, SQL) of interpreters
  - SQL queries, LDAP queries, XPath queries, OS commands, program arguments
- Target
  - Interpreters(e.g. database, OS shell)
- Threat
  - Untrusted data
- Impact
  - A, I, C

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



SQL Injection(SQLi)



Threat

攻擊者經由網站應用程式入侵資料庫

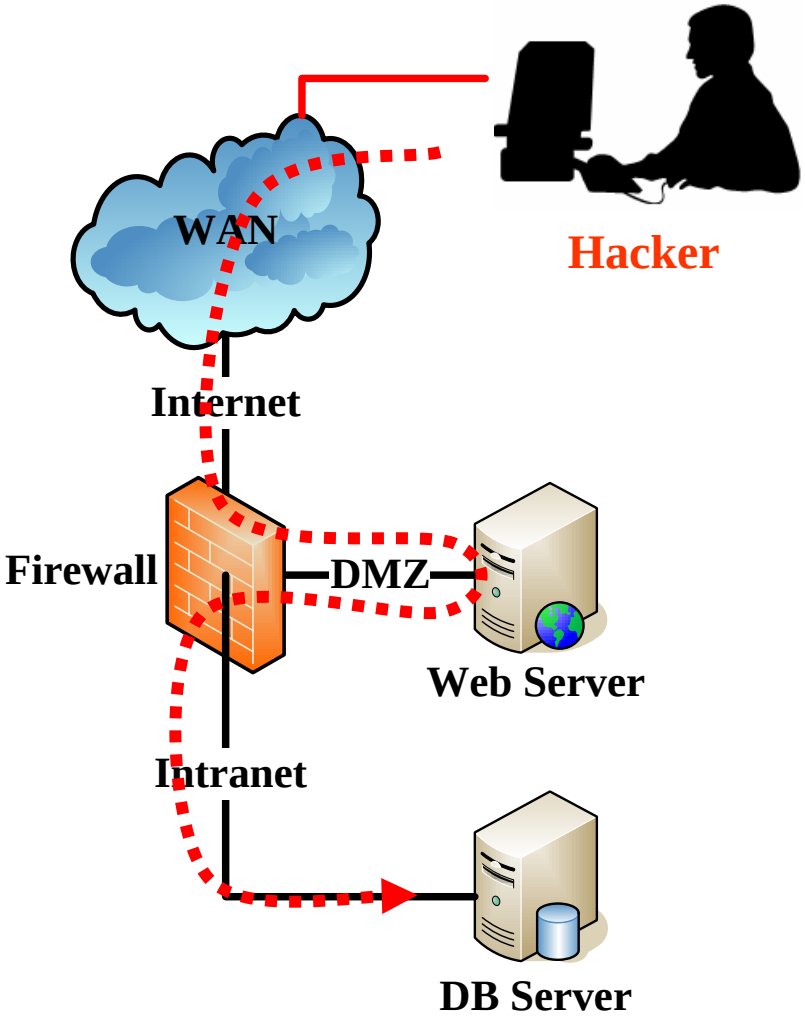
Weakness

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

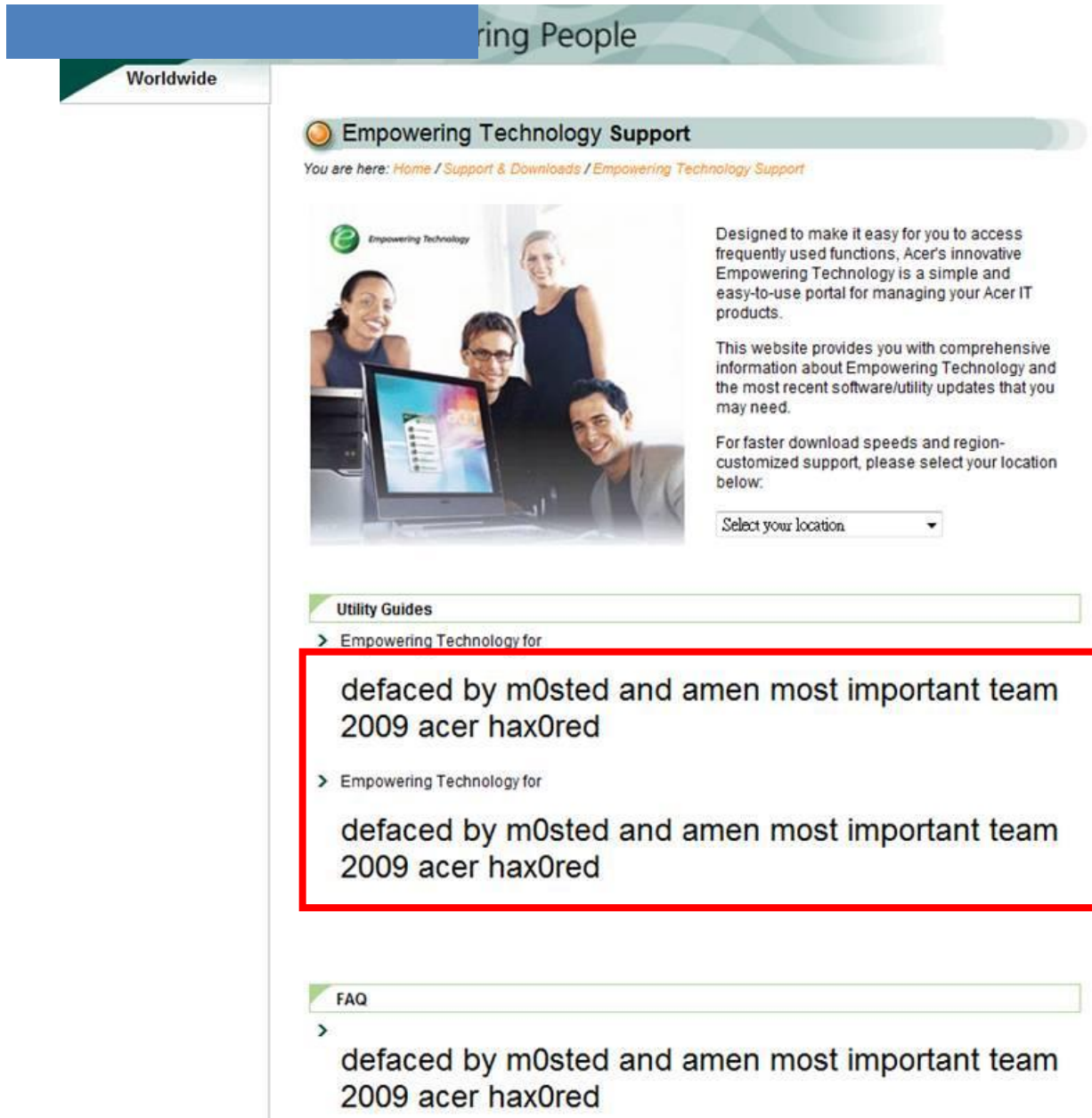
Impact of SQL Injection



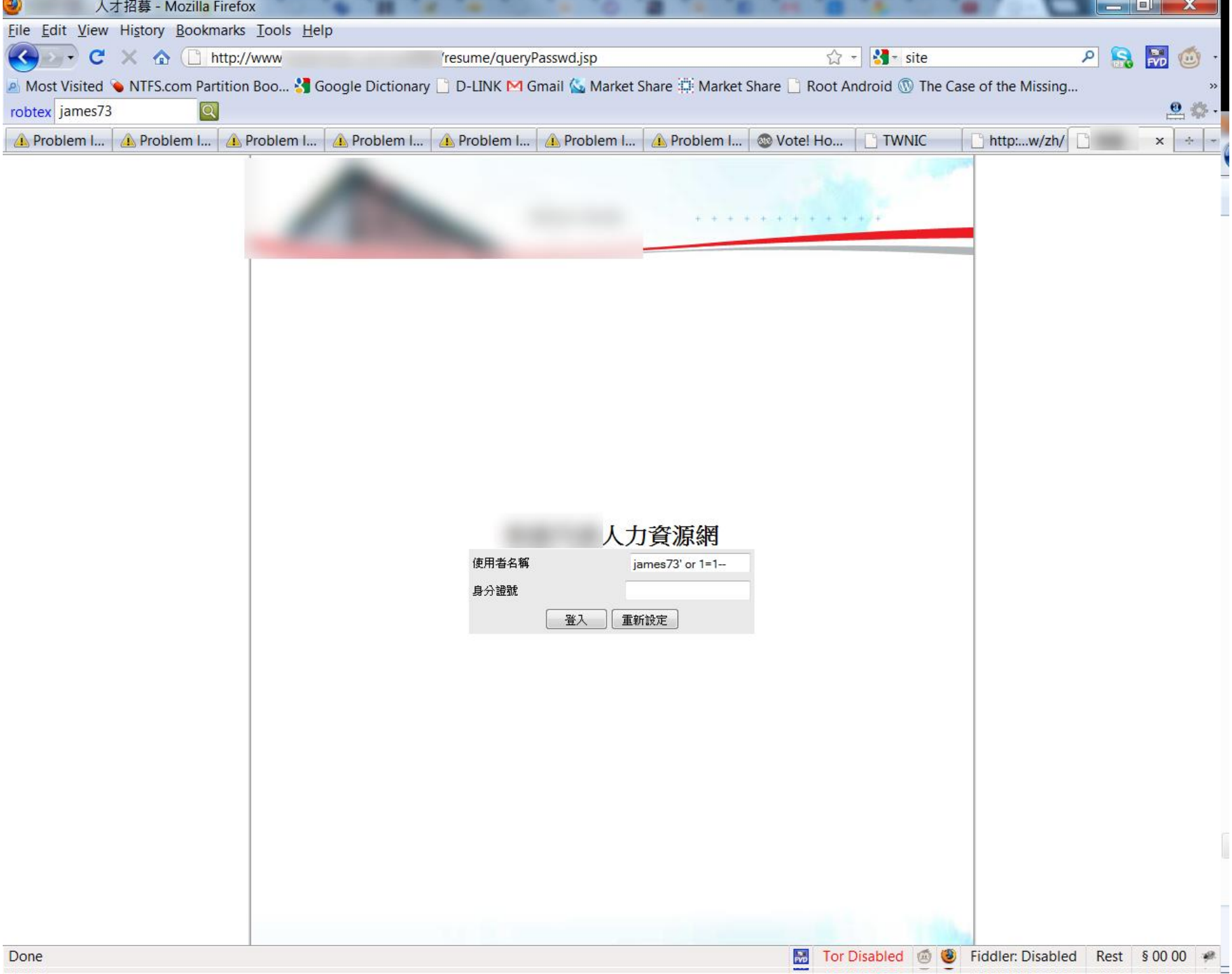
- Bypass Authentication
- Escalate Privilege
- Steal Data
- Tamper with Data
- Tamper with OS Configurations
- Disrupt DB Service


ZU 0666', 0, 0); DROP DATABASE TABLICE;

SQL Injection 篡改資料庫



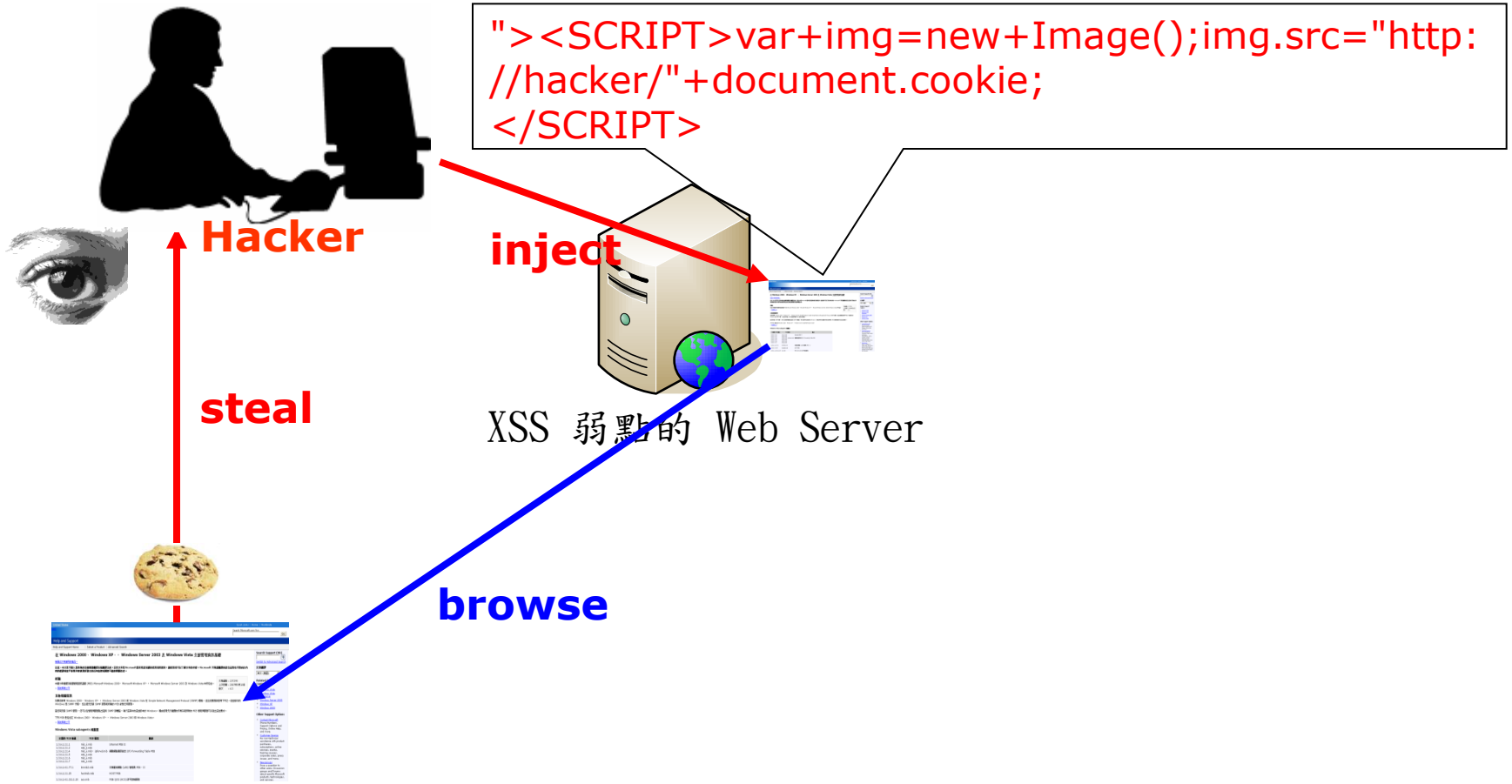
Database Server


人才招募 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www 'resume/queryPasswd.jsp
site
Most Visited NTFS.com Partition Boo... Google Dictionary D-LINK Gmail Market Share Market Share Root Android The Case of the Missing...
robtex james73
Problem l... Problem l... Problem l... Problem l... Problem l... Problem l... Problem l... Vote! Ho... TWNIC http:...w/zh/
人力資源網
使用者名稱 james73' or 1=1--
身分證號
登入 重新設定
Done
Tor Disabled
Fiddler: Disabled
Rest
§ 00 00

Demo：Bypass Authentication

Demo: Data Disclosure

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)

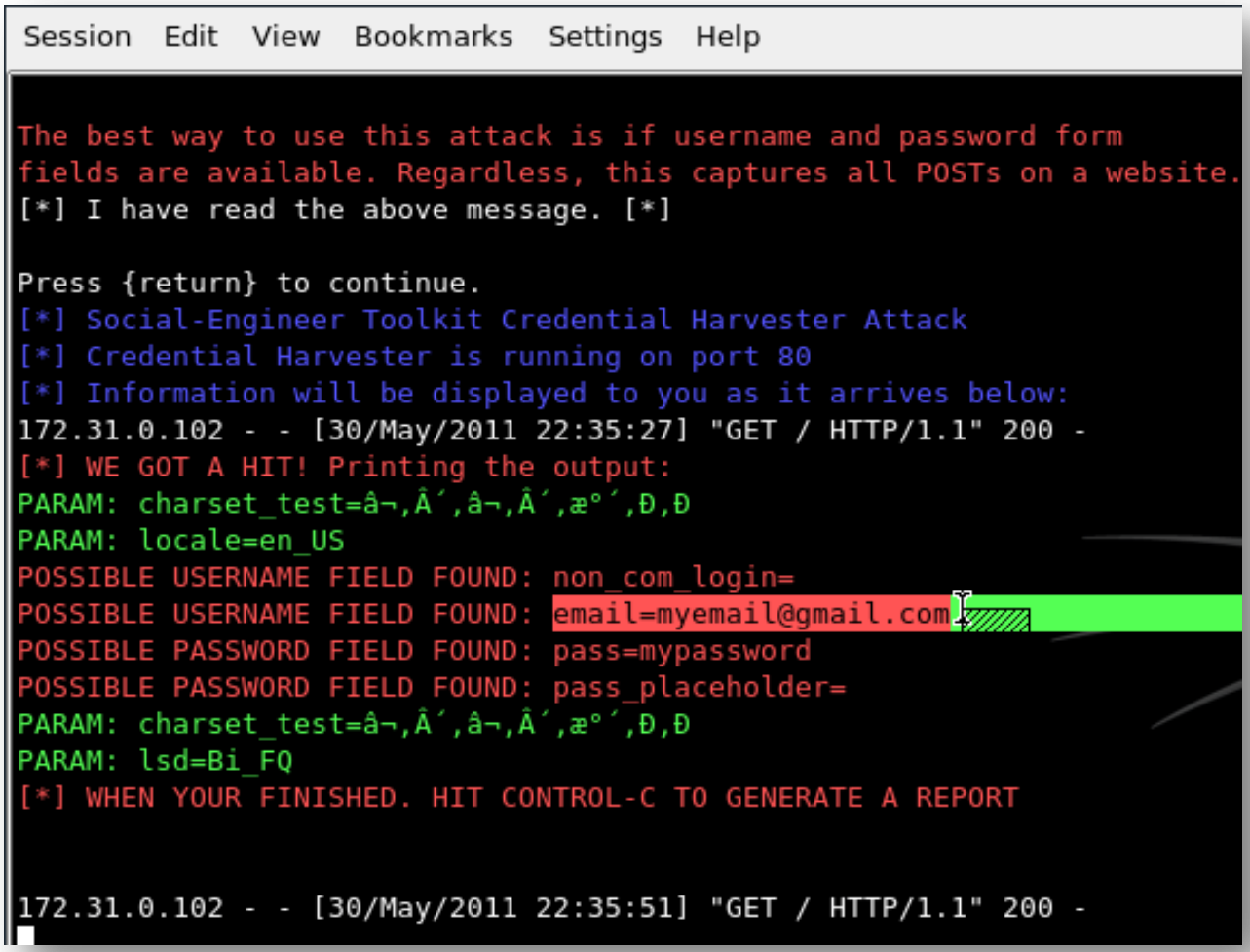
- Impact
  - 駭客偷取使用者的Cookie，存取其身份控管的網站。
  - 將使用者瀏覽器導向釣魚網站，騙取帳號密碼等個人資訊。
  - 將使用者瀏覽器導向惡意網站，安裝惡意後門程式。
  - 攻擊對象並非網站本身，藉由網站為媒介，造成瀏覽網站的無辜使用者受害。

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

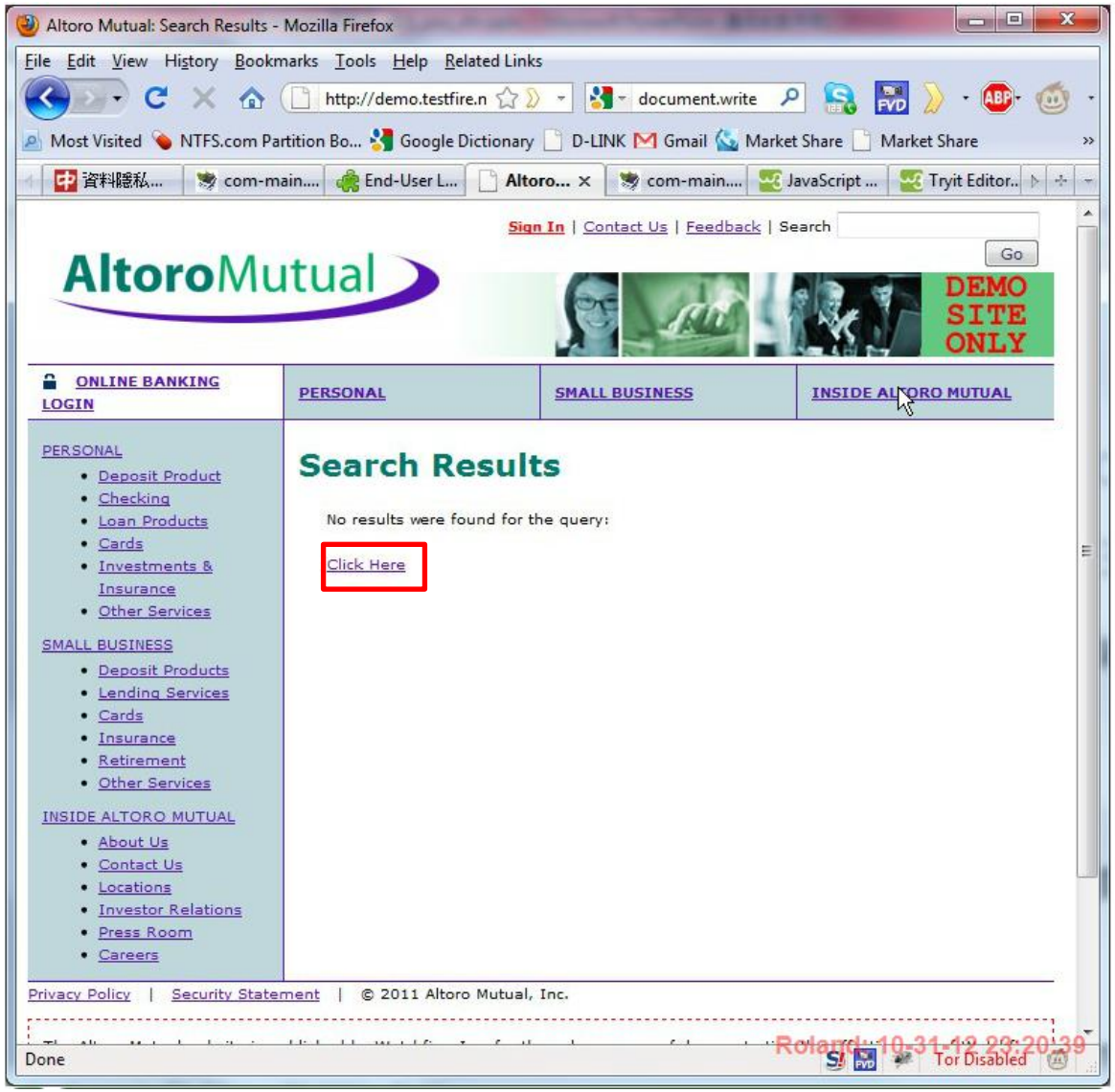
Reflected XSS 用於網路釣魚

受害者被導向釣魚網站

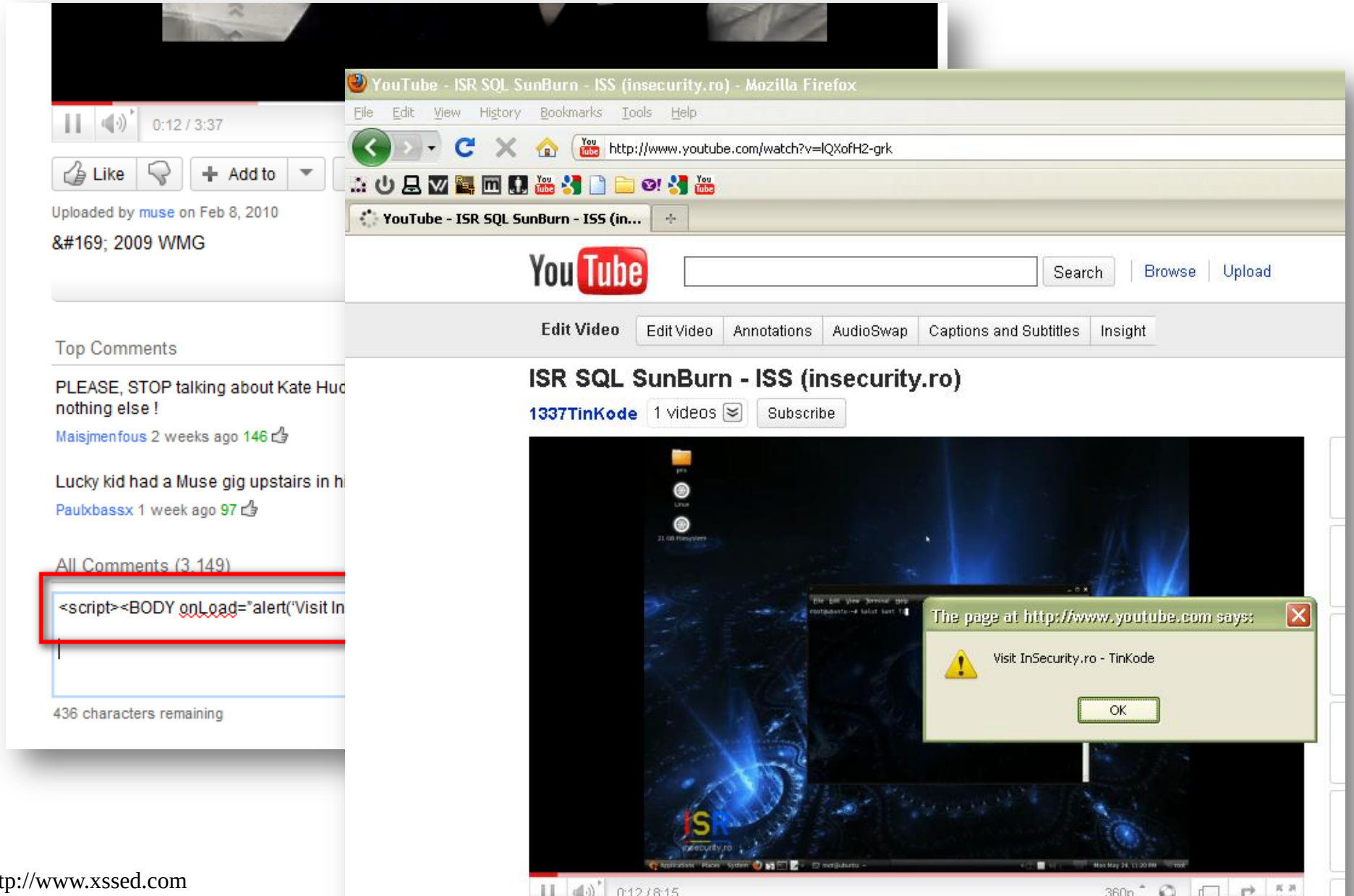
- 駭客竊得帳密



Add a Link Using Reflected XSS



案例:YouTube Stored XSS

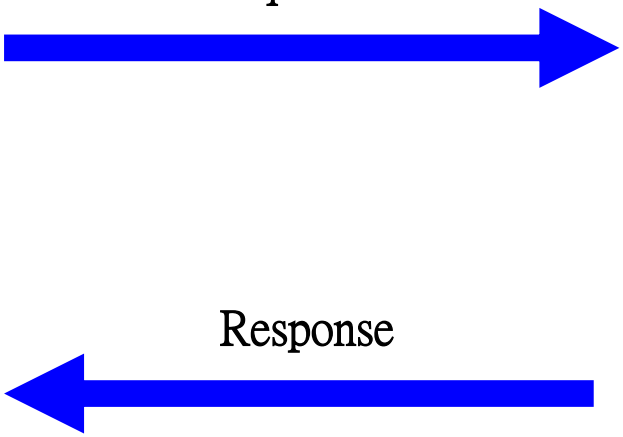


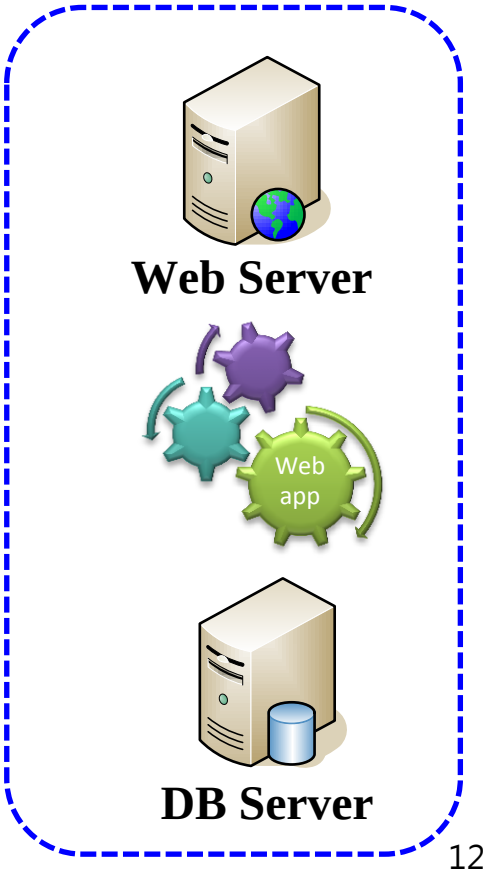
http://www.xssed.com

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)

黑箱檢測工具





IBM AppScan-找到的資安漏洞

Hacking/Test Tools Categories

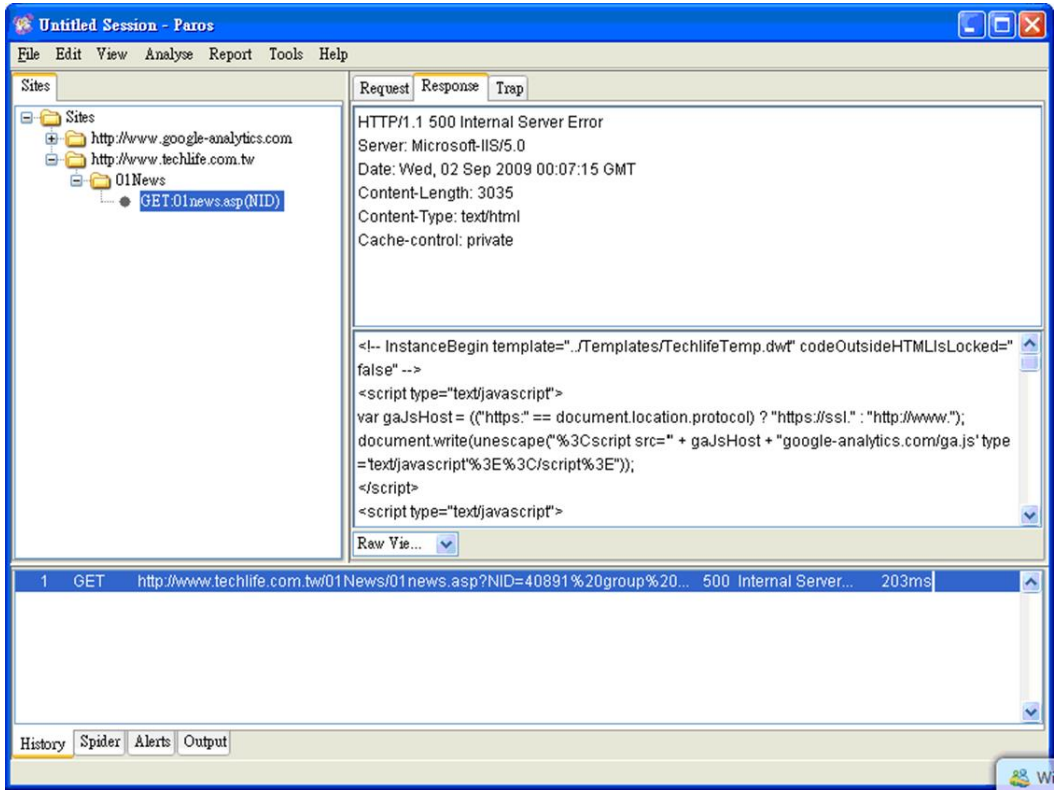
- Stand-alone program
  - Paros - Free
  - Burp Suite - Basic Edition Free
  - Web Scarab - Free, OWASP Project
  - w3af - GNU General Public License
  - Vega
- Browser plugins (Free)
  - Hackbar
  - XSS ME
  - SQL Inject ME
  - Tamper Data
  - Firecat-a suite of plugins
  - Firebug
  - HttpWatch
- Framework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

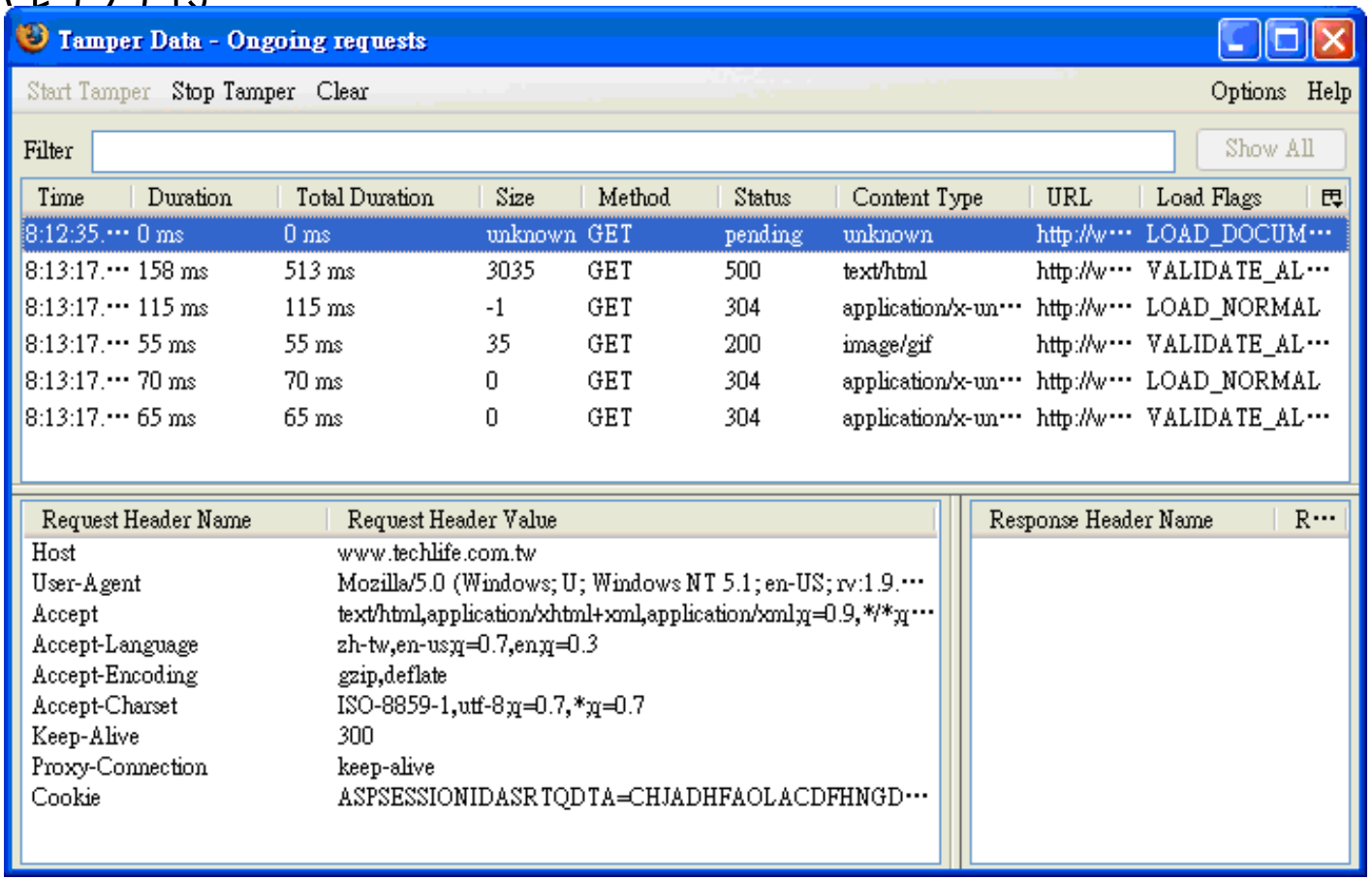
Paros

- Spider
- Scan
- Report
- Recommendation



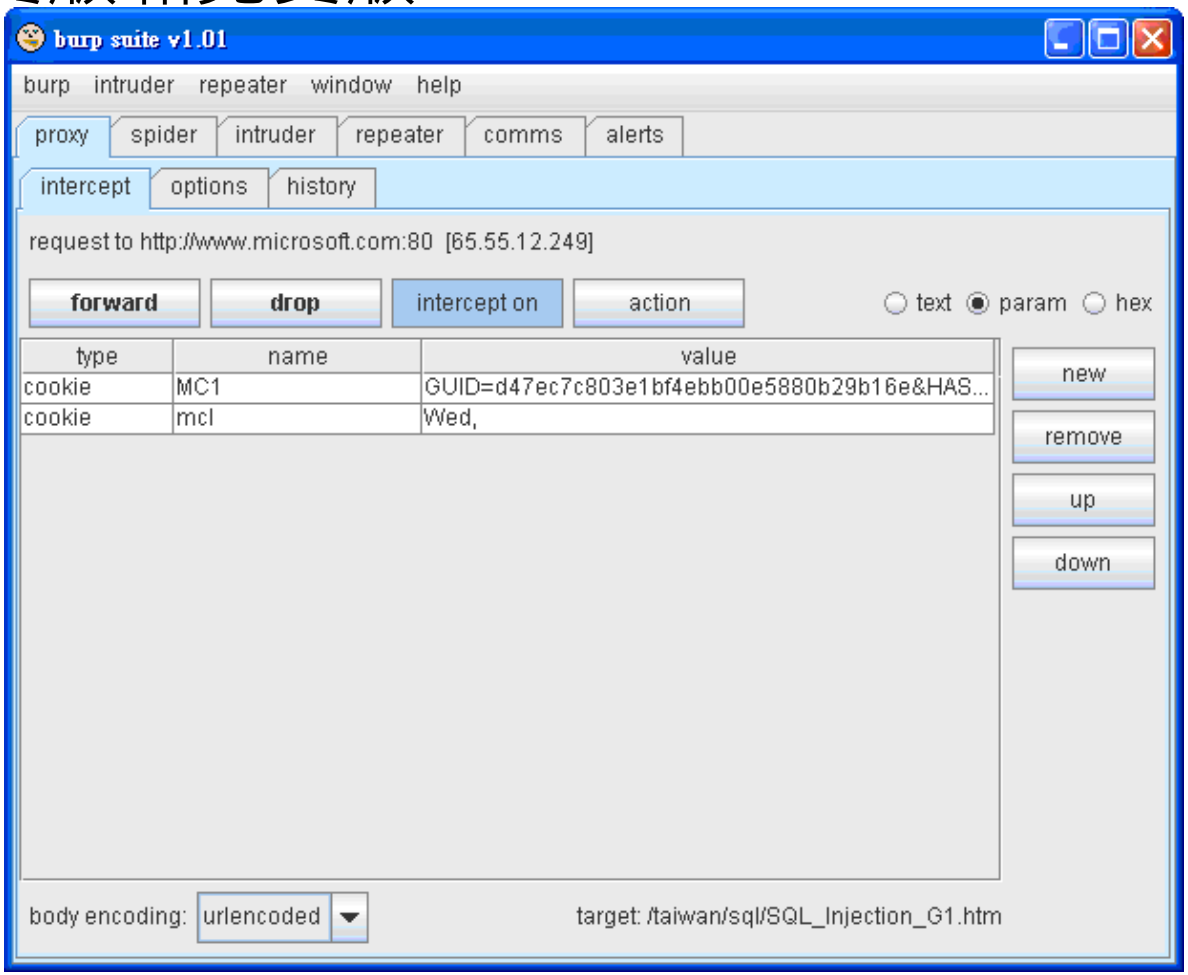
Tamper Data

- Firefox 外掛
- 小巧方便



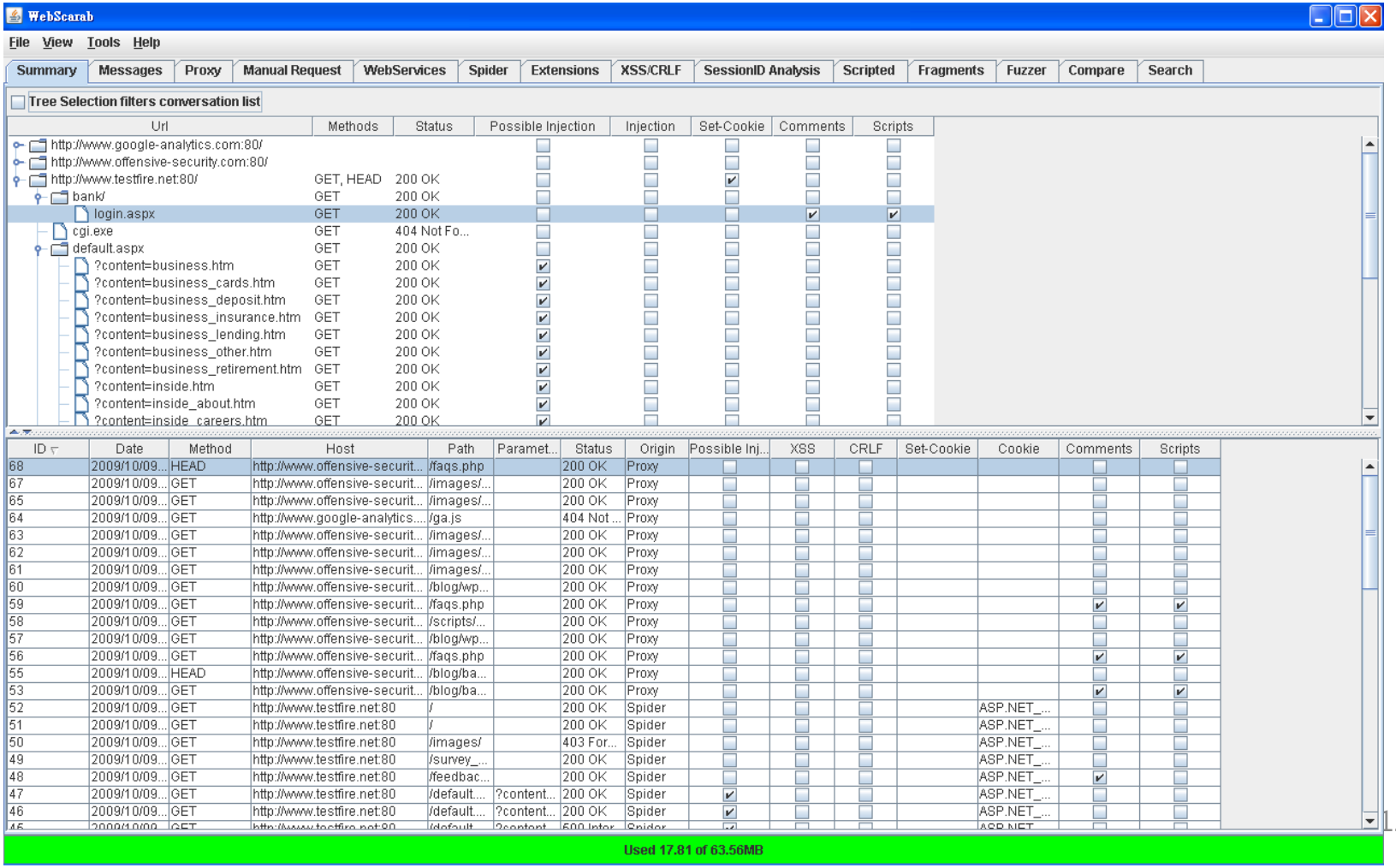
Burp Suite

- 類似 Paros
- 有付費版和免費版



WebScarab

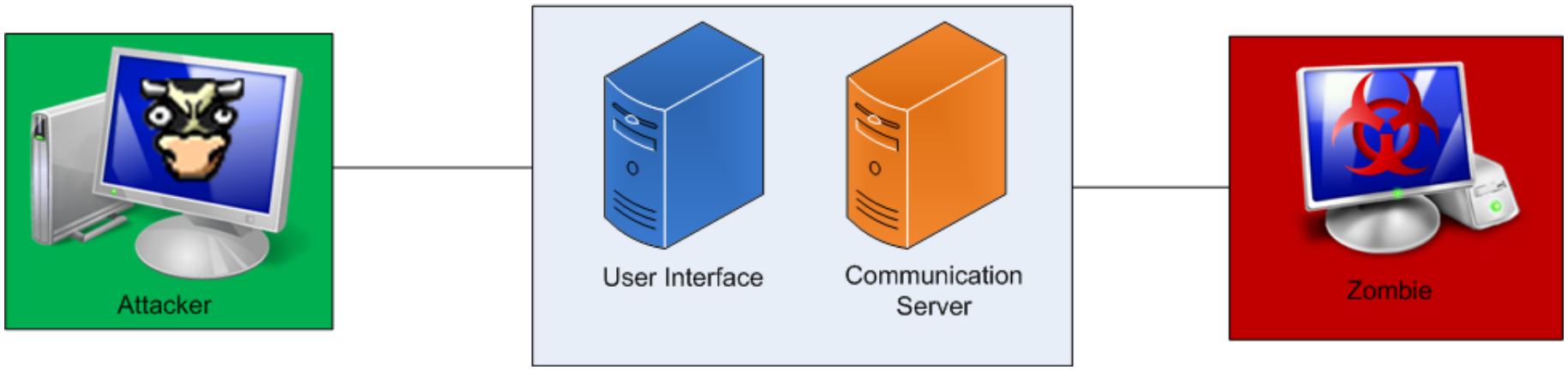
- OWASP 所開發



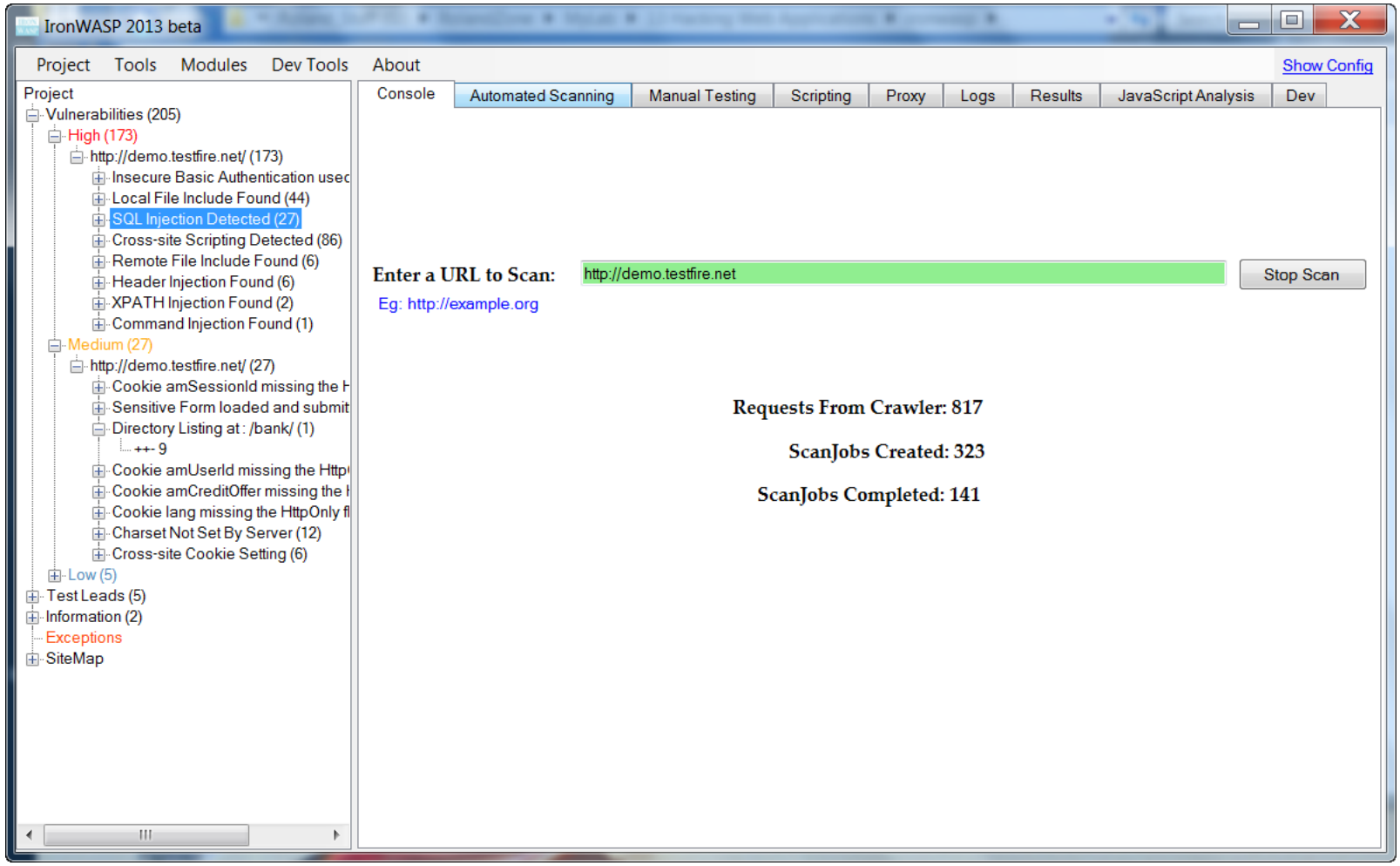
Browser/Client-side Tools

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

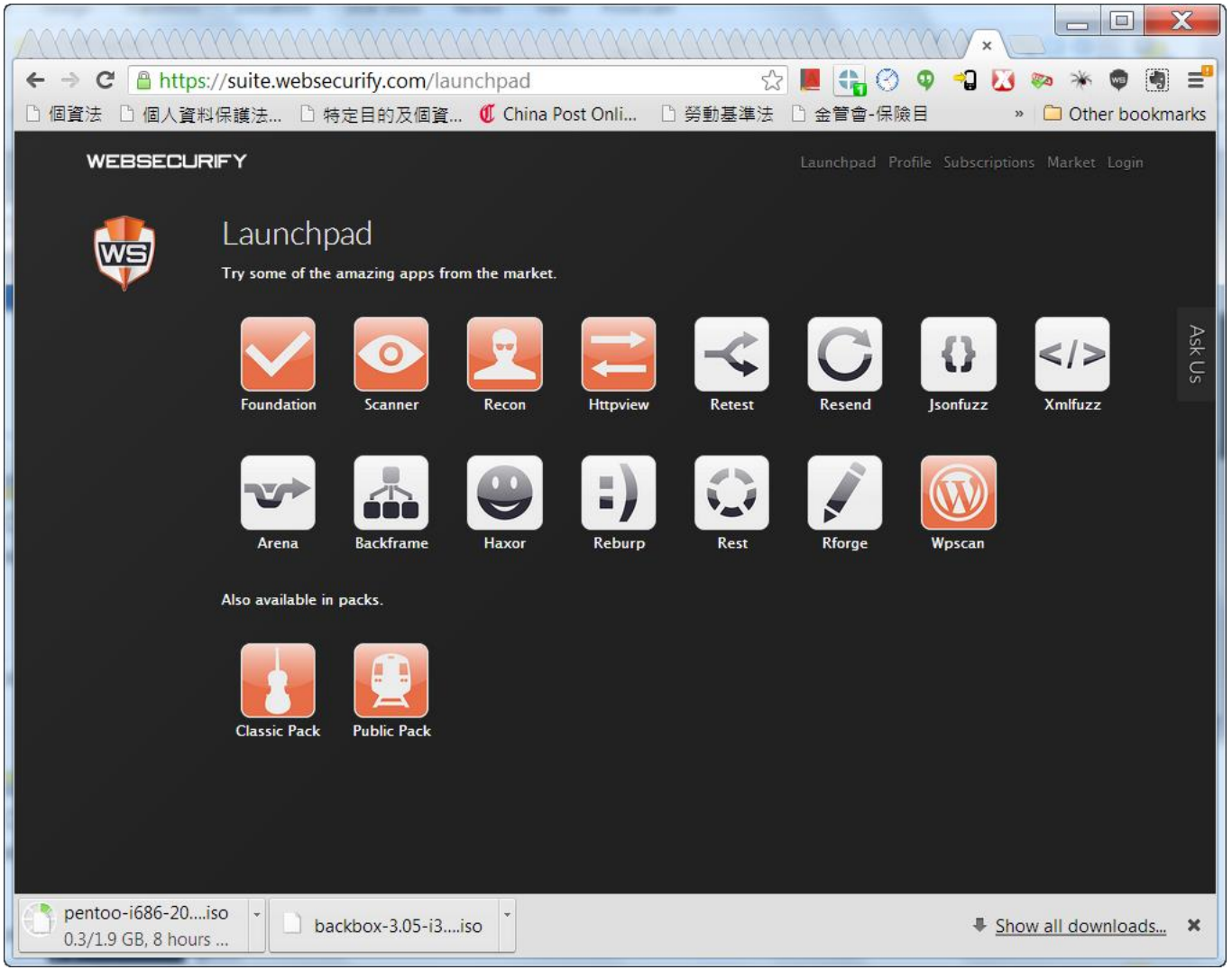
BeEF



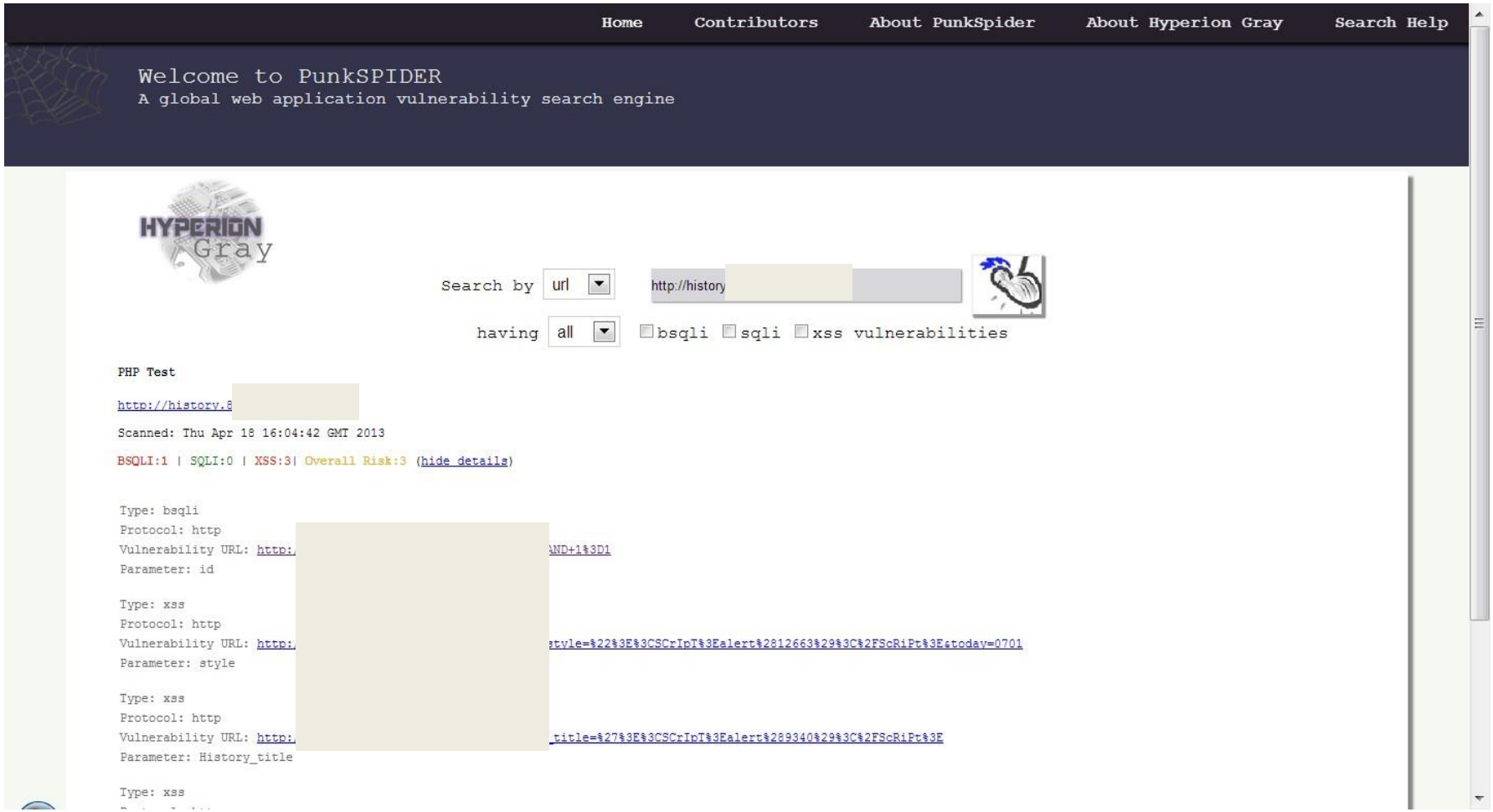
IronWASP


IronWASP 2013 beta
Project
Tools
Modules
Dev Tools
About
Show Config
Project
Vulnerabilities (205)
High (173)
http://demo.testfire.net/ (173)
Insecure Basic Authentication usec
Local File Include Found (44)
SQL Injection Detected (27)
Cross-site Scripting Detected (86)
Remote File Include Found (6)
Header Injection Found (6)
XPATH Injection Found (2)
Command Injection Found (1)
Medium (27)
http://demo.testfire.net/ (27)
Cookie amSessionId missing the H
Sensitive Form loaded and submit
Directory Listing at : /bank/ (1)
++- 9
Cookie amUserId missing the Http
Cookie amCreditOffer missing the
Cookie lang missing the HttpOnly fl
Charset Not Set By Server (12)
Cross-site Cookie Setting (6)
Low (5)
Test Leads (5)
Information (2)
Exceptions
SiteMap
Console
Automated Scanning
Manual Testing
Scripting
Proxy
Logs
Results
JavaScript Analysis
Dev
Enter a URL to Scan:
http://demo.testfire.net
Stop Scan
Eg: http://example.org
Requests From Crawler: 817
ScanJobs Created: 323
ScanJobs Completed: 141

WebSecurity

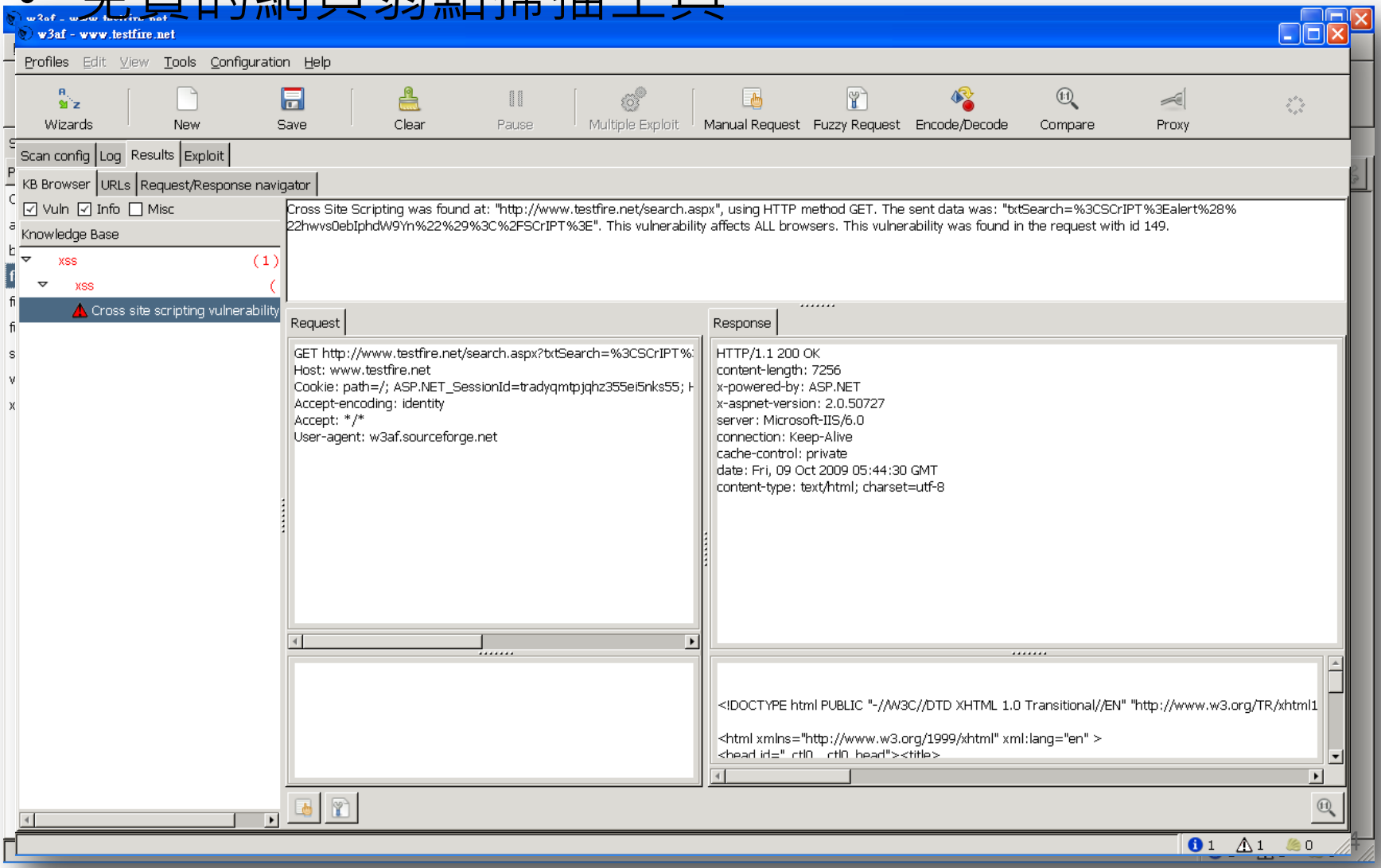


PunkSpider

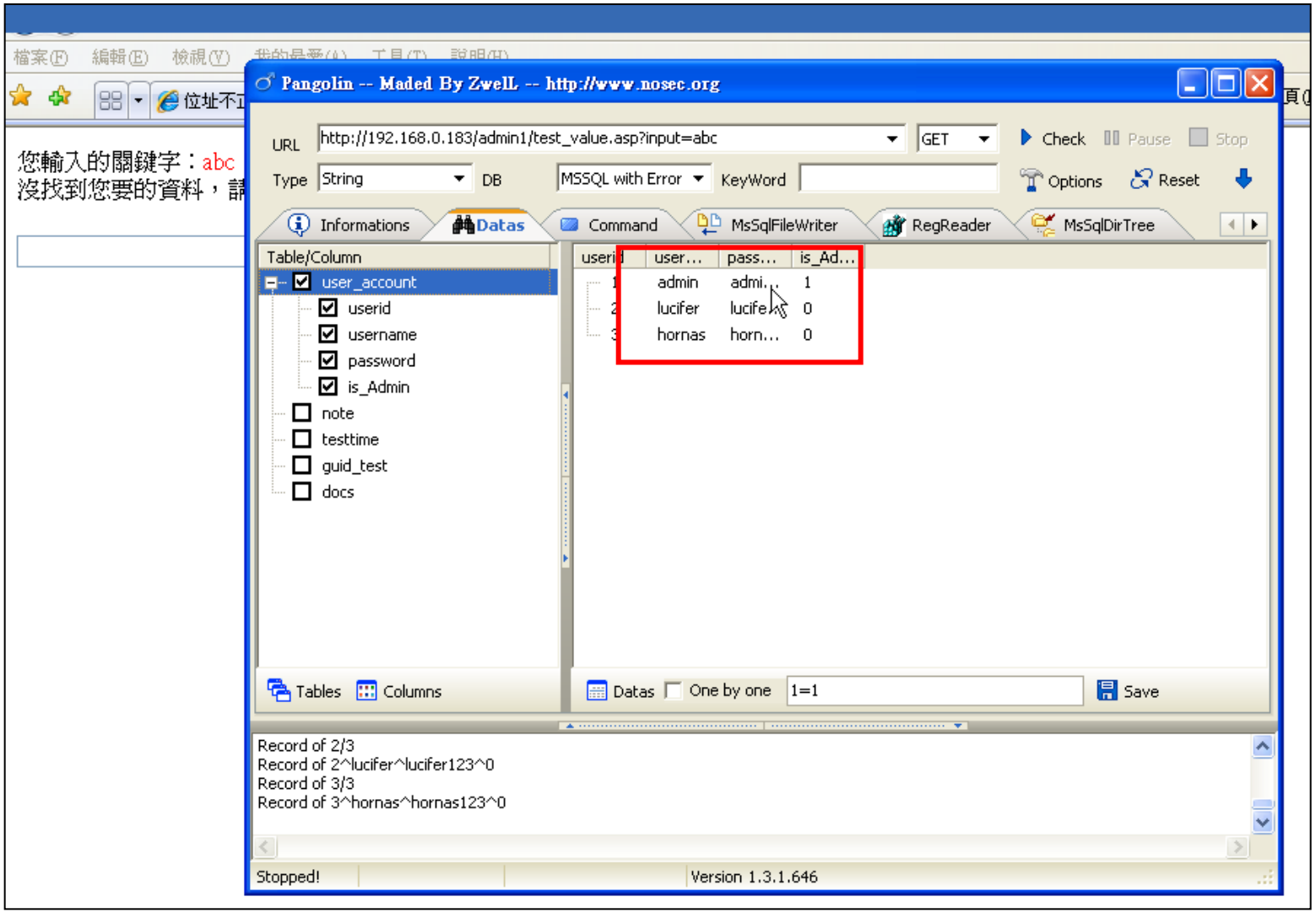

Home
Contributors
About PunkSpider
About Hyperion Gray
Search Help
Welcome to PunkSPIDER
A global web application vulnerability search engine
HYPERION Gray
Search by url
http://history
having all
bsqli sqli xss vulnerabilities
PHP Test
http://history.8
Scanned: Thu Apr 18 16:04:42 GMT 2013
BSQLI:1 | SQLI:0 | XSS:3| Overall Risk:3 (hide details)
Type: bsqli
Protocol: http
Vulnerability URL: http:
AND+1%3D1
Parameter: id
Type: xss
Protocol: http
Vulnerability URL: http:
style=%22%3E%3CSCrIpT%3Ealert%2812663%29%3C%2FScRiPt%3E&today=0701
Parameter: style
Type: xss
Protocol: http
Vulnerability URL: http:
title=%27%3E%3CSCrIpT%3Ealert%289340%29%3C%2FScRiPt%3E
Parameter: History_title
Type: xss

W3af

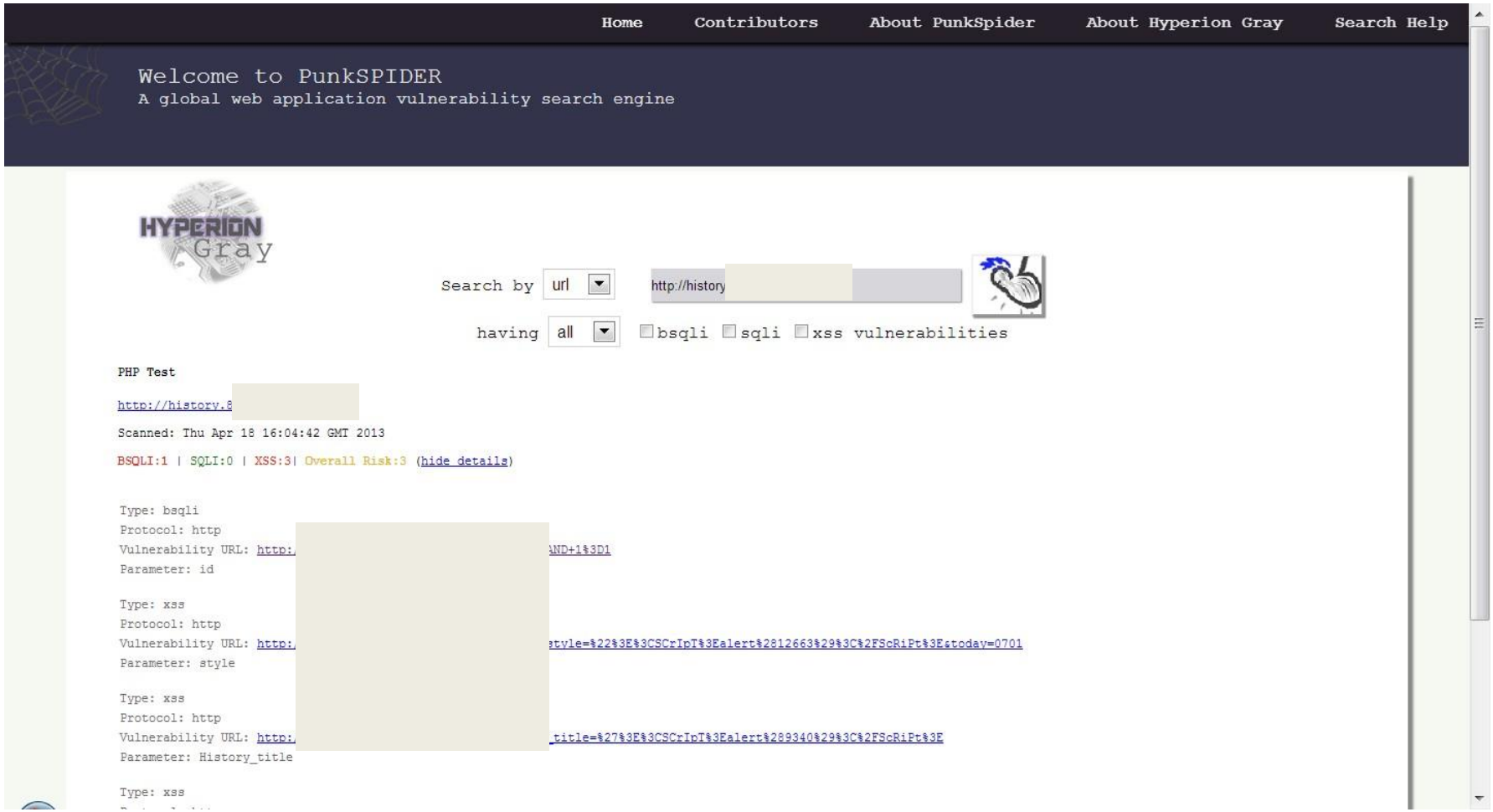
- 免費的網頁弱點掃描工具



Pangolin SQLi



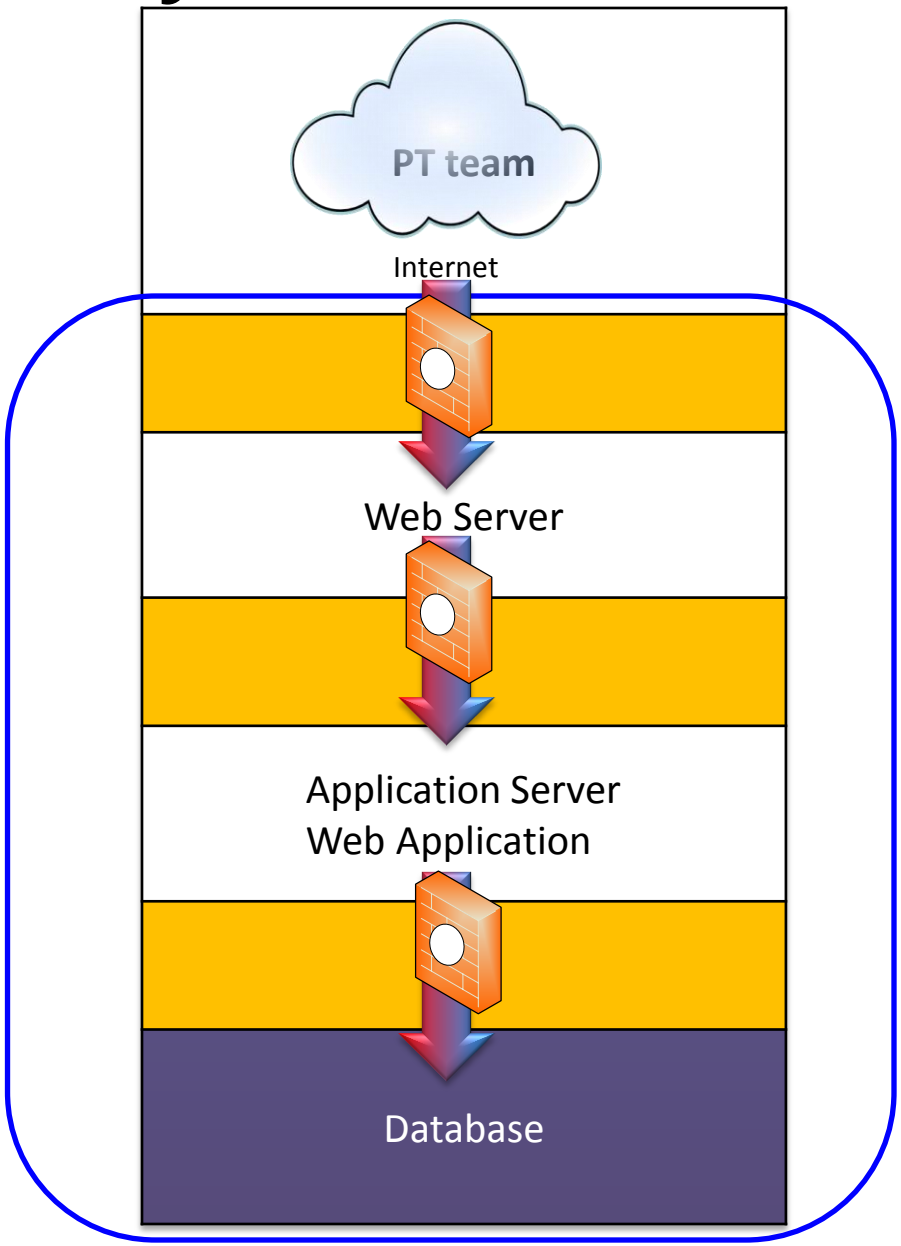
PunkSpider


Home
Contributors
About PunkSpider
About Hyperion Gray
Search Help
Welcome to PunkSPIDER
A global web application vulnerability search engine
HYPERION Gray
Search by url
http://history
having all
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:
AND+1%3D1
Parameter: id
Type: xss
Protocol: http
Vulnerability URL: http:
style=%22%3E%3CSCrIpT%3Ealert%2812663%29%3C%2FScRiPt%3E&today=0701
Parameter: style
Type: xss
Protocol: http
Vulnerability URL: http:
title=%27%3E%3CSCrIpT%3Ealert%289340%29%3C%2FScRiPt%3E
Parameter: History_title
Type: xss

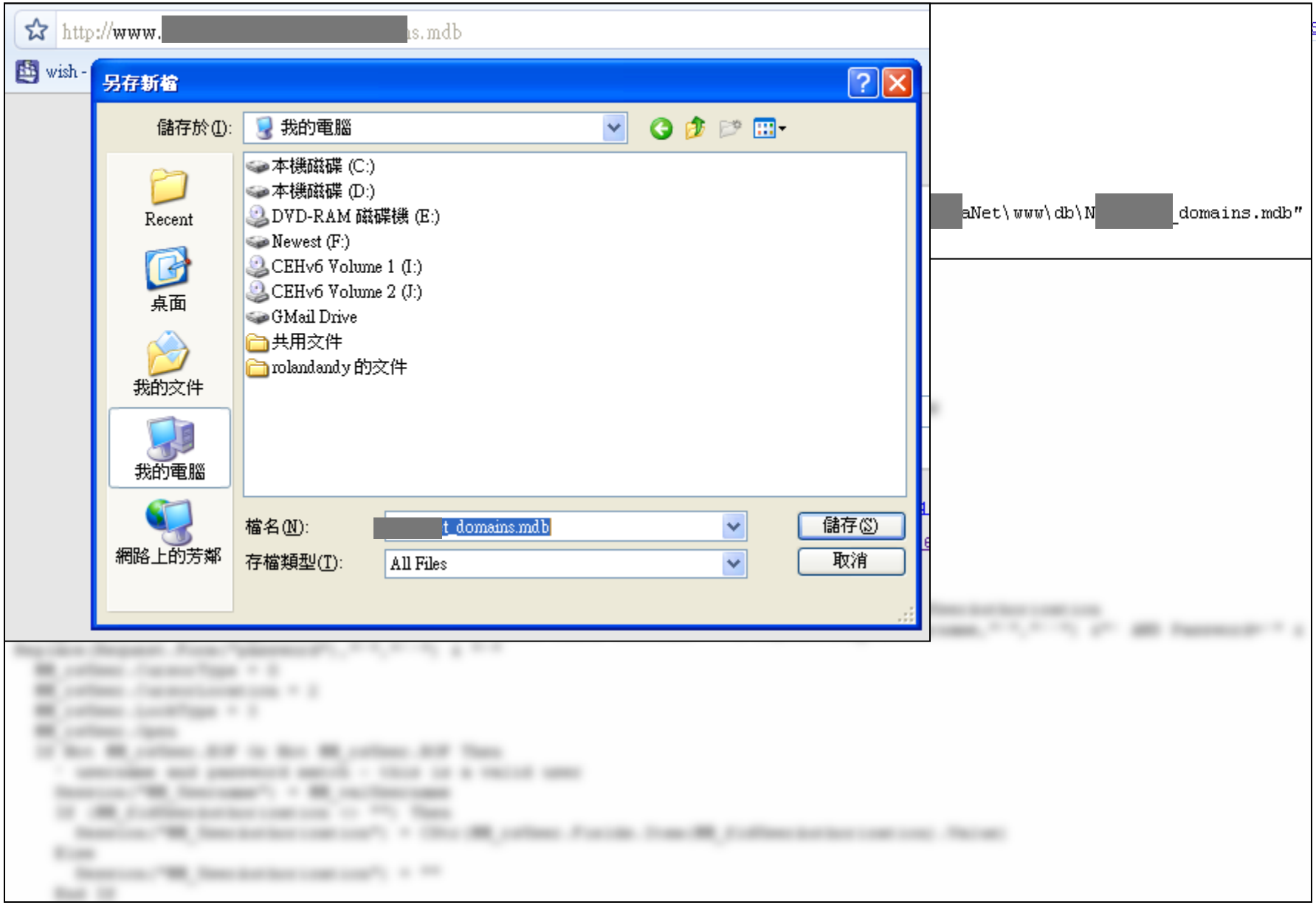
課程大綱

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