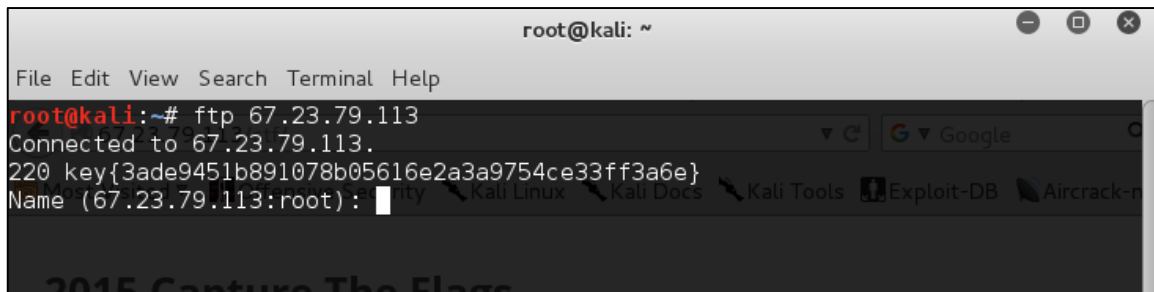


## COMP 116 Capture the Flag: Write-Up Report

### KEY #1

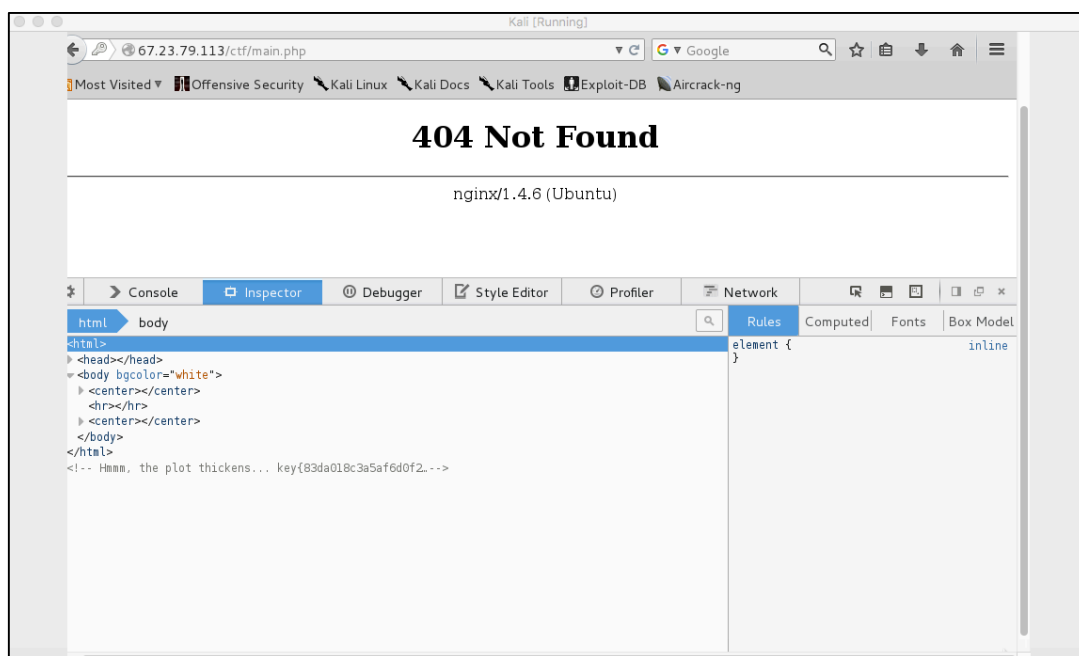
ftp 67.23.79.113 directed us to provide a name and password to gain access but the key was found without needing the credentials.



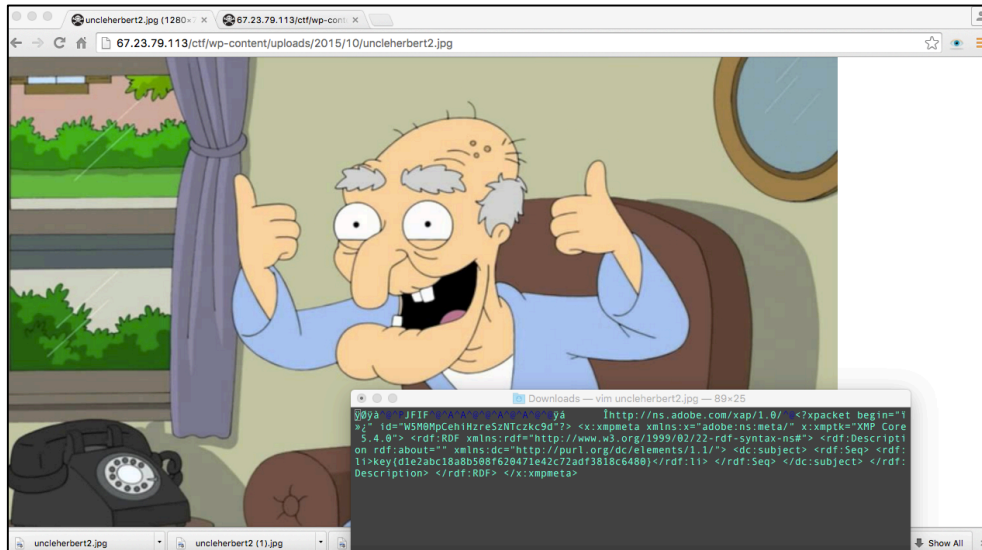
```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ftp 67.23.79.113  
Connected to 67.23.79.113.  
220 key{3ade9451b891078b05616e2a3a9754ce33ff3a6e}  
Name (67.23.79.113:root):
```

### KEY #2

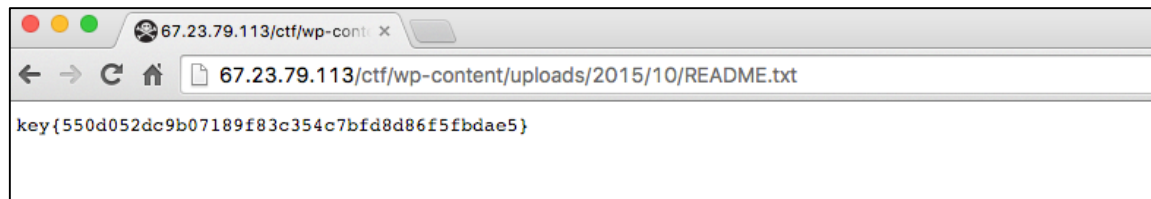
We found the page [67.23.79.113/ctf/admin.php](http://67.23.79.113/ctf/admin.php), which required a login and password. We used SQL injection to bypass knowing the credentials. We entered `1' or '1 = 1` as both the login and password so that the login expression would default to true. This authenticated us and forwarded us to [67.23.79.113/ctf/main.php](http://67.23.79.113/ctf/main.php), which gave us the 404 Error Page shown below. Upon inspecting the page, the key was in the comments.



The pages on [67.23.79.113](#) were made on Wordpress so we took advantage a common Wordpress security flaw and navigated to [67.23.79.113/ctf/wp-content/uploads/](#) to see any files that were uploaded. There we found image files, including *uncleherbert.jpg*, which included a key.



*README.txt* was another file that was in the uploads/ directory. When we opened it, there was a key.



### KEY #5

On the board page located at [67.23.79.113/ctf/board.php](http://67.23.79.113/ctf/board.php) there was an image of a smiley face. When JavaScript was disabled, the image was a crying face. We saved the image and used the strings command to search for strings we found the key.

```
TTS0u0V[u  
uVZk  
uW^{  
;key{5ced54168466390013355d08b2942170d0b3a0f9}  
Danielles-MacBook-Pro-2:Downloads daniellezelin$
```

### KEY #6

There was a file called runme.exe that was at [67.23.79.113/ctf](http://67.23.79.113/ctf). After downloading, we used the file command realized it was not actually an executable but rather a pcap file. Using the strings command, we found that file contained the instruction:

*Watch the video. The key is the SHA1 sum of the number, as a word in all caps, in the video.*

We opened the pcap file in Wireshark and when we followed the TCP stream we were able to find the .mp4 file that contained the video. The number in the sesame street video was 7 and the SHA1 sum of "SEVEN" gave us the key.

**generator**

SEVEN

hash

sha-1 ▼

**Result for**

**sha1: cabd534c35ee6a39365f4ed3bce4eafdcc3d4b8d**