# Project 1

賴文揚 0316025

# robots.txt

- 從這個檔案中擷取到，這個Domain不想讓search engine preview的文件。
  - /backup.tar.gz
    - 可download，內容為網站php原始碼
    - Found password hash function is mysql323
  - /phpMyAdmin_NS_pRojEct_2017
    - Entering /phpMyAdmin_NS_pRojEct_2017/index.php
  - /blog/memorandum.txt
    - 404 NOT FOUND
    - But find out “.memorandum.txt.swp” vim temp file

# PHP source code

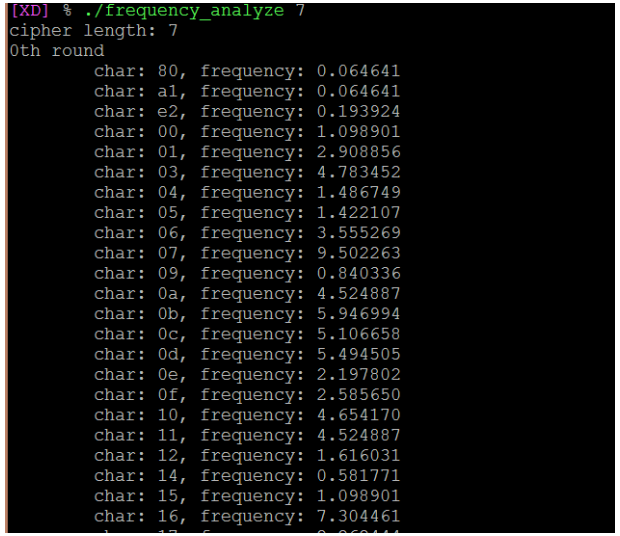
- Get a lot of source code
  - functions.php (Most important)
    - Get hash function information (using mysql323)
  - index.php
  - show.php
  - views(folder)
    - Index.php
    - Show.php
    - element (folder)
      - Css and js files
  - …etc

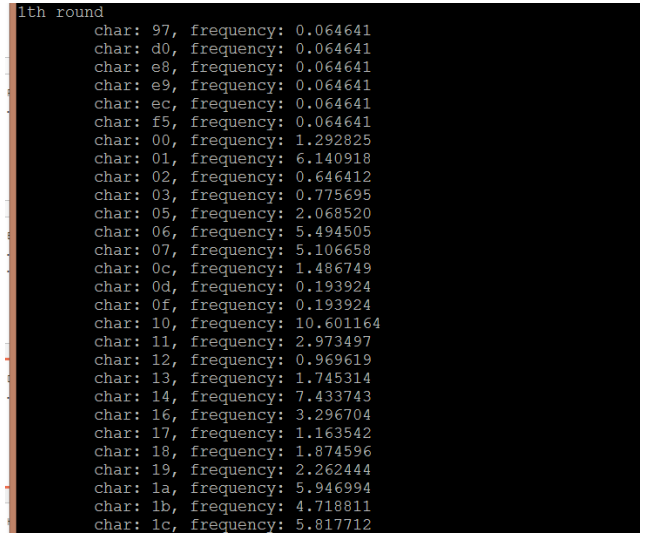
# Base64 Online Decoder

- We can simply use frequency analysis to know “.memorandum.txt.swp” is using Base64 encode
- Using Online tool to recover it!
  - https://www.base64decode.org/

# Decryption the .memorandum.txt.swp

- Guess it is using xor encryption
  - Using my own tool by command
  - $ ./frequency_analyze num
    - “num” indicate the length of password using in xor ecryption
  - And We can get the results when typing num equal to 7



# Decryption the .memorandum.txt.swp (Cont.)

- First I determined the most high frequency character is ‘e’, but it’s not true.
- Second, try the second high frequency character is ‘e’, and decrypt it successfully.
- The using tool is programmed by my self
  - $ ./decypt_xor

# Get Hash Key

- There is myphpadmin login account and password. Log in to the phpmyadmin page get the hashed password value.

# Hash Collision

- Using the mysql323 hash collider
  - From: https://tobtu.com/mysql323.php with command below
  - $ "mysql323 collider 32.exe" -h 3455b9824a3ac89b -m 1024 –t 4
- It cost around 1min.
  - Get the string ”!xYV@Vp0Bn>(p” collide with “3455b9824a3ac89b”

# Get target!

# Summary – What I Learned

- Robots.txt
  - 在這次作業以前，並不曉得在web上有這種機制去避免預覽網頁內容的方法，在這次作業中不但認識了這個機制，並了解了要使用這個機制必須避免一些問題的產生。
- Base64
  - 這種編碼方式，能夠使得一些unprintable character以其他字元表示出來，似乎在WEB中受到廣泛的使用，

# Summary – What I Learned

- Xor encryption decryption
  - 只要藉由去假設password length，當在英文語系下，資料樣本夠大的時候就可以藉由frequency analyze去破解此密碼。
- MySQL323 hash function
  - 由於此function前8byte output與後8byte的output，沒有任何的相依性，以及其簡易的運算導致此hash function unsafe，能夠網路上可以查詢到一些工具使得此hash function能夠簡單的被破解。

# Summary – How to prevent the vulnerability in Bob's blog

1. 不要將backup file 放在 public web server的 document root 底下.
   - 等同將自己的source code open至網路上。
2. 記得移除所有的tmp file，在linux上每次檢查時可以執行 ls –al 以及 grep 搭配 regular expression 的方式確認是否有未刪除乾淨的 tmp file.
3. 不要使用容易遭到破解的加密方式
   1. Xor encryption
   2. Mysql323 hash