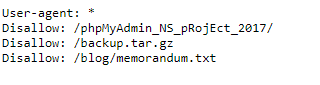
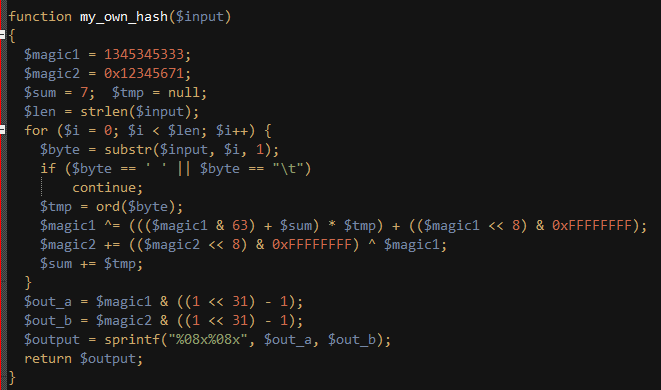
Network Security  
project2 : Web Vulnerability  
林俊翰 0646001

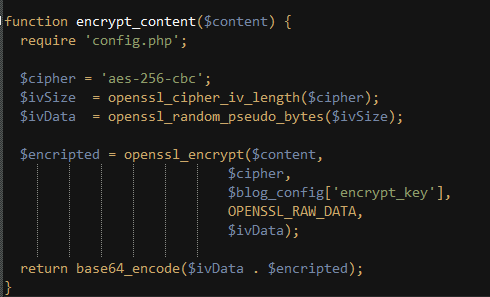
1. The steps and details of hacking.  
   <i> First, go to find the port for this project: <http://140.113.194.78:20084/blog/>

<ii>follow the hints, try the robots.txt . <http://140.113.194.78:20084/robots.txt>



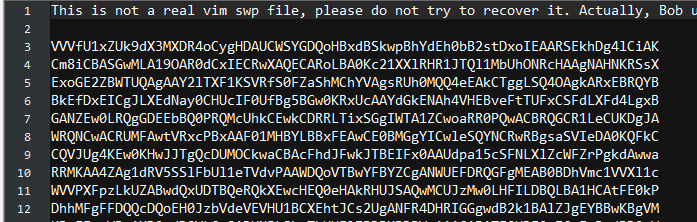
<ii-a> **phpMyAdmin\_NS\_pRojEct\_2017** is the database that Bob used to manage data for his blog. If I can find the username and password , then I can hack the data.

<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.

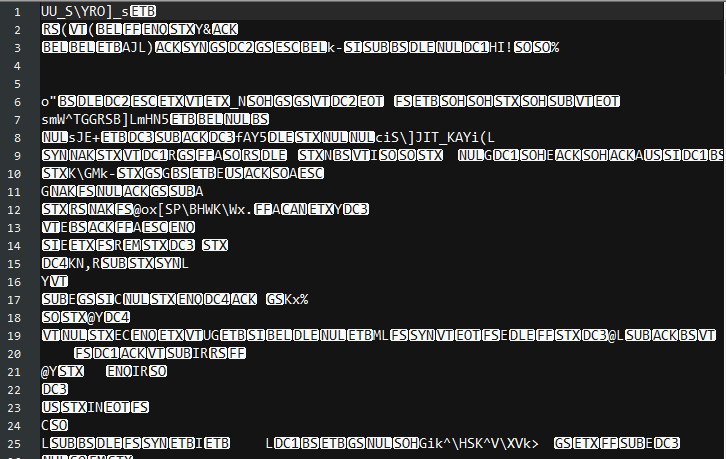


<ii-c> /blog/memorandum.txt is 404 Not Found. In the hints, there may be temporary file I can get . I try this: …/blog/.memorandum.txt.swp, the browser access the Bob’s

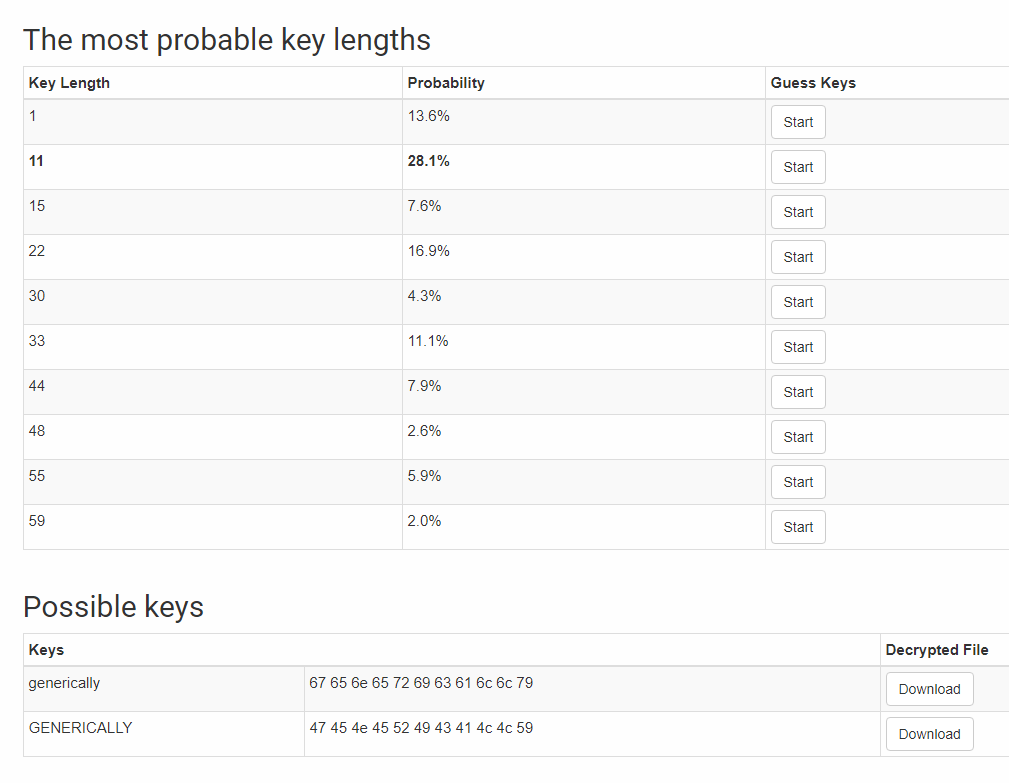
temporary file!! That so lucky!! Then open it:



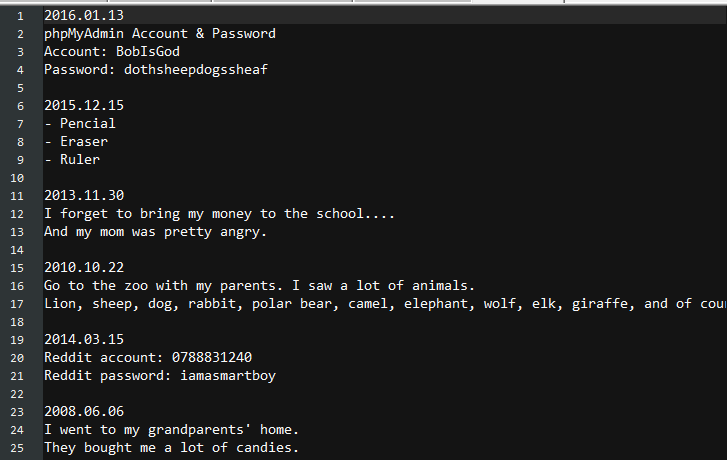
<iii-a>Because the “encrypt\_content” function in “function.php” show the encode process , and the last step is base64\_encode . I used the notepad++ plugin -> MIME Tools -> base64 decode.



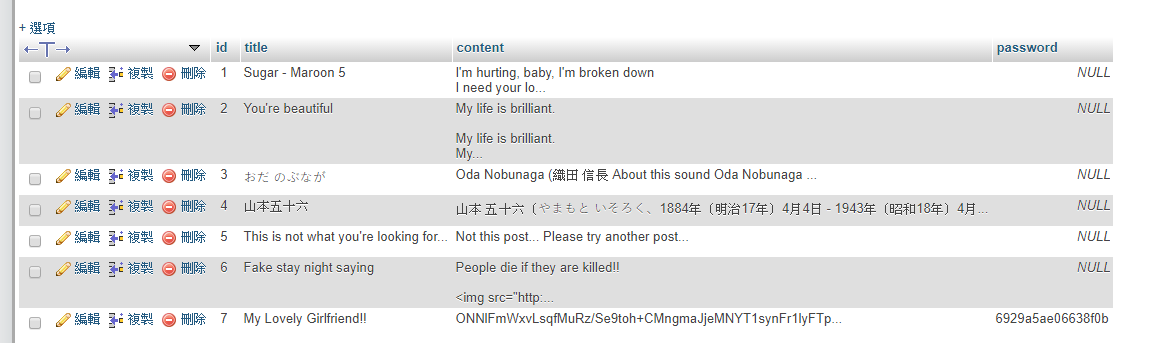
<iii-b>I try the every encryption in hints, I find it. I used the web tool <https://wiremask.eu/tools/xor-cracker/> .



I downloaded the two possible keys.



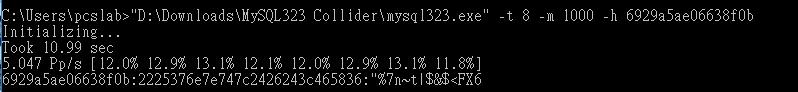
Lucky! There is the phpMyAdmin’s account and password.

<iv> 

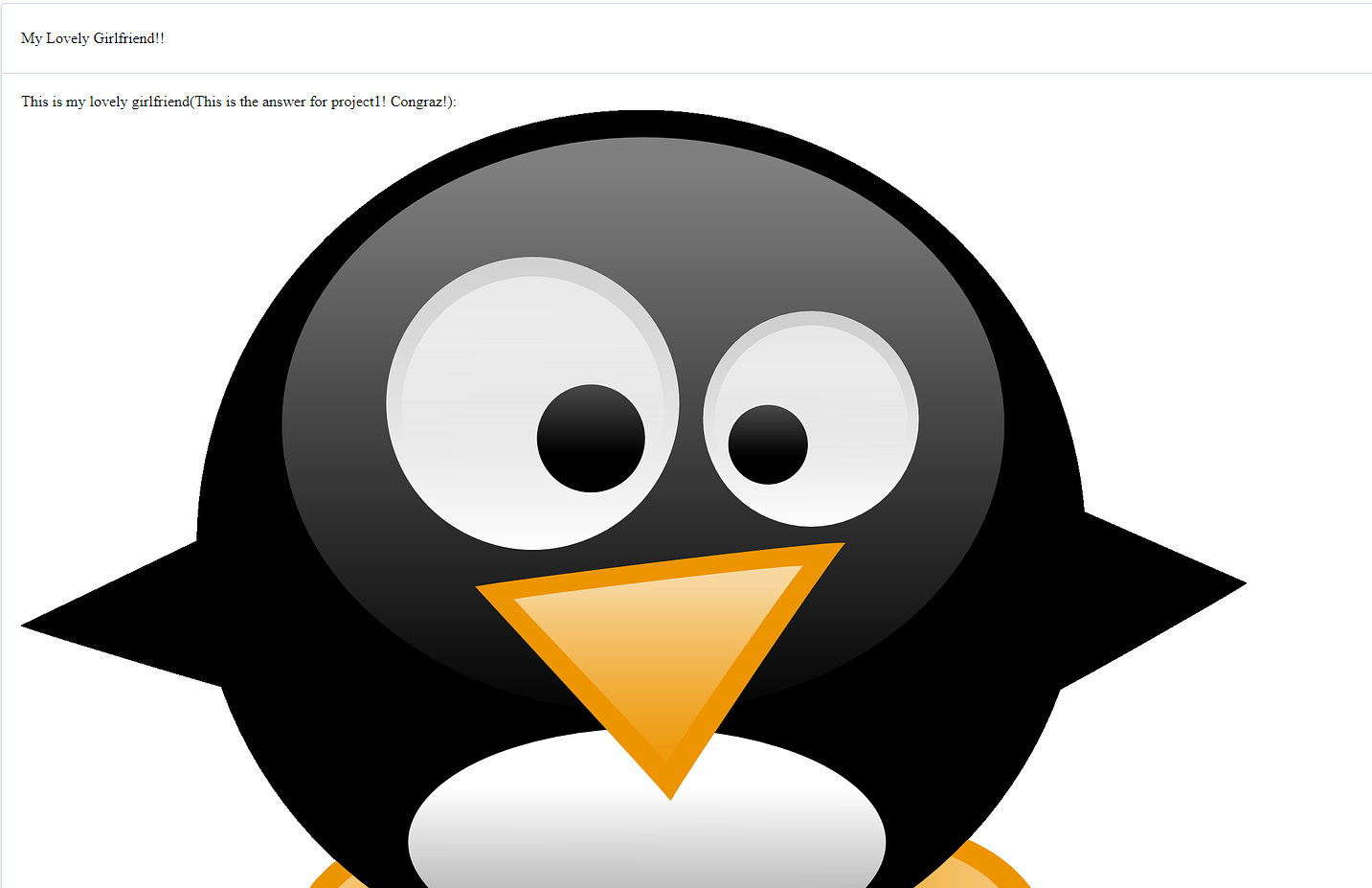
I logged in the database, I can see the password for Bob’s Girlfriend. But the password is still wrong. I realize that Bob used the hash encryption to encrypt the password again. I google the “my\_own\_hash” function. It is “Old MySQL Password Hash Function” which is implemented by MySQL ver.323. After 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.



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



1. 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.

1. 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.