Network Security
Project 2 - Web Vulnerability, Frequency Analysis, Hash Collision

Hacking Step

➢ Get robots.txt

http://140.113.194.78:20013/robots.txt
其中可得到以下三個路徑資訊 ：
- ✓ 該網站的資料庫登入頁面 : /phpMyAdmin_NS_pRojEct_2017/
- ✓ 該網站的原始碼 : /backup.tar.gz
- ✓ 無法瀏覽的檔案 : /blog/memorandum.txt

➢ Try to find temporary files

鑑於第一步中的 memorandum.txt 有些可疑，嘗試尋找它的 temporary file, vim 編輯器在編輯某個檔案後，會在當前目錄下產生一個 .[filename].[ext].swp 的暫存檔案，因此利用連結 ：
http://140.113.194.78:20013/blog/.memorandum.txt.swp
即可下載到一個暫存檔

➢ Decoding using base64

使用指令: base64 –D –i memorandum.txt.swp –o after.txt (On MacOS)

➢ Using XOR cracker

使用線上工具: https://wiremask.eu/tools/xor-cracker/

「Based on knowledge of most frequent char and using frequency analysis it will be able to guess the key used to encrypt the data」
取得 Key 的同時也會輸出解碼完後的明文，在明文中即可得到 Database 的登入帳號密碼，進入後可得到加密文章密碼的 Hash 值.

➢ Crack the hash

由原始碼中檔案 functions.php 中可得知，其使用的 hash 方法為 MySQL323，因此使用線上工具 Tobtu MySQL323 Collider : https://www.tobtu.com/mysql323.php 來進行 Hash Collision 破解

```
C:\Users\liwei\Desktop\MySQL323 Collider>"mysql323 collider 32.exe" -h 606f7c8c50cce482 -m 1024 -t 4
Initializing...
Took 22.32 sec
1.573 Pp/s [21.2% 20.6% 28.6% 29.7%] 7%]
606f7c8c50cce482:214d6f3c576e4a56483e304046:!Mo<WnJVH>0@F

Crack time:    2232.983 seconds
Average speed: 140.3 Tp/s
```

將產生 Collision 的 Hash 原碼: !Mo<WnJVH>0@F 當成該文章密碼輸入，即可得到 Girl friend picture .

➢ Result

What have I learned ?

- 關於 robots.txt 的用途
  - Wiki – robots.txt : https://zh.wikipedia.org/wiki/Robots.txt
- Vim 編輯器的暫存檔 .swp
- 知道了幾個 Hash cracking 的工具
  - TobTu
  - Hashcat

How to prevent or patch these vulnerabilities ?

- 使用 robots.txt 時，不要提及一些機敏的路徑
- 避免使用一些容易遭破解的加密方法
  - XOR encryption
  - MySQL323
- Deploy 前清除不必要的暫存檔案
  - 使用 command : ls -al 來檢查是否還有些不必要暫存檔