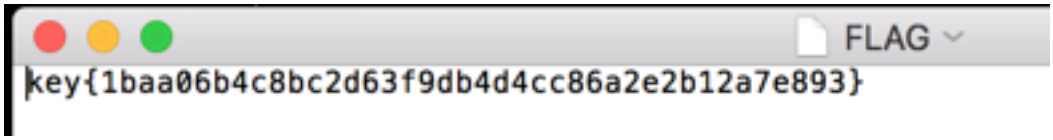
CTF write up for Group 8

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

Challenge 1: Just GET the FLAG. 100 points

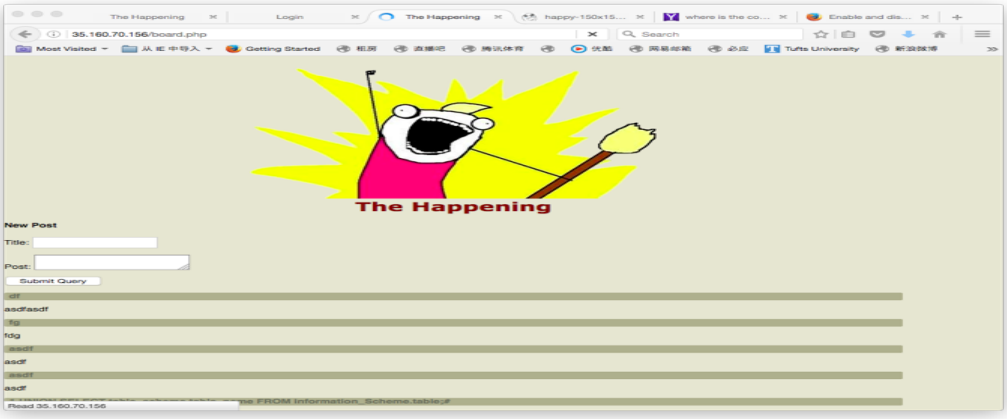
From the Hint, we know we must get the “FLAG”, we tried to enter the url: http://35.160.70.156/FLAG

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

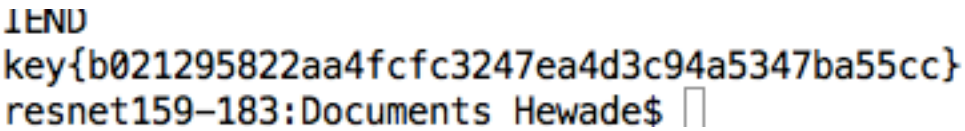


Challenge 2: You are staring right at it. 100 points

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:

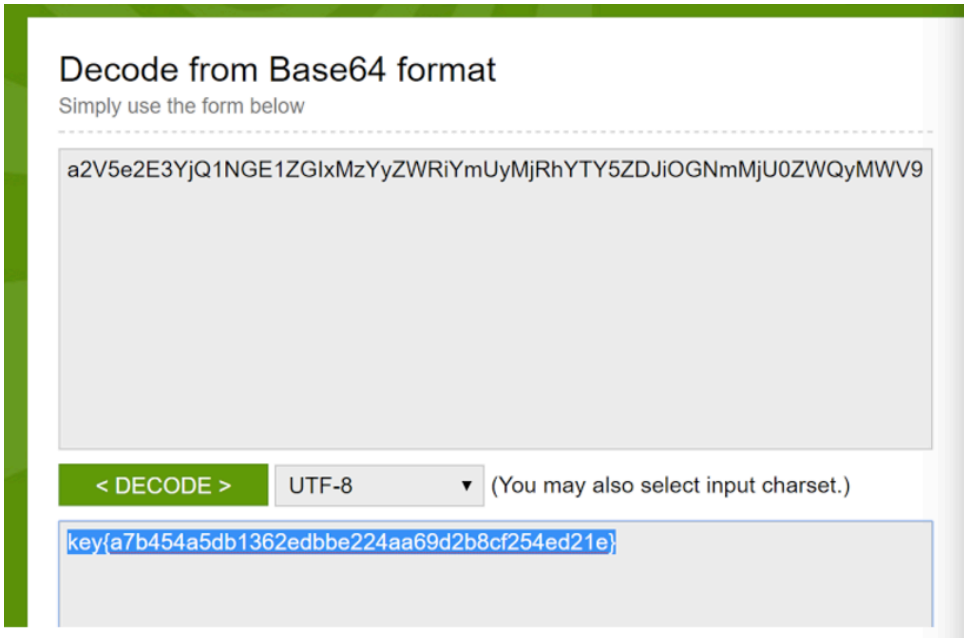


Challenge 3: All your base64 are belong to us. 200 points

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

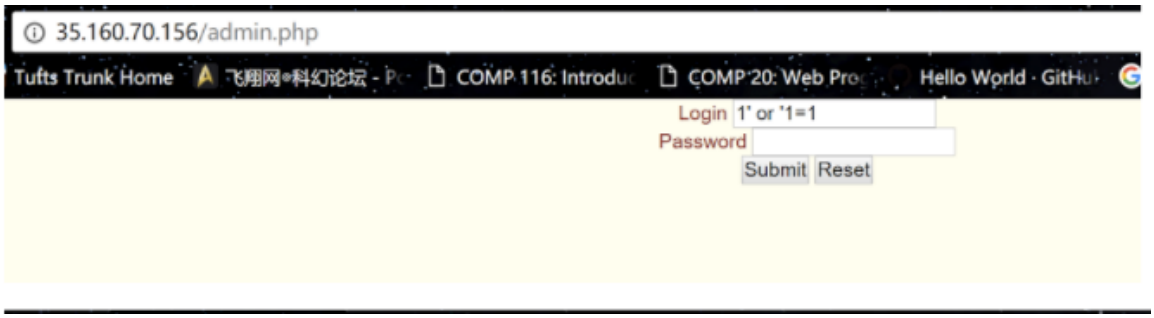
Then we found following page with some coded strings:

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

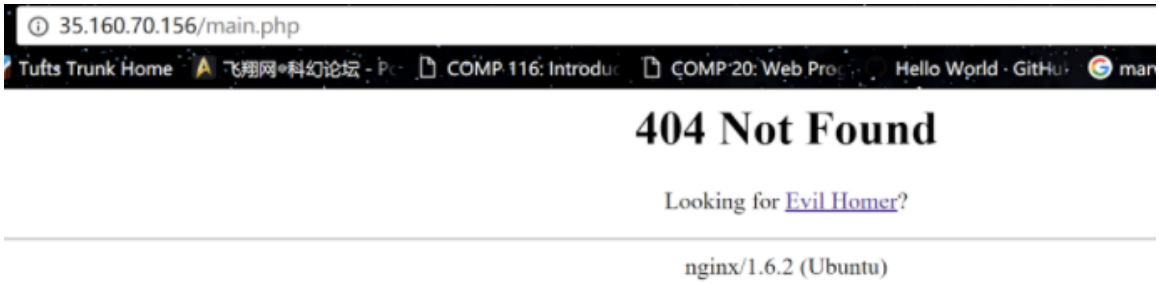


Challenge 4: Don't ask me if something looks wrong. Look again, pay careful attention. 200 points

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



Then we found page:

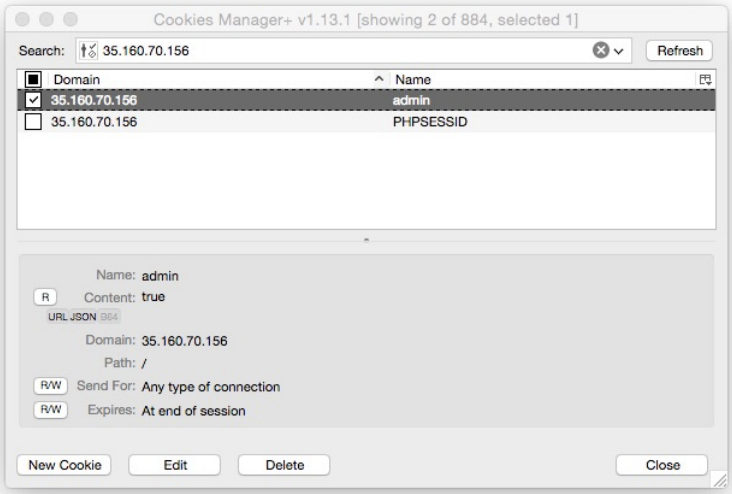


View the page source of this page, we found the key:

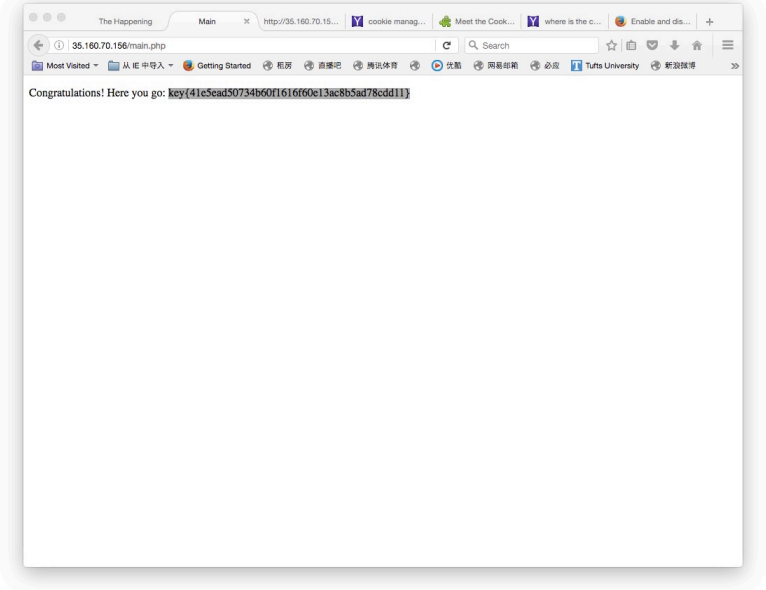
We also found the Evil Homer, which will be used in Challenge 10.

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:

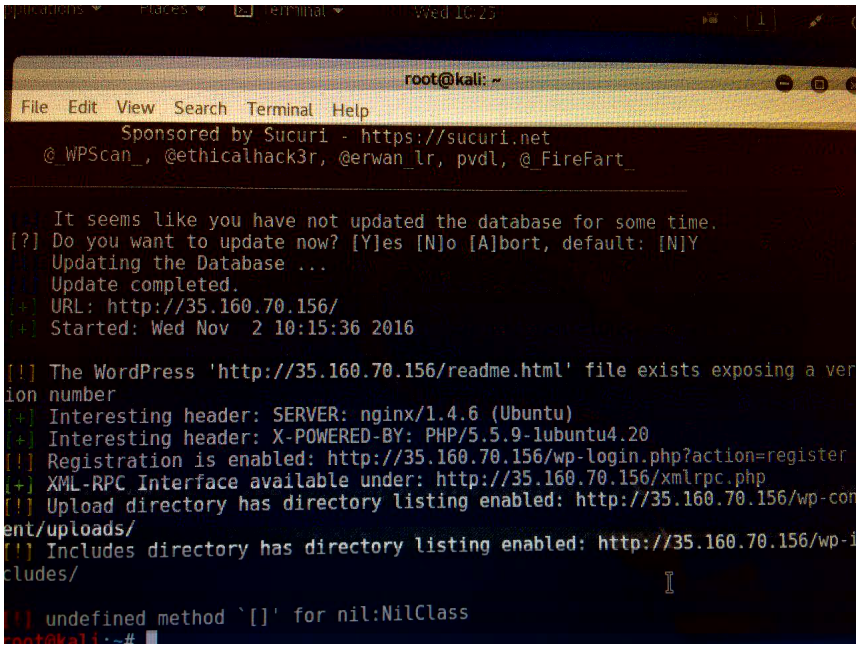


We found the content value is false, this maybe why there is 404 error. So we set the value to true, and refresh the page, it showed the key:

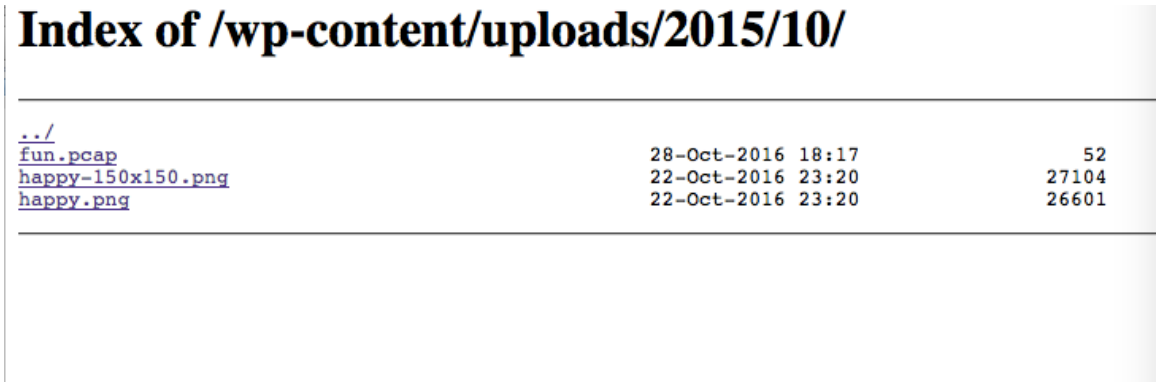


Challenge 6: Buried in the dump of uploads. 100 points

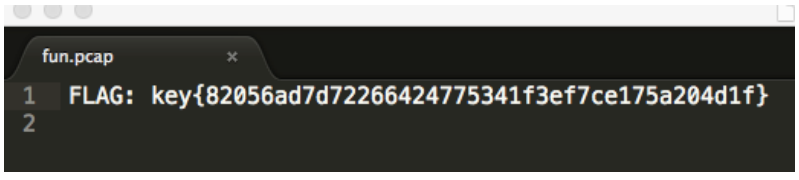
The hint is uploads, so we know the page is using WordPress, so we use wpscan to scan the server, we found following links:



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



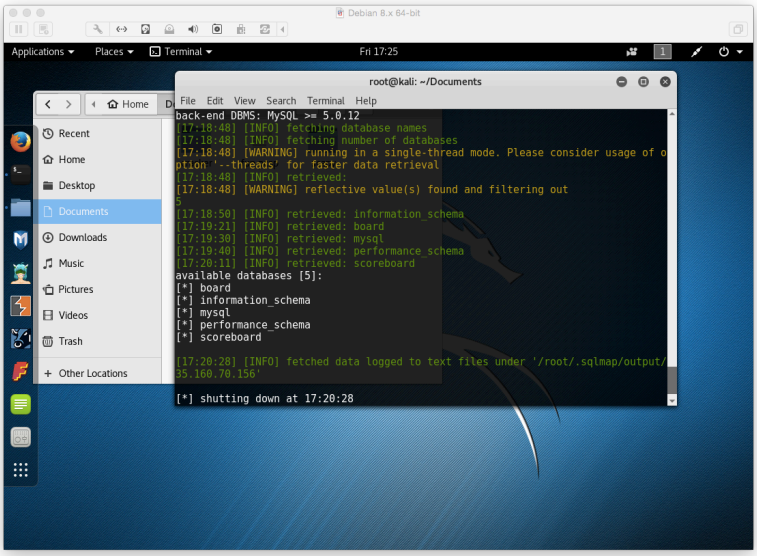
This file is actually a txt file. So open the file we get the key:



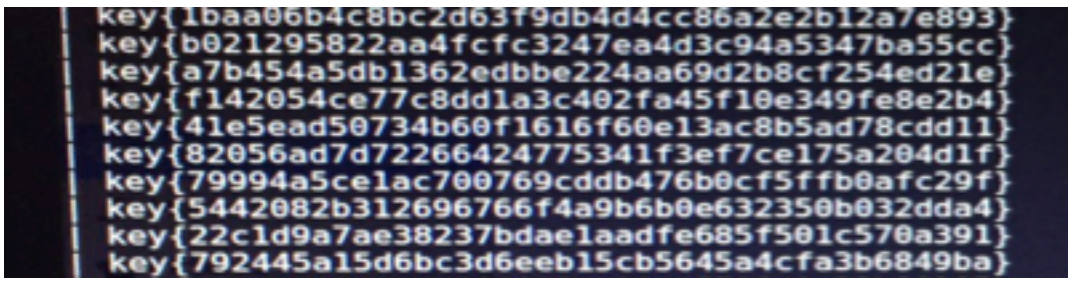
Challenge 7: Buried in the dump: needle in the haystack. 400 points

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

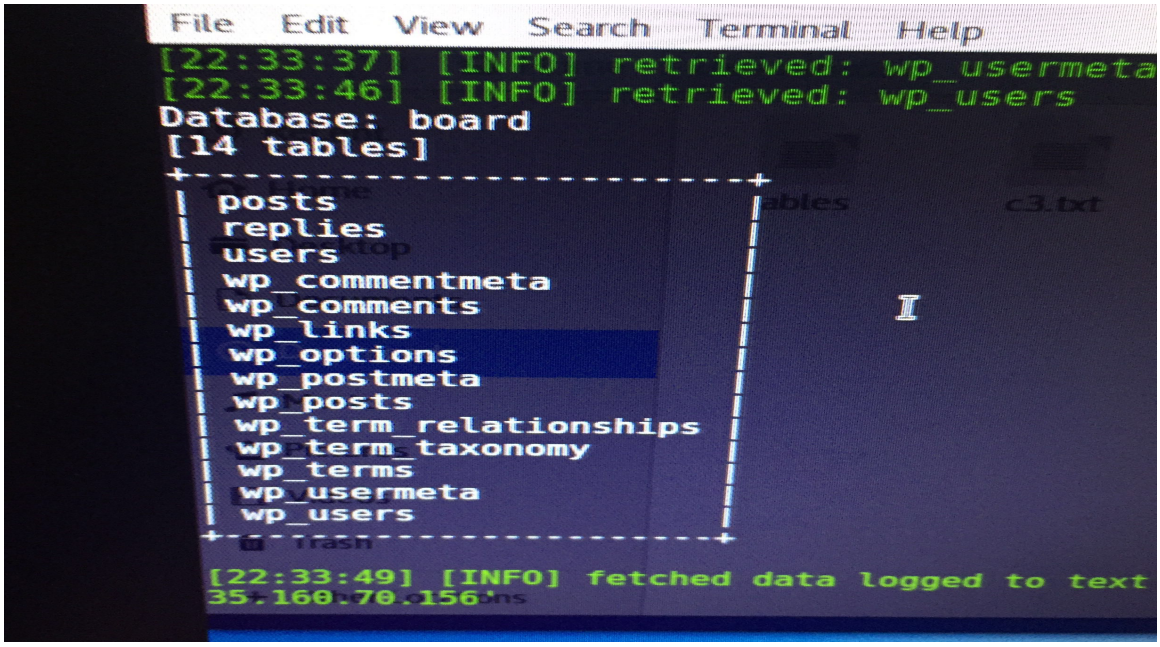


Then we got all the database names. Then we dump the databases, we found all the keys:



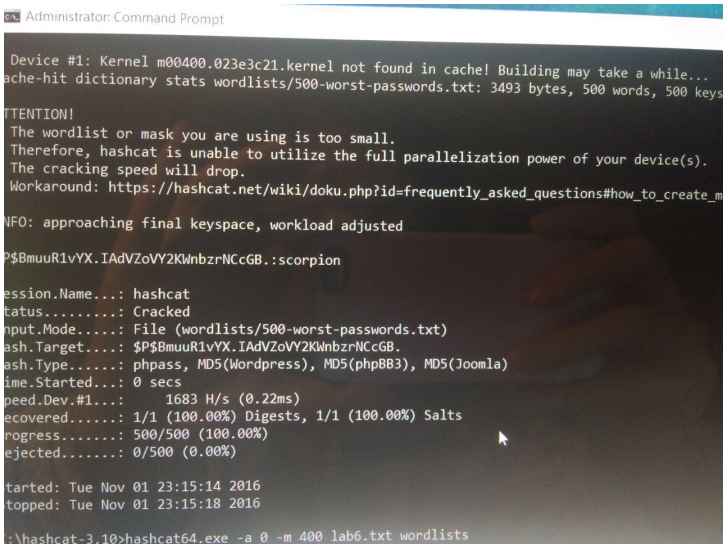
Challenge 8: About my friend bobo... 200 points

Same as challenge 7, we dumped the wp_users, there are user login and password.



we found the login:bobo with the password: PBmuuR1vYX.IAdVZoVY2KWnbzrNCcGB.

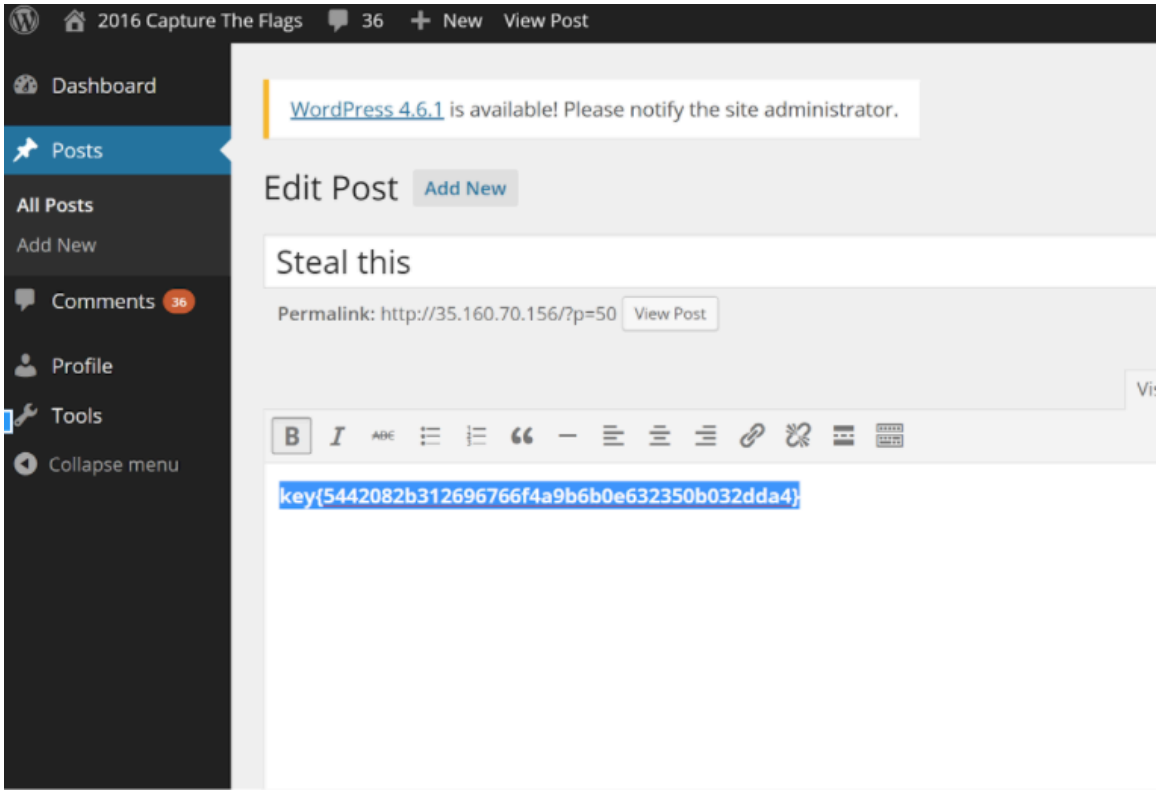
Use hash cat the crack the password, we know password is scorpion



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

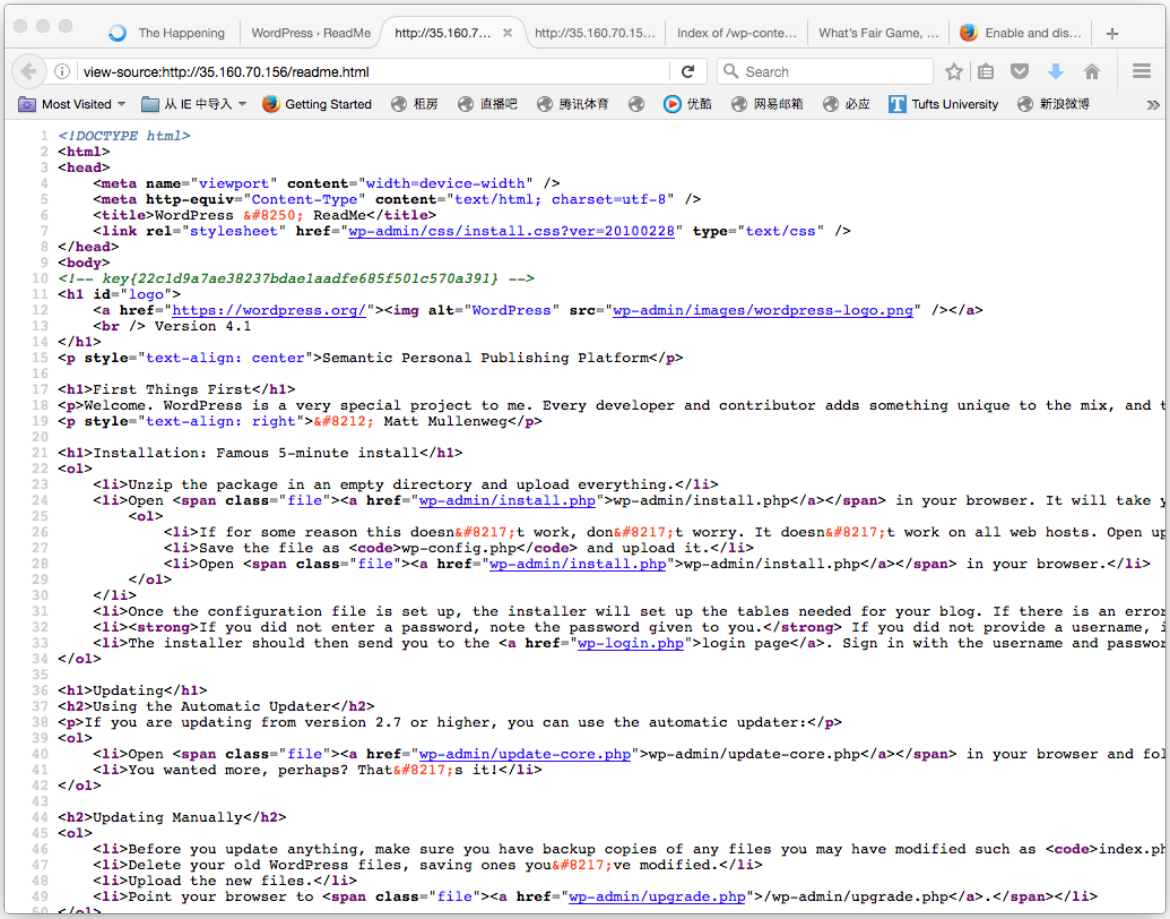
We login as bobo, with the password: scorpion

We found the key:



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:



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..