Project 2. Web Vulnerability

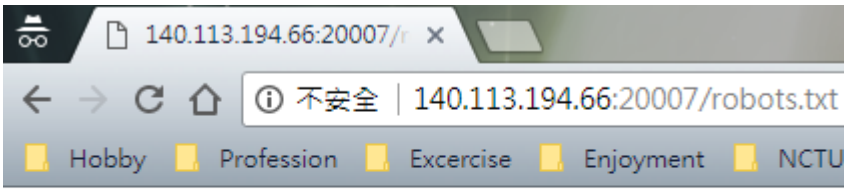
Name: 吳冠霆 Student ID: 0556503

Hacking Steps

0. Bob's blog at http://140.113.194.66:20007/blog/

1. robots.txt

   From http://140.113.194.66:20007/robots.txt, we can get location of Bob's phpMyAdmin, php code of Bob's blog and memo.




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

2. temporary files

   Since http://140.113.194.66:20007/blog/memorandum.txt is not available, we try the format of **vim editor temporary file** http://140.113.194.66:20007/blog/.memorandum.txt.swp instead and finally get information leakage downloaded.

3. base64 encoding

   cat memorandum.txt.swp | base64 -d > memorandum_base64_decode_result
   Eliminate the first line of memorandum.txt.swp, use Linux command base64 to decode it and pipe output to memorandum_base64_decode_result.

4. XOR encoding & frequency analysis

   Online tool: XOR Cracker
   URL: https://wiremask.eu/tools/xor-cracker/

we use this to decrypt memorandum_base64_decode_result. This online tool uses frequency analysis to guess the key used for encrypting the data.

The most probable key lengths

Key Length	Probability	Guess Keys
2	9.3%	Start
4	14.3%	Start
6	8.0%	Start
8	**18.0%**	Start
10	6.8%	Start
12	9.7%	Start
16	12.2%	Start
20	6.9%	Start
24	8.5%	Start
32	6.3%	Start

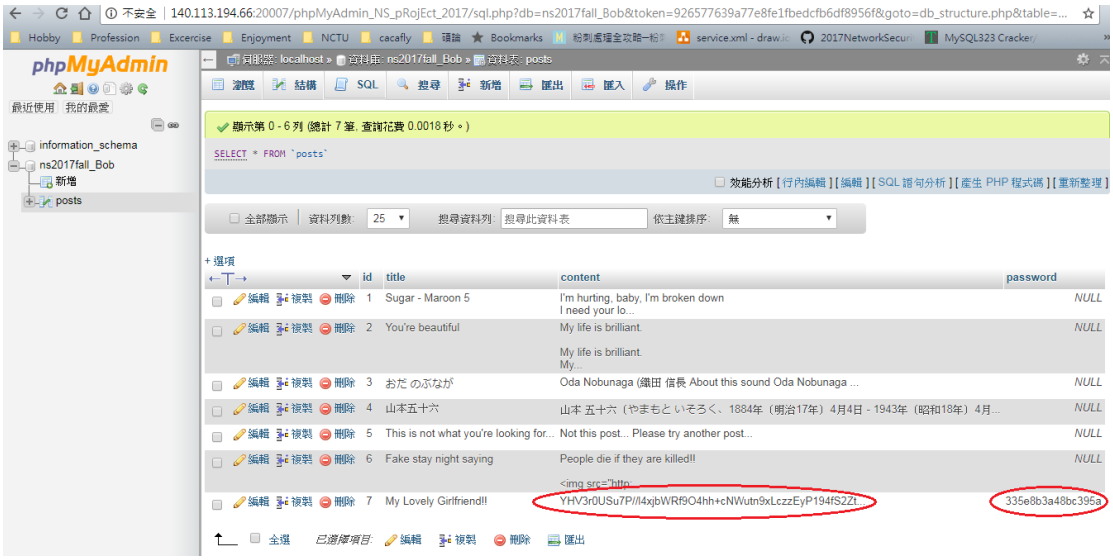
Possible keys

Keys		Decrypted File
fairways	66 61 69 72 77 61 79 73	Download
FAIRWAYS	46 41 49 52 57 41 59 53	Download

From downloading the decrypted file(XOR result of ciphertext), we get the account(BobIsGod) and password(delineatedAelfricpresupposes) to Bob's phpMyAdmin.

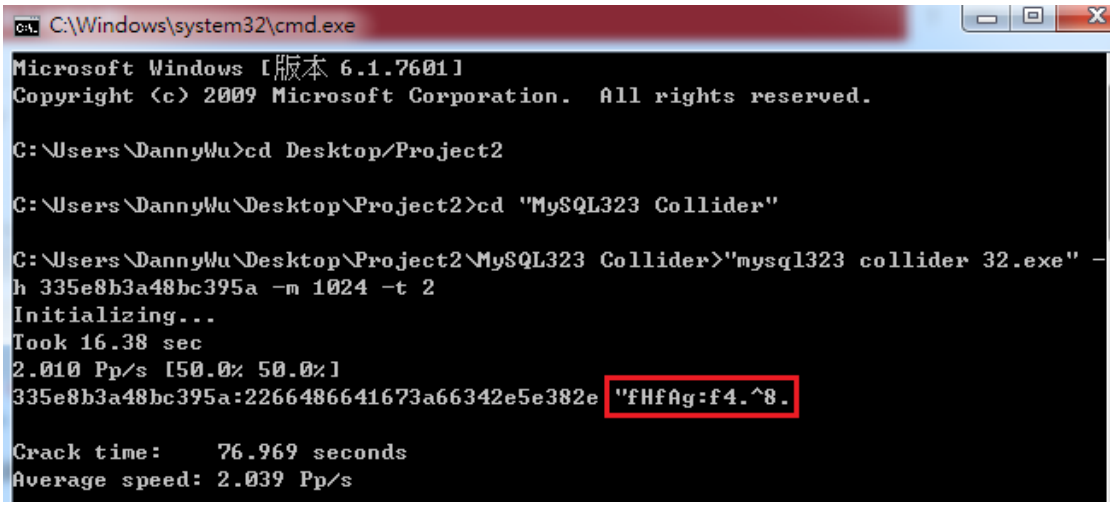
5. hash collision

Tool: MySQL323 Collider
URL: https://tobtu.com/mysql323.php
Then, we can get the encrypted content and hashed password of the post "My Lovely Girlfriend!!".

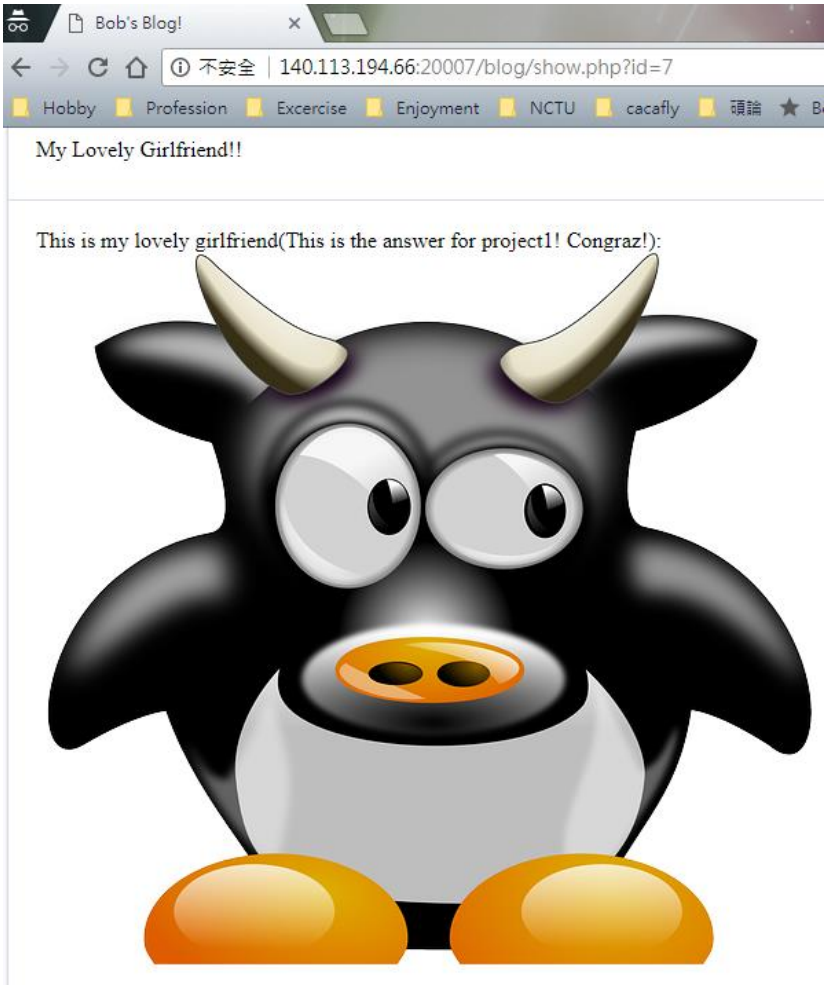


We find out **my_own_hash** in functions.php implements mysql323 hash algorithm, so we end up using MySQL323 Collider.

“fHfAg:f4.^8. is the password we want.



The result of “My Lovely Girlfriend!!”



- **What I Have Learned**

1. Meaning of robots.txt
2. How to access temporary files
3. How frequency analysis works and how to use it for decrypting data
4. Mysql323 hash algorithm and how to break it

- **How to Prevent these Vulnerabilities**

1. Don’t put important information in robots.txt since it can only prevent web crawlers from accessing these important files. Edit .htaccess to make sure important files can’t be accessed.
2. Make sure to clean all of your temporary files.
3. Keep the hash and encryption algorithm you used in secure, or it would be easy to break it since there are plenty of tools can be used for cracking it.