Network Security
project2 : Web Vulnerability
林俊翰 0646001

1. The steps and details of hacking.
   <i> First, go to find the port for this project:
   http://140.113.194.78:20084/blog/
   <ii>follow the hints, try the robots.txt .
   http://140.113.194.78:20084/robots.txt

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

   <ii-a> **phpMyAdmin_NS_pRojEct_2017** is the database that Bob used to manage data for his blog. If I can find the username and password , then I can hack the data.
   <ii-b>backup.tar.gz ,I get the source code of Bob's blog. I discover the way Bob used for encrypting and decrypting data in the "function.php", and here is also telling Bob's hashing mechanism.

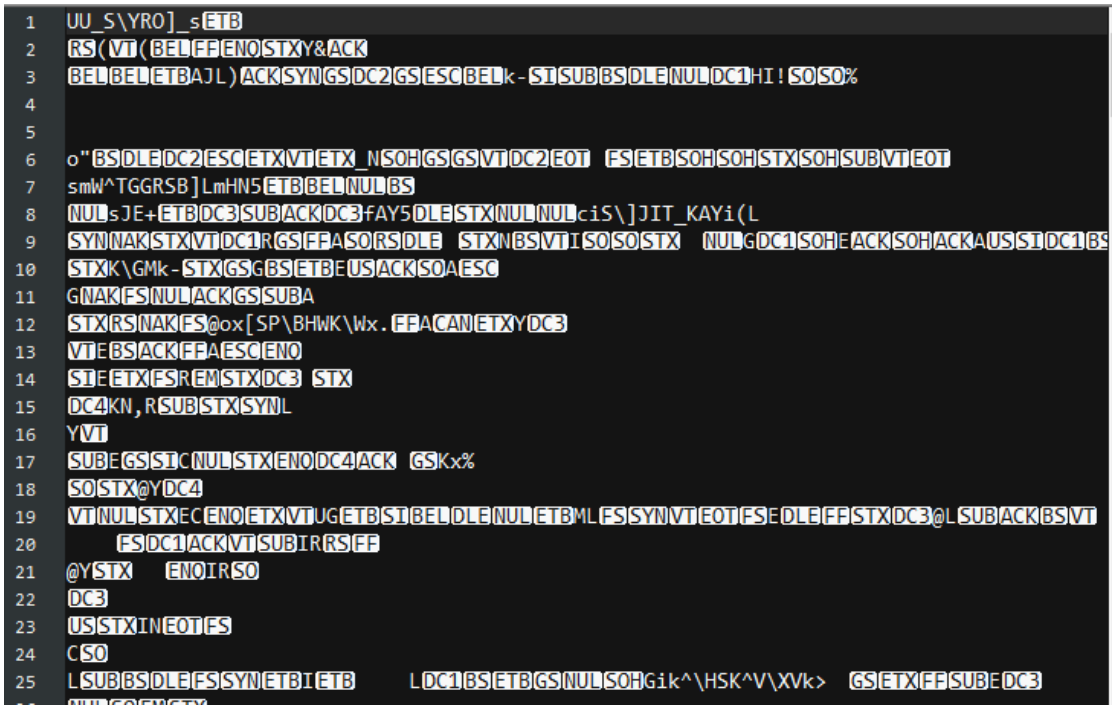

```php
function my_own_hash($input)
{
  $magic1 = 1345345333;
  $magic2 = 0x12345671;
  $sum = 7;  $tmp = null;
  $len = strlen($input);
  for ($i = 0; $i < $len; $i++) {
    $byte = substr($input, $i, 1);
    if ($byte == ' ' || $byte == "\t")
        continue;
    $tmp = ord($byte);
    $magic1 ^= ((($magic1 & 63) + $sum) * $tmp) + (($magic1 << 8) & 0xFFFFFFFF);
    $magic2 += (($magic2 << 8) & 0xFFFFFFFF) ^ $magic1;
    $sum += $tmp;
  }
  $out_a = $magic1 & ((1 << 31) - 1);
  $out_b = $magic2 & ((1 << 31) - 1);
  $output = sprintf("%08x%08x", $out_a, $out_b);
  return $output;
}
```

```php
function encrypt_content($content) {
  require 'config.php';

  $cipher = 'aes-256-cbc';
  $ivSize  = openssl_cipher_iv_length($cipher);
  $ivData  = openssl_random_pseudo_bytes($ivSize);

  $encripted = openssl_encrypt($content,
                               $cipher,
                               $blog_config['encrypt_key'],
                               OPENSSL_RAW_DATA,
                               $ivData);

  return base64_encode($ivData . $encripted);
}
```

<ii-c> /blog/memorandum.txt is 404 Not Found. In the hints, there may be temporary file I can get . I try this: …/blog/.memorandum.txt.swp, the browser access the Bob's temporary file!! That so lucky!! Then open it:

```
1  This is not a real vim swp file, please do not try to recover it. Actually, Bob u
2
3  VVVfU1xZUk9dX3MXDR4oCygHDAUCWSYGDQoHBxdBSkwpBhYdEh0bB2stDxoIEAARSEkhDg4lCiAK
4  Cm8iCBASGwMLA19OAR0dCxIECRwXAQECARoLBA0Kc21XX1RHR1JTQ11MbUhONRcHAAgNAHNKRSsX
5  ExoGE2ZBWTUQAgAAY21TXF1KSVRfS0FZaShMChYVAgsRUh0MQQ4eEAkCTggLSQ4OAgkARxEBRQYB
6  BkEfDxEICgJLXEdNay0CHUcIF0UfBg5BGw0KRxUcAAYdGkENAh4VHEBveFtTUFxCSFdLXFd4LgxB
7  GANZEw0LRQgGDEEbBQ0PRQMcUhkCEwkCDRRLTixSGgIWTA1ZCwoaRR0PQwACBRQGCR1LeCUKDgJA
8  WRQNCwACRUMFAwtVRxcPBxAAF01MHBYLBBxFEAwCE0BMGgYICwleSQYNCRwRBgsaSVIeDA0KQFkC
9  CQVJUg4KEw0KHwJJTgQcDUMOCkwaCBAcFhdJFwkJTBEIFx0AAUdpa15cSFNLXlZcWFZrPgkdAwwa
10 RRMKAA4ZAg1dRV5SSlFbU11eTVdvPAAWDQoVTBwYFBYZCgANWUEFDRQGFgMEAB0BDhVmc1VVXl1c
11 WVVPXFpzLkUZABwdQxUDTBQeRQkXEwcHEQ0eHAkRHUJSAQwMCUJzMw0LHFILDBQLBA1HCAtFE0kP
12 DhhMFgFFDQQcDQoEH0JzbVdeVEVHU1BCXEhtJCs2UgANFR4DHRIGGgwdB2k1BAlZJgEYBBwKBgVM
```

<iii-a>Because the "encrypt_content" function in "function.php" show the encode process , and the last step is base64_encode . I used the notepad++ plugin -> MIME Tools -> base64 decode.



<iii-b>I try the every encryption in hints, I find it. I used the web tool https://wiremask.eu/tools/xor-cracker/ .

The most probable key lengths

Key Length	Probability	Guess Keys
1	13.6%	Start
11	**28.1%**	Start
15	7.6%	Start
22	16.9%	Start
30	4.3%	Start
33	11.1%	Start
44	7.9%	Start
48	2.6%	Start
55	5.9%	Start
59	2.0%	Start

Possible keys

Keys		Decrypted File
generically	67 65 6e 65 72 69 63 61 6c 6c 79	Download
GENERICALLY	47 45 4e 45 52 49 43 41 4c 4c 59	Download

I downloaded the two possible keys.

```
2016.01.13
phpMyAdmin Account & Password
Account: BobIsGod
Password: dothsheepdogssheaf

2015.12.15
- Pencial
- Eraser
- Ruler

2013.11.30
I forget to bring my money to the school....
And my mom was pretty angry.

2010.10.22
Go to the zoo with my parents. I saw a lot of animals.
Lion, sheep, dog, rabbit, polar bear, camel, elephant, wolf, elk, giraffe, and of cou

2014.03.15
Reddit account: 0788831240
Reddit password: iamasmartboy

2008.06.06
I went to my grandparents' home.
They bought me a lot of candies.
```

Lucky! There is the phpMyAdmin's account and password.

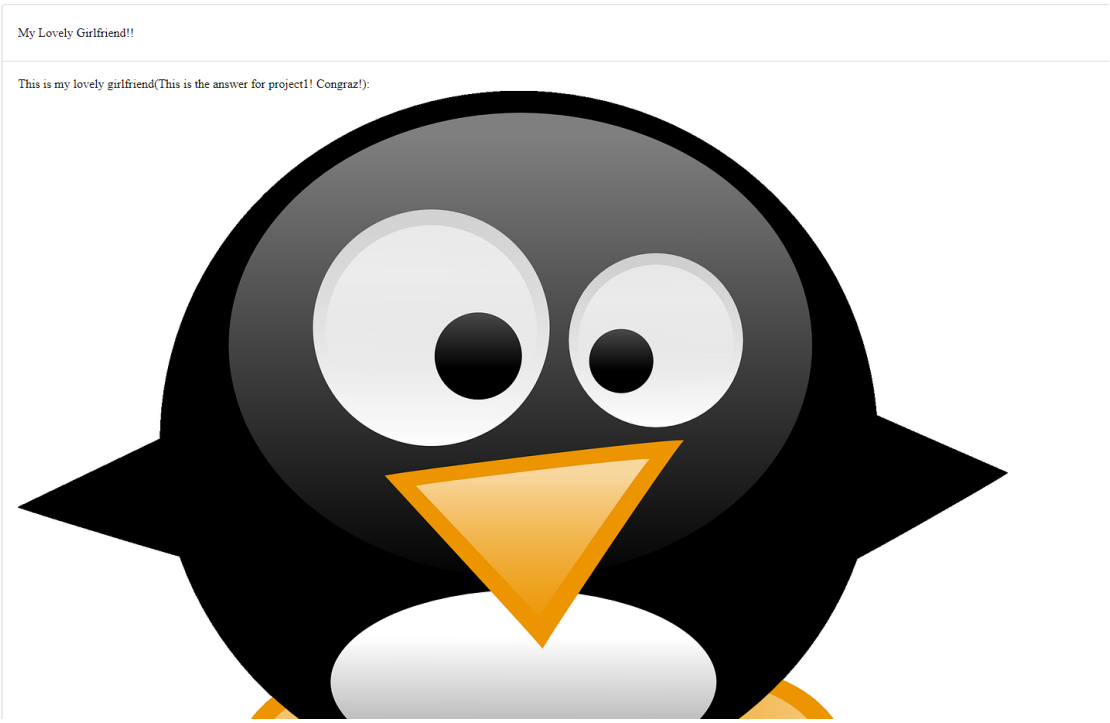
<iv>

	id	title	content	password
編輯 複製 刪除	1	Sugar - Maroon 5	I'm hurting, baby, I'm broken down I need your lo...	NULL
編輯 複製 刪除	2	You're beautiful	My life is brilliant. My life is brilliant. My...	NULL
編輯 複製 刪除	3	おだ のぶなが	Oda Nobunaga (織田 信長 About this sound Oda Nobunaga ...	NULL
編輯 複製 刪除	4	山本五十六	山本 五十六（やまもと いそろく、1884年（明治17年）4月4日 - 1943年（昭和18年）4月...	NULL
編輯 複製 刪除	5	This is not what you're looking for...	Not this post... Please try another post...	NULL
編輯 複製 刪除	6	Fake stay night saying	People die if they are killed!! <img src="http:...	NULL
編輯 複製 刪除	7	My Lovely Girlfriend!!	ONNlFmWxvLsqfMuRz/Se9toh+CMngmaJjeMNYT1synFr1lyFTp...	6929a5ae06638f0b

I logged in the database, I can see the password for Bob's Girlfriend. But the password is still wrong. I realize that Bob used the hash encryption to encrypt the password again. I google the "my_own_hash" function. It is "Old MySQL Password Hash Function" which is implemented by MySQL ver.323. After knowing that, I just need to find the tool to crack it. The web https://tobtu.com/mysql323 .php provide the convenient tool to download, then I use it to start cracking.

```
C:\Users\pcslab>"D:\Downloads\MySQL323 Collider\mysql323.exe" -t 8 -m 1000 -h 6929a5ae06638f0b
Initializing...
Took 10.99 sec
5.047 Pp/s [12.0% 12.9% 13.1% 12.1% 12.0% 12.9% 13.1% 11.8%]
6929a5ae06638f0b:2225376e7e747c2426243c465836:"%7n~t|$&$<FX6
```

Final! The password is **"%7n~t|$&$<FX6** .



2. What have you learned?
   In this project, I have learn the basic security technics. For example: use the hash function to hash plaintext to prevent hacker easily reading the content, or implement XOR encryption with keys to enhance the security level for the ciphertext, and also have learned about what is “robots.txt” and how it works.

3. How to prevent or patch these vulnerabilities?
   First of all, do not easily show any important information on the “robots.txt”, especially those folders or files you don’t want to show for others, because this can be accessed by anyone. Second, the backup zip file tries not to put them on the place where website can reach, and also if you want to back up the files, they should be compressed with some encryption mechanism. Third, don’t leave any temporary files on the website, especially take care of the tool that you write the code because it may secretly create the hidden file, and that will make the vulnerability for hackers. Forth, choose the system wisely, or try to update the system to the latest version. Because the old system is designed based on the old knowledge, and when times go on, those weakness of system may be discovered, for example: PASSWORD function in MySQL323 (which is used by Bob’s blog) has been decrypted, so keep the system up to date may be helpful.