<Write-ups>

Kenji

RingzerOctf.com

Catergory: Forensics

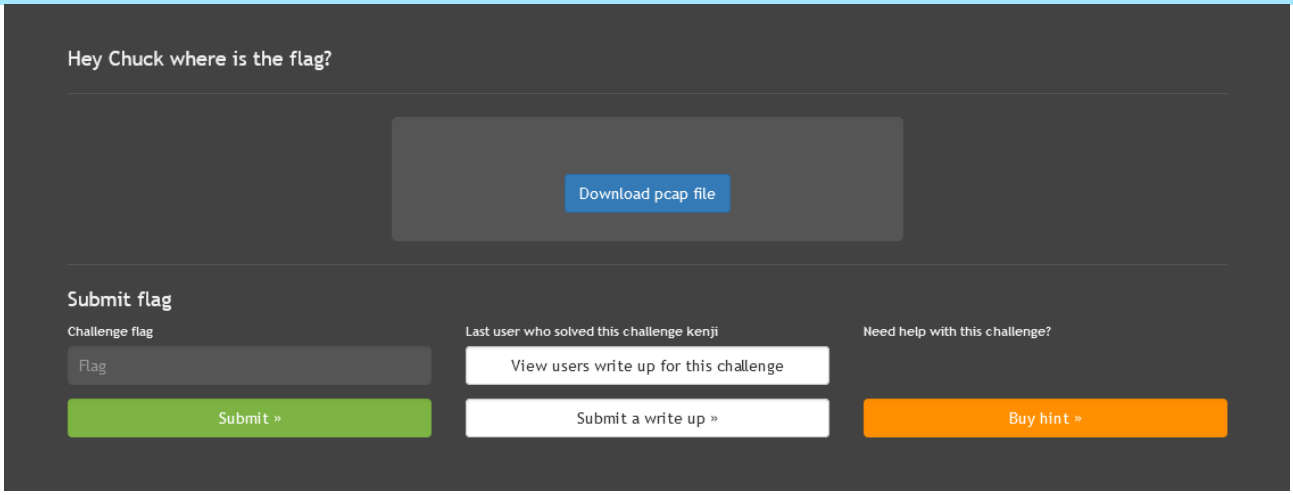
Challenge: [9] 44

“Hey Chuck where is the flag?”

https://ringzer0ctf.com/challenges/44

Contents

1. CHALLENGE



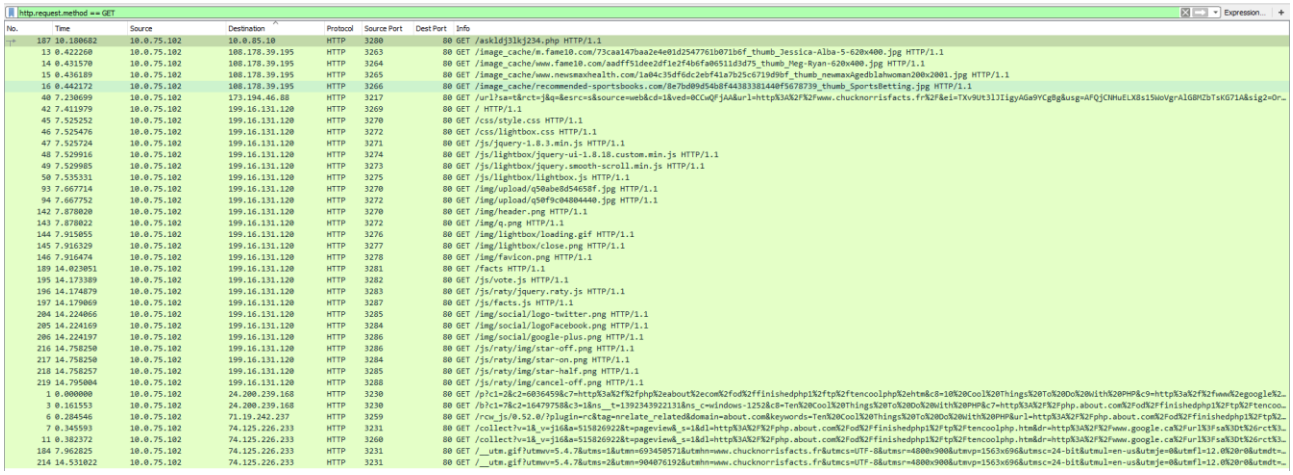
2. HINT I BOUGHT

3. TOOLS & REFERENCES

- Wireshark
- cat

4. CTF

> Let's check the pcap first:



> There's lots of requests coming from multiple sources. After checking the website: http://www.chucknorrisfacts.fr/

⇨ No interest.

(I have check all the image uploaded inside the website. Even those 2 jpg files uploaded shown on pcap:

http://www.chucknorrisfacts.fr/img/upload/q50abe8d54658f.jpg

http://www.chucknorrisfacts.fr/img/upload/q50f9c04804440.jpg

Because the image is no longer exist, but i can still find it on archive.org:

> Turn out: It’s nothing inside and have no flag related.

So...

> After bought the Hint. I find out that I can extract some content/request i cannot see directly on Wireshark by “save” them as gzip and use “cat” command to check them there.

> Right on first try, i have successed read the flag with the packet from: 10.0.85.10

```
root@SIFT -> ~/Downloads
# cat askldj3lkj234.gzip
Hey this is a flag FLAG-GehFMsqCeNvof5szVpB2Dmjxroot@SIFT -> ~/Downloads
#
```

> YES! The Flag!

FLAG-GehFMsqCeNvof5szVpB2Dmjx

</Thank you>