Network Security Project 2

0656511　網工碩一　黃誠發

- 一開始不知道要如何開始破解，所以就把所有的資訊全部搜尋一遍，最後發現第一道秘境
  - robots.txt：是在網頁的根目錄底下的一個不想讓別人爬到的資料的 list，之後我在網址上找到這個隱藏檔案，最後得到有三個不想別人的東西：
    - / phpMyAdmin_NS_pRojEct_2017/
    - / backup.tar.gz
    - / blog/ memorandum.txt

```
User-agent: *
Disallow: /phpMyAdmin_NS_pRojEct_2017/
Disallow: /backup.tar.gz
Disallow: /blog/memorandum.txt
```

  - phpMyAdmin_NS_pRojEct_2017：是 phpMyAdmin 的路徑，可以連到網站
    - 進去後發現需要帳號密碼，所以需要其他的東西做附註
    - 我發現必須透過 / blog/ memorandum.txt 來找帳號密碼
  - / blog/ memorandum.txt：需要應用 tmp file 檔名的方式找到檔案完整的網址應該為：
    http:/ / 140.113.194.66:20032/ blog/ .memorandum.txt.swp
    如此一來就能找到想得到的檔案，但在這之前會遇到裡面是一個長得很像之前作業的編碼，base64，必須先對他做 base64 decode 之後會發現還是一串亂碼，這時候就需要 XOR Cracker 來解碼。
    - 首先，將該檔案先改成檔名為 memorandum.txt 在做 base64 decode
    - 然後將結果存入另一檔案
    - 丟入網路上搜尋的 XOR Cracker tool

- https:/ / wiremask.eu/ tools/ xor-cracker/
- 就能找到兩組可能的解

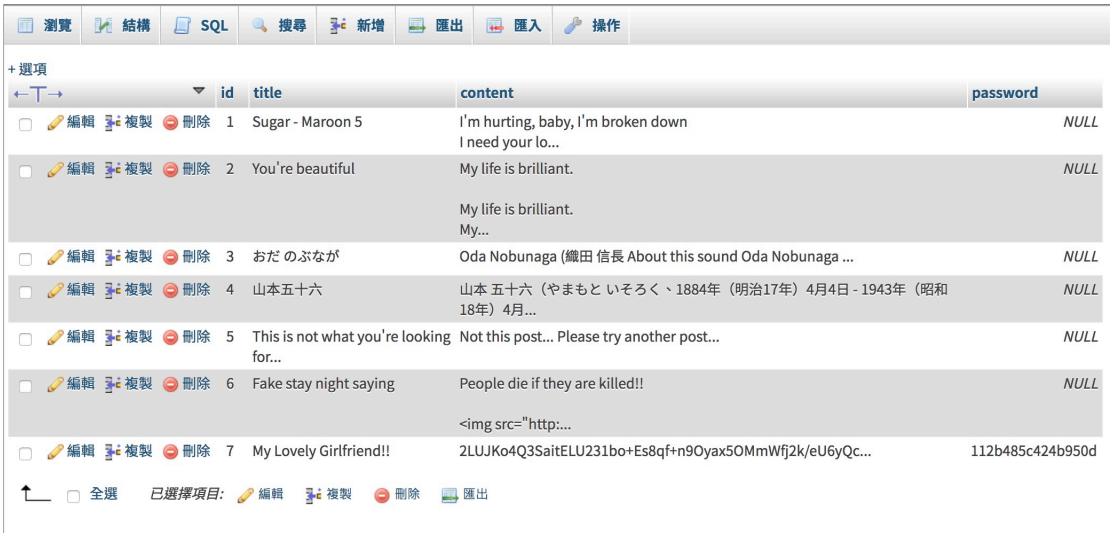
Possible keys

Keys		Decrypted File
multiplicands	6d 75 6c 74 69 70 6c 69 63 61 6e 64 73	Download
MULTIPLICANDS	4d 55 4c 54 49 50 4c 49 43 41 4e 44 53	Download

- 有一個還是亂碼，而另一個裡面就有正確的資訊

```
2016.01.13
phpMyAdmin Account & Password
Account: BobIsGod
Password: trialedMimioutruns
```

- phpMyAdmin：後端存放管理資料的介面



瀏覽 結構 SQL 搜尋 新增 匯出 匯入 操作

+選項

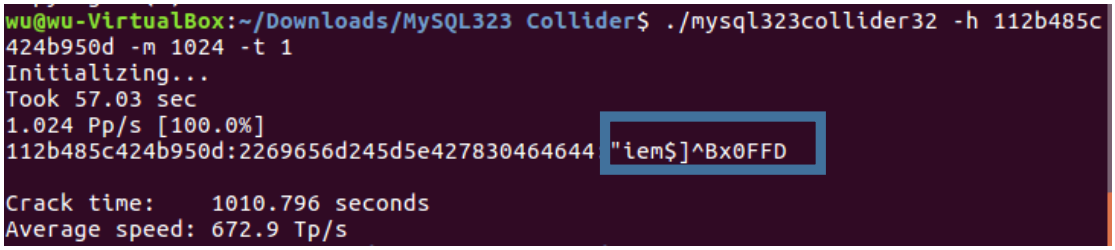
	id	title	content	password
編輯 複製 刪除	1	Sugar - Maroon 5	I'm hurting, baby, I'm broken down I need your lo...	NULL
編輯 複製 刪除	2	You're beautiful	My life is brilliant. My life is brilliant. My...	NULL
編輯 複製 刪除	3	おだ のぶなが	Oda Nobunaga (織田 信長 About this sound Oda Nobunaga ...	NULL
編輯 複製 刪除	4	山本五十六	山本 五十六（やまもと いそろく、1884年（明治17年）4月4日 - 1943年（昭和18年）4月...	NULL
編輯 複製 刪除	5	This is not what you're looking for...	Not this post... Please try another post...	NULL
編輯 複製 刪除	6	Fake stay night saying	People die if they are killed!! <img src="http:...	NULL
編輯 複製 刪除	7	My Lovely Girlfriend!!	2LUJKo4Q3SaitELU231bo+Es8qf+n9Oyax5OMmWfj2k/eU6yQc...	112b485c424b950d

全選 已選擇項目: 編輯 複製 刪除 匯出

- 就能得到密碼了！
- 但是這密碼餵進去是錯的，因為他是經過 hash function 的密碼
- 所以這下我們需要用到最後一個有用的資料

- / backup.tar.gz：解壓縮後是整個網頁的原始碼
  - 我找到它裡面有 function.php 其中就有 hash function 的編碼原始碼，從這可得知他是用 hash 的方式作加密
  - 而我將 magic1 = 1345345333 搭配關鍵字 MySQL 找到了，其實他是用一種很老的 hash function 作加密

- 這方法的名字是：mysql323
  - 這是一個可以透過運算找到一組解經過 hash function 後與先前在 phpMyAdmin 中找到的密碼一樣
- 於是我又在網路上找到 tool 來用：
  https:/ / tobtu.com/ mysql323.php
- 將他的 code 載下來，利用 command line 將其解壓縮更改執行檔的使用權限，然後將 phpMyAdmin 中找到的答案經過計算得到真正的密碼



- 最後再將此密碼輸入，就能得到目標圖片

- What have you learned?
  - Robots.txt 這是一個在網頁根目錄底下的一個檔，用來告訴爬蟲的人不要去爬他，但是這也反而透露了自己的弱點，一些比較敏感的資料一定是從這些地方得到
  - 清楚明白了網頁得結構，能運用其中的提示找到要的答案
  - 暫存檔案太容易被拿到，所以必須有經過適當的加密讓人不會輕易地看到
    - 這次用了 base64 及 XOR encryption 做加密
  - 最後就是進入 phpMyAdmin 後得到的密碼需要做 hash function 的缺陷破解才拿得到解答

- How to prevent or patch these vulnerabilities?
  - 不要將敏感的資料放在根目錄下面給人家拿
  - robots.txt 檔中的資訊需要好好的保護
    - 做完善的加密
    - 挑選不易被破解的加密方式