

# 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

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

參考

[https://www.gnu.org/software/wget/manual/html\\_node/Advanced-Usage.html#Advanced-Usage](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/](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

What to do with the source data:

- ☐ **encode** the source data to a **Base64** string (base64 encoding)  
Maximum characters per line:
- ☒ **decode** the data from a **Base64** string (base64 decoding)

Output data:

- ☐ output to a textbox (as a string)
- ☒ export to a binary file, filename:

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**

The most probable key lengths

Key Length	Probability	Guess Keys
1	18.3%	<input type="button" value="Start"/>
13	30.3%	<input type="button" value="Start"/>
26	17.0%	<input type="button" value="Start"/>
39	10.8%	<input type="button" value="Start"/>
42	3.9%	<input type="button" value="Start"/>
45	3.6%	<input type="button" value="Start"/>
47	3.5%	<input type="button" value="Start"/>
52	7.6%	<input type="button" value="Start"/>
60	2.5%	<input type="button" value="Start"/>
63	2.4%	<input type="button" value="Start"/>

Possible keys

Keys	Decrypted File
inexpressible 69 6e 65 78 70 72 65 73 73 69 62 6c 65	<input type="button" value="Download"/>
INEXPRESSIBLE 49 4e 45 58 50 52 45 53 53 49 42 4c 45	<input type="button" value="Download"/>

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

編輯 複製 刪除 7 My Lovely Girlfriend!! L5YUyyc+Jhr47kFQuTb+7udKr86C1OqBLwUUglqJbweV6yvD... 352cbb8b02be6298

## 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**

```
C:\Windows\System32\cmd.exe
Microsoft Windows [版本 10.0.16299.371]
(c) 2017 Microsoft Corporation. 著作權所有，並保留一切權利。
D:\NCTUA\碩一下\網安\HW2\0653410\mysql323-collider\MySQL323 Collider>mysql323 collider ming64.exe" -h 352cbb8b02be6298 -o found.txt -m 3500 -t 4 -p -v -e
Initializing...
Generating constants...
Took 0.00 seconds
Creating lookup table (3670016000 Bytes)...
Took 2.46 seconds
Sorting lookup table...
Took 24.53 seconds
Creating bitmap table and index...
Took 0.69 sec
Set up took 27.68 sec
7.421 Qp/s (25.1% 25.0% 24.7% 25.2%)
352cbb8b02be6298:250a0e6c3a3a063a2628324a48:%jnl:f:&(2JH
Crack time: 21.752 seconds
Average speed: 7.541 Qp/s
D:\NCTUA\碩一下\網安\HW2\0653410\mysql323-collider\MySQL323 Collider>
```

得到密碼為**%jnl:f:&(2JH**

得到以下圖片

My Lovely Girlfriend!!

This is my lovely girlfriend(This is the answer for project1! Congraz!):



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。