Project 2
Web Vulnerability

Instructor: Shiuhpyng Shieh

TA: Wei-Ti Su & Xin-Yu Wang

Project Goal

- To understand the following topics
  - Web vulnerability
  - Insecure encryption
  - Hash collision

Introduction

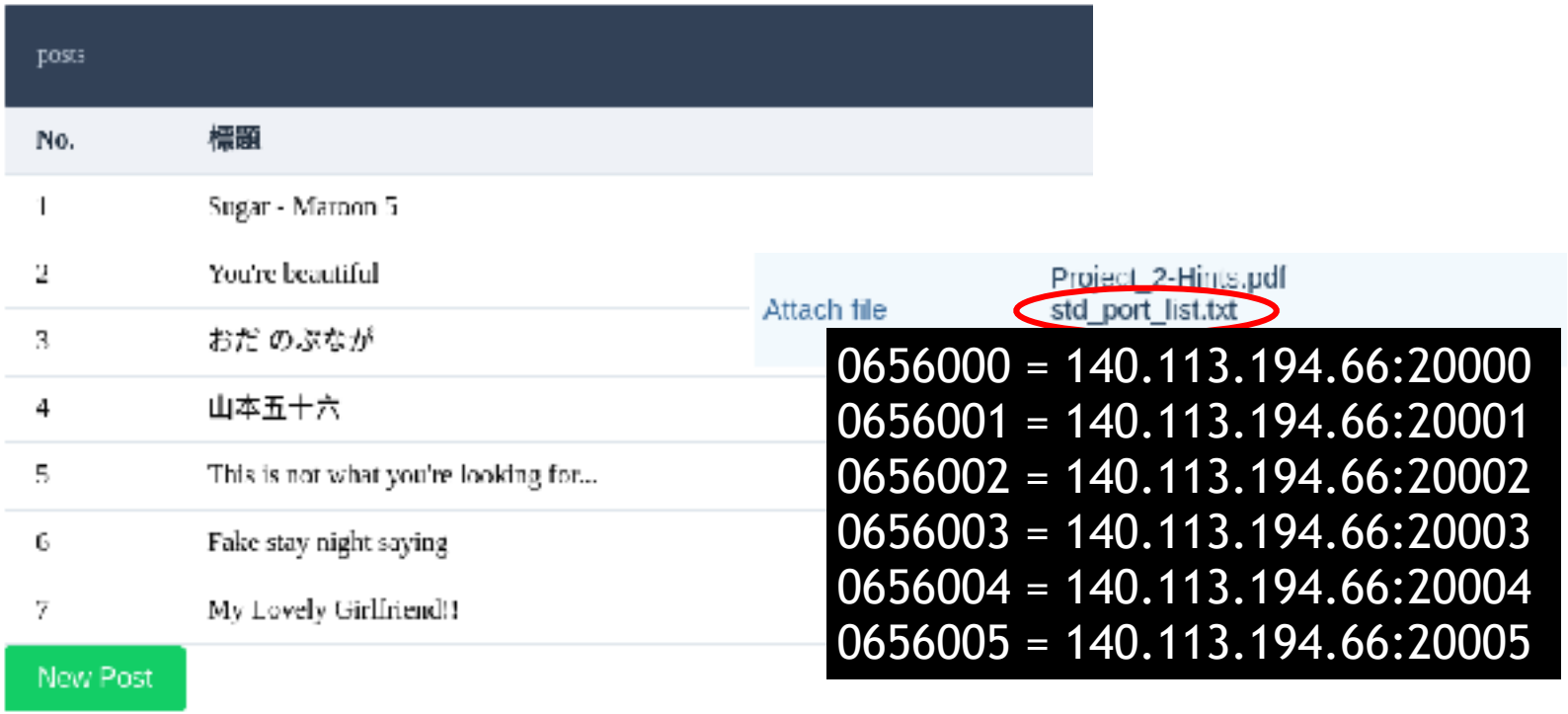
- Bob, whose major is computer science, builds his own blog based on his knowledge.

- Recently, TA found that he had uploaded an intimate picture to his blog.
  But, that picture is in a post protected by the password.

- TA wants to know what is in the picture.
  If you can use the vulnerabilities you find to get the picture and share it with TA, TA would appreciate it.

Introduction (cont.)

- You can access Bob's blog at http://140.113.194.66:xxxxx/blog/.



Related Materials

- PHP
- MySQL
- phpMyAdmin
- Base64 encoding
- Frequency Analysis
- XOR encryption
- Hash collision
- robots.txt
- Temporary files & Git

PHP

- PHP is a server-side scripting language designed primarily for web development.

- Bob builds his own blog with PHP.

MySQL

- MySQL is a famous relational database management system.

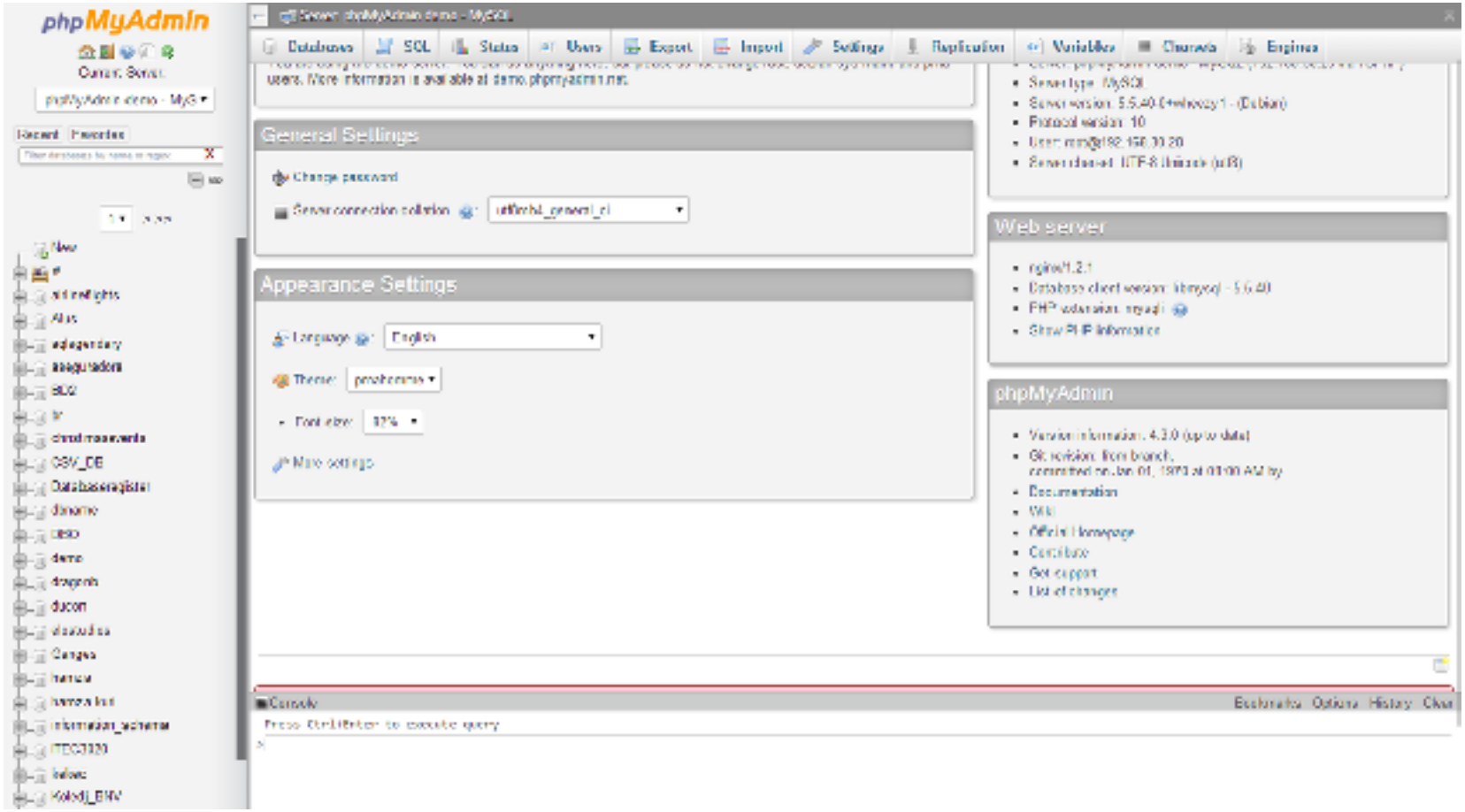
- Bob uses MySQL to store his blog data.

phpMyAdmin

- phpMyAdmin is an administration tool for MySQL.
  It makes the management of database easier for administrators.

- If you find Bob's phpMyAdmin and login successfully, you can browse his blog data.

phpMyAdmin (cont.)



phpMyAdmin screenshot from https://en.wikipedia.org/wiki/PhpMyAdmin

Base64 encoding

- Base64 is a group of similar binary-to-text encoding schemes.

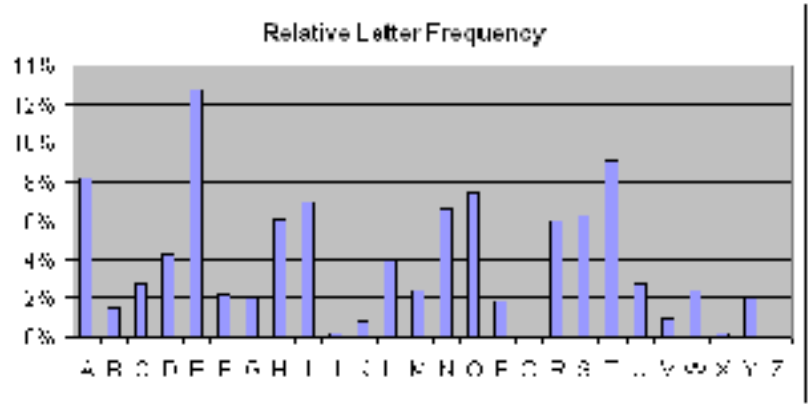
```
$ cat test.txt
[illegible]
```

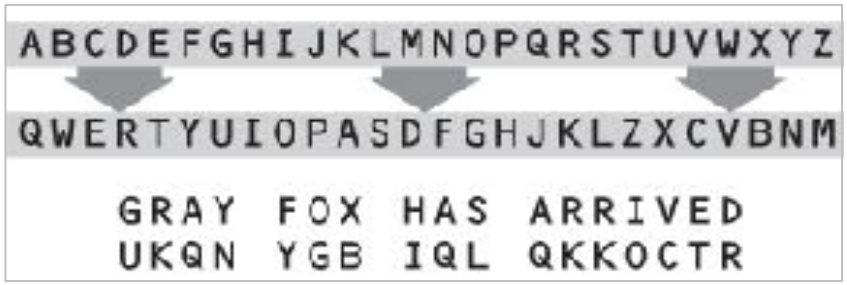
Encoding…

```
$ cat test.txt | base64
H6JQvJ7VEqcxV9daZJ86bycufDCypxEMeMs43dkX0UzIviyD85Qr5GSiDuPbc/Eq2Sx46/iiUtTw
G6FoLKqBeFjhn5JiG9HnpS5CctcJunkhhQ==
```

Frequency Analysis

- Frequency Analysis is a useful technique to break some simple encryption method over certain plaintext (such as English language).



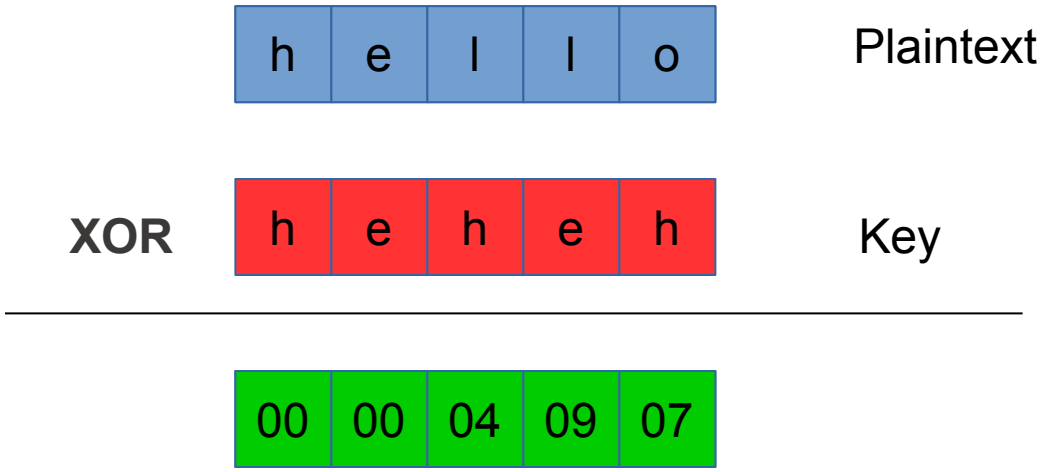


Relative frequency of letters in English from https://en.wikibooks.org/wiki/Cryptography/Frequency_analysis
Substitution cipher from http://www.infosectoday.com/Articles/Intro_to_Cryptography/Introduction_Encryption_Algorithms.htm

XOR encryption

- Get the ciphertext by XORing the plaintext and the key.

- Example



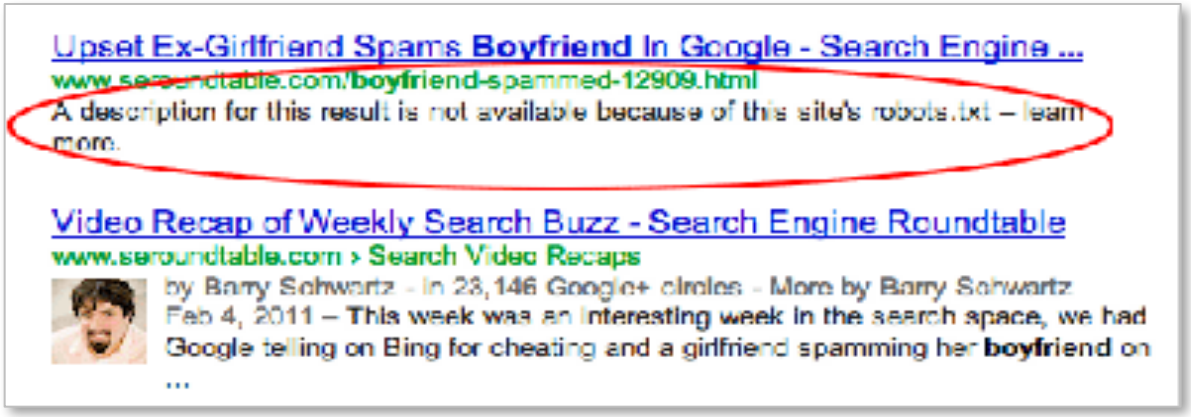
Hash collision

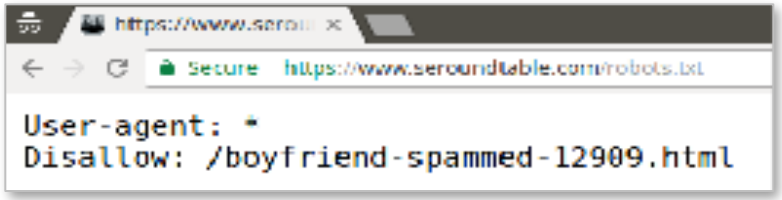
- Given input x, hash function h and h(x)=d.
- If we can find other input y, such that h(y)= h(x)=d.
  It's called hash collision.
- Example

```
1  def my_hash(s):
2      return sum(bytearray(s, 'utf-8')) % 25
3
4  if my_hash('test') == my_hash('heln'):
5      print('Hash collision')
```

robots.txt

- robots.txt is used to inform the web robot about which areas of the website should not be processed or scanned.





robots.txt example from https://www.seroundtable.com/boyfriend-spammed-12909.html

Temporary files & Git

- Some sensitive files may leak a lot of information if you put them on the public web server.

- Examples
  - Git repository folder (.git)
  - Vim editor temporary files (.xxxx.swp)
  - Backup files (xxxx.bak, xxxx.old, etc.)
  - Other temporary files (xxxx.tmp, etc.)

Project Information - Deliverables

- Any source code or program you used in your project. (For online tool, please provide the URL of the online tool.)
- The intimate picture you found after you hack into Bob's blog. (Right click the image and save the original image as a single file. No compression or quality lost is allowed!)
- A report in PDF format:
  - Write down your hacking steps, details, concept, and idea.
  - What have you learned?
  - How to prevent or patch these vulnerabilities?

Project Information (cont.)

1. Compress all the files into a zip file. Use your student ID as file name, for example “0656000.zip”.
2. Upload the zip file to the E3 platform.
3. Well done!!