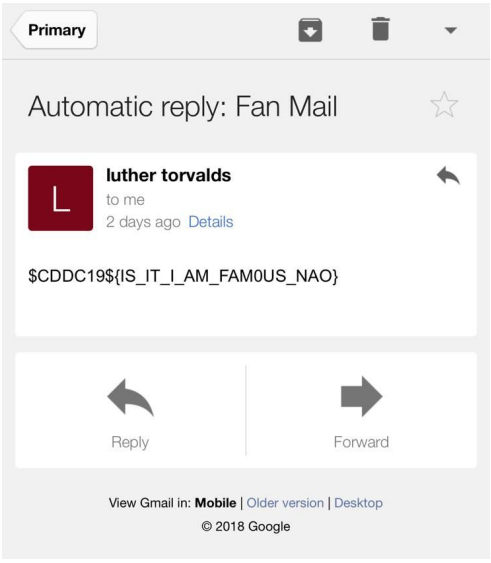
[CDDC19]-TechNoLogic Writeup

by Terence, Azalia, Darren, Zhi Qin

[R0] Everyone <3 Fan Mail

https://who.is/whois/lightspeedcorp.global
You will obtain the administrative email `Luther.Torvalds@outlook.com`
Then email to administrative contact as fan mail. There will be a return email with the flag



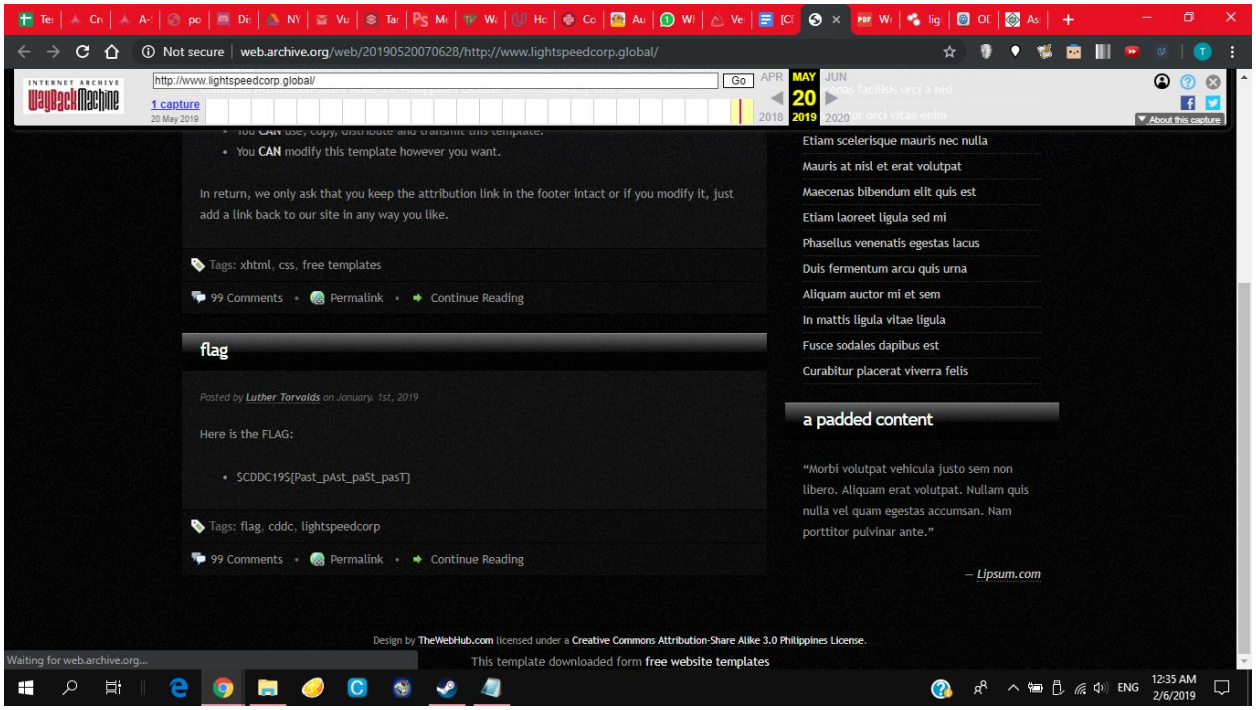
Flag

$CDDC19${IS_IT_I_AM_FAM0US_NAO}

[R-1] Travel to the Past

Solution

http://web.archive.org/web/20190520070628/http://www.lightspeedcorp.global/
Use Wayback machine to get a previous web capture of the website



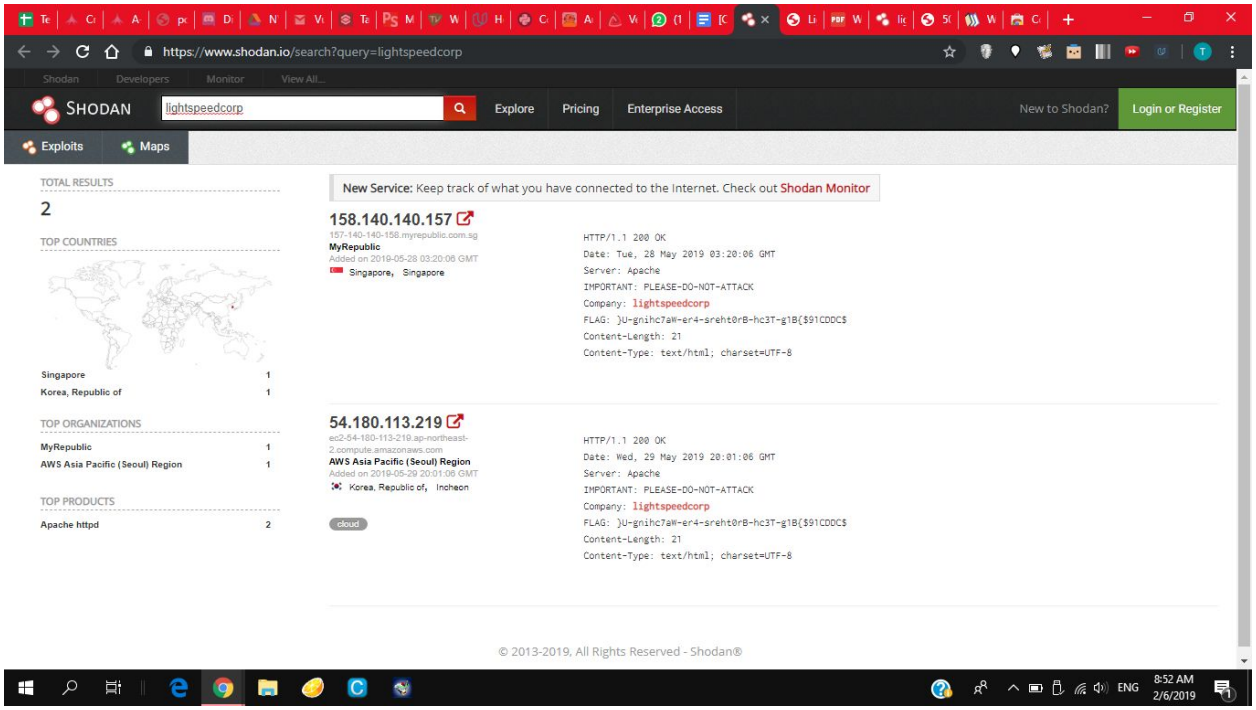
Flag

$CDDC19{Past_pAst_paSt_pasT}

[R-2] I'm Sho Done With This

Solution

https://www.shodan.io/search?query=lightspeedcorp



Reverse the order of `}U-gnihc7aW-er4-sreht0rB-hc3T-g1B{$91CDDC$`

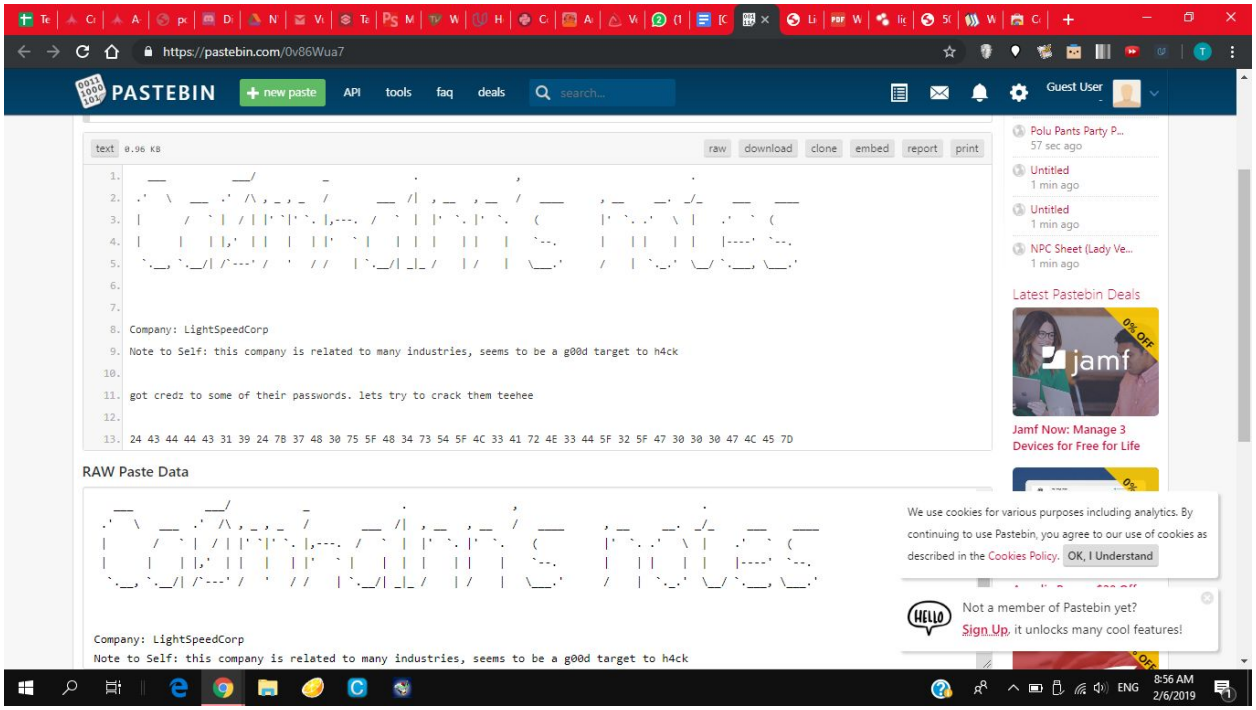
Flag

$CDDC19${B1g-T3ch-Br0thers-4re-Wa7ching-U}

[R-3-1] Have They Been Pwned?

Solution

https://pastebin.com/0v86Wua7




```
24 43 44 44 43 31 39 24 7B 37 48 30 75 5F 48 34 73 54 5F 4C 33 41 72 4E 33 44 5F 32 5F
47 30 30 30 47 4C 45 7D
```

Using a hexadecimal to text converter, you can get the flag

Flag

$CDDC19${7H0u_H4sT_L3ArN3D_2_G000GLE}

[R-4-1] Where I Get All My Memes From

Solution

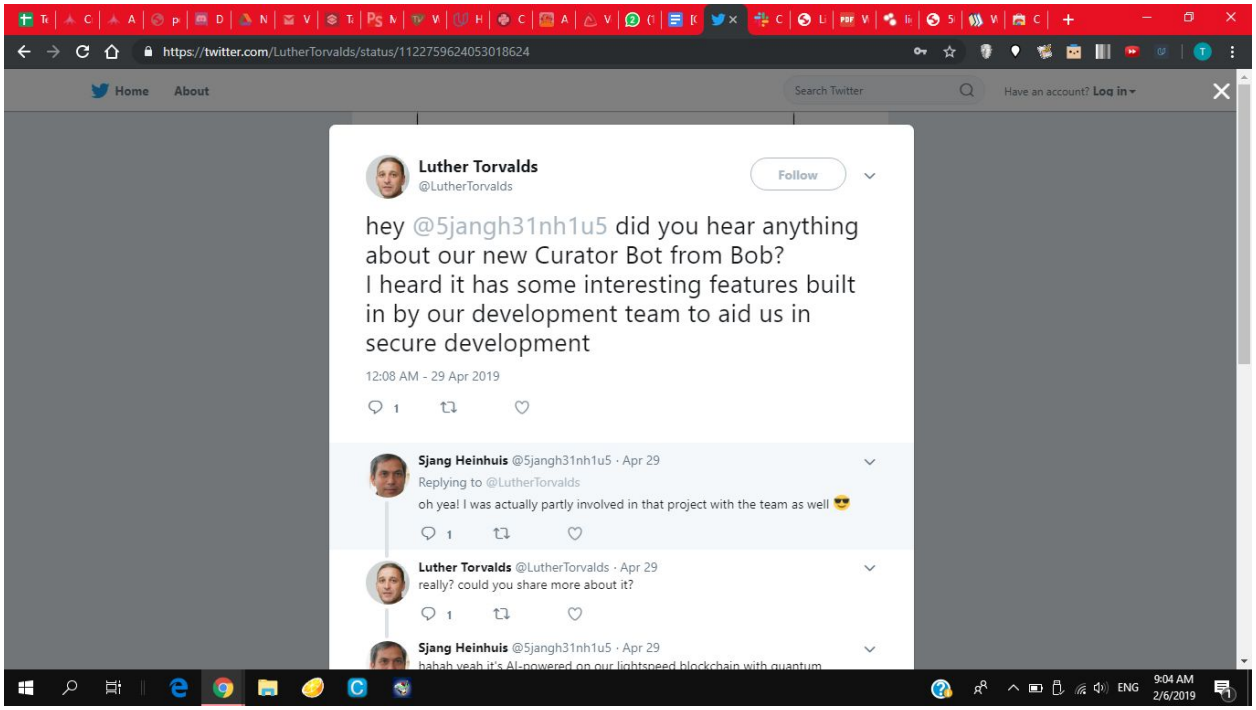
https://twitter.com/LutherTorvalds?lang=en luther torvalds twitter.

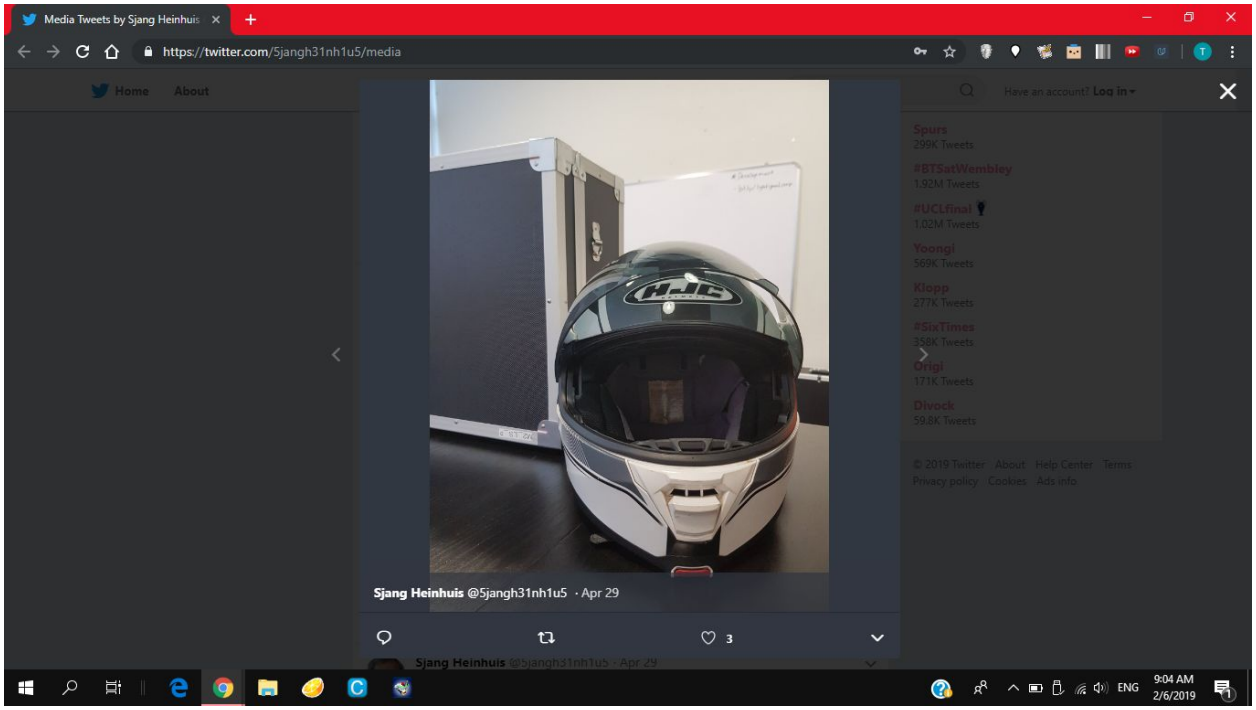
FLAG

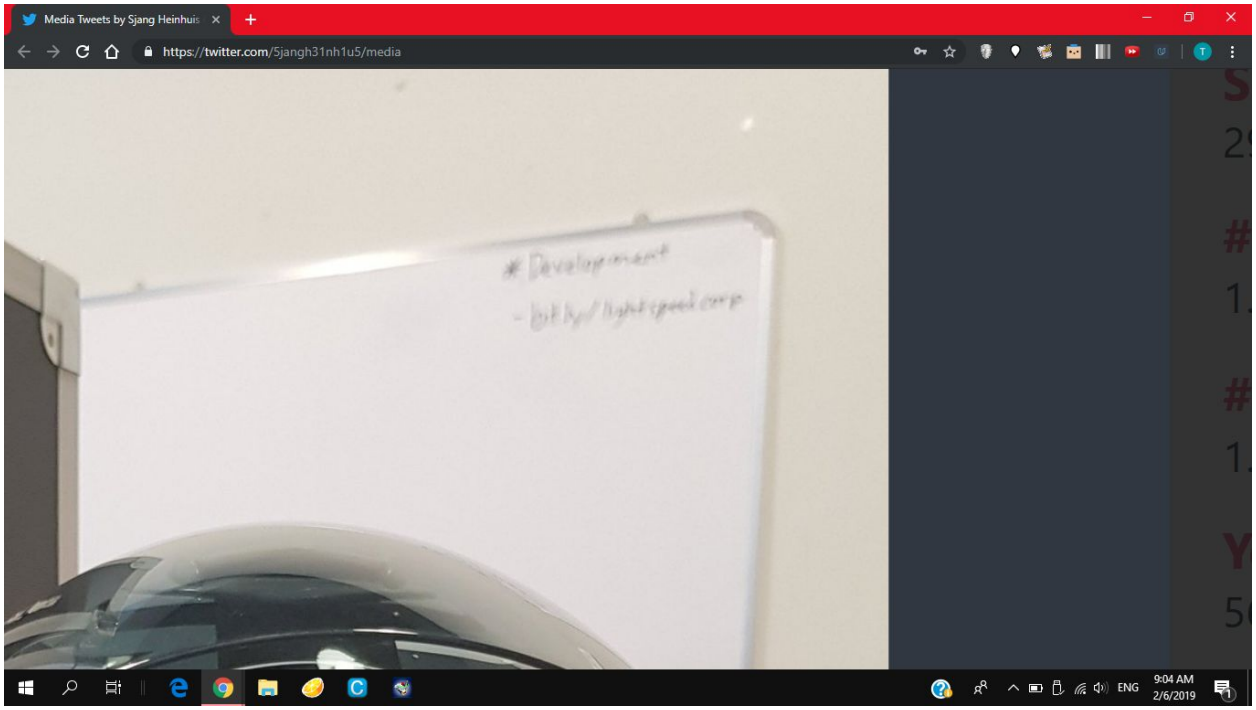
$CDDC19${WHR_R_MY_D4NK_MEMES}

[R-4-1-1] Who Uses Teams Anyway?

https://twitter.com/5jangh31nh1u5/media LINK IS ON THE BOARD OF ONE OF THE PICTURES.

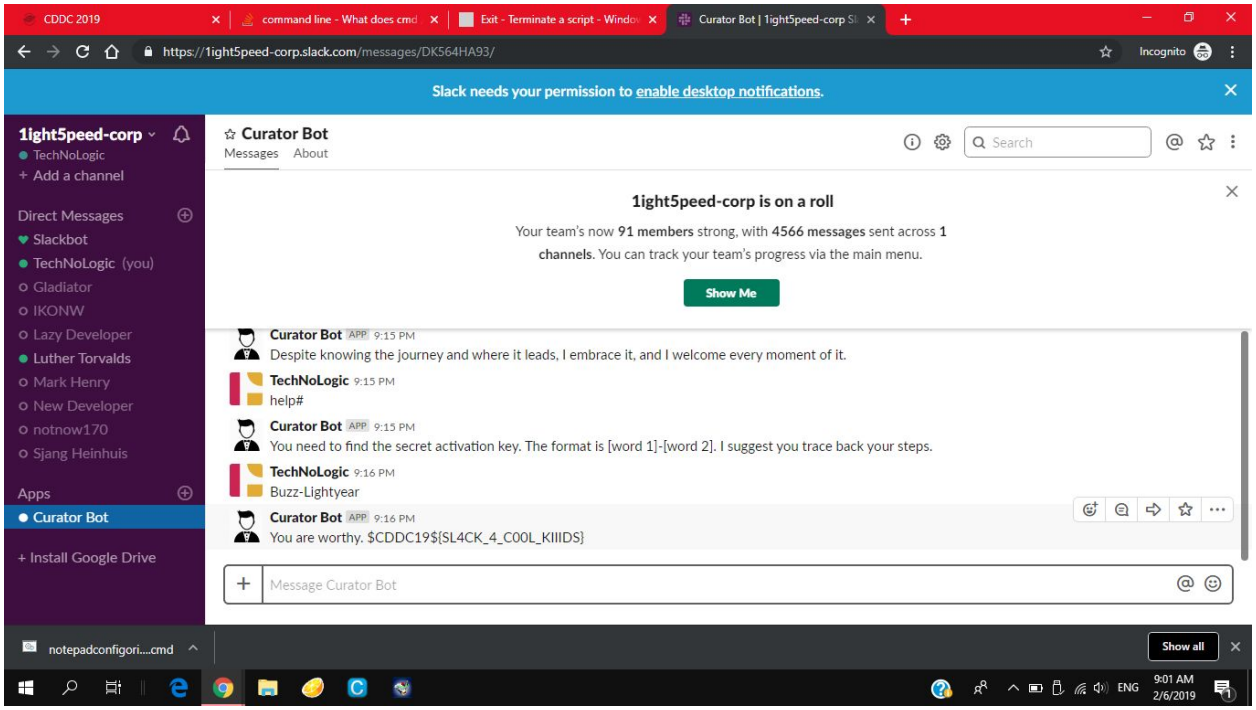






This https://bit.ly/lightspeedcorp is actually a link to the Slack workspace
The Curator Bot will need a secret activation key.

Based on this tweet and a quick google search of ‘star command’,we can derived that Buzz-Lightyear is the secret activation key
Type Buzz-Lightyear in the Curator Bot to get the flag
https://1ight5peed-corp.slack.com/messages/CHPC43SKG/



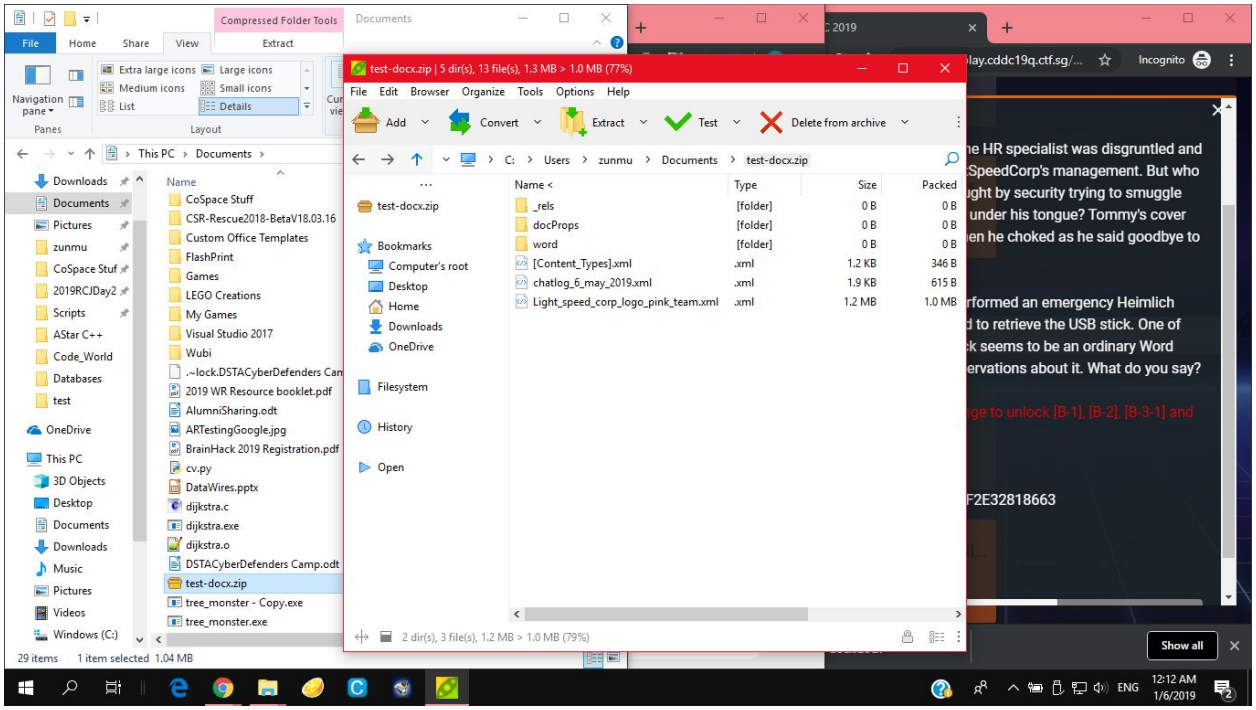
Flag

$CDDC19${SL4CK_4_C00L_KIIIDS}

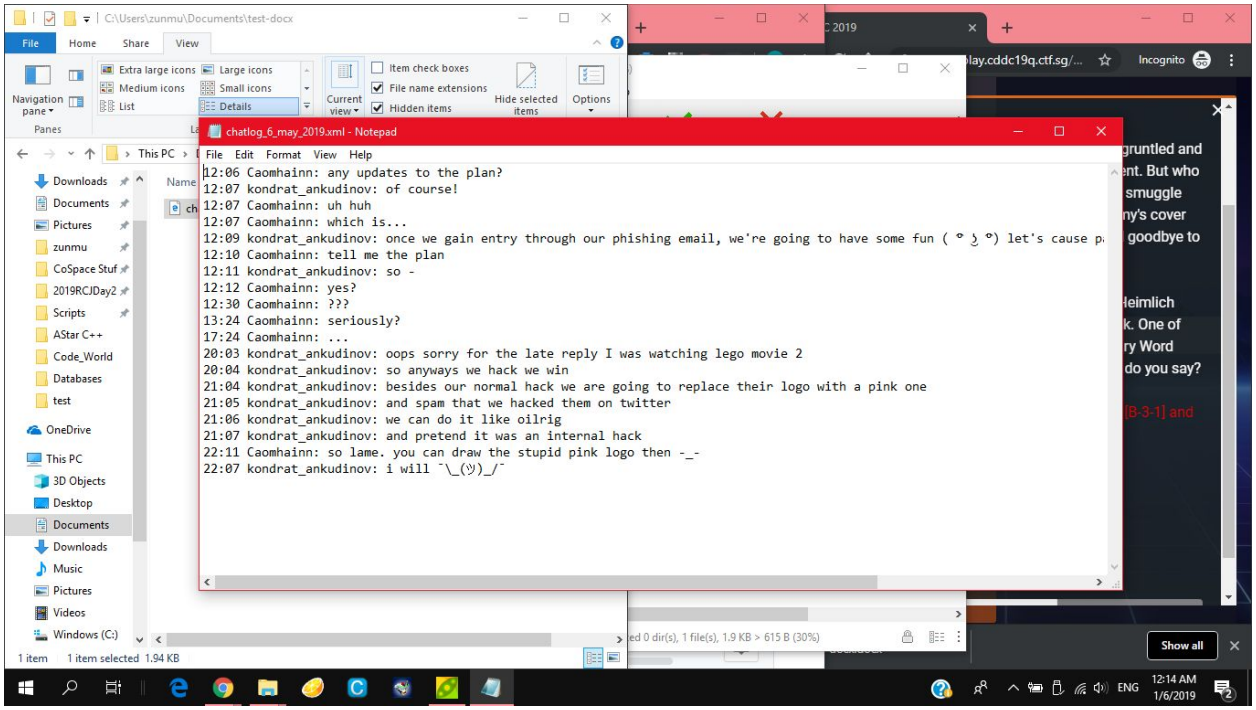
[B-0]What's in, Doc?

Solution

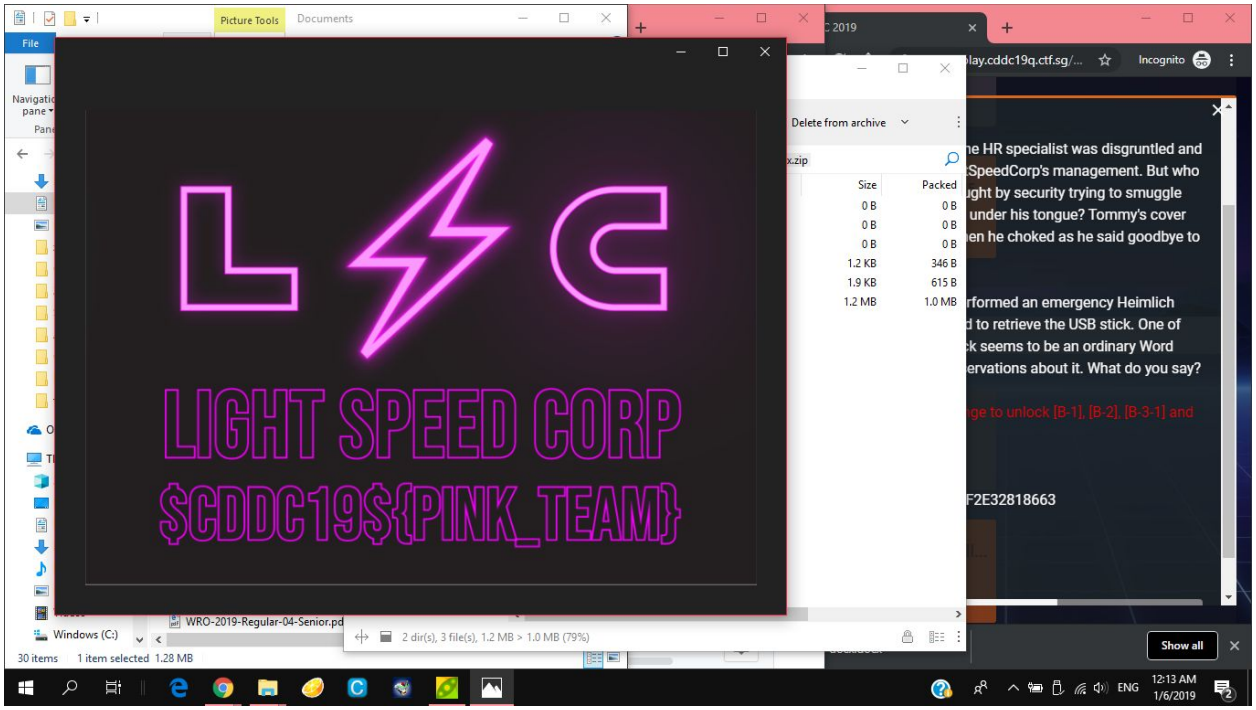
Change the extension of the docx file to zip, and unzip
There are 2 xml files that are not usually in the doc at the root of the extracted folder



chatlog_6_may_2019.xml is about a conversation. Take note as this will be used for the other OSINT_BLUE Tasks



You can change the extension of the other xml file to jpg to get the flag



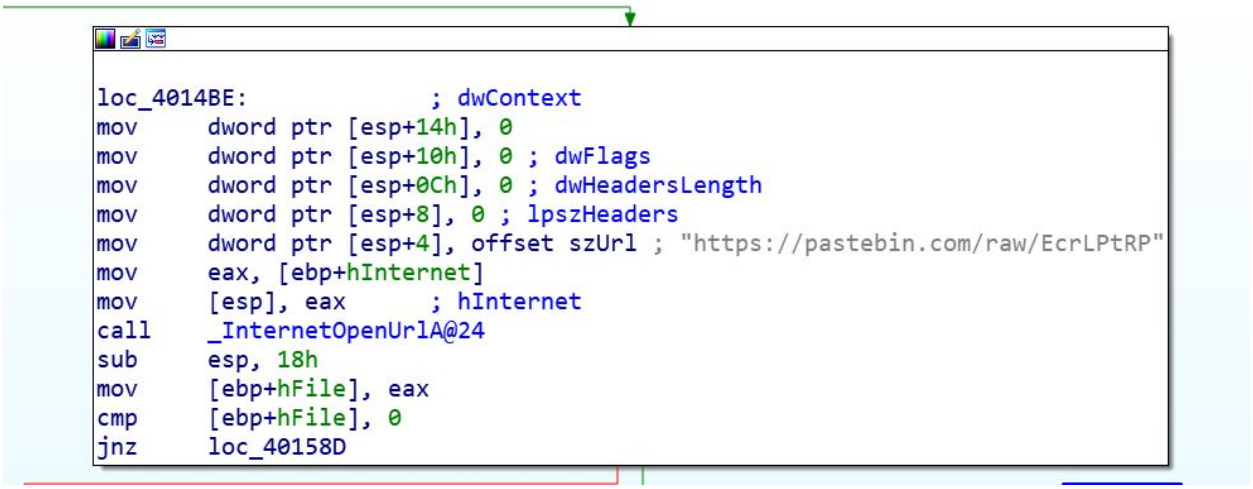
Flag

`$CDDC19${PINK_TEAM}`

[B-1] Fight the Binary Monster

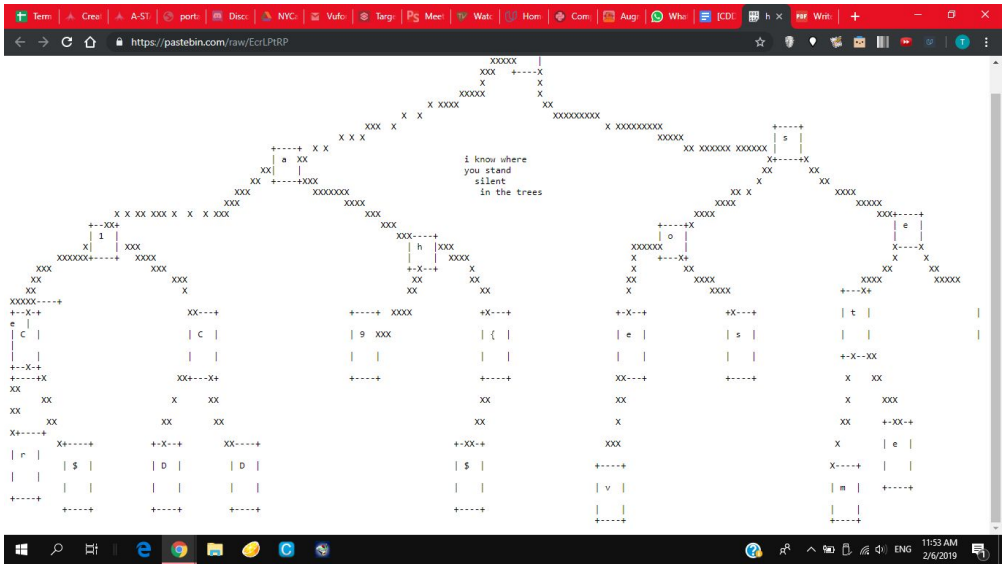
Solution

When you get the executable file, the first thing you might think of is to disassemble it. So putting it in the disassembler, you might see this section in the visual tree:



```
loc_4014BE:             ; dwContext
mov     dword ptr [esp+14h], 0
mov     dword ptr [esp+10h], 0 ; dwFlags
mov     dword ptr [esp+0Ch], 0 ; dwHeadersLength
mov     dword ptr [esp+8], 0 ; lpszHeaders
mov     dword ptr [esp+4], offset szUrl ; "https://pastebin.com/raw/EcrLPtRP"
mov     eax, [ebp+hInternet]
mov     [esp], eax      ; hInternet
call    _InternetOpenUrlA@24
sub     esp, 18h
mov     [ebp+hFile], eax
cmp     [ebp+hFile], 0
jnz     loc_40158D
```

So just open the link: https://pastebin.com/raw/EcrLPtRP



Start from bottom of tree first. Move through child nodes from left up to right, then to parent node

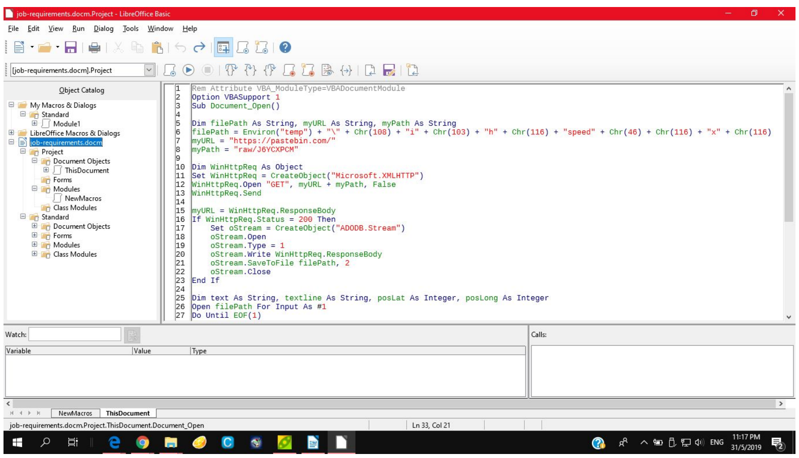
Flag

$CDDC19${havesometrees}

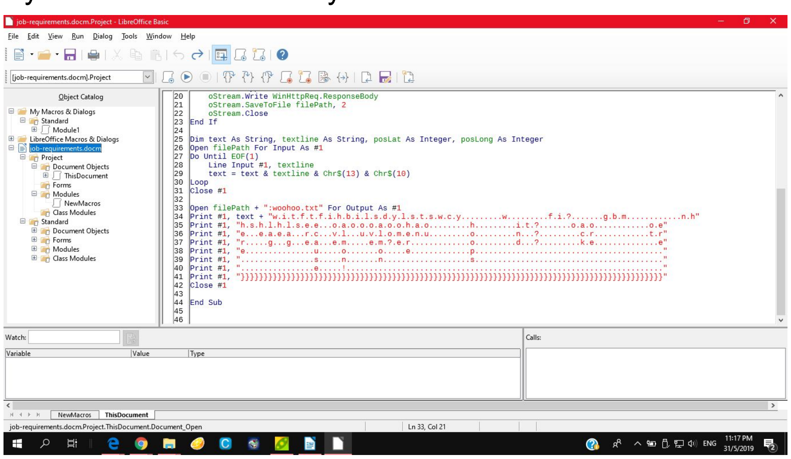
[B-2] I <3000 PHISH

Solution

Looking at the macros code in the docm file, you will notice a https://pastebin.com/raw/J6YCXPCM url



If you scroll further down you will also notice a section of text



Piece them together and you get this:

```
.............TTTTTTTTTTTTTTTTTT..........................A............................SAD...
.............HHHHHHHHHHHHHHHHHH.............................................................
.............EEEEEEEEEEEEEEEEEE.............................................................
......................................................Q...........A.........................
...................FFFFF....................................................................
...................LLLLL....................................................................
...................AAAA......................................D..................h...........
...................GGGG.....................................................................
.........................................................................y..................
.....................II.....................................................................
....................S.S.....................................................................
........................................................AA..................................
...............$$$$$$.$.................................................X...................
........eifbeC........C.C...................................................................
....................D.DD................................................................SS..
.....................DDD.....................................O..............................
.....................CCC....................................................................
....................1111..........................................................::........
.....................999999999877777.....................................C..................
..................$$$$$$....................................................................
{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{{
w.i.t.f.t.f.i.h.b.i.l.s.d.y.l.s.t.s.w.c.y.........w.........f.i.?.......g.b.m............n.h
h.s.h.l.h.l.s.e.e...o.a.o.o.o.a.o.o.h.a.o.........h.........i.t.?.......o.a.o............o.e
e...e.a.e.a...r.c...v.l...u.v.l.o.m.e.n.u.........o.........n...?.........c.r............t.r
r.....g...g...e.a...e.m.....e.m.?.e.r.............o.........d...?.........k.e..............e
e...............u.....o.......o.....e.............p.........................................
................s.....n.......n...................s.........................................
................e.....!.....................................................................
}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}
```

Try looking at the bottom section vertically. “What is the flag the flag is here because i love salmon! Do you love salmon too? Where can you whoops find it???? Go back more not here” Then you realise that one of the columns has the words: “THE FLAG IS $CDDC19${salmon!}”

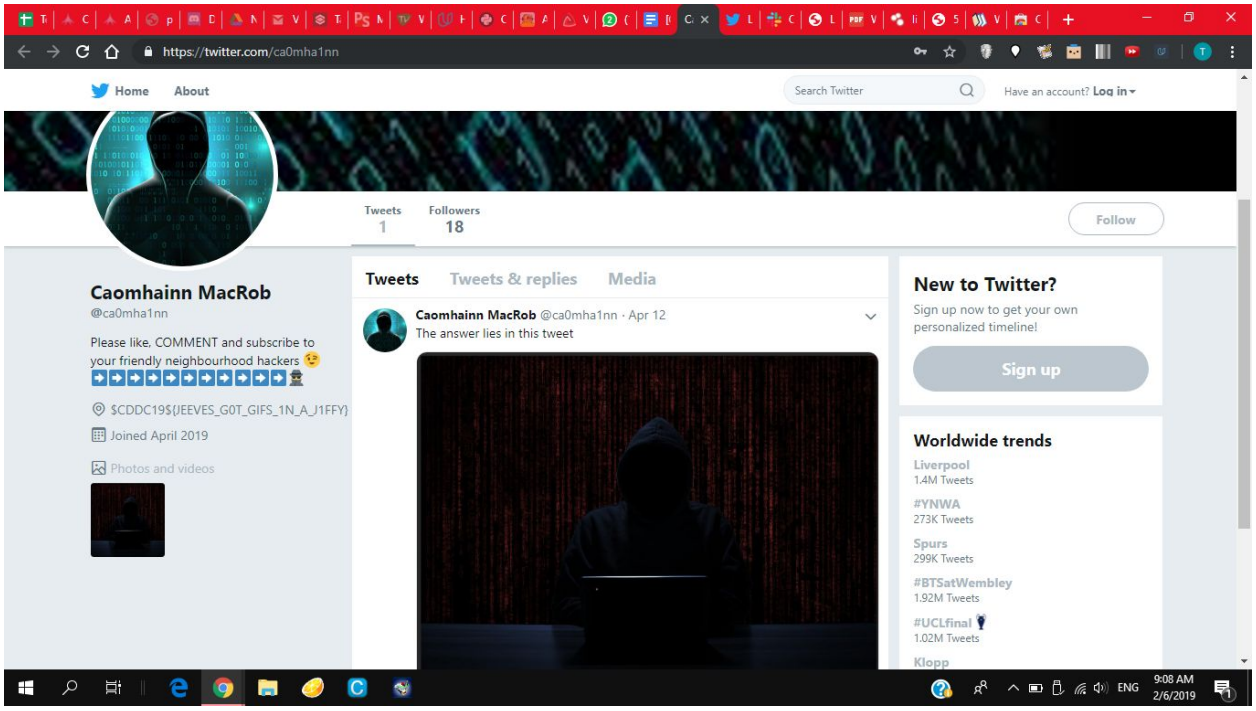
Flag

$CDDC19${salmon!}

[B-4-1] Where I Get All My GIFs From

Solution

By searching on twitter you can find the social media account of a person in the conversation (in the docm file)
https://twitter.com/ca0mha1nn



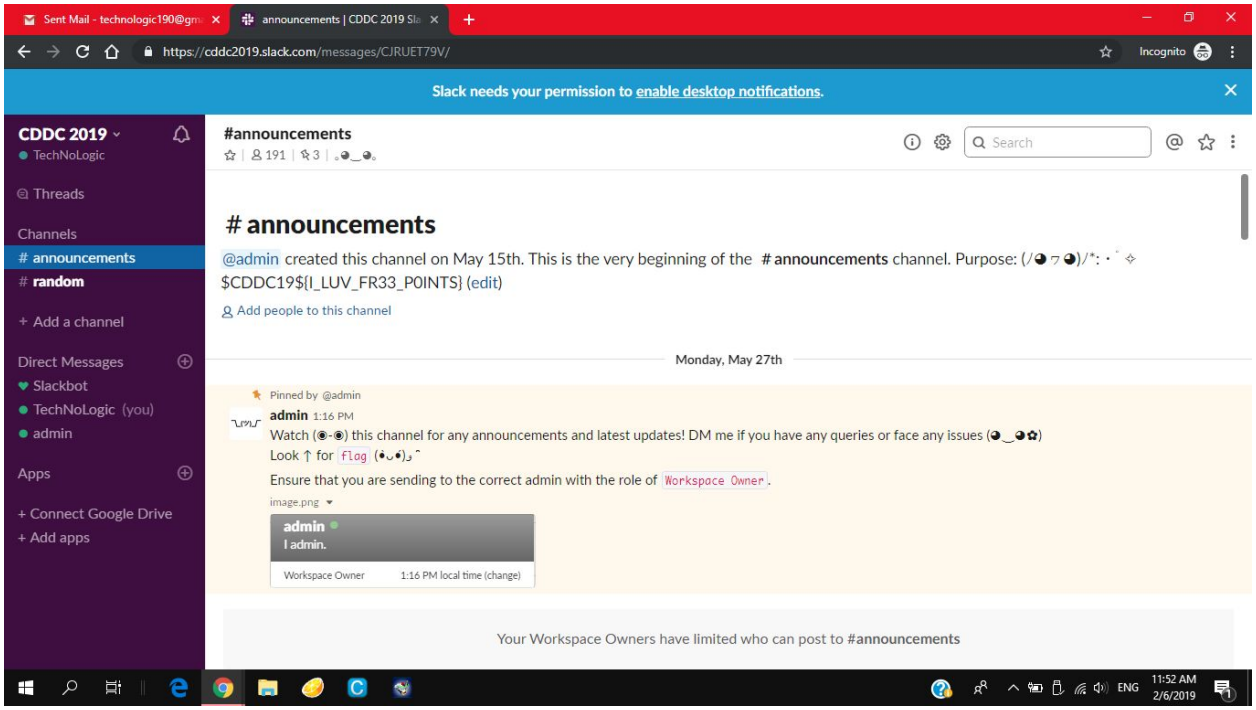
Flag

$CDDC19${JEEVES_G0T_GIFS_1N_A_J1FFY}

[Slackers, Unite!]

Solution

Get the flag from the slack channel https://cddc2019.slack.com



Flag

$CDDC19${I_LUV_FR33_P0INTS}

[Polyglot]

There are multiple languages that says’ The first character of this language creates a flag.’
Hindi
Indonesian
Chinese
Dutch
Danish
Catalan
Norwegian
Spanish
Hmong
Croatian

Flag

$CDDC19${HI~CDDC&NSHC!}

[Do you fancy numbers?]

Solution

Numbers are in Suzhou numerals.
When translated, the numbers are
36.67.68.68.67.49
.57.36.123.53.48.
95.121.48.117.95.
102.52.78.99.89.9
5.102.108.48.87.5
1.114.95.78.117.7
7.98.51.82.53.125
These values are in the ASCII table, so by converting them to ASCII, you get the flag

Flag

$CDDC19${50_y0u_f4NcY_fl0W3r_NuMb3R5}

[Very Serious Problem]

Solution

Just… do the survey?

[Count 1: Baby]

Solution

main(){int(i)=0;for(;++i<1e4;)printf(“%d,”,i);}

```
Your code : main(){int(i)=0;for(;++i<1e4;)printf("%d,",i);}
Flag : $CDDC19${Count2_is_waiting_Please_enjoy!}
```

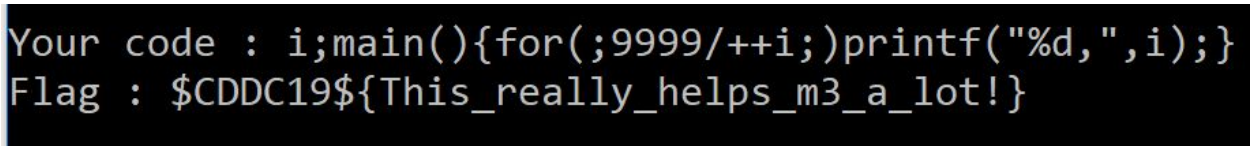
Flag

$CDDC19${Count2_is_waiting_Please_enjoy!}

[Count 2: Wildness]

Solution

i;main(){for(;9999/++i;)printf("%d,",i);}



Flag

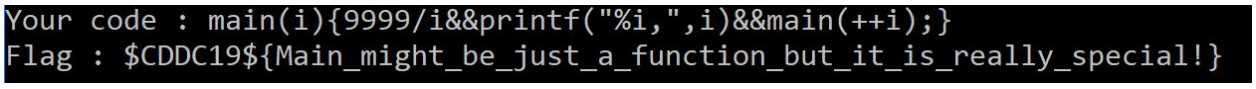
$CDDC19${This_really_helps_m3_a_lot!}

[Count 4: Madness - Filter]

Solution

A recursive implementation, so that you do not need to use for loops, and can use only the letters in “mad printf”:

main(i){9999/i&&printf("%i,",i)&&main(++i);}



Flag

$CDDC19{Main_might_be_just_a_function_but_it_is_really_special!}

Write-up

- We encourage players to submit write-ups for the challenges to gain bonus points.
- Submit your write-ups to cddc2019@nshc.net.
- All write-ups for completed challenges should be compiled into 1 single PDF document. Save this document as: "[CDDC19]-TEAM_NAME.pdf".

- The mail subject should be the same as the submitted PDF file. e.g. "[CDDC19]-TEAM_NAME".
- If there are any mistakes in the file name and/or mail subject header, we will consider the submission as void.
- You will receive an acknowledgement email from the organiser when your email and write-up document has been verified to be in the correct format.
- Only one team representative is required to submit this PDF document using your CDDC registered email.
- Only the last submission before the deadline will be considered.
- The deadline for submission is 2nd June 2019, Sunday, 23:59.
- Write-up for a particular challenge is only valid if the team has submitted the correct flag for that challenge during game time (i.e. between 31st May 2019 10:00 to 2nd June 2019 10:00).
- Write-ups will be counted per team, not per player. Bonus points awarded will be fixed at up to 5% of the respective challenge (based on dynamic scoring), depending on the quality of the write-up.
e.g. 1000 points challenge => team received 766 points due to dynamic scoring => writeup gives a maximum of 38.3 bonus points.
- If two or more teams have the same number of points, we will rank according to the timestamp in which the email write-up was received by the organiser.
- You are free to publish your write-ups on the Internet, but you may only do so after 2nd June 2019, Sunday, 23:59.
- You can find a sample write up format here (https://drive.google.com/file/d/1NNJwHpC0TLFpsNEftwAxT88wqO_ZwxMP/view).