HackDay

滲透測試報告書

2017/3/14

**目錄**

內容

[**1.報告細節** 3](#_Toc477312529)

[**2.測試目標** 3](#_Toc477312530)

[**3.測試日期** 3](#_Toc477312531)

[**4.執行流程** 4](#_Toc477312532)

[4.1.方法 4](#_Toc477312533)

[4.2.測試範圍 4](#_Toc477312534)

[4.3.發現總結 4](#_Toc477312536)

[**5.發現漏洞** 6](#_Toc477312537)

[5.1. Password Transmitted over HTTP 6](#_Toc477312538)

[5.2. robots.txt 7](#_Toc477312539)

[5.3. Programming Error Message 7](#_Toc477312540)

[5.4. SQL injection 9](#_Toc477312541)

[5.5. File Upload 9](#_Toc477312542)

[**6.參考資料** 11](#_Toc477312543)

1. **.報告細節**

|  |  |
| --- | --- |
| 標題 | HackDay 滲透測試報告書 |
| 版本 | HackDay-Albania |
| 作者 | R-73eN |
| 測試者 | 許嘉修 |
| 審查 | XXX |
| 分類 | 機密 |

1. **.測試目標**

|  |  |
| --- | --- |
| 名稱 | IP |
| HackDay | 192.168.56.102 |

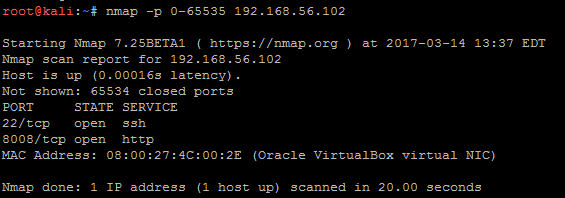
1. **.測試日期**

|  |  |
| --- | --- |
| 日期 | 結束日期 |
| 2017/3/14 | 2017/3/14 |

1. **. 執行流程**
   1. **方法**

* 對目標進行漏洞掃描
* 識別及辨識漏洞
* 漏洞分級
* 漏洞影響
  1. **測試範圍**

針對目標系統IP:192.168.56.102進行nmap掃描如下圖，發現ssh服務與web服務，此次進行web服務漏洞掃描。



針對目標系統進行nmap掃描之結果

* 1. **發現總結**

|  |  |
| --- | --- |
| 等級 | 數量 |
| High | 1 |
| Medium | 2 |
| low | 2 |

1. **.發現漏洞**

5.1 Password Transmitted over HTTP

**風險等級**：低

**來源**：<http://192.168.56.102:8008/unisxcudkqjydw/vulnbank/client/login.php/>

**檢測**：檢測到該網頁透過HTTP傳輸敏感資訊，如使用者帳號密碼。

**分析**：如果攻擊者可以攔截網絡流量，那可能會遭攻擊者竊取使用者的敏感資訊。

**修補**：所有敏感數據應透過HTTPS而不是HTTP傳輸，提供給使用者輸入訊息的介面也應透過HTTPS傳輸。



圖1.該網站使用HTTP傳輸

5.2 robots.txt

**風險等級**：中

**來源**：http://192.168.56.102:8008/robots.txt

**檢測**：檢測到具有可能敏感內容的robots.txt檔案。

**分析**：robots.txt是一種存放於網站根目錄下的文字檔案，用在於告訴網路搜尋引擎該網站中哪些內容是不應被搜尋的，但如果未做好文字檔案保護，根據文件的內容，攻擊者可能會發現隱藏的目錄。

**修補**：如果具有敏感資訊的路徑，例如管理介面的路徑，請不要將其寫入robots.txt，應透過身份驗證才能瀏覽敏感路徑。

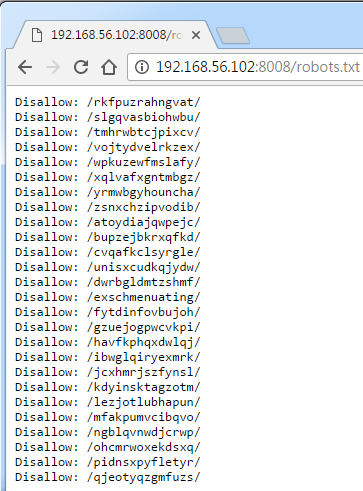
****

圖2.該網站具有robots.txt安全漏洞

5.3 Programming Error Message

**風險等級**：中

**來源**：<http://192.168.56.102:8008/unisxcudkqjydw/vulnbank/client/login.php/>

**檢測**：檢測到使用者登入網頁，會輸出錯誤訊息。

**分析**：當測試使用者登入網頁時，輸入'送出時會出現錯誤並帶出網站目錄路徑，這使攻擊者攻擊成功的話，攻擊者很輕易的就可置放後門網頁。

**修補**：不能在輸出給使用者的介面提供網站系統內部的錯誤消息。

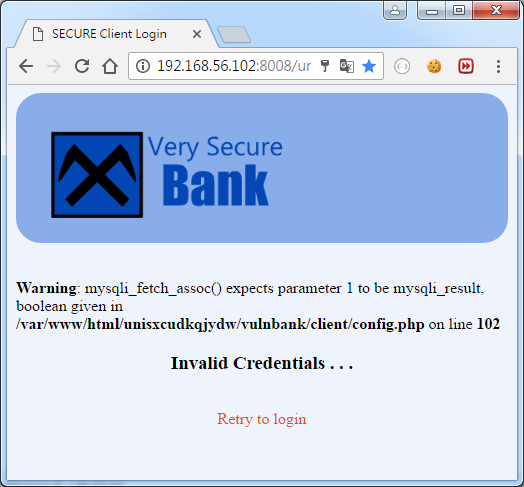


圖3.該網站具有輸出錯誤訊息的安全漏洞

5.4 SQL injection

**風險等級**：高

**來源**：<http://192.168.56.102:8008/unisxcudkqjydw/vulnbank/client/login.php/>

**檢測**：檢測到使用者登入網頁，具有SQL injection漏洞。

**分析**：使用sqlmap滲透工具測試，可發現該網站具有SQL injection漏洞。

**修補**：在處理使用者所輸入的資料前，先驗證所有客戶端提供的資料，包括所有的參數、URL內容，之後過濾敏感的字元，如果危險的字串必須做為輸入的一部分，在使用之前必須轉議或編碼，也不能動態組合SQL語法。

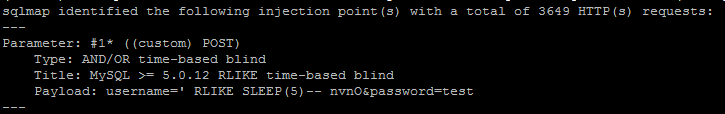


圖4.使用sqlmap工具進行滲透測試結果

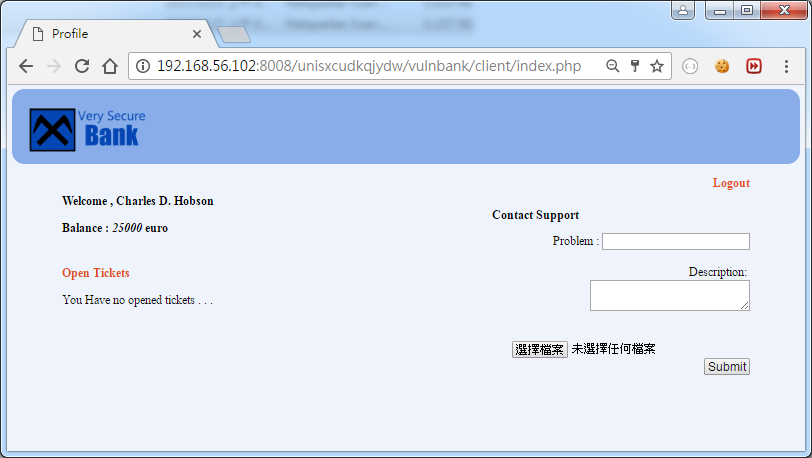


圖5.該網站具有SQL injection安全漏洞

5.5 File Upload

**風險等級**：高

**來源**：<http://192.168.56.102:8008/unisxcudkqjydw/vulnbank/client/index.php>

**檢測**：該網站具有檔案上傳漏洞，攻擊者能繞過附檔名驗證置入後門網頁，進而入侵系統。

**分析**：雖網站的上傳系統規定只能上傳jpg附檔名，但仍可透過附檔名修改方式上傳php後門網頁。

**修補**：禁止php使用view\_file.php?filename=test3.jpg方式打開jpg檔案，雖然附檔名是jpg但實際內容是php程式碼，讀取jpg時應使用html標籤<img src="test3.jpg" />，才能防止惡意攻擊。

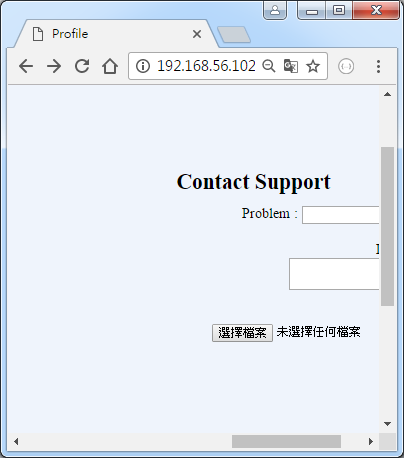


圖6.該網站具有檔案上傳的安全漏洞

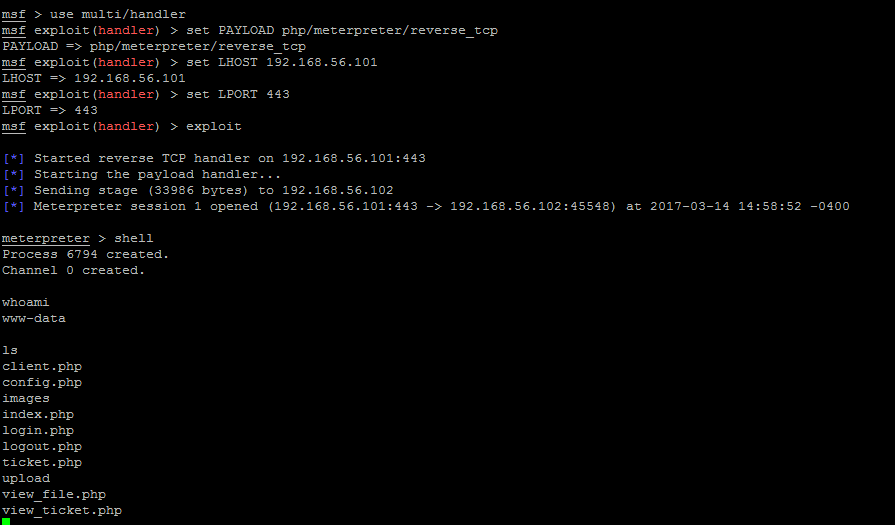


圖7.透過檔案上傳漏洞可植入後門網頁達到系統入侵

1. **.參考資料**

[1] Vulnhub , https://www.vulnhub.com/entry/hackday-albania,167/