

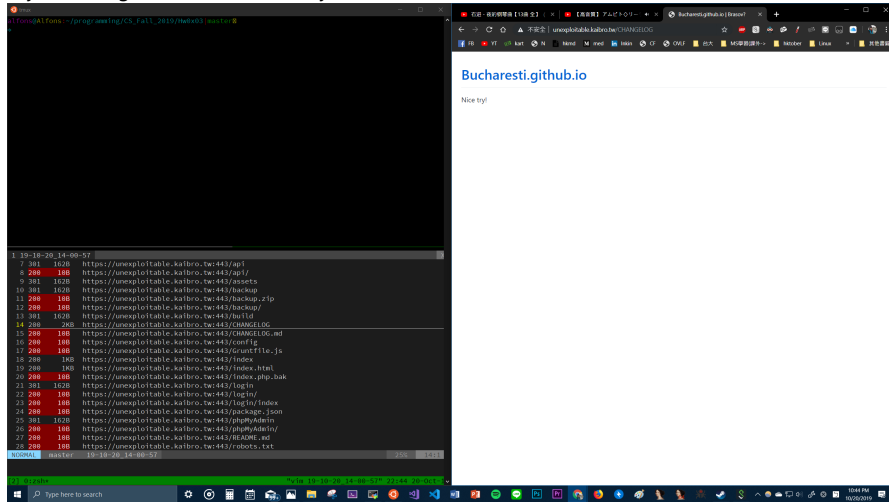
# Computer Security Hw0x03 Writeup

- Realname: 胡安鳳
- ID on course web: alfons0329
- Student ID: R08922024

tags: Computer Security NTU CS CS CTF Writeup

## Unexploitable (Basic recon)

- Step 1: Use `dirsearch` to search all the possible path (hidden included) on the site.
- Step 2: We found the **github.io** (<http://github.io>) site that is different from all the Nice Try! (By checking the file size != 10Bytes)



- Step 3: Google it, and found the github repo corresponding to such weblink, check the git history and found the deleted file --> that is the flag.

added robots.txt

w181496 committed 3 days ago ✓

delete secret file

w181496 committed 4 days ago ✓

added some files

w181496 committed 4 days ago ✓

Commits on Oct 16, 2019

Code Issues 0 Pull requests 0 Projects 0 Wiki

delete secret file

master

w181496 committed 4 days ago

Showing 1 changed file with 0 additions and 1 deletion.

```
1 this_is_th3_r3al_flag
...
@@ -1 +0,0 @@
1 - FLAG{baby_recon_dont_forget_to_look_github_page}
...
```

0 comments on commit c2dc70b

Write Preview

Leave a comment

# Safe R/W (Php protocol knowledges)

使用 data: 這個協議，讓他丟什麼就吐什麼，所以在檢查檔案內容的時候並不會檢查到php的開頭，反而是只有那串字串而已，而最後就繞過了

```
if(isset($i) && strpos(file_get_contents($i), '<') === FALSE)
```

然後自己再利用php的shell指令把跟目錄印出來，找到flag

