Writeup Jeopardy

LKS Jakarta Timur 2024



**Jakarta Timur**

**SMKN 40 Jakarta**

Muhammad Faiz Hidayat

Auriza Irhamnas

# Daftar Isi

[Daftar Isi 1](#_Toc165380489)

[Cryptography 2](#_Toc165380490)

[Baby Shifter 2](#_Toc165380491)

[FLAG: LKSJAKTIM{ROT13\_f0r\_newbies\_bef0re\_knowing\_randomness} 2](#_Toc165380492)

[Warmup 3](#_Toc165380493)

[Sanity Check 3](#_Toc165380494)

[FLAG: LKSJAKTIM{wh!te\_colored\_fl4g\_!s\_here\_lol} 3](#_Toc165380495)

[Digital Forensics 4](#_Toc165380496)

[Sniffed 4](#_Toc165380497)

[FLAG: LKSJAKTIM{w!re\_tr4nsfer\_15\_3xp0sed} 4](#_Toc165380498)

[Reverse Engineering 5](#_Toc165380499)

[Baby RE 5](#_Toc165380500)

[FLAG: LKSJAKTIM{1\_@m\_str1ng!fied\_yeay} 5](#_Toc165380501)

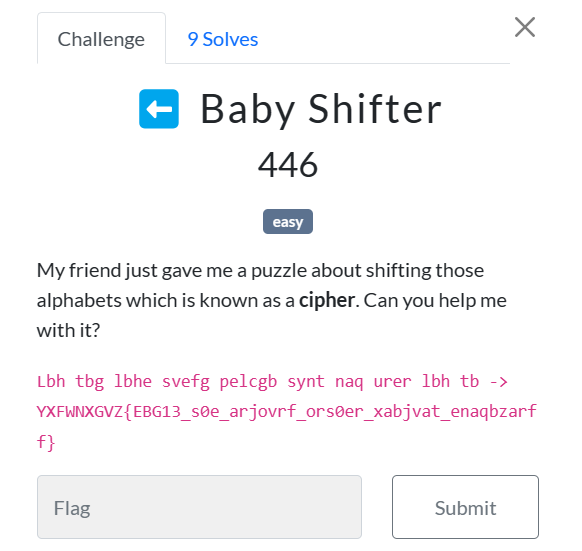
[Web Exploitation 6](#_Toc165380502)

[Spider 2 6](#_Toc165380503)

[FLAG: LKSJAKTIM{370f257c86de0b7b86c7c30c11c17488} 7](#_Toc165380504)

# Cryptography

## Baby Shifter

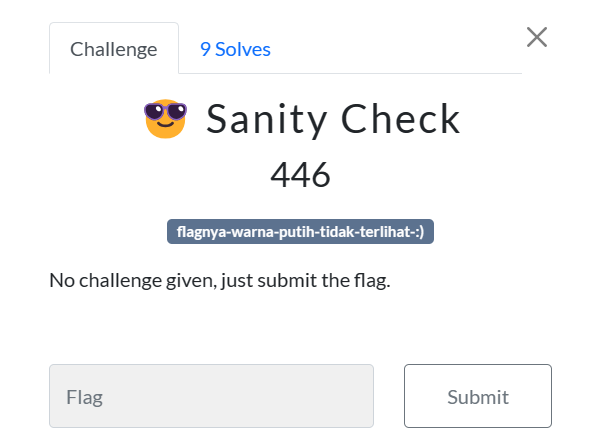


Terdapat poin yaitu **cipher**, kita bisa langsung beranggapan bahwa text yang dihighlight merah “Lbh tbg lbhe svefg pelcgb synt naq urer lbh tb -> YXFWNXGVZ{EBG13\_s0e\_arjovrf\_ors0er\_xabjvat\_enaqbzarff}” adalah text yang di encode dengan ROT13 langsung saja kita decode dengan menggunakan [tools online](https://dencode.com/en/)  

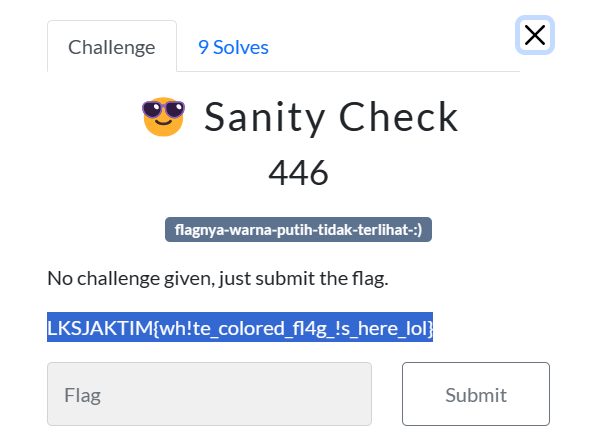

### FLAG: LKSJAKTIM{ROT13\_f0r\_newbies\_bef0re\_knowing\_randomness}

# Warmup

## Sanity Check



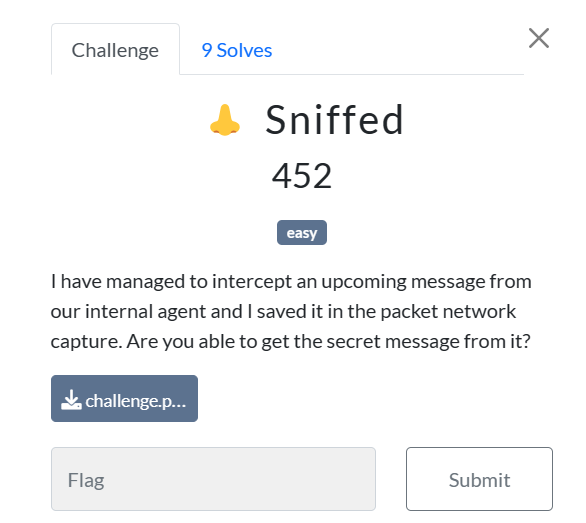
Dapat dilihat ada hint “flagnya-warna-putih-tidak-terlihat” yang berarti flagnya nyaruh dengan color backroundnya, kita bias langsung highlight saja dengan mouse yang menurut kita ada element yang mencurigakan yaitu space kosong



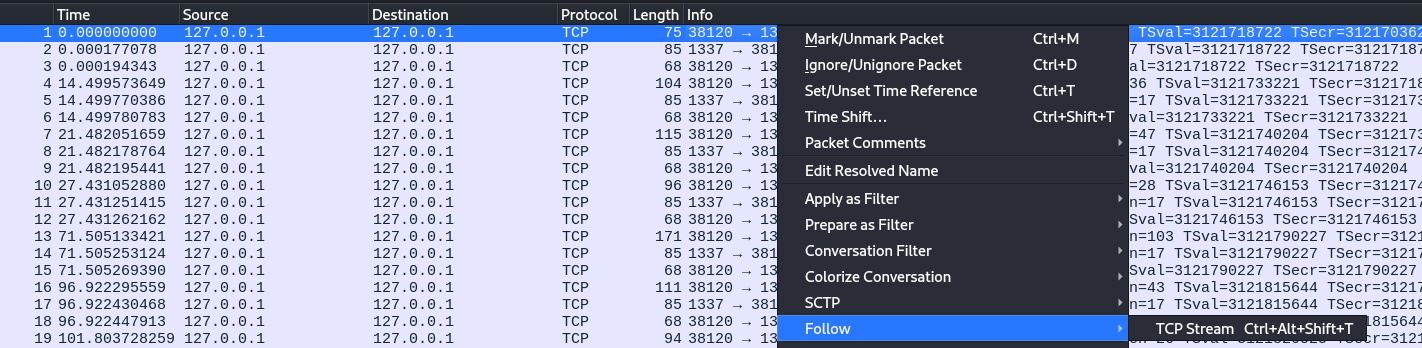
### FLAG: LKSJAKTIM{wh!te\_colored\_fl4g\_!s\_here\_lol}

# Digital Forensics

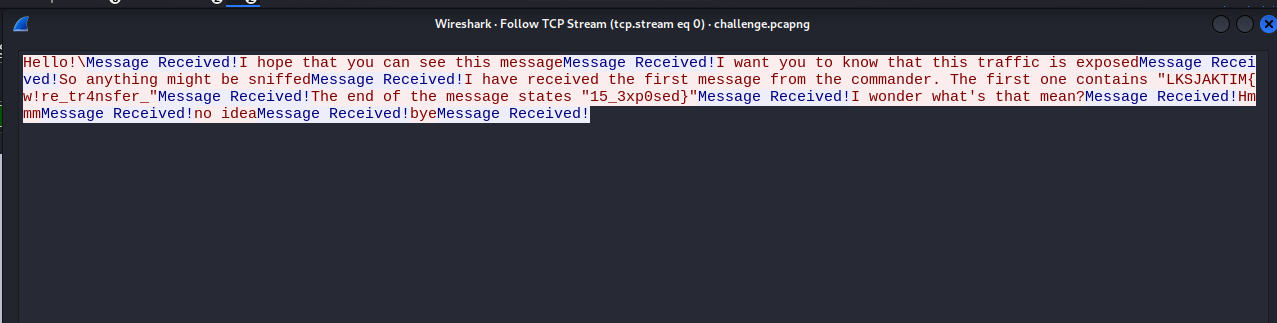
## Sniffed



Disini ada file dengan format .pcapng yaitu sebuah packet network atau history traffic network, jadi langsung kita buka saja filenya dengan wireshark



Dan selanjutnya kita langsung klik kanan protocol pertamanya saja lalu Follow > TCP Stream

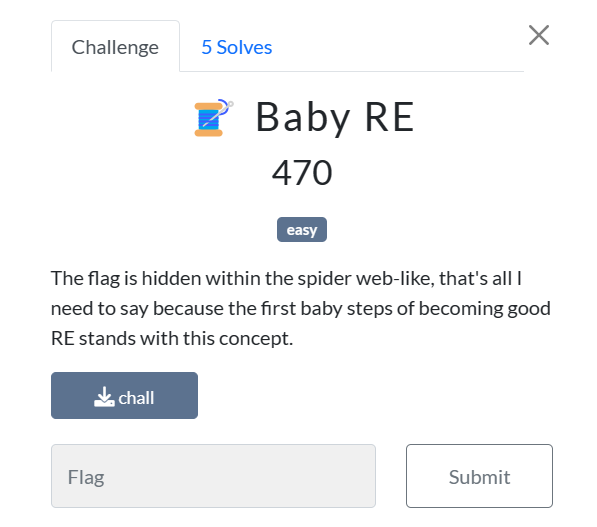


Flagnya mungkin sedikit terpisah yaitu “LKSJAKTIM{w!re\_tr4nsfer\_” dan “15\_3xp0sed}”

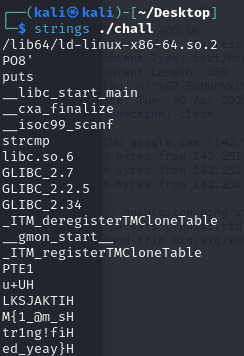
### FLAG: LKSJAKTIM{w!re\_tr4nsfer\_15\_3xp0sed}

# Reverse Engineering

## Baby RE



strings ./chall

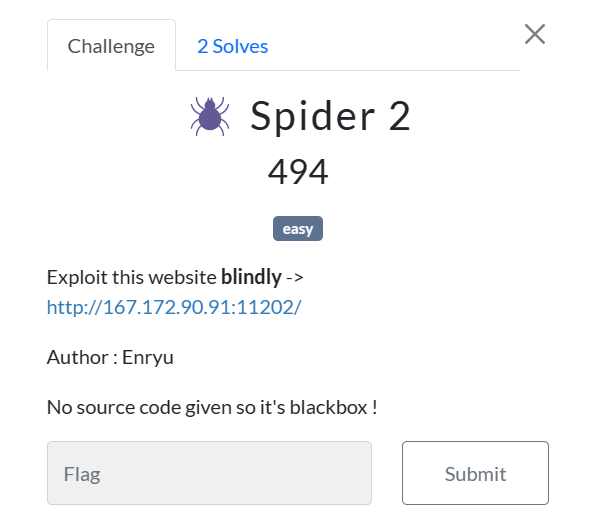


“LKSJAKTIHM{1\_@m\_sHtr1ng!fiHed\_yeay}” flagnya sedikit berantakan yaa… tidak usah khawatir tinggal hapus saja huruf Hnya

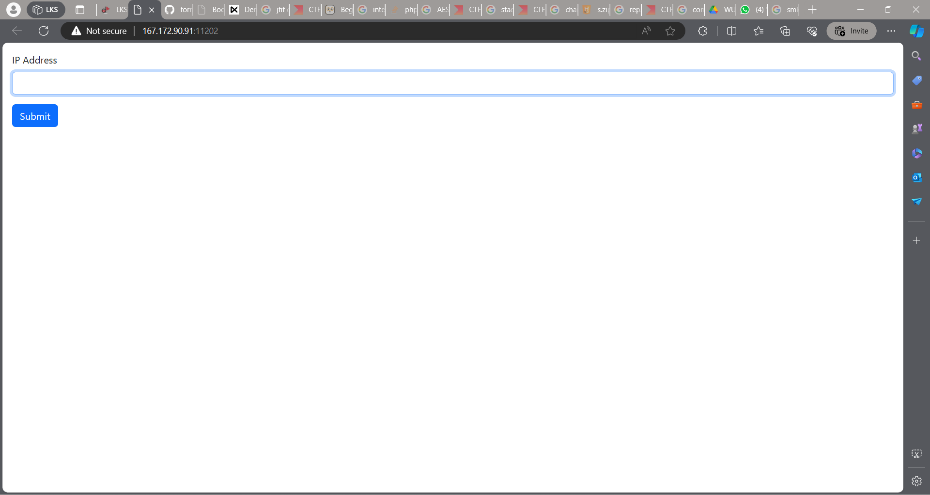
### FLAG: LKSJAKTIM{1\_@m\_str1ng!fied\_yeay}

# Web Exploitation

## Spider 2



Terdapat web [167.172.90.91:11202](http://167.172.90.91:11202/) yang jika dibuka mendirect ke sebuah website ICMP atau website untuk mengeping sebuah domain atau ip address



Kita coba untuk mengeping ip 1.1.1.1 dan website tersebut mengeksekusi kode ping atau command



Kita beranggapan bahwa command injection adalah vulnerability web ini, sekarang kita coba command untuk melisting directory saat ini dengan :



1.1.1.1;ls

Nampaknya terdapat file tersembunyi yaitu flag.txt, langsung saja kita lihat isinya dengan command “cat”:

Gunakan command ini “1.1.1.1;cat${IFS}flag.txt” karena website tersebut memblokir whitespace pada inputan

### FLAG: LKSJAKTIM{370f257c86de0b7b86c7c30c11c17488}