CTF Write-up

Team #9

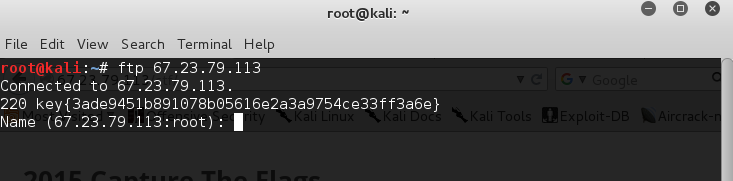
Hayley Cohen

Danielle Zelin

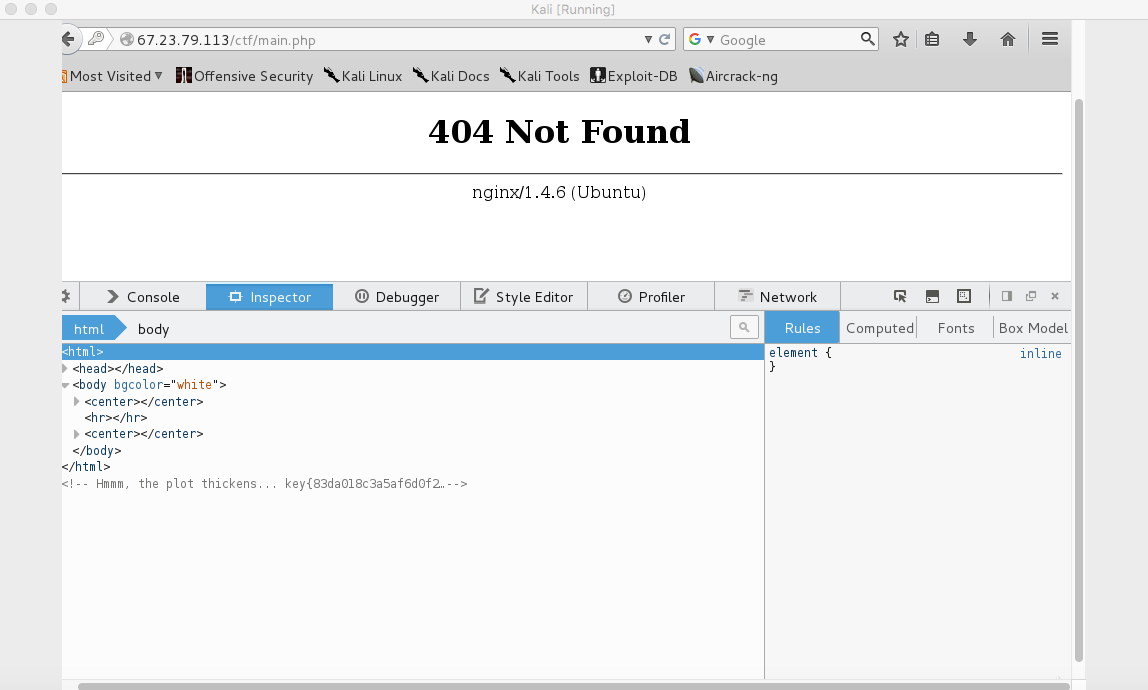
Zach Kirsch

Jay DeStories

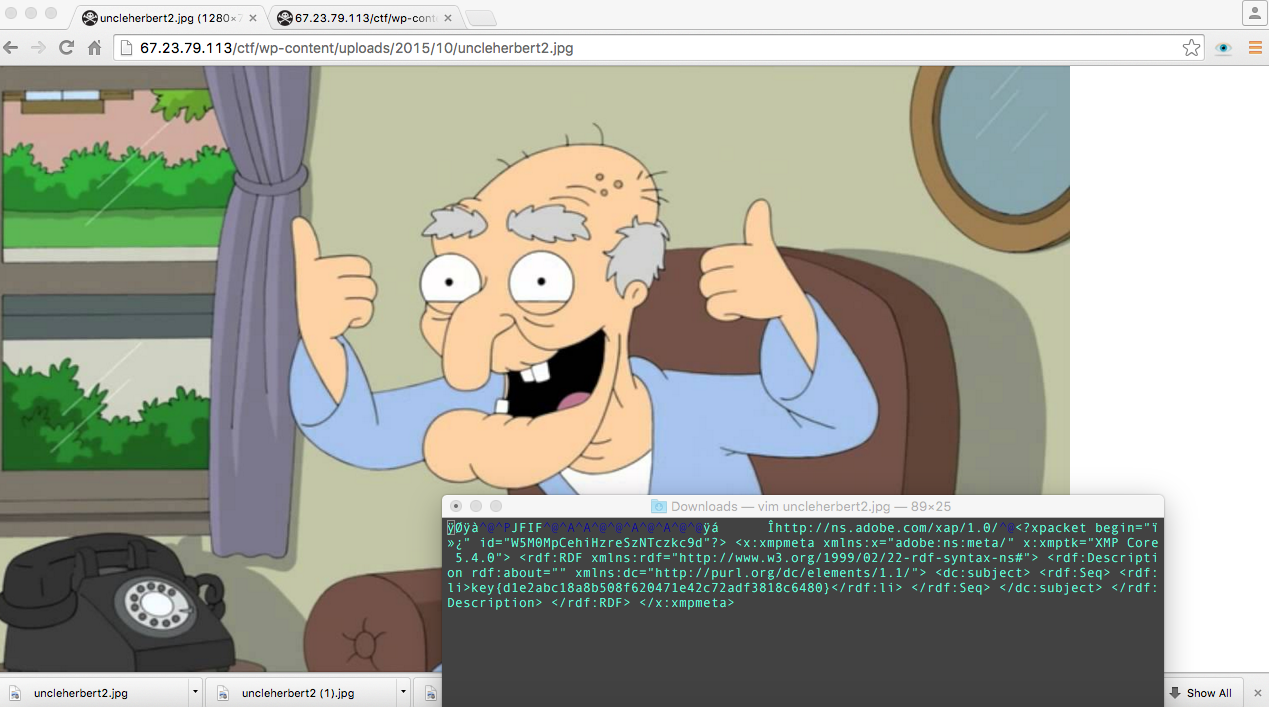
1. “FTP 67.23.79.113” directed us to provide a name and password to gain access but the key was found without needing the credentials.



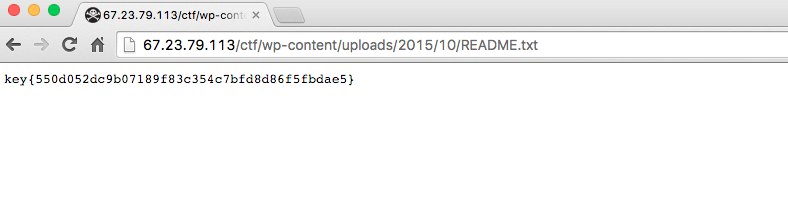
2. We found the page 67.23.79.113/ctf/admin.php, which required a login and password. We used SQL injection to bypass knowing the credentials. We entered 1’ or ‘1 =1 as both the login and password. This led us to 67.23.79.113/ctf/main.php, which gave us the 404-error page shown below. Upon inspecting the page, the key was in the comments.



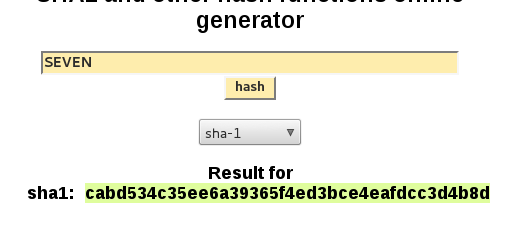
3.The pages on 67.23.79.113 were made on wordpress so we realized that we were able to go to 67.23.79.113/ctf/wp-content/uploads/ to see any associated files that were uploaded. There we found the uncleherbert.jpg files. We downloaded the files and opened them in text editors. There was a key hidden in uncleherbert2.jpg



4. README.txt was another file that was in the wp-content/uploads. When we opened it, there was a key.



5. There was a file called runme.exe that was on the main page for the CTF. After trying to download it, we realized it was not actually an executable but rather a pcap file so we downloaded it has runme.pcap. We checked the file for strings and we found that it said that the key was the SHA1 of the number in the movie and we obtained the specific location of the video. [Does anyone have the actually wording from the terminal??] We opened the pcap 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 of SEVEN gave us the key.



6. On the board page located at 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 opened the file in a text editor. When we searched for strings we found the key.

