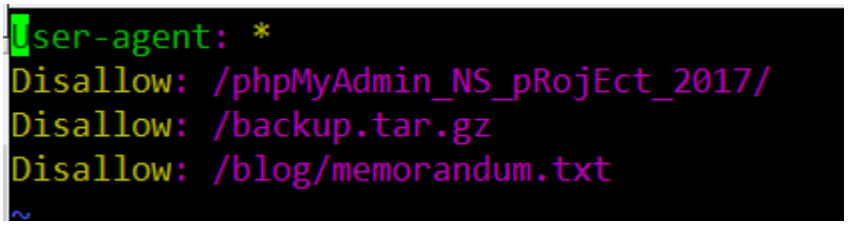
Network Security Project 2

0653410 黃伯靜

1. Finding robot.txt

利用指令

wget --mirror -p --convert-links -P ./bob http://140.113.194.66:20013/blog/
找到 robot.txt，裡面有以下內容



參考

https://www.gnu.org/software/wget/manual/html_node/Advanced-Usage.html#Advanced-Usage

沒有密碼無法進入後台管理網頁
http://140.113.194.66:20013/phpMyAdmin_NS_pRojEct_2017/

輸入 http://140.113.194.66:20013/backup.tar.gz 下載壓縮檔，裡面有一個 php 的檔案

輸入 http://140.113.194.66:20013/blog/memorandum.txt　但是沒辦法打開

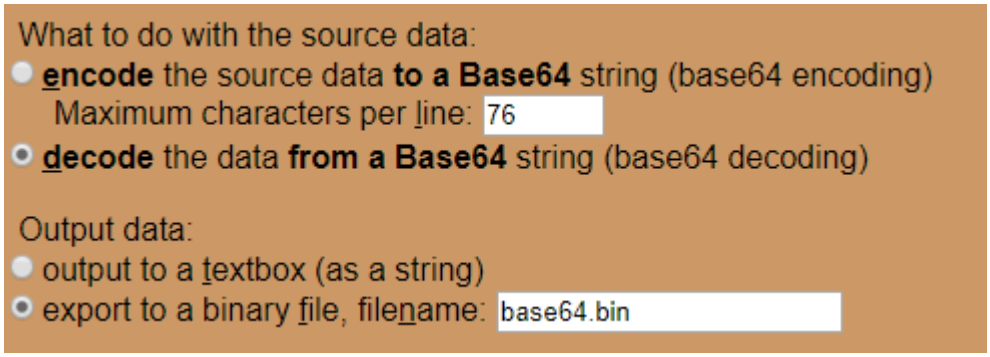
2. Getting memorandum.txt

沒辦法得到 memorandum.txt,但是可以得到以下這個檔案
http://140.113.194.66:20013/blog/.memorandum.txt.swp
可以看到被加密的內容

3. Decode memorandum.txt using base64 decoding online tool

利用此網站

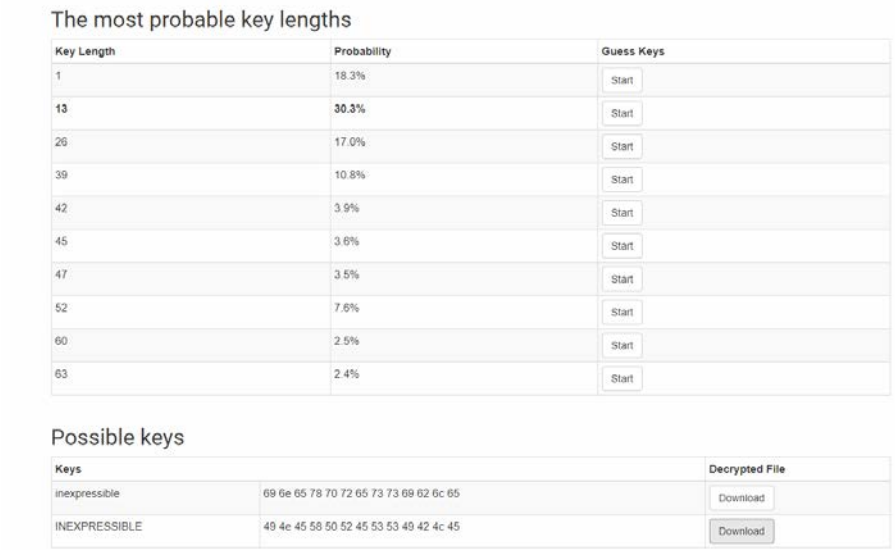
https://www.motobit.com/util/base64-decoder-encoder.asp
並選擇



去解密

4. Using Online XOR cracker tool

利用 https://wiremask.eu/tools/xor-cracker/ 並選擇有 30.3%機率去得到 key 為 introspectionuplandstellers

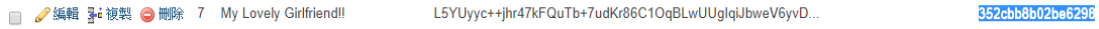


下載解密檔案，裡面有以下訊息.

2016.01.13
phpMyAdmin Account & Password
Account: BobIsGod
Password: introspectionuplandstellers

5. Go to PHPMyAdmin to see the contents inside

利用上步驟得到的帳號密碼去登入，但是只看的到 hash 過後的密碼



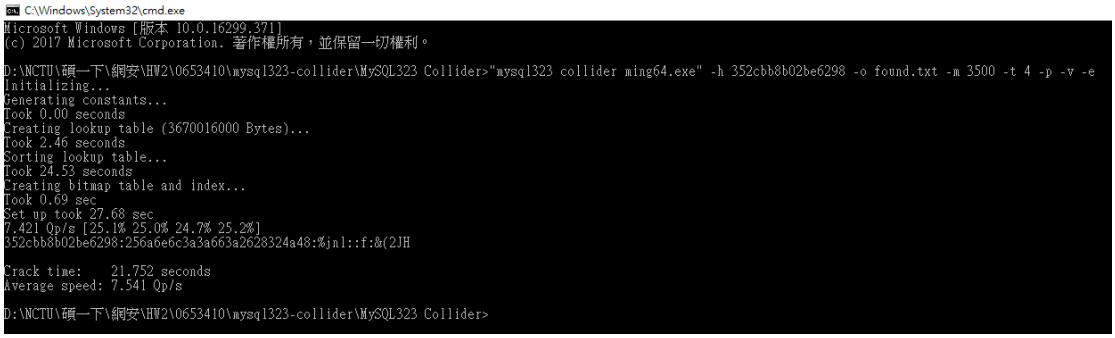
6. Download Hash cracker tool to get the possible unhashed password

利用以下工具

MySQL323 Collider Source 1.1

在 cmd 下以下指令

"mysql323 collider ming64.exe" -h 352cbb8b02be6298 -o found.txt -m 3500 -t 4 -p -v –e



得到密碼為%jnl::f:&(2JH

得到以下圖片

7. 在這個作業中我學到很多關於如何駭進 BOB blog 的方法以及很多有助於破解的工具。也許我們可以利用破解的過程，反過來幫助我們在架設一個網頁的安全方面，千萬不要留重要的訊息在 robot.txt 裡面。還要記得刪掉 temporally 檔案。