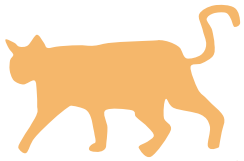
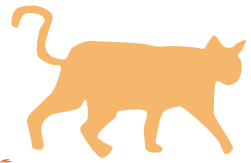


滲透測試-從技術到實作

Pedro

大綱



1. 駭客想得和你不一樣
2. 淺談資安測試
3. 滲透測試流程介紹與常用標準

駭客想得跟你不一樣

- 問題：A，D，G，J，__？

一般人答案：

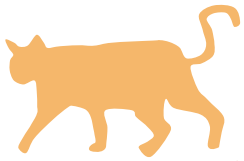
M

A,(B,C,)D,(E,F,)G,(H,I,) J ,(K,L,),M

駭客答案可能是：

L

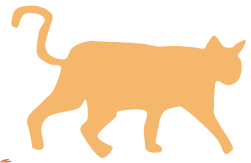
Why?



先别急著看答案...

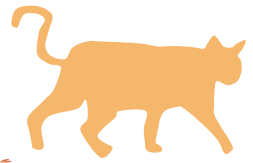

esc
delete
tab
Q W E R T Y U I O P
caps lock
A S D F G H J K L
return
shift
Z X C V B N M
shift
fn
control
option
command
command
option

駭客心理學



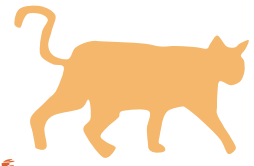
- 心態差異
- 資訊安全木桶理論
- 已知弱點V.S.未知弱點
- 商業邏輯漏洞

心態差異



- × 攻擊者積極
- × 防守者消極
- × 主事者過度自信

資訊安全木桶理論

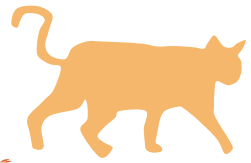


- 資訊安全環境就像一個由許多長度不同的木板所綁起來的水桶，每片木板各自代表資訊安全環境的不同環節，每片木板的長度則代表該個環節的安全強度，而水桶所能承載水量的高度將取決於最短的那片木板，換句話說，整體資訊安全環境的強度其實也取決於最弱的一個環節，而非最強的一個環節。

所以...

- 一再地針對原本強度就較高的環節持續補強，倒不如把資源分散到各個較為脆弱的環節，讓所有環節的安全強度達到較為均衡的程度，對整體資訊安全強度的提昇會有比較正面的意義。

就像少林功夫一樣...

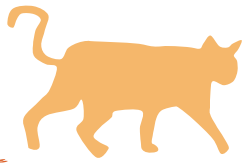


- 沒練到的地方還是會被打趴
  - 你練鐵頭功，我打你腳
  - 你練金剛腿，我打你頭

另一個常見的迷思

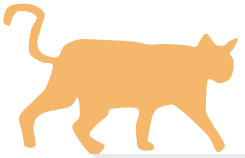

VeriSign Secured
繁體中文
[redacted] 服務如下：
網站名稱： ww[redacted]
憑證狀態： 有效（11-Apr-2006 至 10-Apr-2008）
公司/機構： [redacted]
Taiwan, TW
加密的資料傳輸
該網站可以透過使用 VeriSign SSL 憑證 保護您的私人資訊。 傳輸之前，使用 SSL 與以 https 開頭的任何地址交換的資訊已加密。
SSL 識別資料已確認
已經確認 [redacted] 的擁有者或操作者 [redacted] 的企業。
出於最佳安全性考量，瀏覽網站時，請務必輸入與您希望瀏覽之網站完全相符的位址，並且該驗證網頁的位址總是以此字串開始："https://seal.verisign.com"
>> REPORT SEAL MISUSE

反思：SSL能防止對Web應用程式的攻擊?



- 對於 SSL 的期待:
  - “We are secure because we use SSL!”
  - “Strong 128 bit crypto being used”
  - “We use Digital Certificates signed by VeriSign”
- SSL 和 Session/Application 一般是獨立的
  - 多數 SSL 僅提供 Client 辨識 Server 的身分, 以及**連線過程的私密性**
  - Web 各個層級的安全弱點仍會存在
  - 資料加密的連線內容，IDS/IPS是看不懂的！

Heartbleed漏洞(CVE-2014-0160)



cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-0160

Printer-Friendly V

CVE-ID

CVE-2014-0160 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, bug.

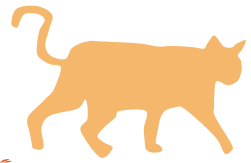
References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:66690
- URL:http://www.securityfocus.com/bid/66690
- BUGTRAQ:20141205 NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities
- URL:http://www.securityfocus.com/archive/1/534161/100/0/threaded
- CERT:TA14-098A
- URL:http://www.us-cert.gov/ncas/alerts/TA14-098A
- CERT-VN:VU#720951
- URL:http://www.kb.cert.org/vuls/id/720951
- CISCO:20140409 OpenSSL Heartbeat Extension Vulnerability in Multiple Cisco Products
- URL:http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed
- CONFIRM:http://advisories.mageia.org/MGASA-2014-0165.html
- CONFIRM:http://cogentdatahub.com/ReleaseNotes.html
- CONFIRM:http://download.schneider-electric.com/files?p_Doc_Ref=SEVD%202014-119-01
- CONFIRM:http://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=96db9023b881d7cd9f379b0c154650d6c108e9a3

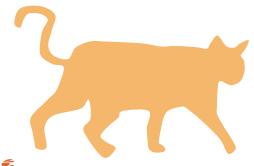
Ref: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-0160

當然...



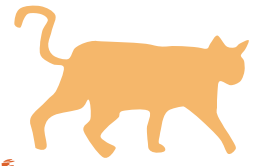
- 連線加密還是很重要的
- 但...你的資安設備有作配套措施嗎?
  - Ex：封包解密檢測

已知弱點V.S.未知弱點

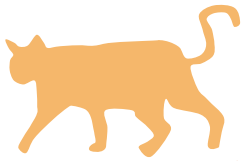


- 資訊安全風險隨時間演變也會有所不同
- 守舊的防禦策略將無法對抗最新的駭客攻擊
- 駭客持續研發各種0-day
- 駭客暗嵌很多未公開0-day

已知弱點V.S.未知弱點

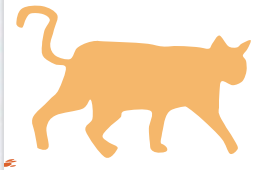


- 資訊安全風險隨時間演變也會有所不同
- 守舊的防禦策略將無法對抗最新的駭客攻擊
- 駭客持續研發各種0-day
- 駭客暗嵌很多未公開0-day
- https://reurl.cc/KlbveM

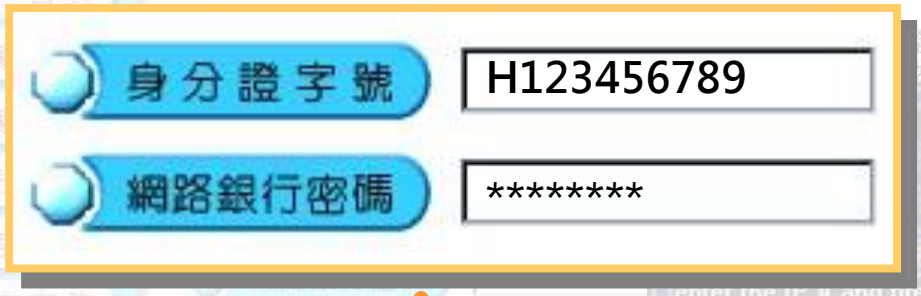


動態鍵盤很安全?

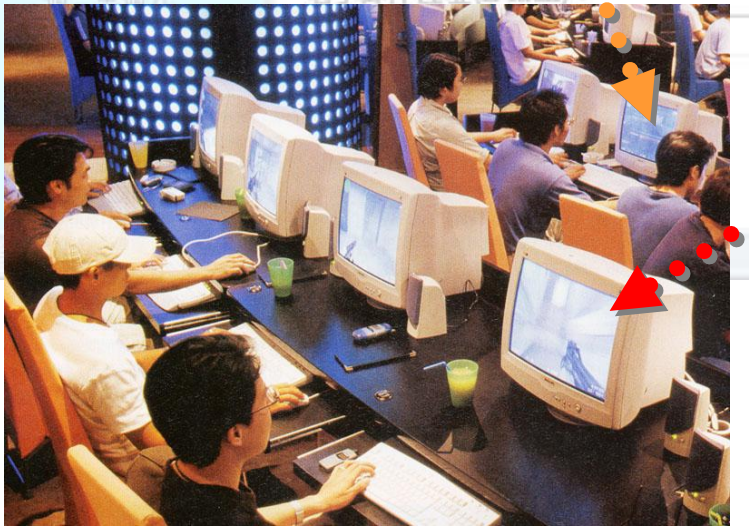
傳統型鍵盤側錄程式的運作方式

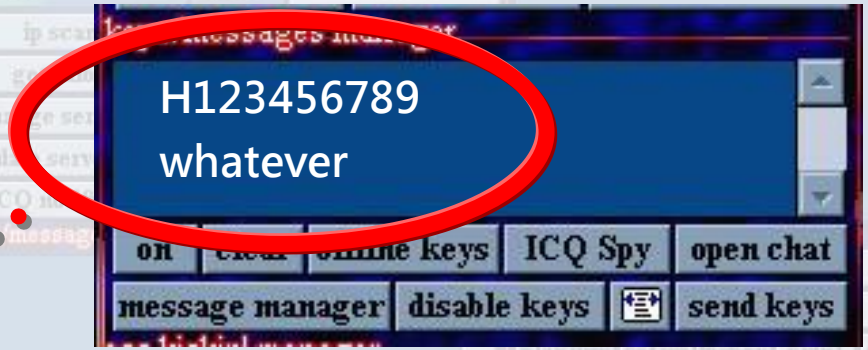


使用者在已經被植
入竊聽木馬的PC上
登入網路銀行



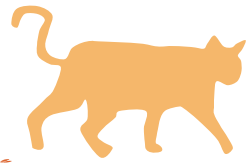
帳號和密碼得手！





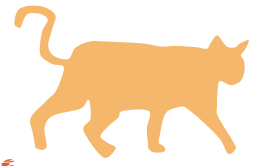
網路身分竊犯在另
一部PC利用接收器
竊聽的所有按鍵

常見後門程式已經可以...



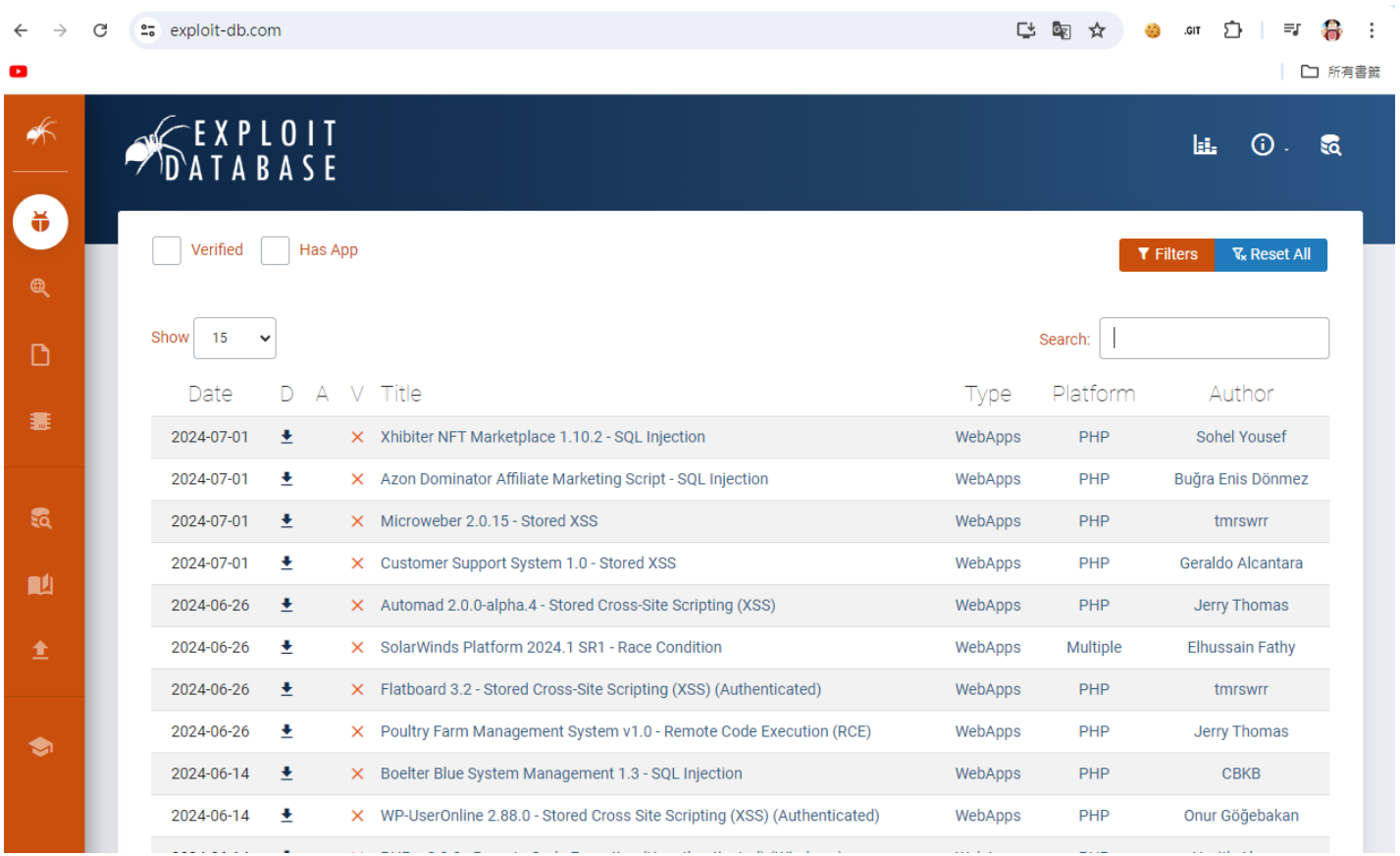
- × 防毒軟體免殺
- × 正常對外連線防火牆無法阻擋
- × 隱藏啟動方式
- × 支援Win11
- × 支援更多種類密碼格式
- × 支援IPv6 Sniffer
- × 支援滑鼠點擊快照

已知弱點V.S.未知弱點



- 資訊安全風險隨時間演變也會有所不同
- 守舊的防禦策略將無法對抗最新的駭客攻擊
- 駭客持續研發各種0-day
- 駭客暗嵌很多未公開0-day

駭客持續研發各種0-day



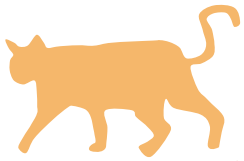
https://www.exploit-db.com/

商業邏輯漏洞

- 一般商業邏輯流程中，所出現的技術漏洞
- 甚至不需具備高度技術能力
- 超過半數網站都具有商業邏輯漏洞

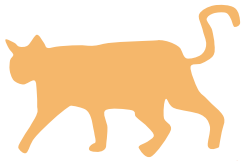
點餐漏洞

Ref:https://zeroday.hitcon.org/vulnerability/ZD-2023-00380



還有.... 人的問題

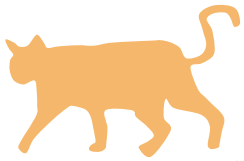
人是最難被patch的弱點，
也是永遠的0-day...



還有更多...

你想都沒想過的手法

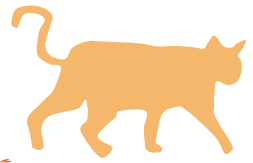
http://www.zdnet.com.au/sweet-bypass-for-student-finger-scanner-339306878.htm



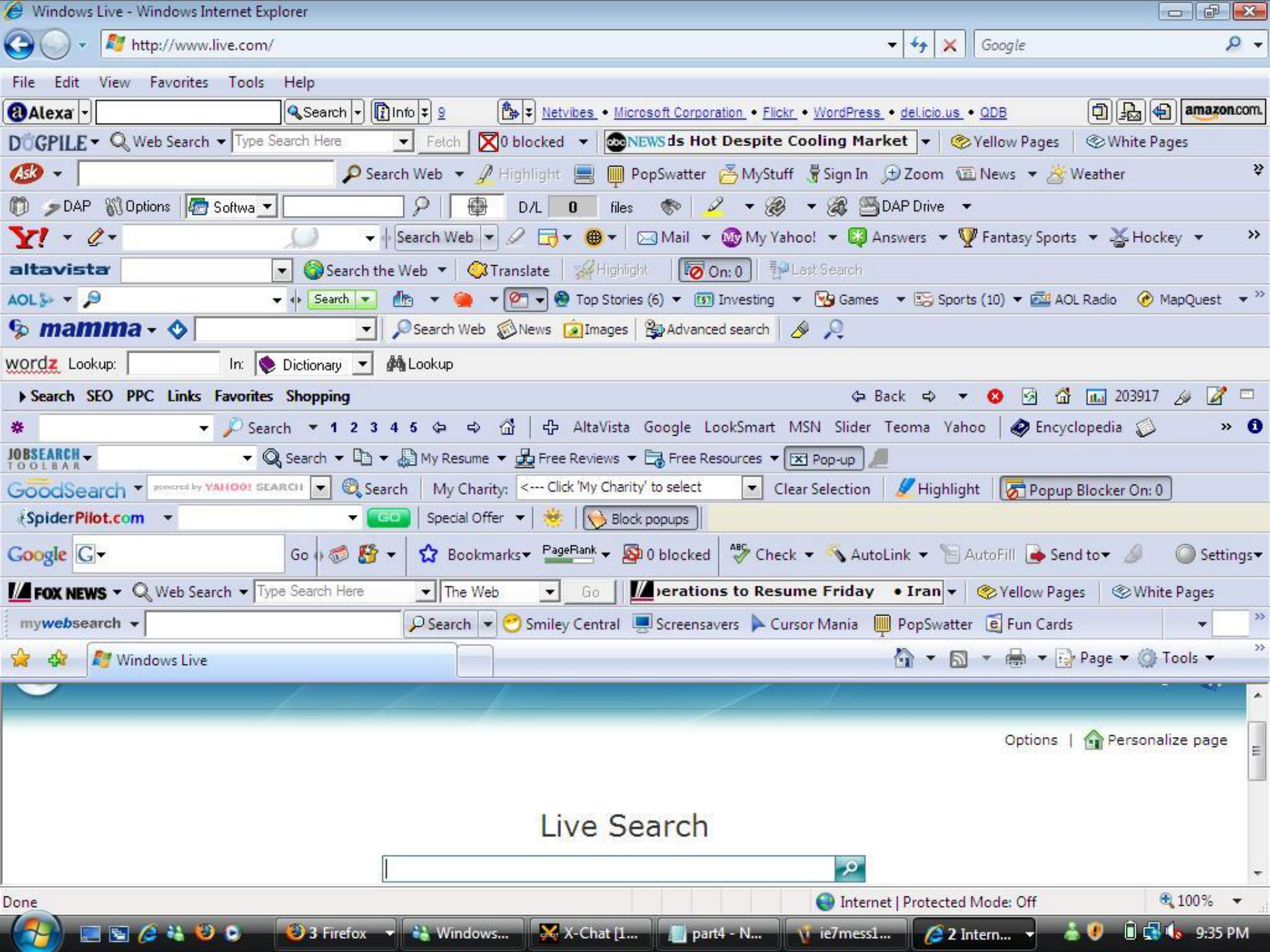
不明確的資安需求...

反而是一種負擔

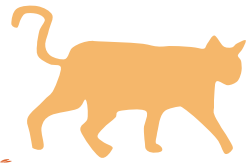
常犯錯誤



- × 疊床架屋
- × 預設值上線
- × 設定不良
- × 過度依賴資安產品
- × 未定期檢視設定與更新
- × 未做紀錄檔分析

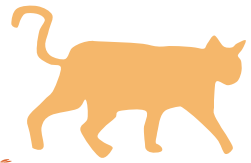

Windows Live - Windows Internet Explorer
http://www.live.com/
Google
File Edit View Favorites Tools Help
Alexa Search Info 9 Netvibes • Microsoft Corporation • Flickr • WordPress • del.icio.us • QDB amazon.com
DOGPILE Web Search Type Search Here Fetch 0 blocked NEWS ds Hot Despite Cooling Market Yellow Pages White Pages
Ask Search Web Highlight PopSwatter MyStuff Sign In Zoom News Weather
DAP Options Softwa D/L 0 files DAP Drive
Search Web Mail My Yahoo! Answers Fantasy Sports Hockey
altavista Search the Web Translate Highlight On: 0 Last Search
AOL Search Top Stories (6) Investing Games Sports (10) AOL Radio MapQuest
mamma Search Web News Images Advanced search
wordz Lookup: In: Dictionary Lookup
Search SEO PPC Links Favorites Shopping Back 203917
Search 1 2 3 4 5 AltaVista Google LookSmart MSN Slider Teoma Yahoo Encyclopedia
JOBSEARCH TOOLBAR Search My Resume Free Reviews Free Resources Pop-up
GoodSearch powered by YAHOO! SEARCH Search My Charity: <--- Click 'My Charity' to select Clear Selection Highlight Popup Blocker On: 0
SpiderPilot.com GO Special Offer Block popups
Google Go Bookmarks PageRank 0 blocked Check AutoLink AutoFill Send to Settings
FOX NEWS Web Search Type Search Here The Web Go erations to Resume Friday • Iran Yellow Pages White Pages
mywebsearch Search Smiley Central Screensavers Cursor Mania PopSwatter Fun Cards
Windows Live
Page Tools
Options | Personalize page
Live Search
Done
Internet | Protected Mode: Off
100%
3 Firefox Windows... X-Chat [1... part4 - N... ie7mess1... 2 Intern...
9:35 PM

常犯錯誤



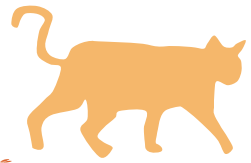
- × 疊床架屋
- × 預設值上線
- × 設定不良
- × 過度依賴資安產品
- × 未定期檢視設定與更新
- × 未做紀錄檔分析

大綱



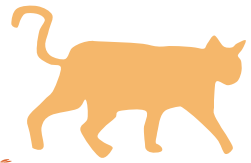
1. 駭客想得和你不一樣
2. 淺談資安測試
3. 滲透測試流程介紹與常用標準

常見資安檢測



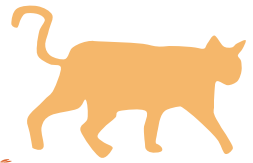
- 弱點掃描
- 網站弱點掃描
  - 黑箱檢測
  - 白箱檢測
- 滲透測試
- (紅隊演練)

弱點掃描



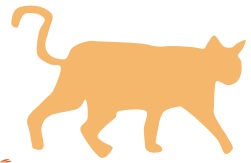
- 評估和發現電腦、網路或應用程式的已知漏洞以及識別和檢測防火牆、路由器、網路伺服器、應用伺服器等中由於錯誤設定或有缺陷的應用程式所產生的漏洞。

常見弱點掃描工具



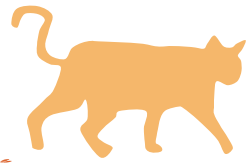
- Nessus
- OpenVAS

網站弱點掃描



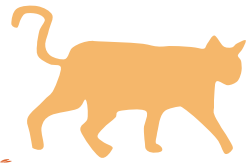
- 僅針對網站與網頁應用程式進行弱點掃描
- 因網頁應用程式多為自行開發，所以常會產生弱點掃描工具無法檢測的未知漏洞

常見網站弱掃工具



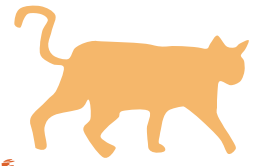
- 黑箱檢測工具
  - Burp Suite
  - Nikto
  - AppScan
  - WebInspect
  - Accunetix

常見網站弱掃工具



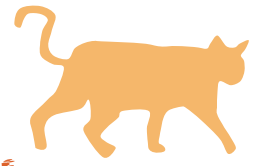
- 白箱檢測工具
  - SonarQube
  - Fortify
  - Checmarx

黑箱檢測



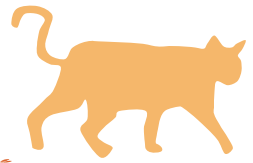
- 優勢
  - 誤判率低
  - 不受程式語言限制
  - 可檢測網頁伺服器弱點
  - 不需提供原始碼
- 劣勢
  - 中繼處理的弱點
  - 管理層面的弱點
  - 無法檢測商業邏輯漏洞
  - 難以檢測權限提升漏洞
  - 檢測路徑不夠完整
  - 檢測速度較慢

白箱檢測



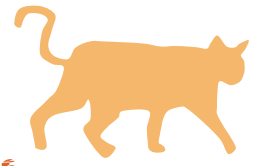
- 優勢
  - 檢測速度相對較快
  - 與開發流程整合容易
  - 程式覆蓋率完整
  - 明確指出程式問題點
- 劣勢
  - 中繼處理的弱點
  - 管理層面的弱點
  - 無法檢測商業邏輯漏洞
  - 難以檢測權限提升漏洞
  - 必須取得原始碼
  - 受程式語言限制
  - 難以判斷自訂的過濾函式

滲透測試



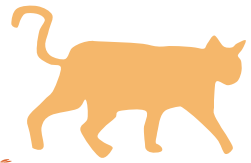
- 以駭客角度發動模擬攻擊的測試
- 測試涵蓋範圍較完整
- 測試品質取決於測試人力的素質

滲透測試著力點



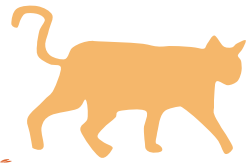
- 自動化檢測工具
  - Input Validation
  - 已知漏洞
- 人工檢測
  - 複測工具檢測出漏洞
  - 延伸工具檢測出漏洞
  - 中繼處理漏洞
  - 管理層面漏洞
  - 商業邏輯漏洞
  - 權限提升漏洞

大綱



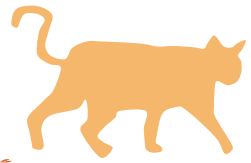
1. 駭客想得和你不一樣
2. 淺談資安測試
3. 滲透測試流程介紹與常用標準

滲透測試



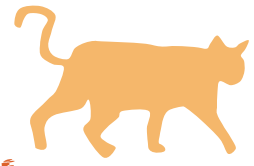
- **滲透測試簡介**
- 滲透測試流程
- 滲透測試實作

滲透測試簡介



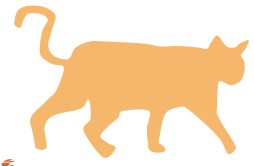
- 滲透測試
- 滲透測試的規範及標準

何謂滲透測試



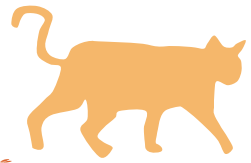
- 辨識出指定目標的系統、應用程式及網路的弱點
- 攻擊發現的弱點並測試安全機制是否有效
- 以駭客攻擊觀點的一種安全模擬測試
- 由一群具有系統及網路安全相關知識的道德安全團隊所執行

滲透測試的目的



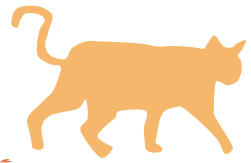
- 資訊安全管理的一部份
  - 了解入侵者可能利用的途徑
  - 了解系統及網路的安全強度
- 如同演習
  - 安全產品的效益
  - 安全事件回應處理
- 強化整體網路與系統安全

滲透測試與弱點掃描



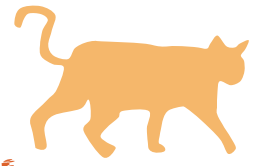
- 弱點掃描
  - 利用自動化工具掃描目標主標並產生弱點報告
  - 會有誤判的情形，無法證實是否真的可被入侵
- 滲透測試
  - 深層檢示每一個弱點
  - 可針對自動化工具沒辦法偵測到的弱點作檢示並證實是否真的有漏洞
  - 所有可入侵的弱點、方法、途徑都被證實過，因此不會有誤判

滲透測試的執行地點



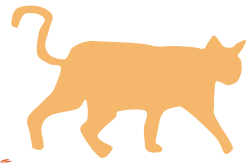
- 遠端執行
  - 遠端滲透測試是指由企業網路外部發起，針對目標企業對外提供的服務主機與防火牆進行專業安全性測試，檢視防火牆與路由器的弱點，並針對防火牆之安全政策進行驗證。
- 現場執行
  - 現場滲透測試是指由企業內部發起，針對目標的主要主機或內部架構進行專業測試。本項測試模擬企業網路防火牆與路由器保護失效、以及入侵者為公司內部員工、或防火牆無法保護公司資訊資產時，駭客可能進行的攻擊手法，對重要伺服器的安全進行更嚴格的安全性驗證。

滲透測試的執行方式

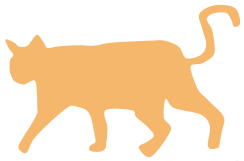


- Black Box
  - 僅知道客戶公司名稱
  - 完全模擬駭客攻擊方式
- White Box
  - 知道所有的客戶資訊
  - 較偏向系統稽核
- Gray Box
  - 僅知道部份的客戶資訊

滲透測試檢驗項目

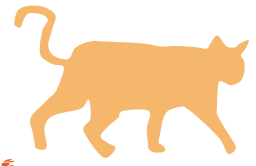


- 作業系統安全漏洞滲透。
- 應用軟體、程式安全瑕疵滲透。
- 軟硬體設定安全漏洞滲透。
- 利用跳板擴大滲透深度。
- 企業網路規劃外之主機或網路設備搜尋
- 系統不當設定、預設設定檢測
- 緩衝區溢位(Buffer Overflow)、格式化字串(Format String)、堆積溢位(Stack Overflow)問題檢測
- 認證跳脫、越權方式檢測
- 垂直權限跳脫檢測、水平權限跳脫檢測
- 密碼強度、懶人密碼檢測
- 信任關係檢測
- 已知可攻擊的漏洞檢測
- 資訊隱碼(SQL Injection)檢測
- 網址注入(XSS)檢測
- 資訊洩漏、目錄洩漏(Information Leakage)檢測



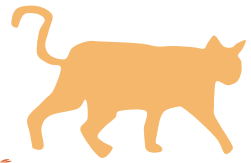
滲透測試的規範及標準

國際組織及標準



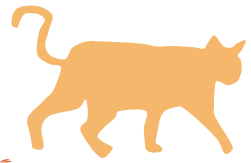
- OWASP
  - Open Web Application Security Project，OWASP Foundation
- OSSTMM
  - Open-Source Security Testing Methodology Manual
- NIST
  - National Institute of Standards and Technology美國國家標準與技術研究院，前身為1901年成立的美國國家標準局， 於1988年改名為國家標準與技術研究院。
- The SANS Institute
  - SysAdmin, Audit, Network, Security

為何需要滲透測試方法論



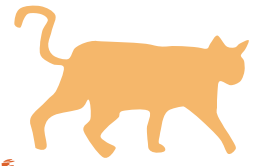
- 確保執行的項目確實執行
- 確保執行範圍不會超出合約規範
- 獲得客戶的信任

方法論驗證結果分析報告



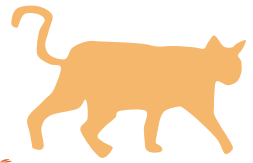
- 整體安全性總結評估
- 既有風險的評估
- 潛在風險的評估
- 測試期間所發現的安全漏洞、其危險程度及修正方式
- 詳列利用工具或漏洞收集到的資訊(如帳號、密碼、檔案、機器組態、資料庫資料、機密網頁內容、程式、原始碼等)
- 對於安全政策與所發現的問題提供相關之改善計畫

執行滲透測試執行的遊戲規則



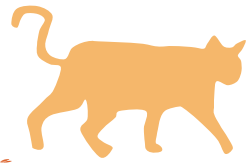
- 是否使用社交工程
- 是否可入侵使用者的電腦
- 是否執行阻斷服務攻擊
- 詳細定義範圍(Scope)

Scope



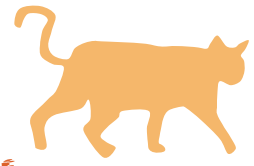
- 通常依據Scope大小決定人天與時程
- 常用單位：主機數、網站數、網段數

執行滲透測試的注意事項



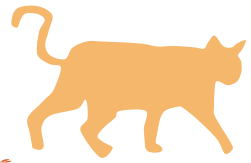
- 所有動作、資料都有記錄，並保持一個可控制的態度
- 滲透測試執行皆在獨立網段、封閉空間、行為記錄
- 執行過程中電腦需有詳細記錄，包含文件、跳板使用工具等...

滲透測試合約注意事項



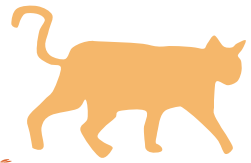
- 完整的報告內容及建議
- 滲透成功的佐證資料
- 隱私權保護
- 資料不可外洩
- 資料不可以被破壞、修改，保持資料及系統的完整性(Integrity)
- 符合相關法律條文之規定
- 簽署「保密協定」，並遵循貴單位安全規範

滲透測試效益



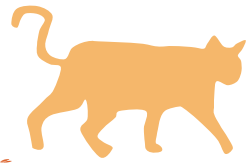
- 了解入侵者可能利用的途徑，提出改善之建議
- 稽核資安防護規劃的強度
- 驗證現有系統安全性
- 檢驗現行的資訊安全政策之弱點
- 了解系統、應用程式、及網路的安全強度
- 對重要主機的安全性提供專業的評估與建議

滲透測試



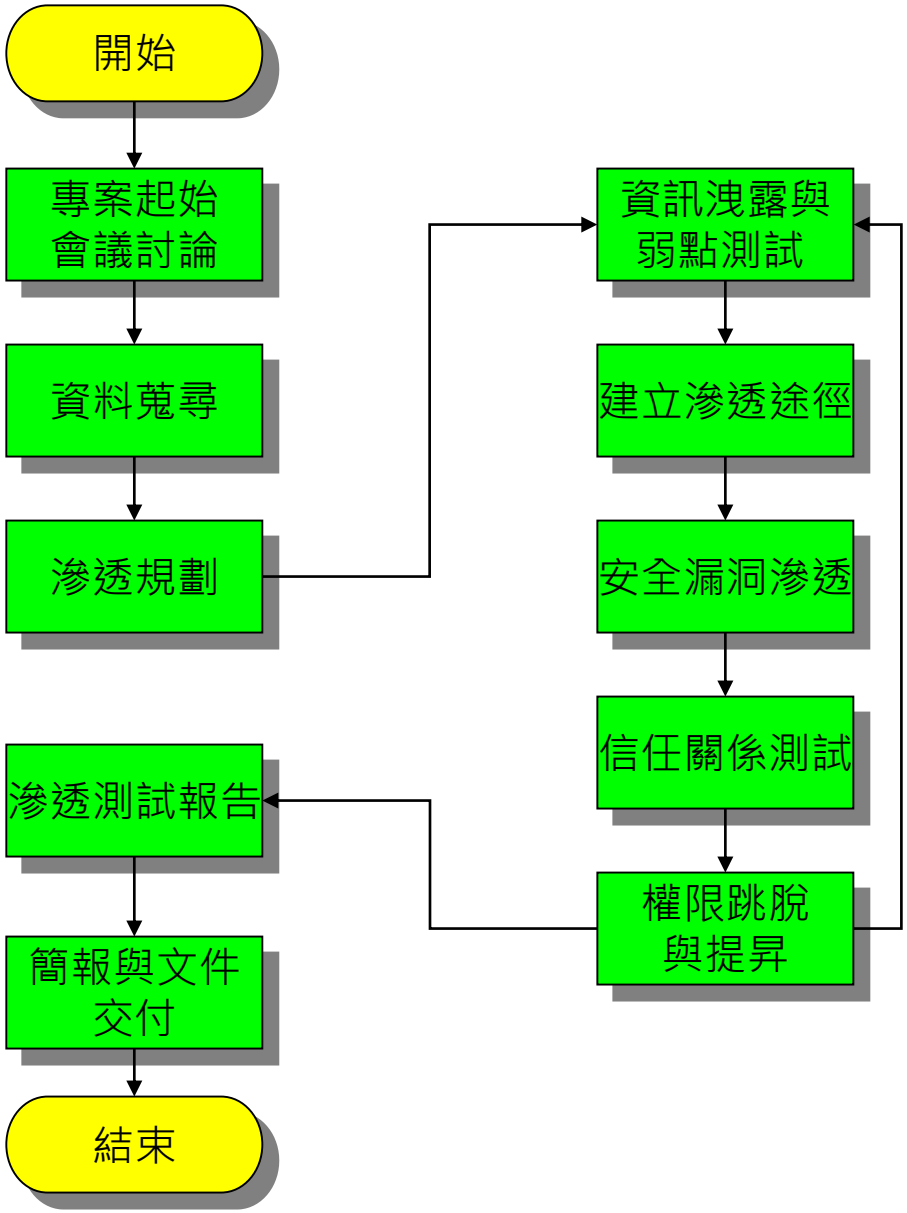
- 滲透測試簡介
- **滲透測試流程**
- 滲透測試實作

滲透測試的流程

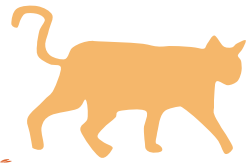


- 資訊收集
- 資訊分析
- 弱點檢測
- 滲透攻擊
- 權限提升
- 清除
- 分析及報告

服務作業流程

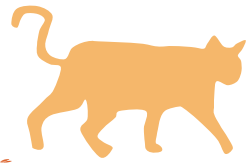

開始
專案起始
會議討論
資料蒐尋
滲透規劃
資訊洩露與
弱點測試
建立滲透途徑
安全漏洞滲透
信任關係測試
權限跳脫
與提昇
滲透測試報告
簡報與文件
交付
結束

資訊收集



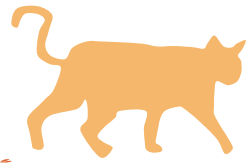
- 單位各種資訊收集
  - Public organization information
  - Web browsing
  - Web crawling
  - Social engineering
- 尋找各個存取點
- 尋找並繪出單位網路架構

資訊分析



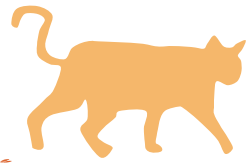
- 分析所得的資訊
- 擬定攻擊計畫
- 確認攻擊目標
- 評估所需的人力及時間

弱點檢測



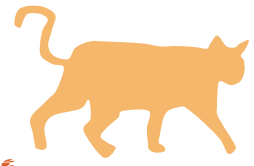
- 使用自動化掃描工具
- 手動掃描並研究弱點
- 取得弱點清單

滲透攻擊



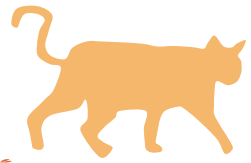
- 使用已知攻擊程式攻擊弱點
- 客製化攻擊程式
- 開發並測試攻擊程式
- 發動攻擊

權限提升



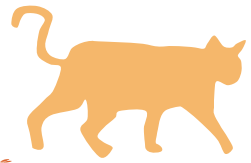
- 滲透(入侵)成功
- 提高權限
- 建立跳板/繼續滲透
- 回到資訊收集(Information Gathering)階段

清除

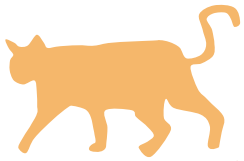


- 擬定清除的標準作業程序
- 清除使用工具等

分析及報告

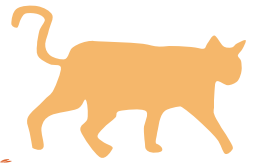


- 分析結果及撰寫建議書
- 交付建議書
- 現場報告



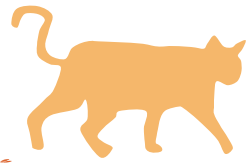
以下僅為情境模擬

滲透測試實作



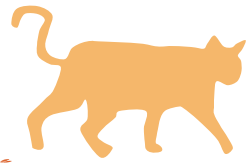
- 遠端檢測
- 現場檢測

滲透測試實作



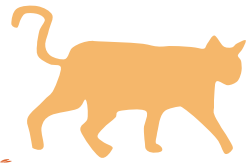
- **遠端檢測**
- 現場檢測

遠端檢測



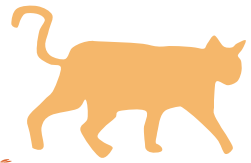
- 腳印拓取
- 網路設備
- 伺服主機
- 其他

遠端檢測



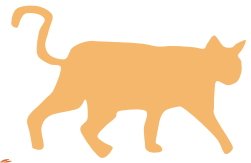
- **腳印拓取**
- 網路設備
- 伺服主機
- 其他

腳印拓取



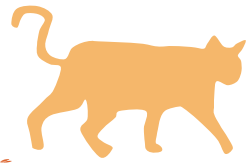
- 常用工具
  - Nmap
  - Nessus
  - ....etc

腳印拓取



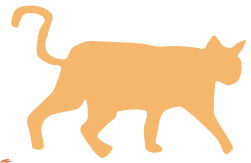
- 目的
  - 找尋可用主機
  - 找尋開放服務
  - 找尋可用弱點

遠端檢測



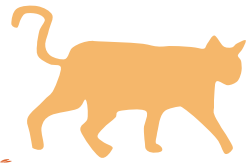
- × 腳印拓取
- × **網路設備**
- × 伺服主機
- × 其他

網路設備



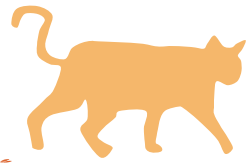
- 檢測登入頁面
- 檢測密碼
- 使用預設SNMP community
- 其他漏洞

檢測登入頁面



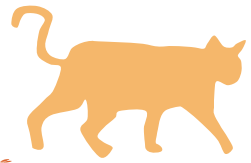
- 允許任意IP存取管理頁面??
- 開放哪些存取介面??

檢測密碼



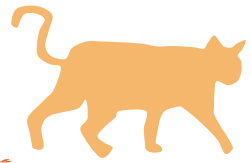
- 預設密碼表：
  - Ex： https://datarecovery.com/rd/default-passwords/
- 預設密碼不一定只有一組??
  - Ex：早期的Avaya Cajun Switch 有三組預設帳密
    - root/root
    - diag/danger
    - manuf/xxyyzz
- Sniffer聽到的密碼
- 其他簡易或常用密碼
- Brute Force

預設SNMP community



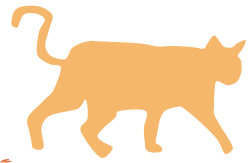
- Public
- Private
- SNMP version
- RO or RW??

攻擊效益



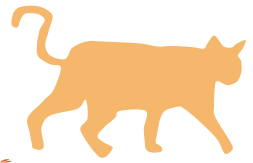
- DoS (DDoS)
- 取得網路架構資訊
- 取得policy資訊
- 跳板
- 建立tunnel
- …etc

遠端檢測



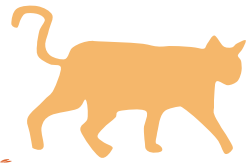
- × 腳印拓取
- × 網路設備
- × 伺服主機
- × 其他

伺服主機



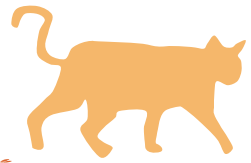
- 作業系統
- 開放服務種類
- AP

開放服務種類



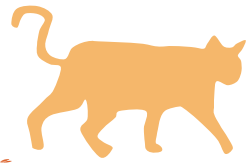
- Web
- FTP
- DNS
- 目錄服務
- …etc

AP



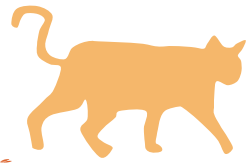
- × 已知弱點
- × 預設帳密
- × 簡易或常用密碼
- × 新弱點發掘

攻擊效益



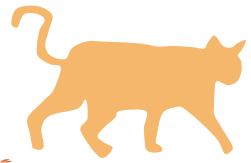
- 取得機敏資料
- 破壞系統運作
- 繼續向內滲透
- ...etc

遠端檢測



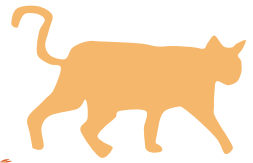
- × 腳印拓取
- × 網路設備
- × 伺服主機
- × 其他

其他



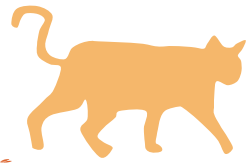
- Wireless
- VoIP
- 社交工程
- …etc

滲透測試實作



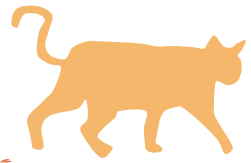
- × 遠端檢測
- × **現場檢測**

現場檢測



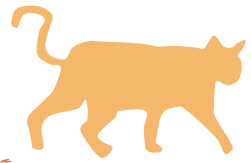
- × 腳印拓取
- × 網路設備
- × 伺服主機
- × 使用者電腦
- × 共享資源搜索
- × 連線竊聽
- × 其他

現場檢測



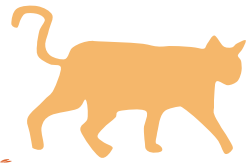
- × 腳印拓取
- × 網路設備
- × 伺服主機
- × **使用者電腦**
- × 共享資源搜索
- × 連線竊聽
- × 其他

使用者電腦



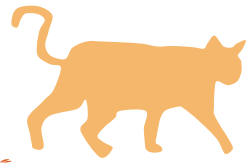
- 系統漏洞
- 弱密碼
- 惡意程式植入
- 不當資源開放
  - IIS
  - FTP
  - P2P
  - Remote control

攻擊效益



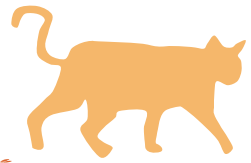
- 搜括有用資料
- 監看資訊
- 肉雞

現場檢測



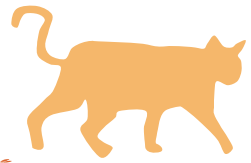
- × 腳印拓取
- × 網路設備
- × 伺服主機
- × 使用者電腦
- × **共享資源搜索**
- × 連線竊聽
- × 其他

共用資源搜索



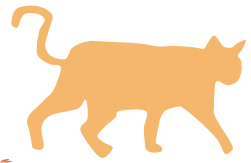
- 常有好康的...XD
  (電影、mp3、甚至是source code！！！)
- 技術及工作手冊
  (網路架構圖、隱藏的主機、甚至是管理者帳號密碼？？)
- 檢查可疑檔案
- 還有.....

現場檢測



- × 腳印拓取
- × 網路設備
- × 伺服主機
- × 使用者電腦
- × 共享資源搜索
- × **連線竊聽**
- × 其他

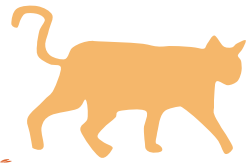
連線竊聽



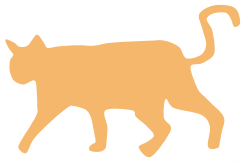
- Sniffer Tools

- Switch環境無法sniffer??
  - You can try
    - Mac flooding
    - ARP spoofing
    - And…

滲透測試補充

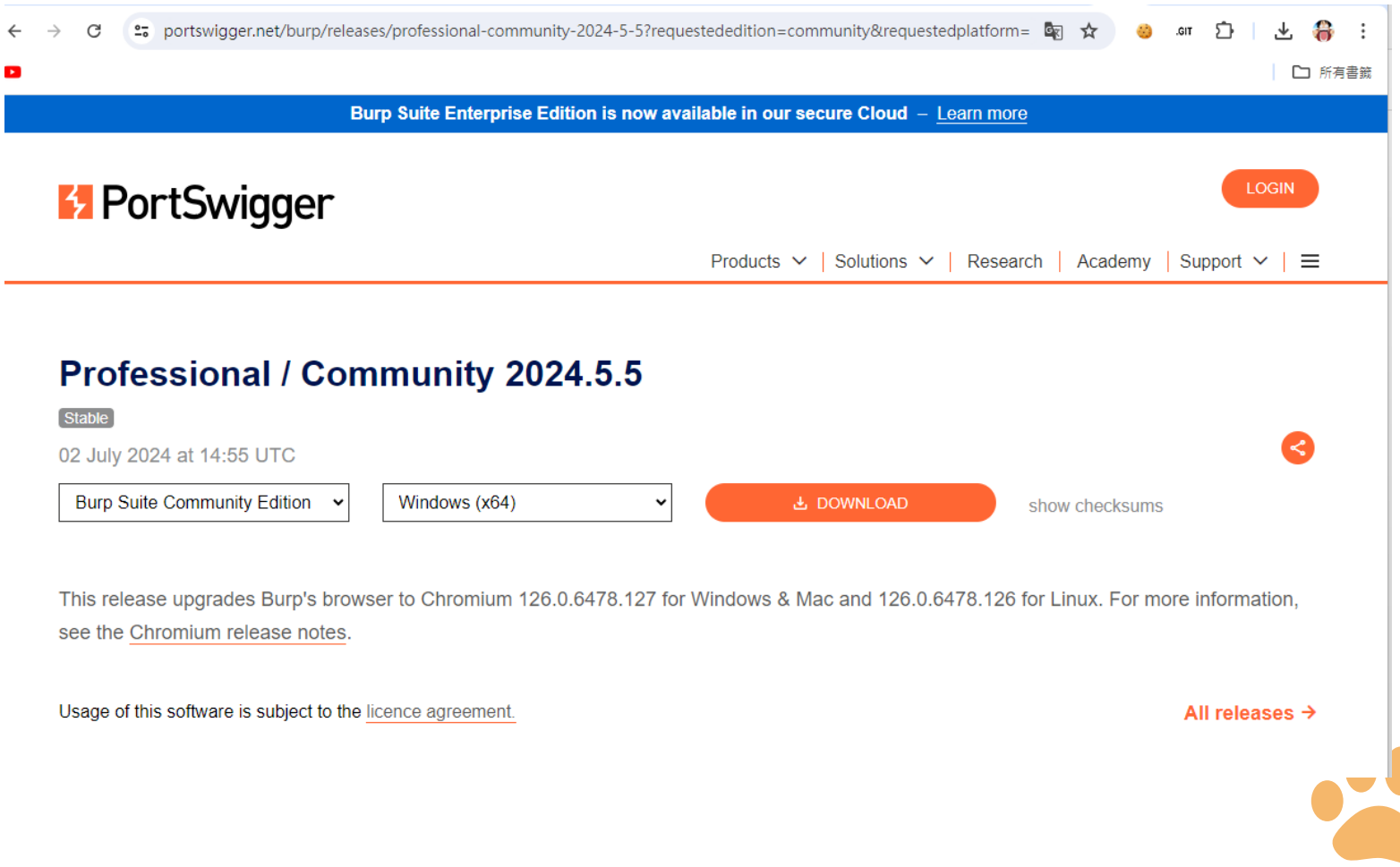


- × 沒有標準ＳＯＰ
- × 著重觀察力與敏銳度
- × 須具一定程度技術能力
- × 須保持客觀角度

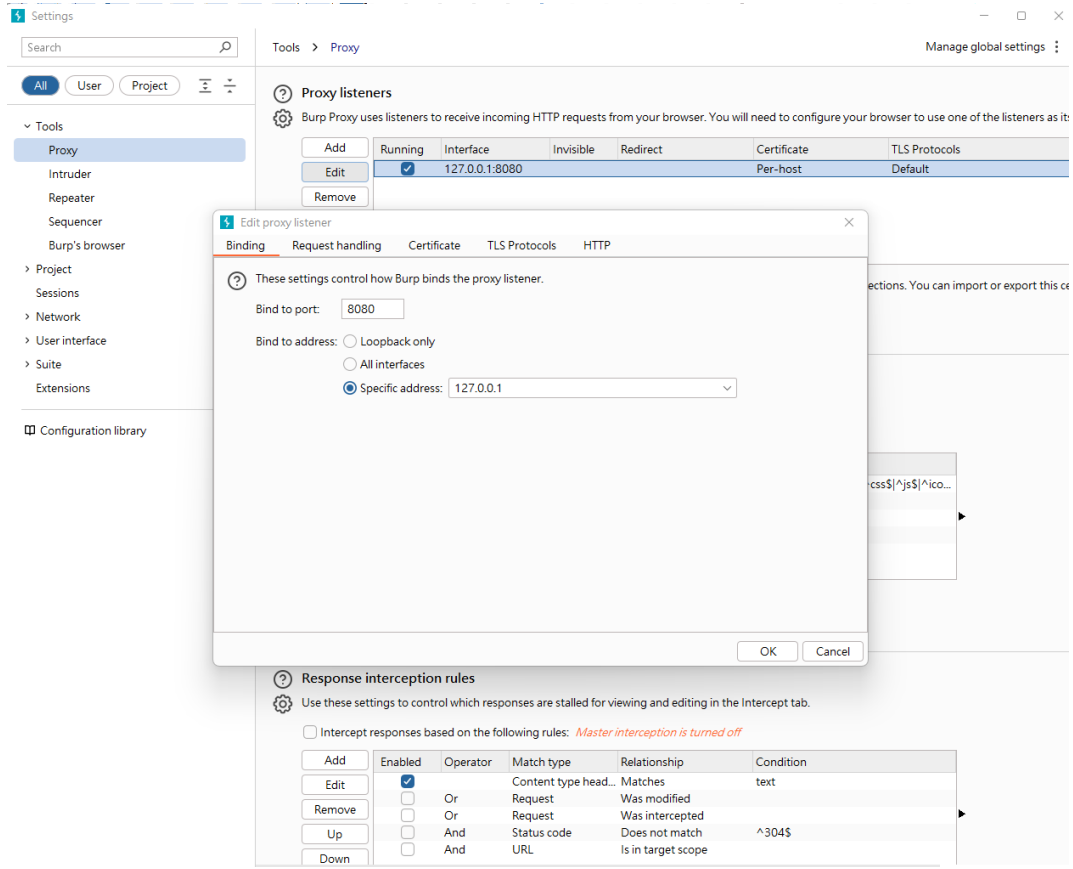


LAB實作

下載/安裝burp suite



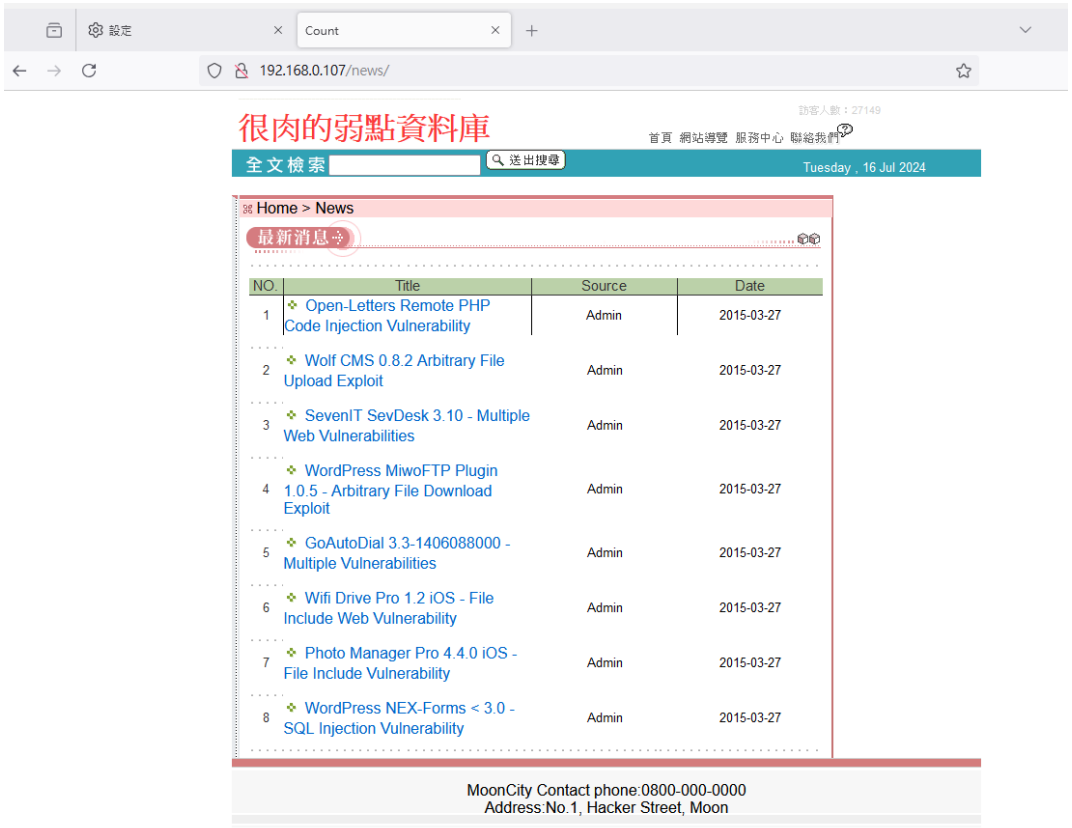
設定burp suite



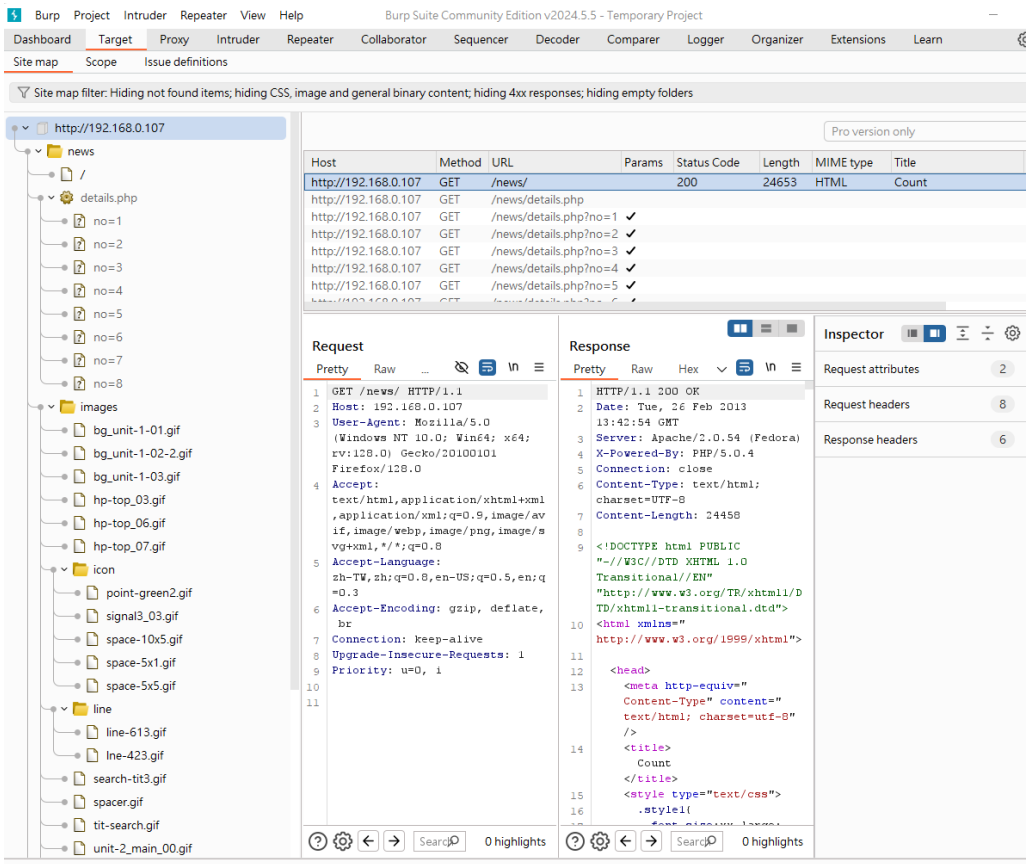
設定瀏覽器


設定
Firefox about:preferences
您的瀏覽器受到組織管理。
搜尋選項
一般
首頁
搜尋
隱私權與安全性
同步
Mozilla 的更多產品
擴充套件與佈景主題
Firefox 技術支援
連線設定
設定存取網際網路的代理伺服器
不使用 Proxy (Y)
自動偵測此網路的 Proxy 設定 (W)
使用系統 Proxy 設定 (U)
手動設定 Proxy (M)
HTTP Proxy (X) 127.0.0.1 埠 (P) 8080
也針對 HTTPS 連線使用此代理伺服器 (S)
HTTPS Proxy (H) 127.0.0.1 埠 (O) 8080
SOCKS 主機 (C) 埠 (T) 0
SOCKS v4 (K) SOCKS v5 (V)
Proxy 自動設定網址 (A)
重新載入 (E)
直接連線 (N)
範例: .mozilla.org, .net.tw, 192.168.1.0/24
與 localhost、127.0.0.1/8 與 ::1 的連線永遠不會經過代理伺服器。
若已儲存密碼則不要提示驗證 (I)
使用 SOCKS v4 時也代理 DNS 查詢 (4)
使用 SOCKS v5 時也代理 DNS 查詢 (D)
確定
取消

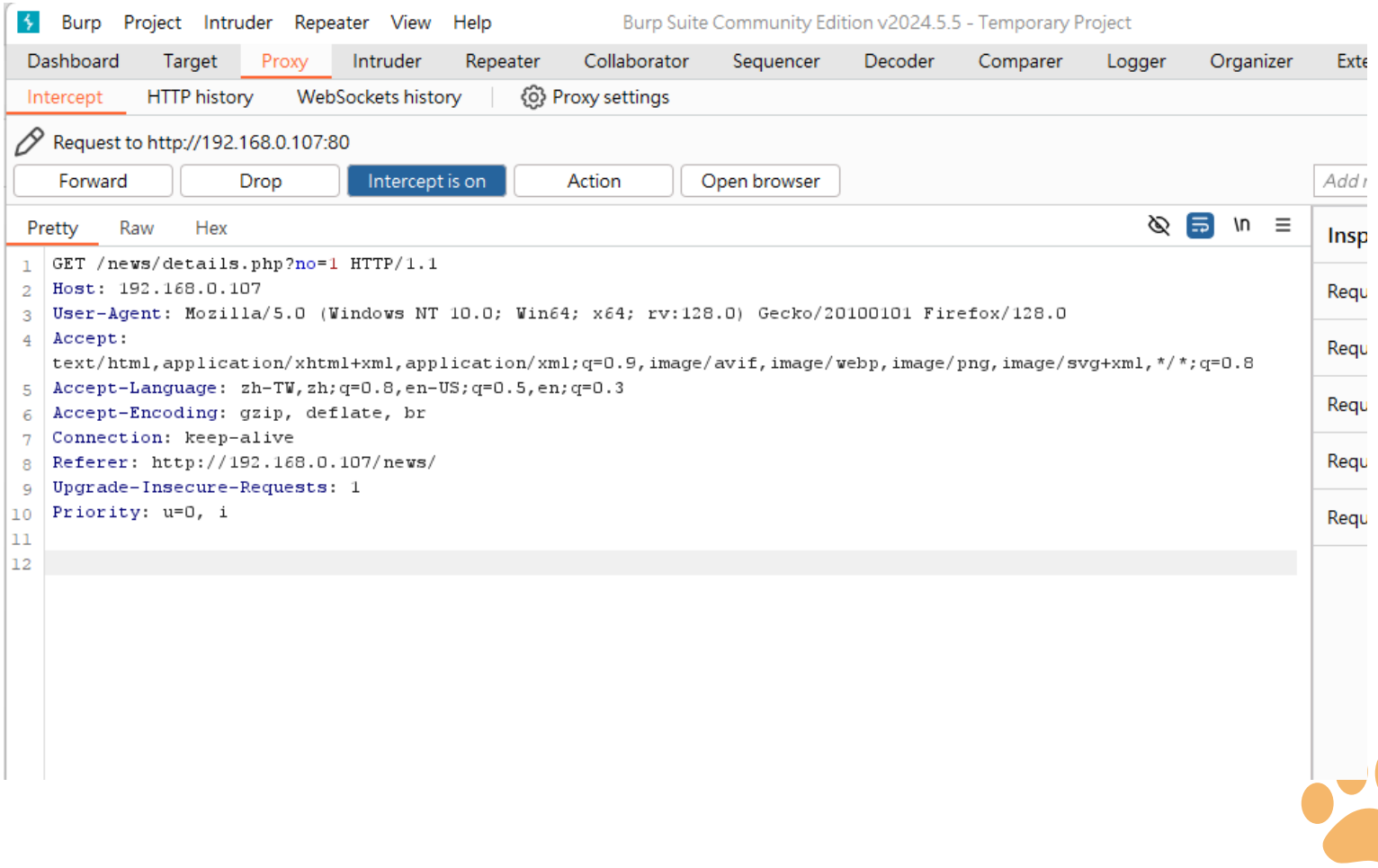
連接lab環境

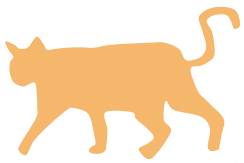

設定
Count
192.168.0.107/news/
很肉的弱點資料庫
訪客人數：27149
首頁 網站導覽 服務中心 聯絡我們
全文檢索
送出搜尋
Tuesday , 16 Jul 2024
Home > News
最新消息
NO. Title Source Date
1 Open-Letters Remote PHP Code Injection Vulnerability Admin 2015-03-27
2 Wolf CMS 0.8.2 Arbitrary File Upload Exploit Admin 2015-03-27
3 SevenIT SevDesk 3.10 - Multiple Web Vulnerabilities Admin 2015-03-27
4 WordPress MiwoFTP Plugin 1.0.5 - Arbitrary File Download Exploit Admin 2015-03-27
5 GoAutoDial 3.3-1406088000 - Multiple Vulnerabilities Admin 2015-03-27
6 Wifi Drive Pro 1.2 iOS - File Include Web Vulnerability Admin 2015-03-27
7 Photo Manager Pro 4.4.0 iOS - File Include Vulnerability Admin 2015-03-27
8 WordPress NEX-Forms < 3.0 - SQL Injection Vulnerability Admin 2015-03-27
MoonCity Contact phone:0800-000-0000
Address:No.1, Hacker Street, Moon

Burp上出現剛連接的站台



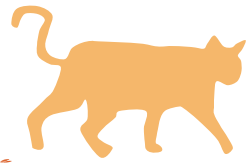
嘗試攔截封包


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.5.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer
Intercept HTTP history WebSockets history Proxy settings
Request to http://192.168.0.107:80
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
GET /news/details.php?no=1 HTTP/1.1
Host: 192.168.0.107
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://192.168.0.107/news/
Upgrade-Insecure-Requests: 1
Priority: u=0, i



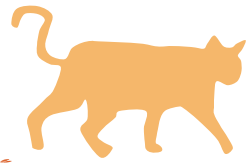
常見網站攻擊手法介紹與實作

Injection Flow



- 常見有
  - SQL Injection
  - Command Injection
  - LDAP Injection
  - XML Injection
  - …etc
- 未驗證輸入值錯誤（Input Validation Error）的安全弱點

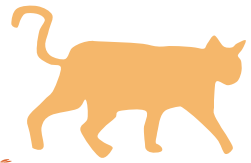
SQL Injection



- 中文翻譯
  - SQL資料隱碼
  - SQL指令植入式攻擊
- 產生成因
  - 網頁程式
  - ~~資料庫~~
- 資安設備能夠有效防禦SQL Injection嗎？
  - ~~防火牆~~
  - 入侵偵測系統
  - 網頁應用程式防火牆

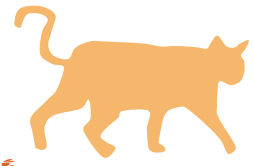
Ref:
https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OTG-INPVAL-005)

可以...



- 跳脫驗證
- 取得權限
- 竊取機敏資訊
- 增刪資料
- 掛馬
- ....
- etc

如何偵測SQL Injection



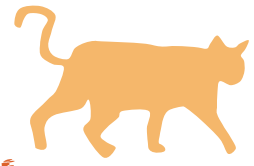
插入特殊符號：’ 、 ”、;

[Simple URL]
http://www.example.com
/news.asp?id=10

[Test SQL Injection]
http://www.example.com/
news.asp?id=10'

觀察網頁回應內容

如何偵測SQL Injection



插入運算字元

[Simple URL]

http://www.example.com/news.asp?id=10

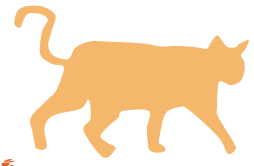
[Test SQL Injection]

http://www.example.com/news.asp?id=11-1

http://www.example.com/news.asp?id=10’ or ‘1’ = ‘1

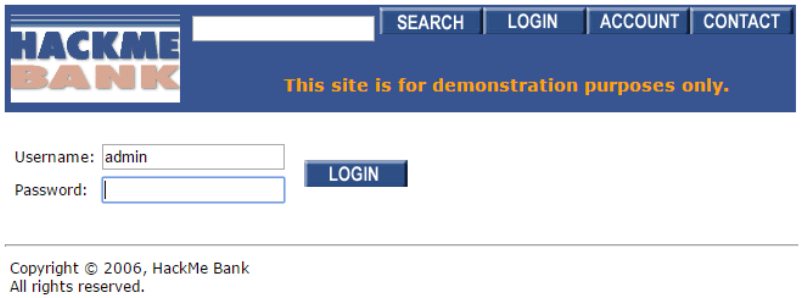
觀察網頁回應內容

SQL Injection利用：繞過驗證



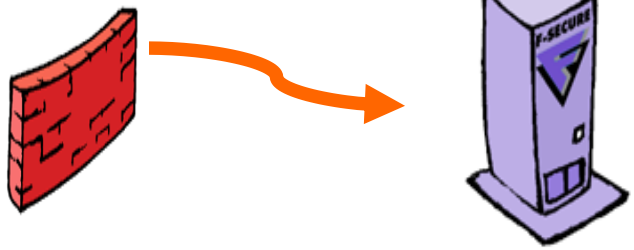
- 登入頁面的SQL Injection
- 利用登入頁面的驗證程式未進行參數過濾來達到繞過驗證的目的
- 早期最常見利用方式
- 目前較為少見

正常連線狀態

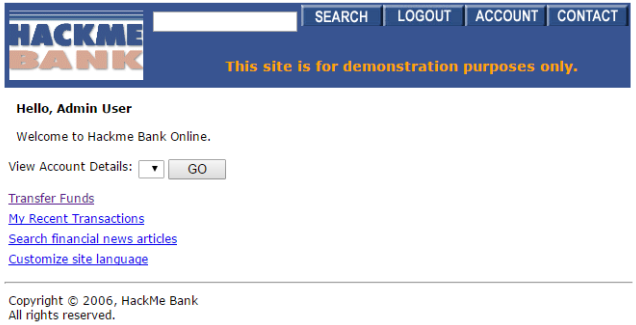


ID=qoo
Passwd=1234

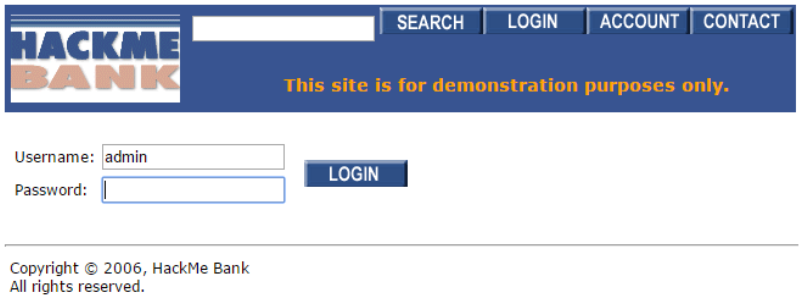
Internet



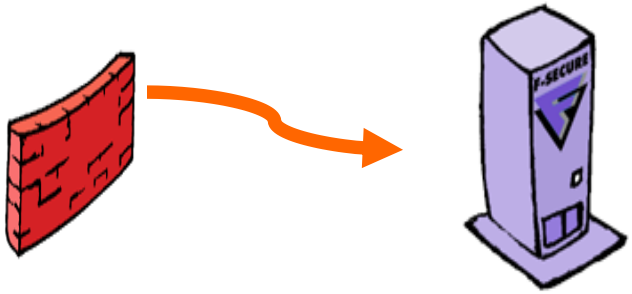
select * from member where
UID ='qoo'
And Passwd='1234'



嘗試繞過驗證

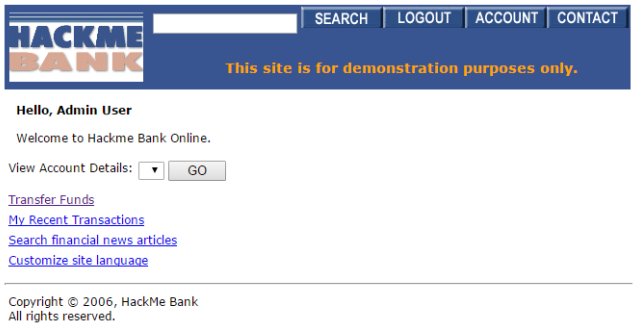


ID=qoo
Passwd=’ or ‘1’ = ‘1



Internet

select * from member where
UID ='qoo'
And Passwd= ‘ or ‘1’ = ‘1



SQL Injection原理

- 一般輸入帳號密碼的網站的SQL語法

select * from member where UID =' "& request("ID") & " '
And Passwd =' "& request("Pwd") & " '

正常輸入

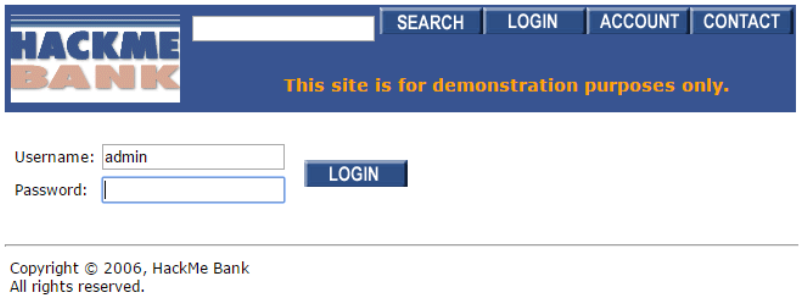
select * from member where UID = 'qoo' And Passwd='1234'

嘗試繞過

select * from member where UID = 'qoo'
And Passwd=' ' or '1' = '1'

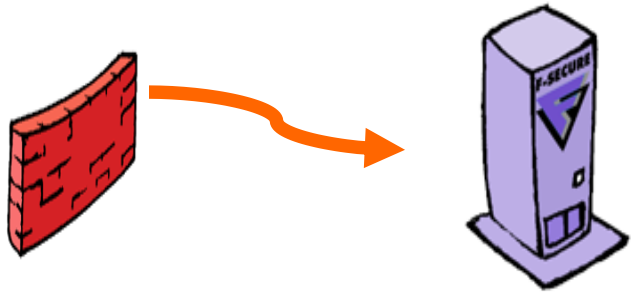
- 因為or後面的 '1' = '1' 為真，所以順利登入成功

嘗試繞過驗證 II

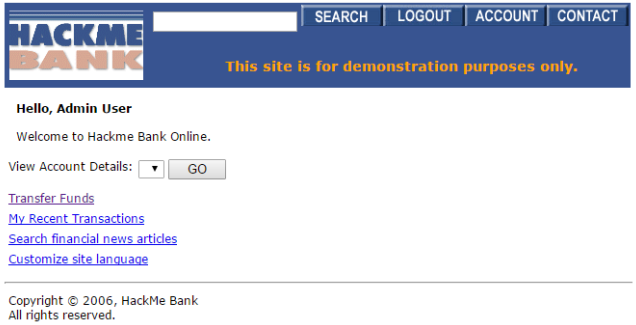


ID=Admin' --
Passwd=

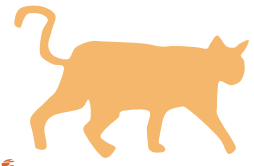
Internet



select * from member
whereUID = 'Admin' --'
And Passwd= ''



SQL Injection原理



- 一般輸入帳號密碼的網站的SQL語法

select * from member where UID =' "& request("ID") & " '
And Passwd =' "& request("Pwd") & " '

正常輸入

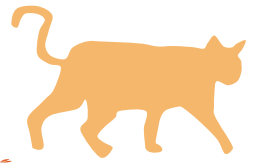
select * from member where UID = 'qoo' And Passwd='1234'

嘗試繞過

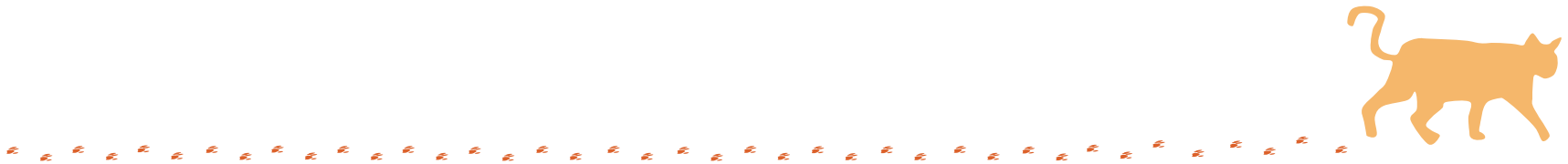
select * from member where UID = 'Admin' --'
And Passwd= ''

- 因為UID = 'Admin' 後接的是註解符號，所以後面的條件就不繼續進行比對，直接以Admin帳號登入成功

Thinking

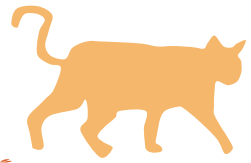


- 在IPS上設定偵測 1=1有用嗎?
- 從1=1設定到100=100進行偵測有用嗎?
- Why?



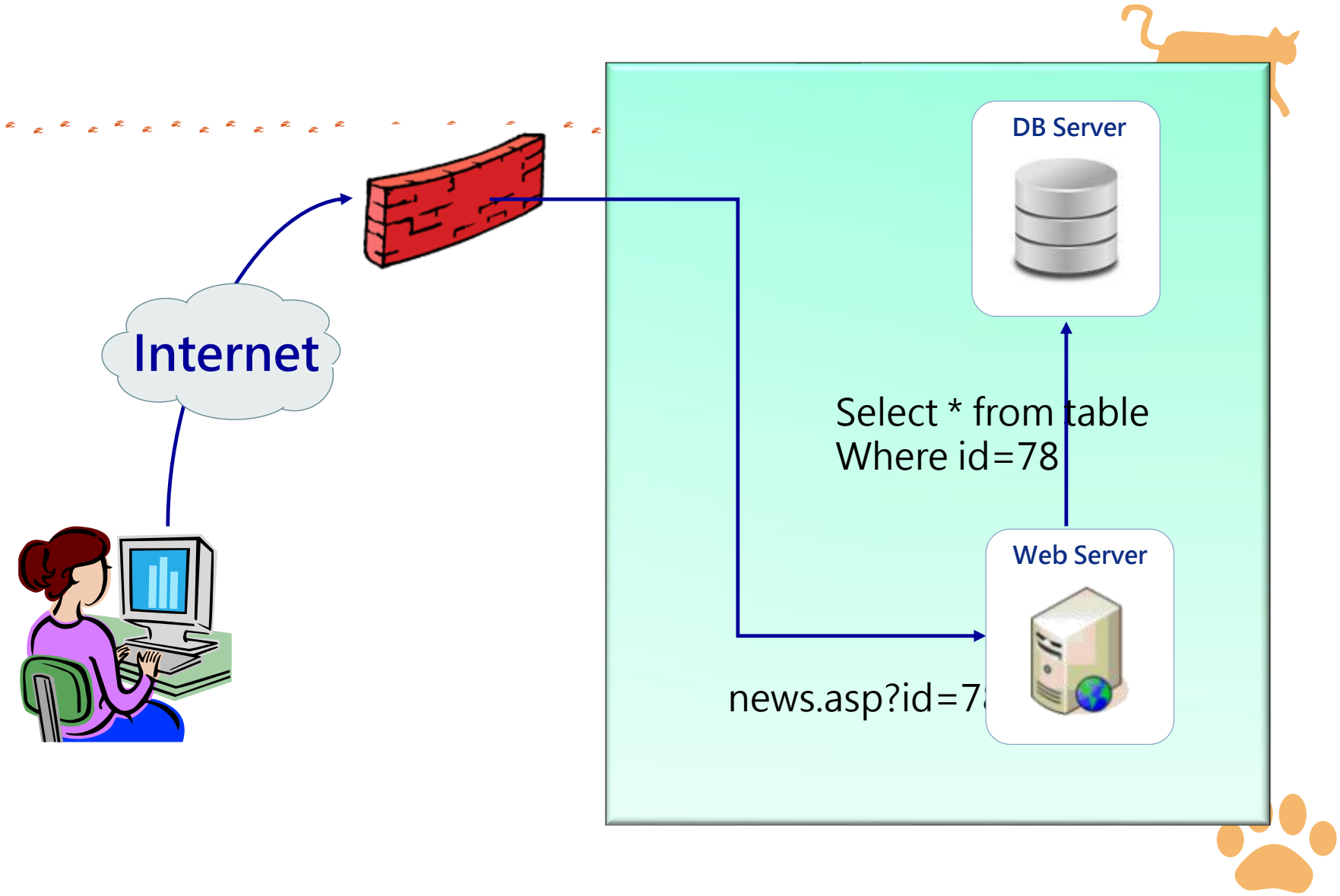
Normal SQL Injection

正常網站資料查詢

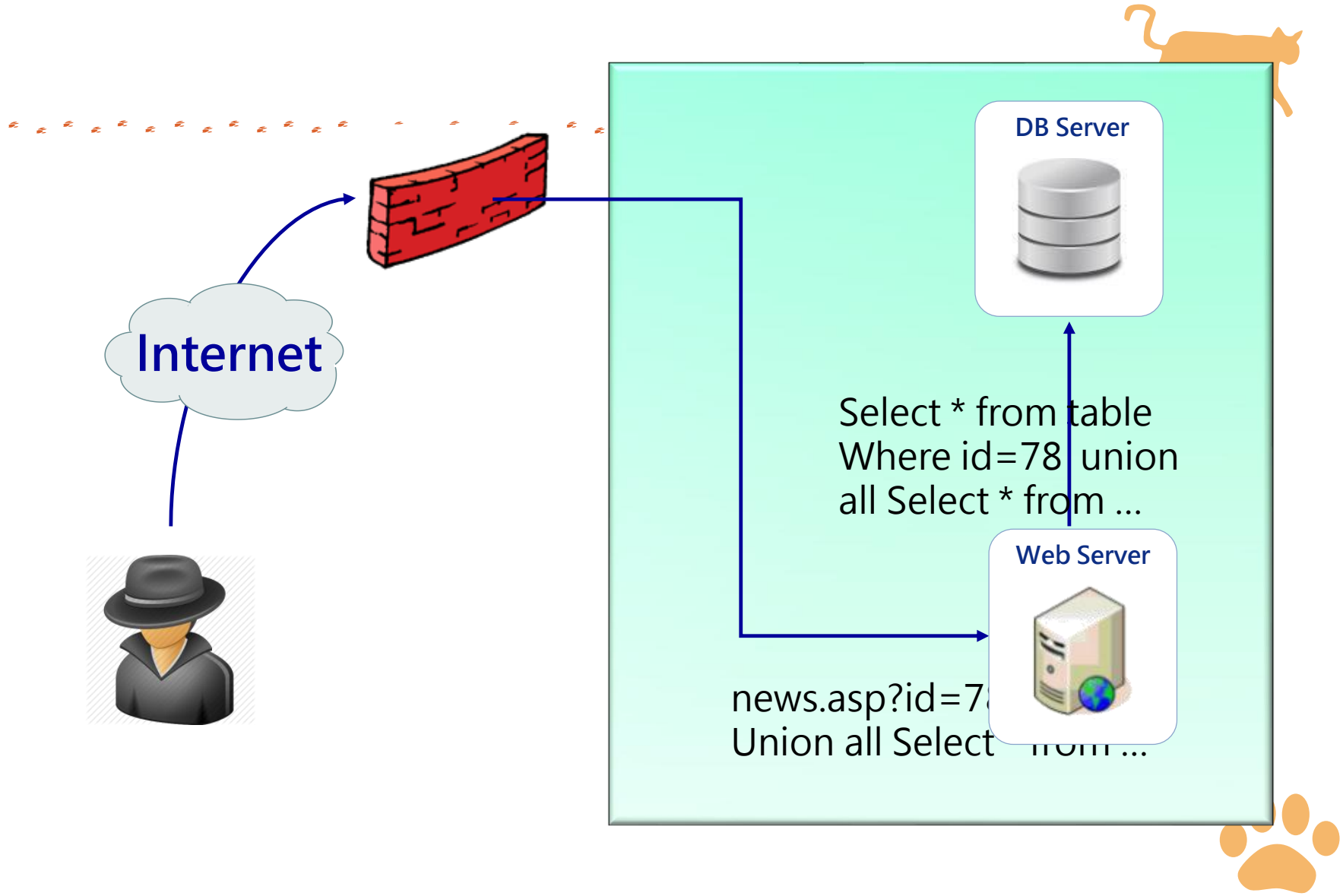


- 參數對應到後端資料庫資料
- 能不能輸入其他SQL指令?

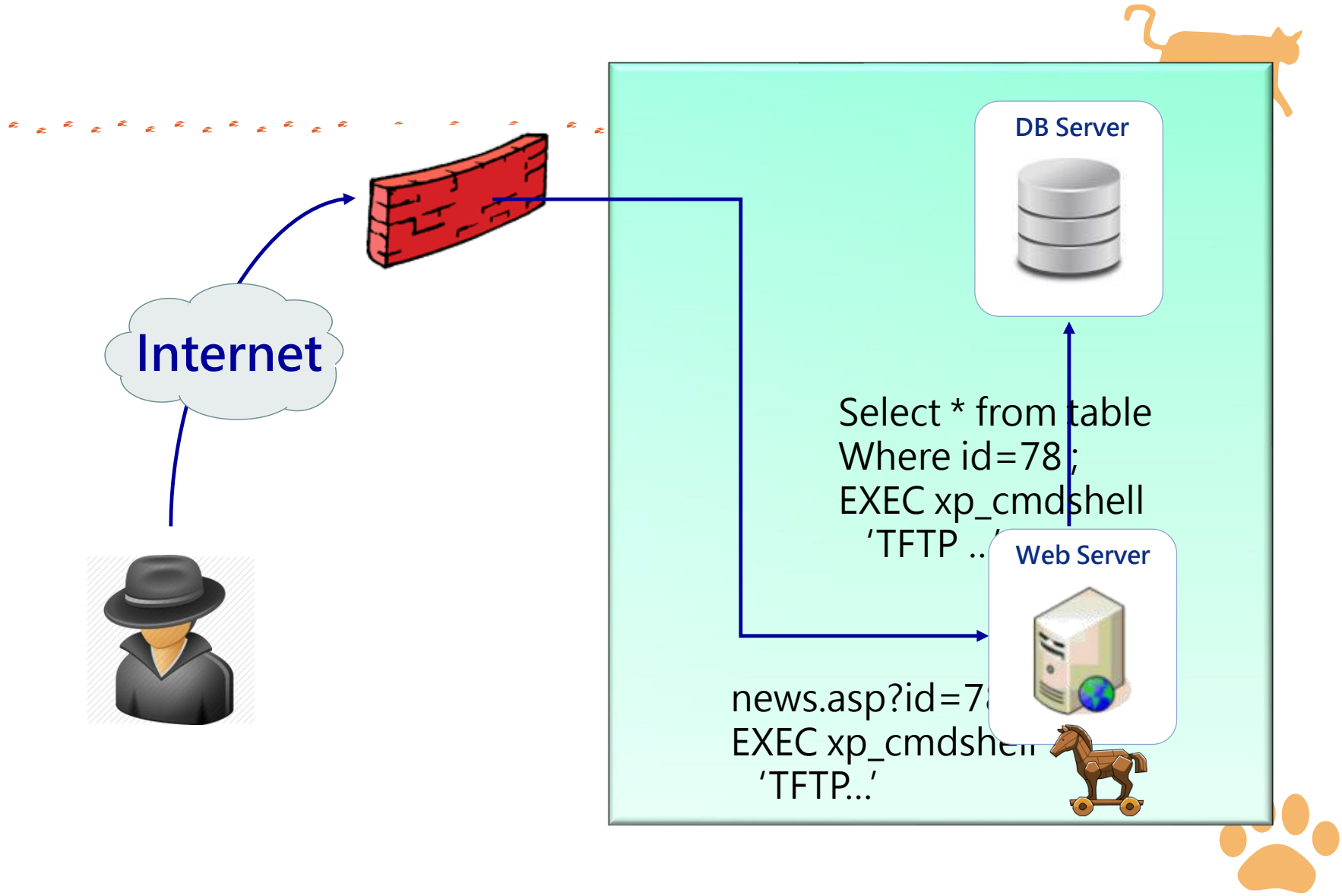
正常網站資料查詢

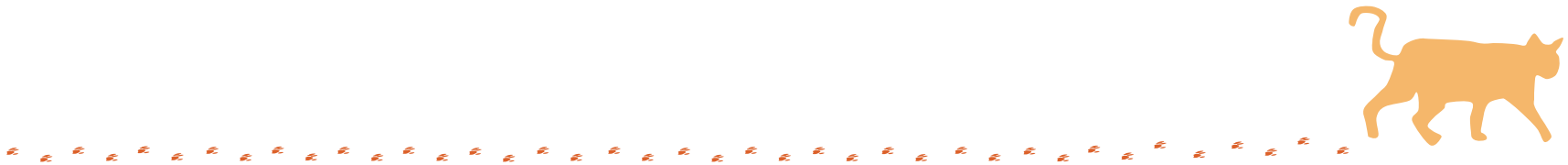

DB Server
Internet
Select * from table
Where id=78
Web Server
news.asp?id=7

不正常網站資料查詢


DB Server
Internet
Select * from table
Where id=78 union
all Select * from ...
Web Server
news.asp?id=7
Union all Select

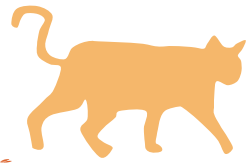
不正常網站資料查詢


DB Server
Internet
Select * from table
Where id=78 ;
EXEC xp_cmdshell
'TFTP ..
Web Server
news.asp?id=7
EXEC xp_cmdshell
'TFTP...'



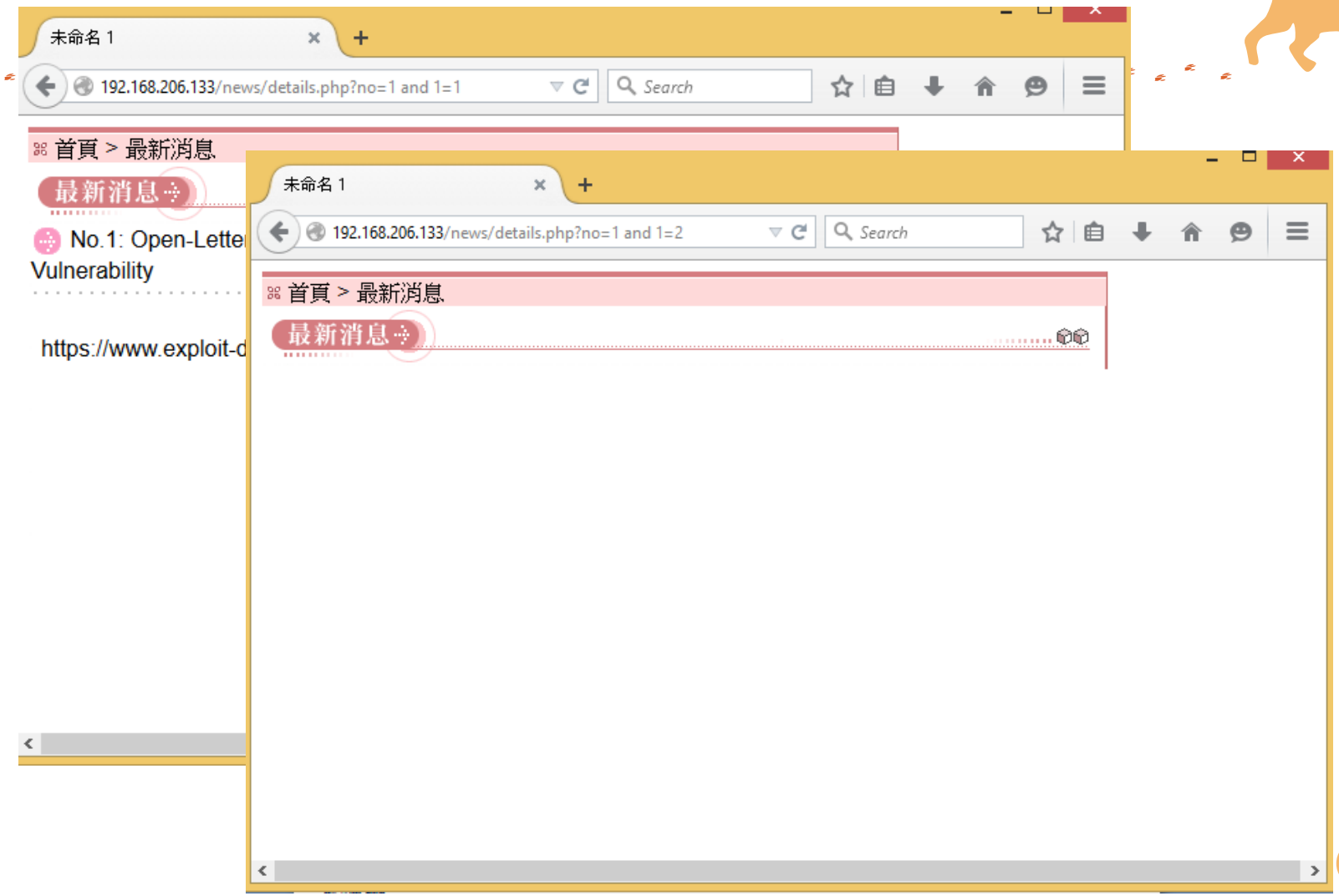
Blind SQL Injection

Blind SQL Injection

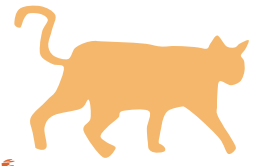


- 沒有錯誤訊息的回應
- 要如何列舉資料？

Blind SQL Injection

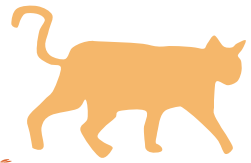


防SQL injection實戰篇



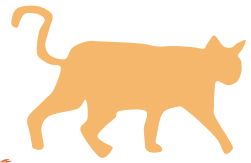
- 資料庫伺服器方面
  - 定期修補作業系統與資料庫伺服器的漏洞
  - 避免提供過高的權限
- 網站伺服器方面
  - 關閉或重導錯誤訊息回應
- 程式設計方面
  - 絕對不要將 SQL 命令寫在網頁/JavaScript中
  - 針對參數型態處理
  - 於網站後端程式加入特殊字元的檢查、濾除或轉化（如：'、"、--、;、@等）

Command Injection



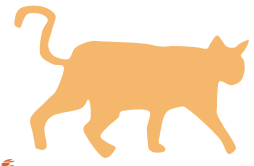
- 開發人員為了節省開發時間，常直接引用系統指令
- 當使用者輸入沒有被適當地檢查時，攻擊者就可能透過執行這些作業系統指令來進行惡意的操作

Cross Site Scripting



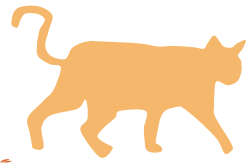
- 跨站腳本攻擊
- 俗稱xss
- 輸入值驗證錯誤（Input Validation Error）的安全弱點
- 攻擊對象非網站本身
- 隔山打牛式的攻擊

Cross-Site Scripting



- 在 Web 應用程式中，當 參數 或 資料 顯示成HTML 網頁前，未檢查內容是否含 HTML tag 或 網頁腳本，導致被駭客利用，攻擊其他瀏覽網站的無辜使用者
- 簡單的攻擊例子
  - http://www.victim.com/function.cgi?data=<script>alert("XSS!")</script>
  - http://www.victim.com/function.cgi?data=<iframe src= "*<惡意URL>*"></iframe>

幾個簡單具 XSS 弱點程式例



- ASP

```
<% Response.Write(Request("Name")) %>
```

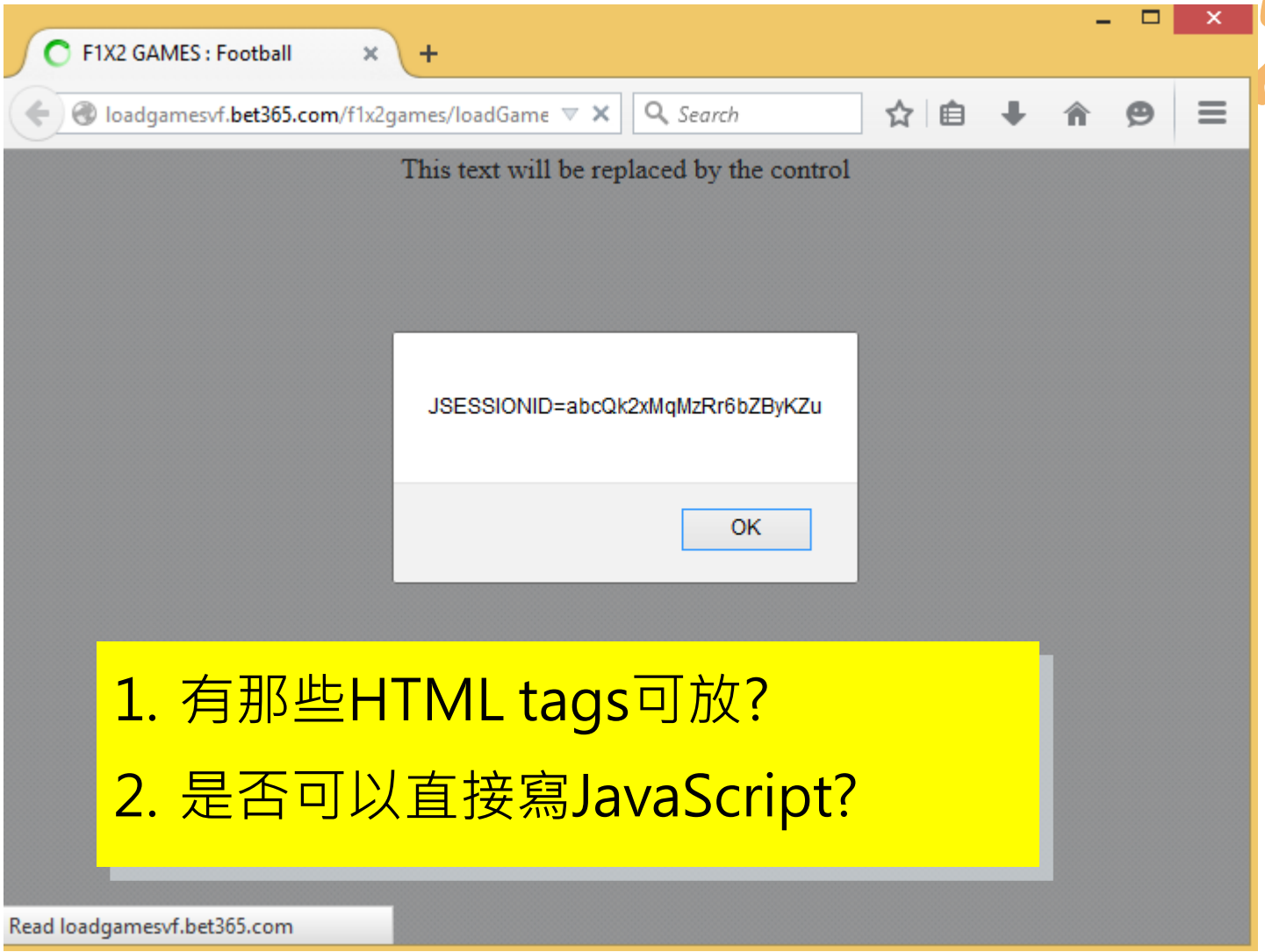
- JSP

```
<%= request.getParameter("Name") %>
```

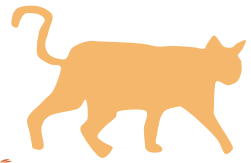
- PHP

```
<?php
  echo $_GET['name'];
?>
```

跨站網頁腳本攻擊
(Cross-Site Scripting, XSS)

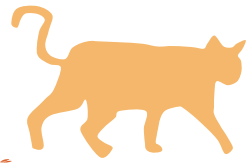


常見利用



- 竊取cookie等機敏資訊
  - <script>alert(document.cookie)</script>
- 掛馬
  - <iframe src=”惡意連結位址”></iframe>
- 網路釣魚
  - <iframe src=”釣魚網站位址”></iframe>

常見散播管道

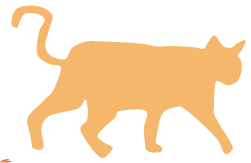


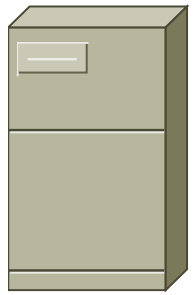
- 廣告信
- 論壇發文
- 縮網址
  - http://0rz.tw
  - http://tinyurl.com
  - ...etc
- 關鍵字與網頁看板廣告
- ...etc

竊取cookie

魚兒上鉤了

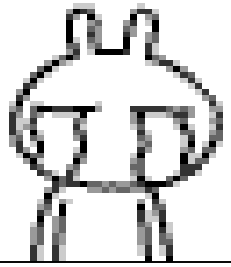
利用取得身分作壞事





網站有XSS漏洞

反彈cookies值至駭客端



哭哭...我什麼也沒做阿！！

登入後瀏覽惡意文章

利用XSS竊取cookies：對網站管理者而言

- 攻擊者並未對網站本身進行攻擊
- 登入者為使用者本身權限
- 所有的操作都是使用者本身權限所做的

掛馬

你是我的肉雞.
你是我的Baby

發送包含惡意連結信件

入口網站A有XSS漏洞

駭客取得遠端控制權限

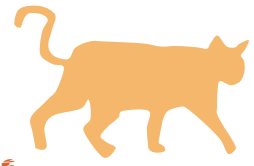
又中了！買樂透也沒這麼準...

放心點下去

下載惡意程式

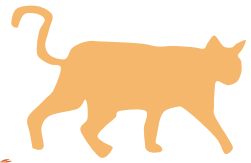
Hackers Server

利用XSS掛馬：對網站管理者而言



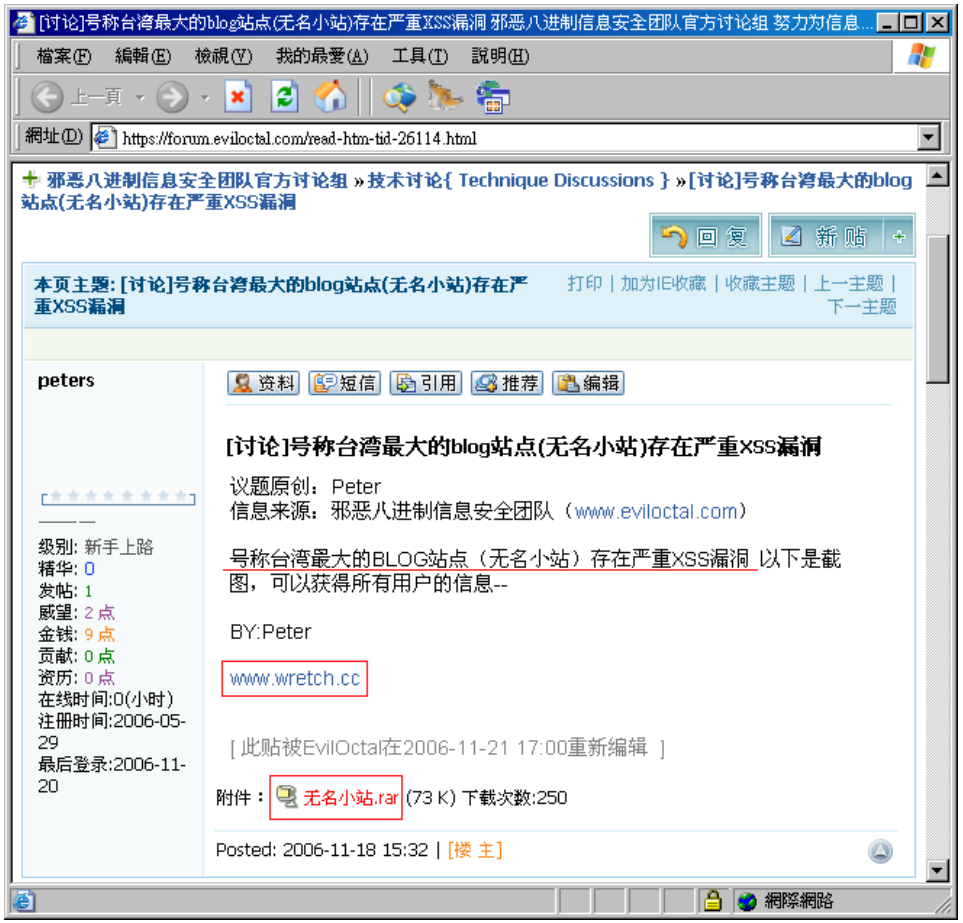
- × 攻擊者並未對網站本身進行攻擊
- × 資料庫並未被撈走或遭竄改
- × 受害者不是網站本身

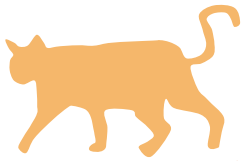
XSS防護建議



- 作好『輸入內容合法性驗證』措施（Input Validation）
  - 過濾或轉化 & < > “ ‘ ASP
    - Server.HTMLEncode()
  - http://www.faqs.org/docs/htmltut/characterentities_famsupp_69.html
  - 長度檢驗
- 設定正向與負向表列過濾
- 內容檢查
- 資安防禦設備
- 切勿使用javascript做過濾

大陸論壇也放了一份


[讨论]号称台湾最大的blog站点(无名小站)存在严重XSS漏洞 邪恶八进制信息安全团队官方讨论组 努力为信息...
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁
網址(D) https://forum.eviloctal.com/read-htm-tid-26114.html
邪恶八进制信息安全团队官方讨论组 »技术讨论{ Technique Discussions } »[讨论]号称台湾最大的blog站点(无名小站)存在严重XSS漏洞
回复
新贴
本页主题: [讨论]号称台湾最大的blog站点(无名小站)存在严重XSS漏洞
打印 | 加为IE收藏 | 收藏主题 | 上一主题 | 下一主题
peters
资料 短信 引用 推荐 编辑
[讨论]号称台湾最大的blog站点(无名小站)存在严重XSS漏洞
议题原创：Peter
信息来源：邪恶八进制信息安全团队（www.eviloctal.com）
号称台湾最大的BLOG站点（无名小站）存在严重XSS漏洞 以下是截图，可以获得所有用户的信息--
BY:Peter
www.wretch.cc
[此贴被EvilOctal在2006-11-21 17:00重新编辑]
附件： 无名小站.rar (73 K) 下载次数:250
Posted: 2006-11-18 15:32 | [楼 主]
级别: 新手上路
精华: 0
发帖: 1
威望: 2 点
金钱: 9 点
贡献: 0 点
资历: 0 点
在线时间:0(小时)
注册时间:2006-05-29
最后登录:2006-11-20
網際網路



感恩<(_ _)>

Pedro[小老鼠]pdcyber.com