Cyber Defenders Discovery Camp 2019

Qualifiers Write-Up

Category: JCIPITE

Team Name: QWERTY

[R-0] Everyone <3 Fan Mail

Solution:

Step 1: We did a whois lookup on the domain and found the registrar's website.
Step 2: Afterwards, we did a whois lookup on the registrar's website to find more information.
Step 3: We emailed the registrant email as a fan and the auto reply is the flag.

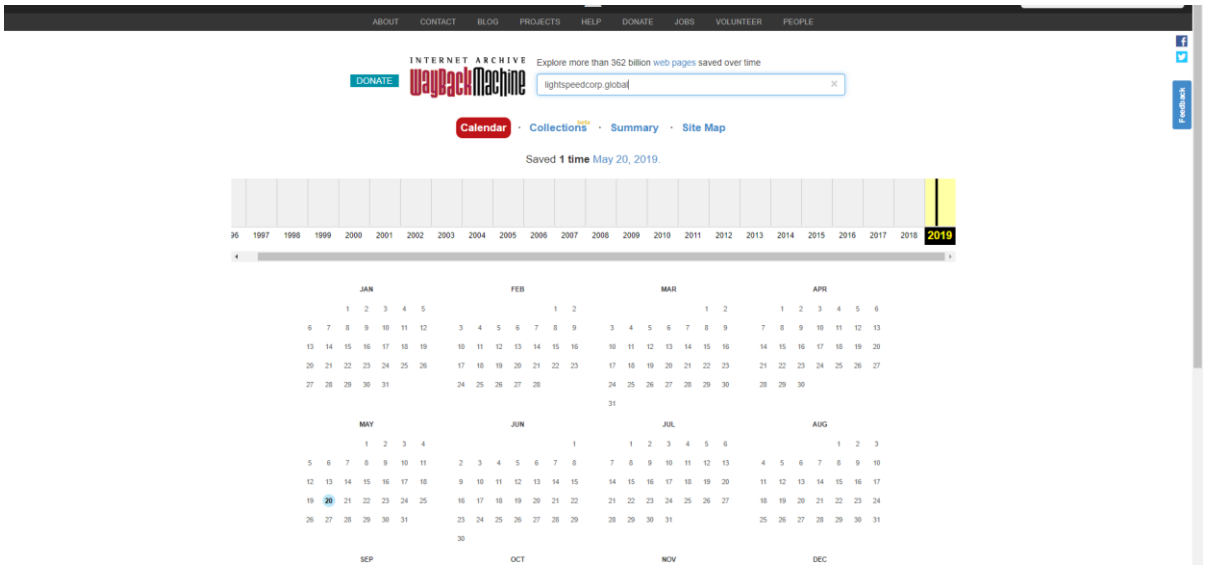
Flag: $CDDC19${IS_IT_I_AM_FAM0US_NAO}

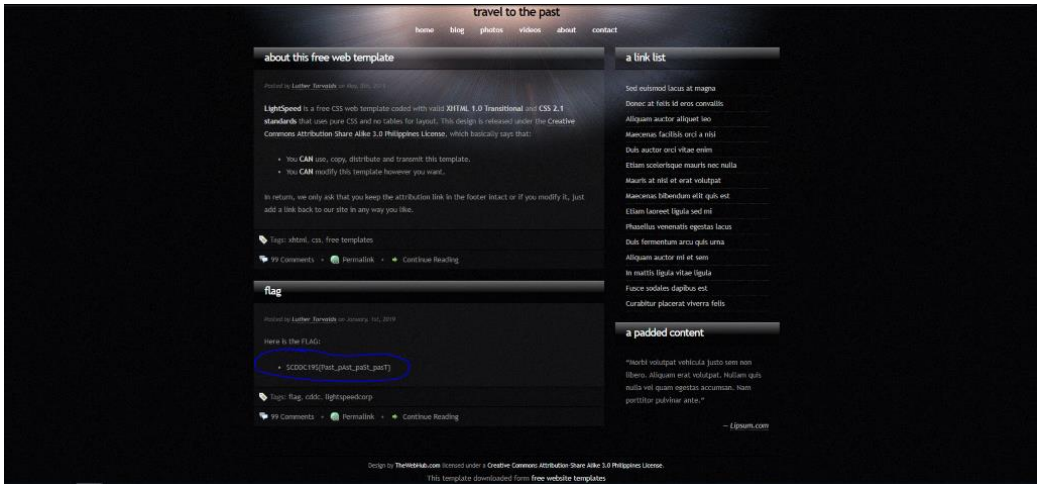
[R-1] Travel to the Past

Solution:

Step 1: We went to https://archive.org/ and type in lightspeedcorp.global

Step 2: Click on the date that is highlighted by the site to view what was captured from lightspeedcorp.global during the given time period



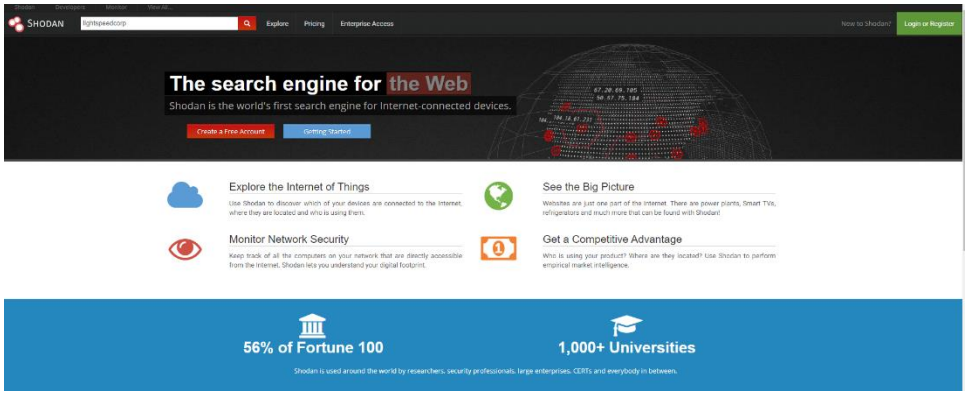


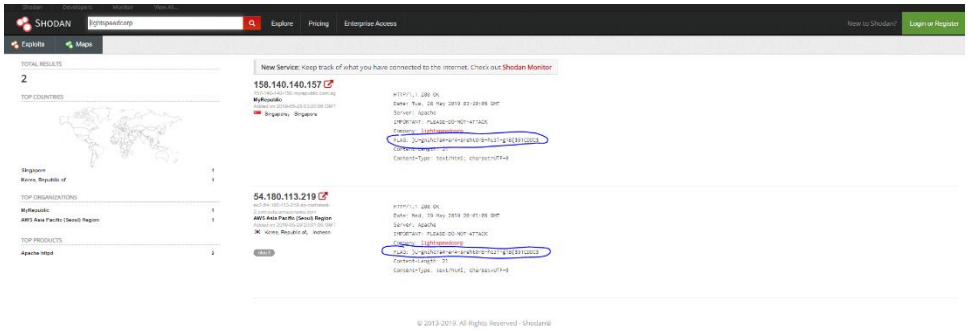
Flag: $CDDC19${Past_pAst_paSt_pasT}

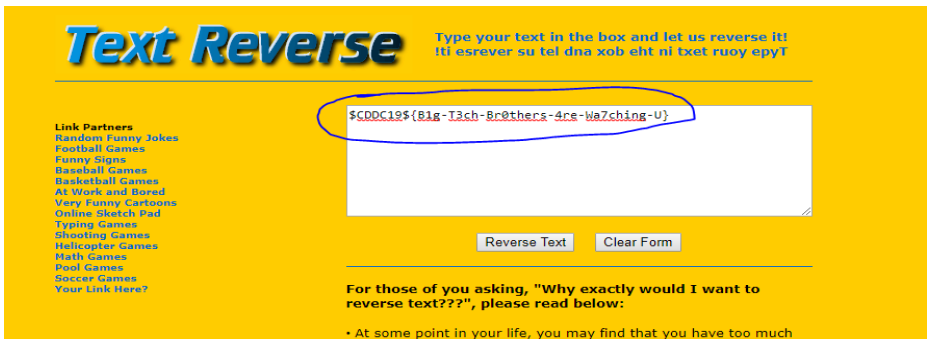
[R-2] I'm Sho Done With This

Solution:

Step 1: Go to shodan.io and search for lightspeedcorp
Step 2: There will be a flag display reversed.
Step 3: We used a online text reverser (https://www.textreverse.com/) to reverse the text to get the flag.







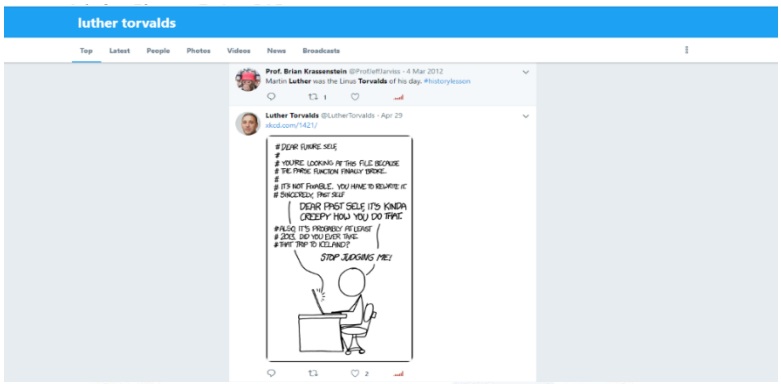
Flag: $CDDC19${B1g-T3ch-Br0thers-4re-Wa7ching-U}

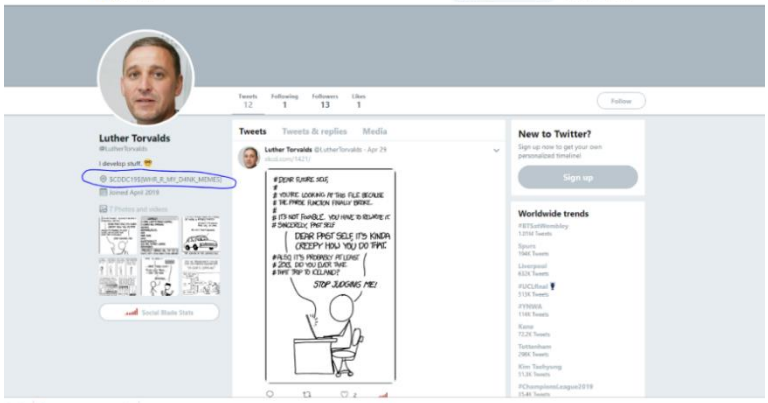
[R-4-1] Where I Get All My Memes From

Solution:

Step 1: We used information from R-0, namecheap.com, to find the admin's name.
Step 2: Search for the admin on the 3 social media giants. (Twitter,Facebook and Instagram)
Step 3: The flag can be seen in the admin's twitter bio.

```
"Domain name: lightspeedcorp.global
Registry Domain ID: D42550000010103369 3-AGRS
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2019-04-05T05:00:44.00Z
Creation Date: 2019-04-05T05:00:44.00Z
Registrar Registration Expiration Date: 2020-04-05T05:00:44.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Registry Registrant ID:
Registrant Name: Luther Torvalds
Registrant Organization: LightSpeedCorp
Registrant Street: Add 1 Add 2
Registrant City: Singapore
Registrant State/Province: NA
Registrant Postal Code: 123456
Registrant Country: SG
Registrant Phone: +65.62353535
Registrant Phone Ext: 213
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Luther.Torvalds@outlook.com
Registry Admin ID:
Admin Name: Luther Torvalds
Admin Organization: LightSpeedCorp
Admin Street: Add 1 Add 2
Admin City: Singapore
Admin State/Province: NA
Admin Postal Code: 123456
Admin Country: SG
Admin Phone: +65.62353535
```





Flag: $CDDC19${WHR_R_MY_D4NK_MEMES}

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

Solution:

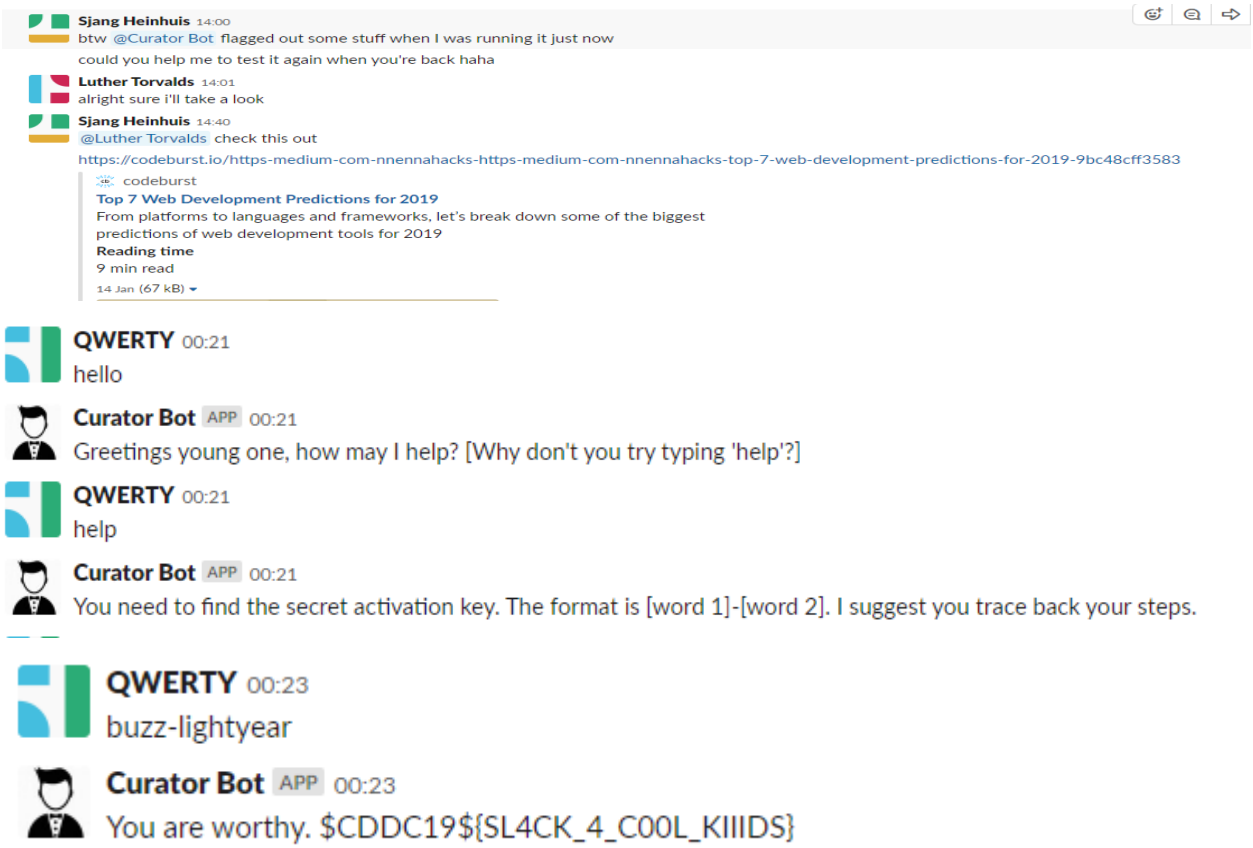
Step 1: We took a look around Luther Torvald's Twitter and we saw a conversation between him and Sjang Heinhuis. We took a closer look at his profile(Sjang Heinhuis) and found a picture of a helmet with a whiteboard in the background and a link on it. (bit.ly/lightspeedcorp)

Step 2: We went to the website and it redirected us to join a slack group.

Step 3: In the slack group, a conversation between Sjang Heinhuis and Luthor Torvalds can be seen and in one of the messages Sjang Heinhuis mentions the Curator Bot which was also mentioned in their conversation on twitter which only star command members have access to.

Step 4: We messaged the bot and it asked for a secret activation key with 2 words.

Step 5: We tried keying in "buzz-lightyear" as we searched up star command and multiple images with buzz lightyear came up. There was also a user named "ame26536075" who tagged Luther Torvalds in a post with #starcommand and #buzzlightyear.



Flag: $CDDC19${SL4CK_4_C00L_KIIIDS}

[R-4-1-2] Don't Be A Git

Solution:

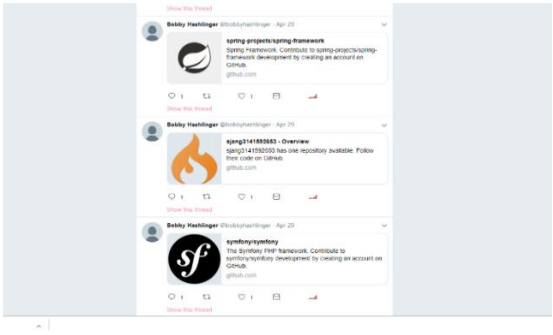
Step 1: We went to the Admin's twitter and found a conversation with someone else.
Step 2: After taking a look at the other user he was talking to, we found that he liked a few Github pages on twitter.

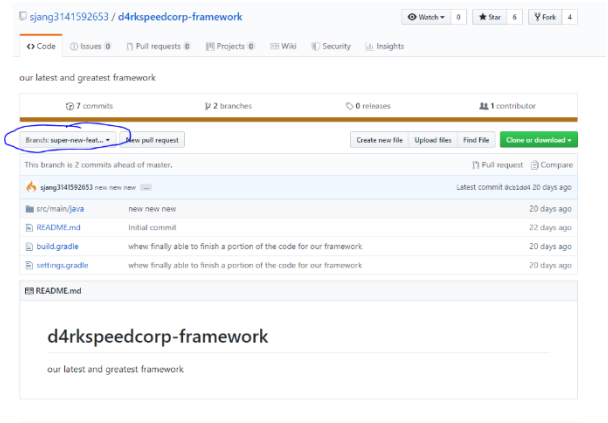
Step 3: We browsed through the liked pages and found one called "d4rkspeedcorp-framework".

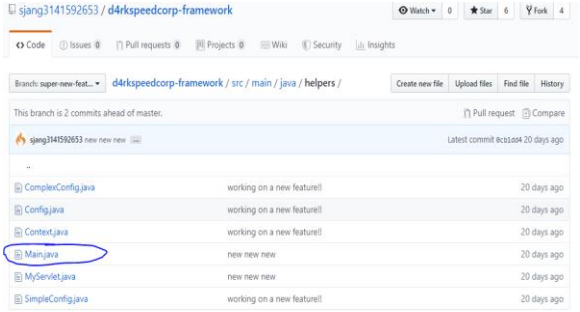
Step 4: We found a branch called "super-new-feature" in "d4rkspeedcorp-framework" and took a look around in it.

Step 5: Found the flag inside main.java but it was flipped so we used a online text flipper(http://www.upsidedowntext.com/) to flip the text.

Step 6: We couldn't flip the text (C, D and T) completely so we replaced the characters manually and the flag was able to be submitted.







sjang3141592653 new new new 0cb1dd4 20 days ago

1 contributor

66 lines (54 sloc) | 1.32 KB Raw Blame History

```
rs;

ted.*;
til.concurrent.ExecutorService;
til.concurrent.Executors;

Main

c static void main(String[] args) throws Exception {
   long count = Long.MAX_VALUE;
   long waitMillis = 1000;
   long startSleep = 0;

   if (args.length > 0) {
           count = parseInt(args[0], count);

           if (args.length > 1) {
                   waitMillis = parseInt(args[1], waitMillis);

                   if (args.length > 2) {
                           startSleep = parseInt(args[2], startSleep);
                   }
           }
   }

   System.out.println("ehehehehe inserting a sneaky little comment here I wonder if anyone can find it{ʇʎʇʇǝʍ_ʇǝʃ_ɟo_ʎuɐ_ʎuo_ɟuɐɟ_ʎɐʍ_ʎǝʞ_ʎuɐ_ʎǝʞ_ʎuɐ_ʎǝʞ$CDDC19$}");

   try
   {
```

UpSideDOWNTextt.com

It's almost Valentine's Day! Check out the Love Calculator to see if you're compatible.

Type text, words, letters, or symbols here: 39

$CDDC19${D0n7_b3_5cAr3D_0f_c0MM1tM3nT5}

Text Effects:

- ☑ Backwards Effect (Reverses text)
- ☑ Upside Down Effect (Flips text)

Post to:

Copy this text to Facebook, Twitter, YouTube, MySpace, MSN, AIM, Gmail, Word, etc:

$CDDC19${D0n7_b3_5cAr3D_0f_c0MM1tM3nT5}

View HTML

Flag: $CDDC19${D0n7_b3_5cAr3D_0f_c0MM1tM3nT5}

[B-1] Fight the Binary Monster

Solution:

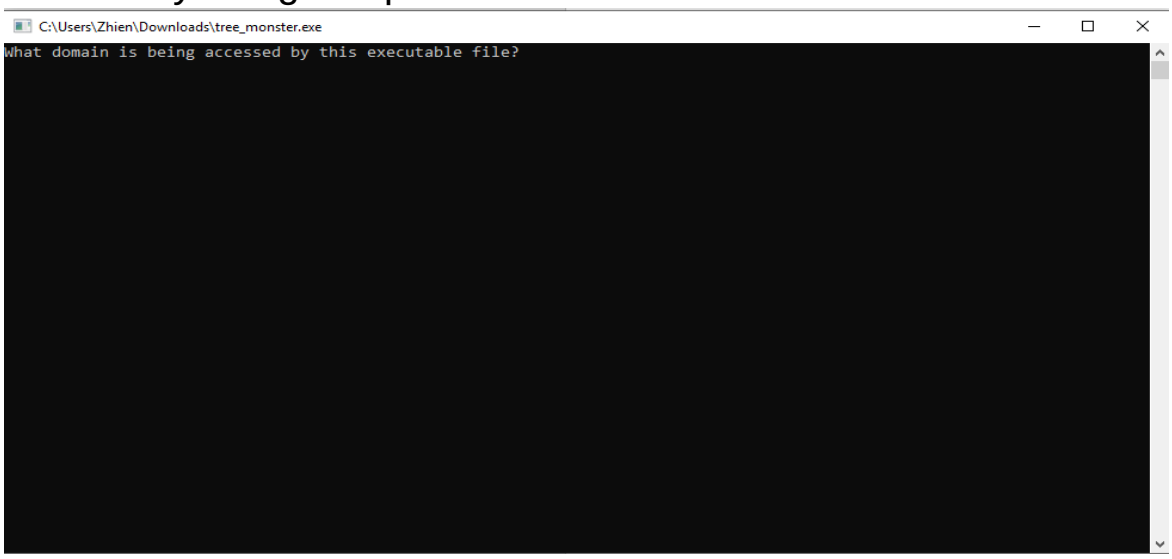
Step 1: Run tree_monster.exe and “What domain is being accessed by this executable file?” can be seen.

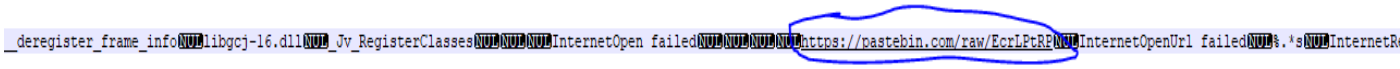
Step 2: Right click on tree_monster.exe and edit with Notepad++.

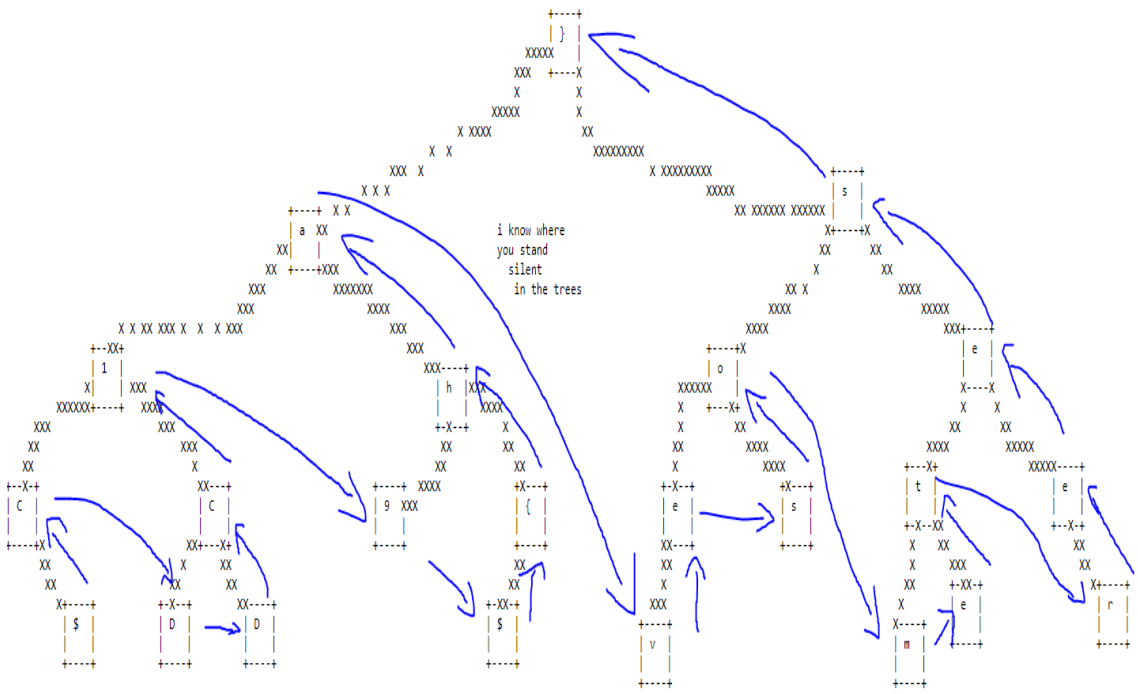
Step 3: Press ctrl + f on your keyboard to search the file. Search for “domain”

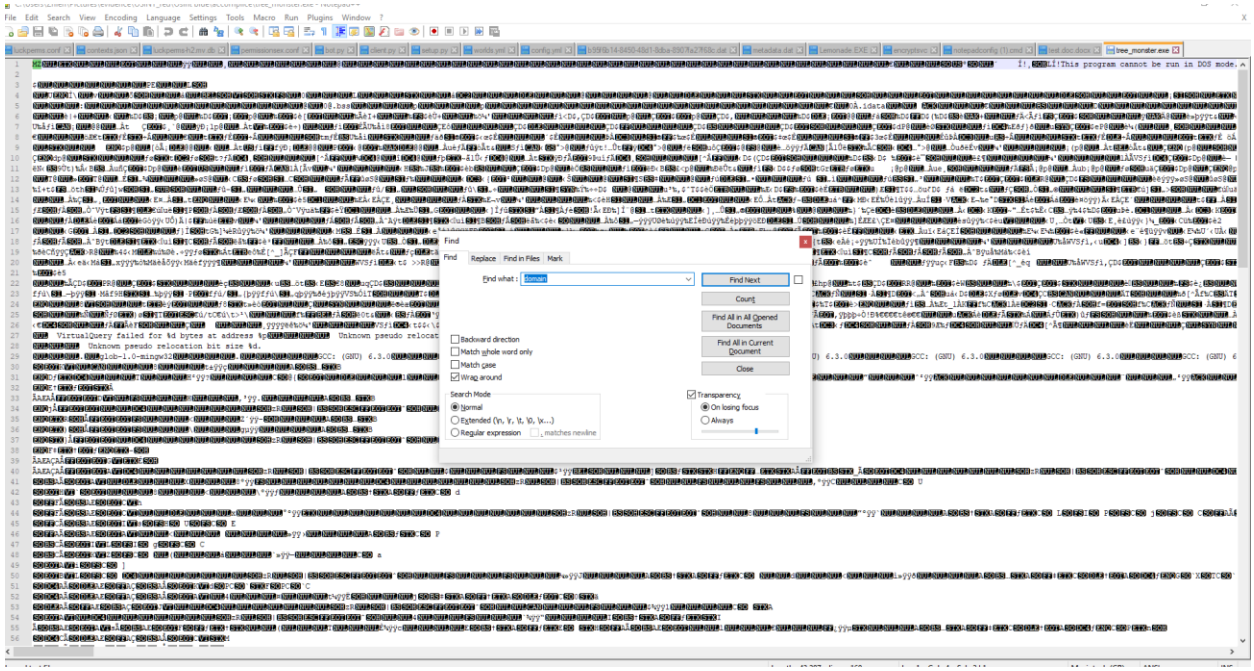
Step 4: Double click on the paste bin link. Note they may be two pastebin but the correct one is the tree as its similar to the name of the programme.

Step 5: Once inside, we can solve it by putting the words in the box together. There is a pattern from which we can see from $cddc$19{ which is up, down, right(only if there is a box beside it), up, up, down, right, up. Only the second branch uses the furthest to the top box. So by using this pattern we can the find out the code.









Flag: $CDDC19${havesometrees}

[B-2] I <3000 PHISH

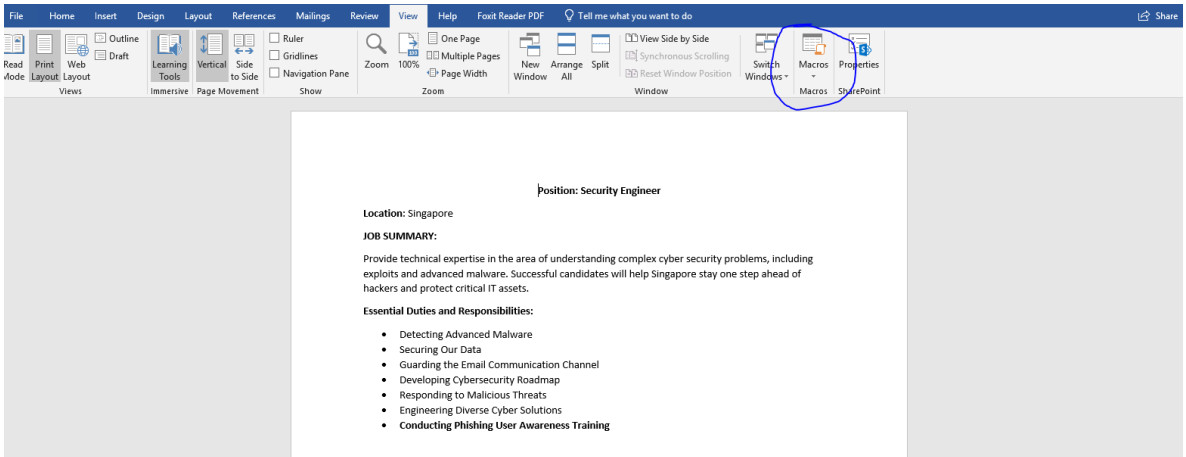
Solution:

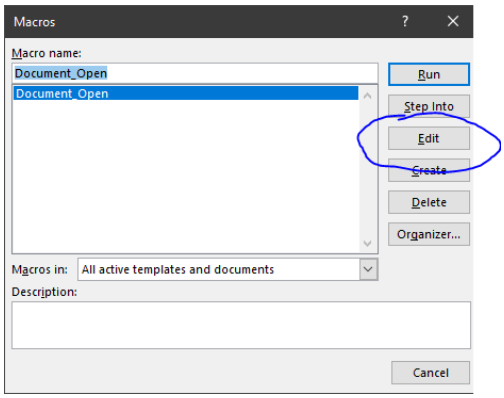
Step 1: We downloaded job-requirements.docm and opened it using Microsoft Word.

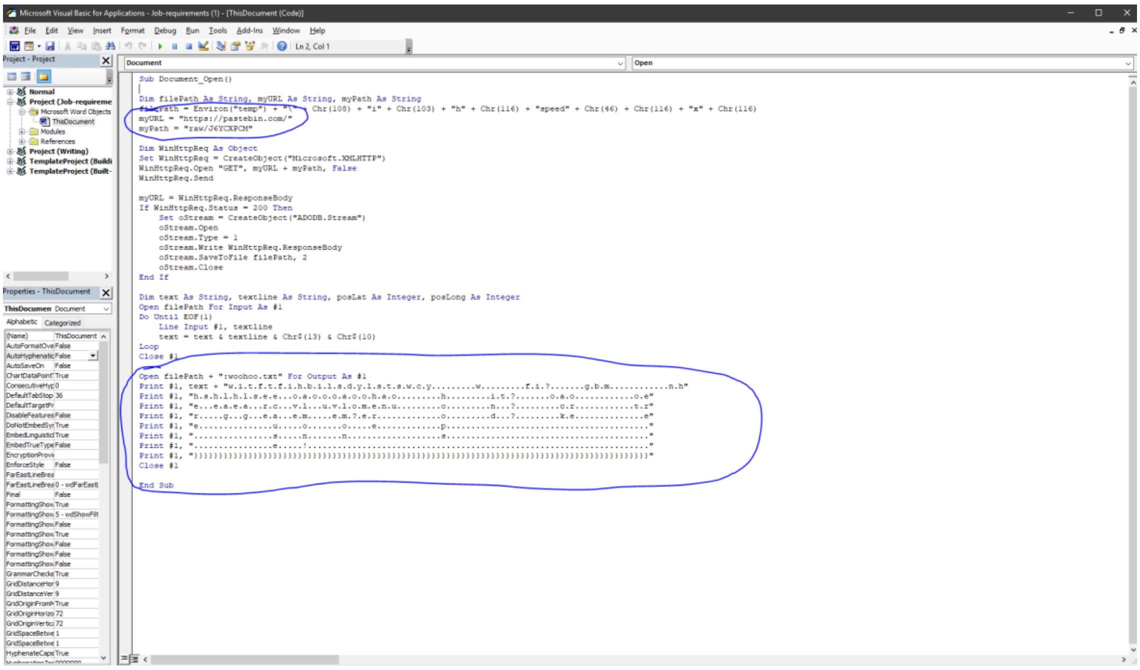
Step 2: We went to View > Macros > Edit to open Visual Basic and found a pastebin link split into 2 parts in the code. (https://pastebin.com/raw/J6YCXPCM)

Step 3: In the pastebin, we found “THE FLAG IS $CDDC19${“ typed vertically so we believed the 2nd part of the flag was hidden somewhere else.

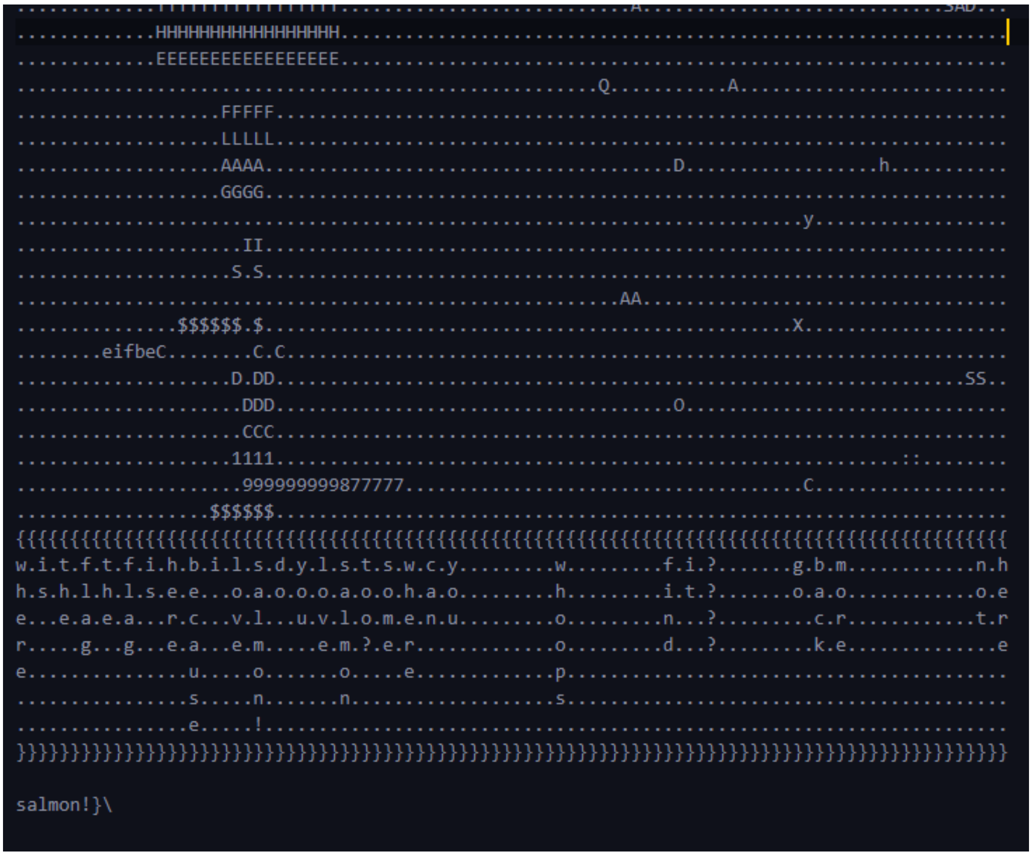
Step 4: We went back to visual basic and saw a similar pattern on the code at the bottom, we copied both sections and pasted it into a notepad to find the flag.







```
Sub Document_Open()

Dim filePath As String, myURL As String, myPath As String
filePath = Environ("temp") + "\" + Chr(108) + "i" + Chr(103) + "h" + Chr(116) + "speed" + Chr(46) + Chr(116) + "x" + Chr(116)
myURL = "https://pastebin.com/"
myPath = "raw/J6YCXPCM"

Dim WinHttpReq As Object
Set WinHttpReq = CreateObject("Microsoft.XMLHTTP")
WinHttpReq.Open "GET", myURL + myPath, False
WinHttpReq.Send

myURL = WinHttpReq.ResponseBody
If WinHttpReq.Status = 200 Then
    Set oStream = CreateObject("ADODB.Stream")
    oStream.Open
    oStream.Type = 1
    oStream.Write WinHttpReq.ResponseBody
    oStream.SaveToFile filePath, 2
    oStream.Close
End If

Dim text As String, textline As String, posLat As Integer, posLong As Integer
Open filePath For Input As #1
Do Until EOF(1)
    Line Input #1, textline
    text = text & textline & Chr$(13) & Chr$(10)
Loop
Close #1

Open filePath + ":woohoo.txt" For Output As #1
Print #1, text + "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"
Print #1, "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"
Print #1, "e...e.a.e.a...r.c...v.l...u.v.l.o.m.e.n.u.........o.........n...?.........c.r............t.r"
Print #1, "r.....g...g...e.a...e.m.....e.m.?.e.r.............o.........d...?.........k.e..............e"
Print #1, "e...............u.....o.......o.....e.............p........................................."
Print #1, "................s.....n.......n...................s........................................."
Print #1, "................e.....!....................................................................."
Print #1, "}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}"
Close #1

End Sub
```



```
.............HHHHHHHHHHHHHHHHH..............................................................
.............EEEEEEEEEEEEEEEEE..............................................................
......................................................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.....!.....................................................................
}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}}

salmon!}\
```

FLAG: $CDDC19${salmon!}

[B-3-1] Onion Sauce

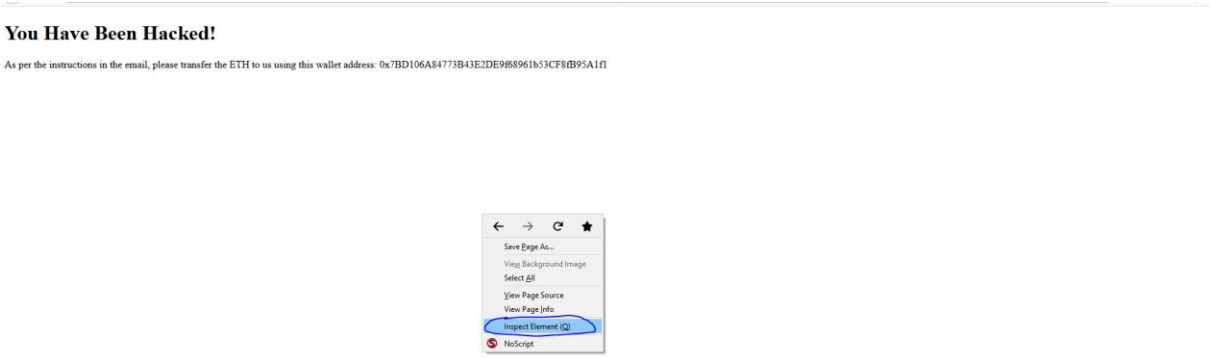
Solution:

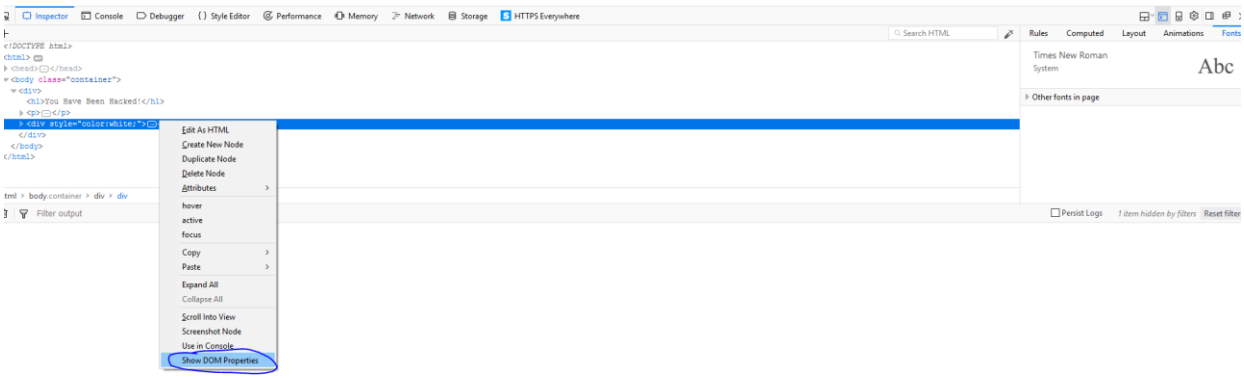
Step 1: Use Tor (https://www.torproject.org/download/) to access the .onion link.

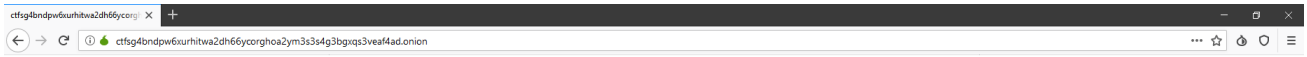
Step 2: Right click the spaces without text and select Inspect Element.

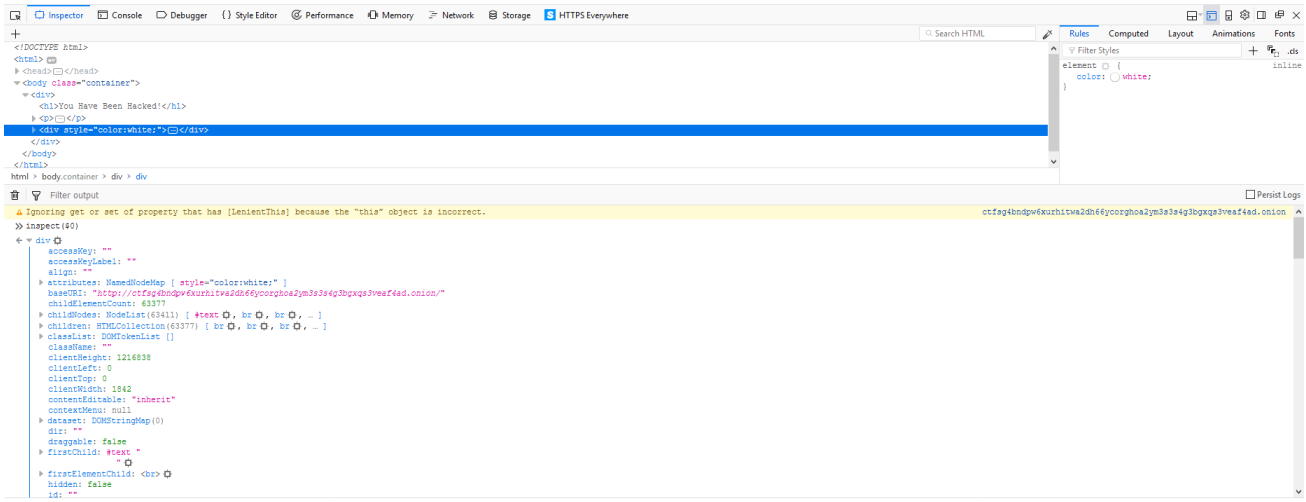
Step 3: Right click in Inspect element and select Show Dom Properties.

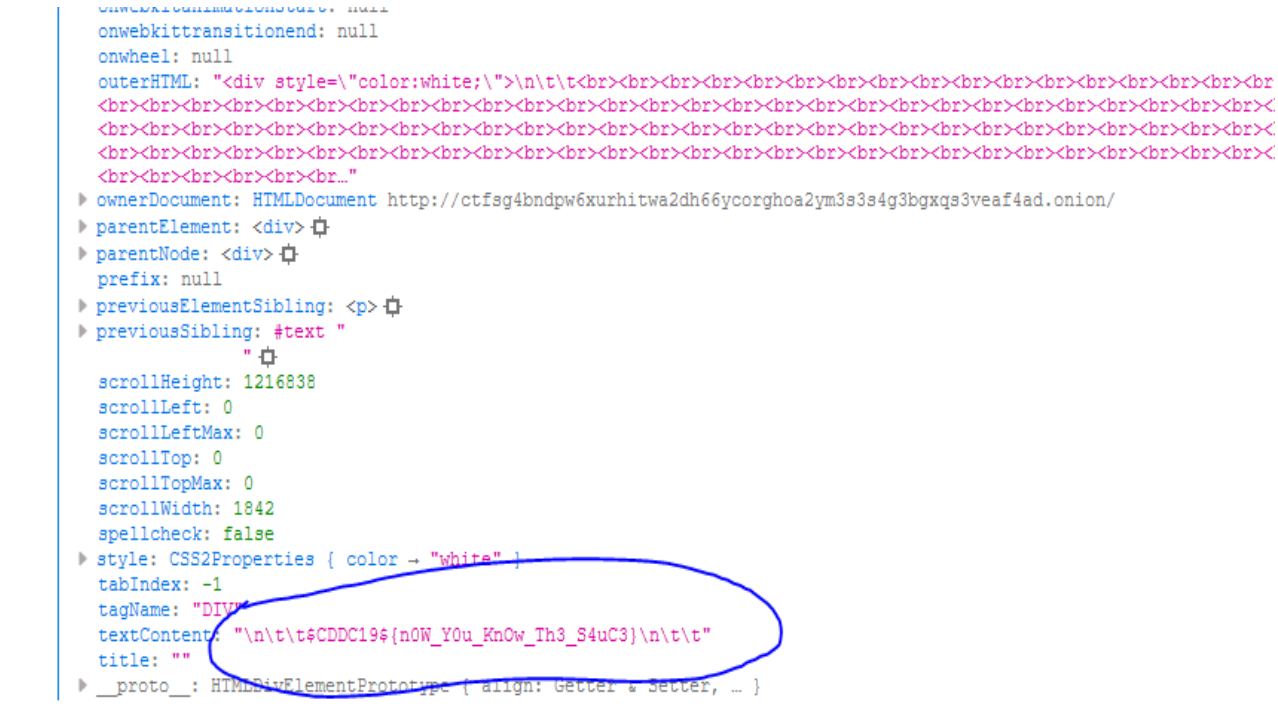
Step 4: Scroll to the bottom of Dom Properties and the flag would be there.











You Have Been Hacked!

As per the instructions in the email, please transfer the ETH to us using this wallet address: 0x7BD106A84773B43E2DE9f68961b53CF8fB95A1f1

```
<!DOCTYPE html>
<html>
  <head>…</head>
  <body class="container">
    <div>
      <h1>You Have Been Hacked!</h1>
      <p>…</p>
      <div style="color:white;">…</div>
    </div>
  </body>
</html>
```

html > body.container > div > div

```
element { 
  color: white;
}
```

Filter output

```
Ignoring get or set of property that has [LenientThis] because the "this" object is incorrect.    ctfsg4bndpw6xurhitwa2dh66ycorghoa2ym3s3s4g3bgxqs3veaf4ad.onion
>> inspect($0)
<- div
     accessKey: ""
     accessKeyLabel: ""
     align: ""
   ▶ attributes: NamedNodeMap [ style="color:white;" ]
     baseURI: "http://ctfsg4bndpw6xurhitwa2dh66ycorghoa2ym3s3s4g3bgxqs3veaf4ad.onion/"
     childElementCount: 63377
   ▶ childNodes: NodeList(63411) [ #text, br, br, … ]
   ▶ children: HTMLCollection(63377) [ br, br, br, … ]
   ▶ classList: DOMTokenList []
     className: ""
     clientHeight: 1216838
     clientLeft: 0
     clientTop: 0
     clientWidth: 1842
     contentEditable: "inherit"
     contextMenu: null
   ▶ dataset: DOMStringMap(0)
     dir: ""
     draggable: false
   ▶ firstChild: #text "
               "
   ▶ firstElementChild: <br>
     hidden: false
     id: ""
```

```
     onwebkittransitionend: null
     onwheel: null
     outerHTML: "<div style=\"color:white;\">\n\t\t<br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br
     <br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><
     <br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><
     <br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><br><
     <br><br><br><br><br><br…"
   ▶ ownerDocument: HTMLDocument http://ctfsg4bndpw6xurhitwa2dh66ycorghoa2ym3s3s4g3bgxqs3veaf4ad.onion/
   ▶ parentElement: <div>
   ▶ parentNode: <div>
     prefix: null
   ▶ previousElementSibling: <p>
   ▶ previousSibling: #text "
                  "
     scrollHeight: 1216838
     scrollLeft: 0
     scrollLeftMax: 0
     scrollTop: 0
     scrollTopMax: 0
     scrollWidth: 1842
     spellcheck: false
   ▶ style: CSS2Properties { color → "white" }
     tabIndex: -1
     tagName: "DIV"
     textContent: "\n\t\t$CDDC19${n0W_Y0u_KnOw_Th3_S4uC3}\n\t\t"
     title: ""
   ▶ __proto__: HTMLDivElementPrototype { align: Getter & Setter, … }
```

Flag: $CDDC19${n0W_Y0u_KnOw_Th3_S4uC3}

[B-3-2] When Your ZIL Turns to NIL :’(

Solution:

Step 1: Go to the .onion link from the previous question using Tor

Step 2: Copy the ETH address in the .onion address

Step 3: Go to Etherscan(https://etherscan.io/) and paste the address in.

Step 4: Click on the first “From” address at the bottom and copy the address

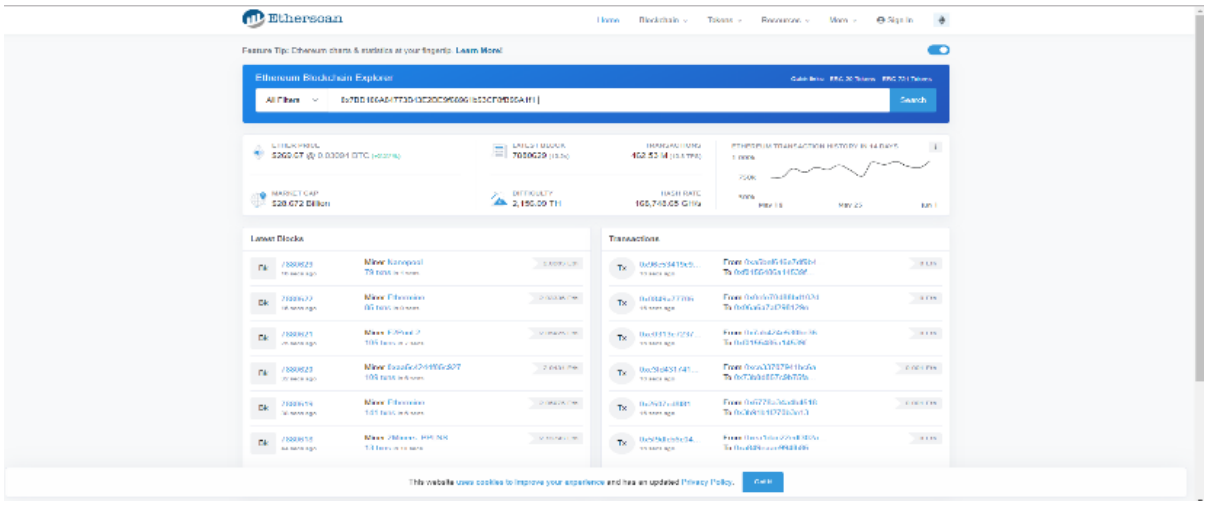
Step 5: Paste the address and capitalize everything except the first “x”

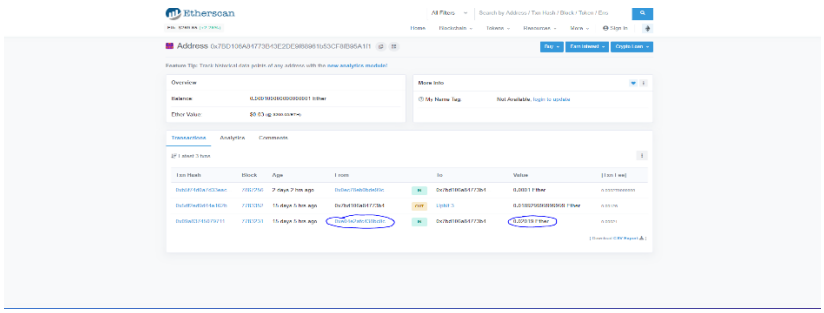
Step 6: Go back to Etherscan and copy the first ETH value at the bottom

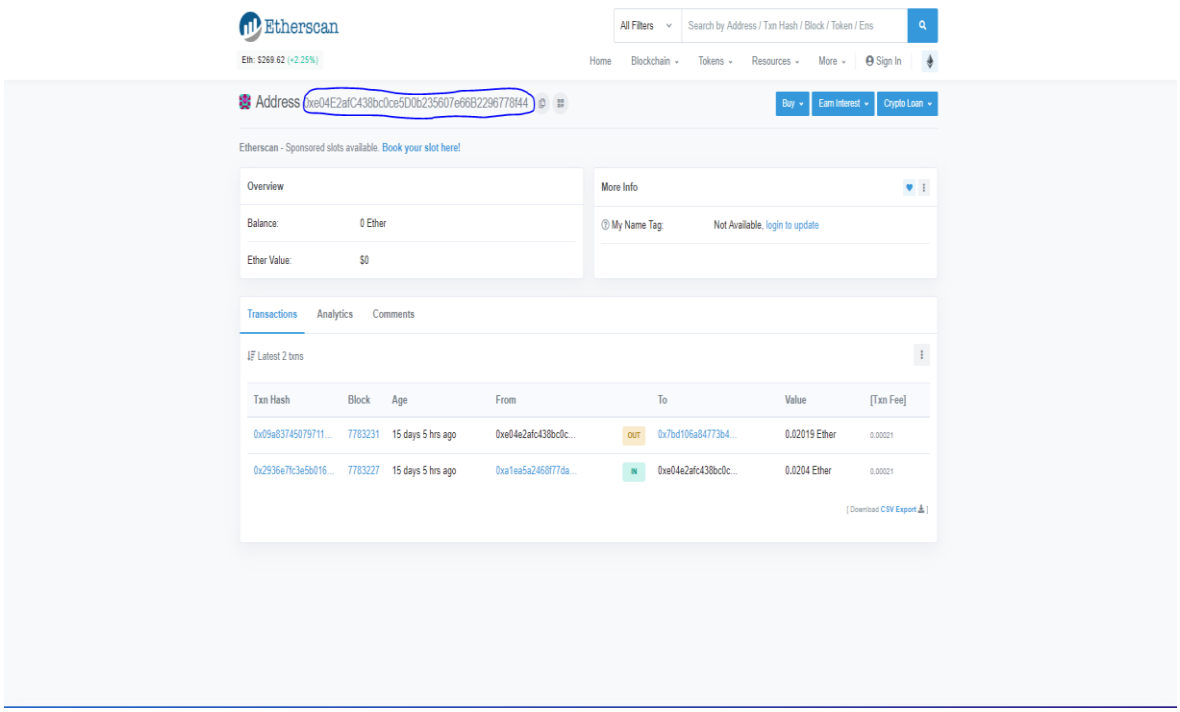
Step 7: The flag format is CapitalizedAddress_ETHValue.

You Have Been Hacked!

As per the instructions in the email, please transfer the ETH to us using this wallet address: 0x7BD106A84773B43E2DE9f68961b53CF8fB95A1f1








```
0xe04E2afC438bc0ce5D0b235607e66B2296778f44

0xE04E2AFC438BC0CE5D0B235607E66B2296778F44_0.02019
```

Flag: $CDDC19${0xE04E2AFC438BC0CE5D0B235607E66B2296778F44_0.02019}

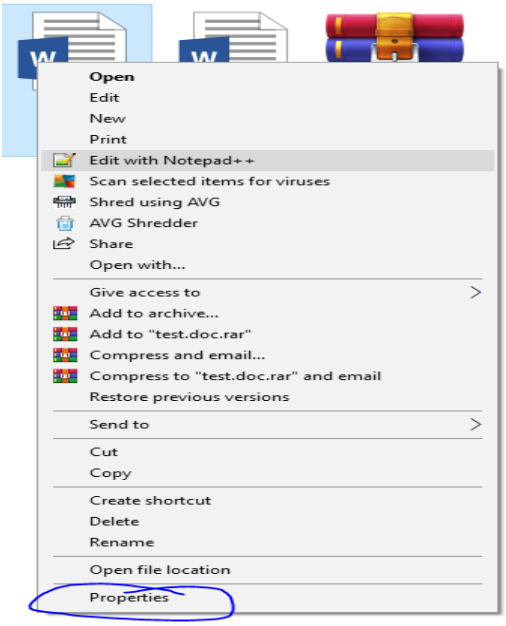
[B-4-1] Where I Get All My GIFs From

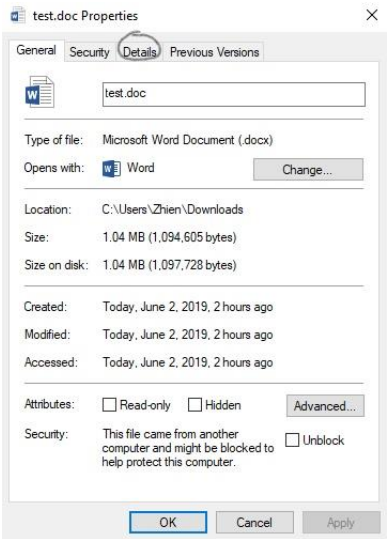
Solution:

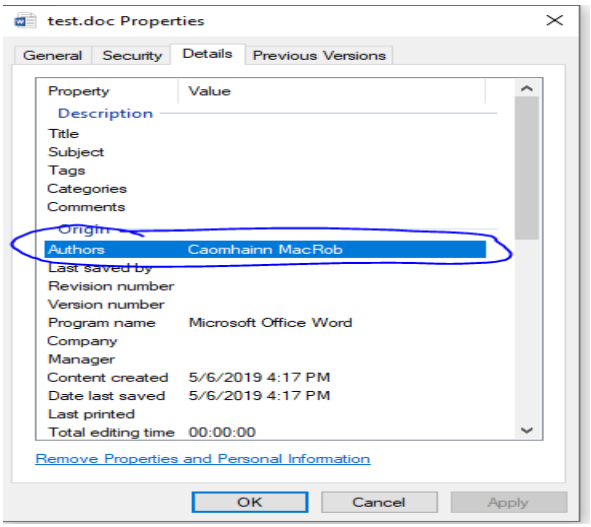
Step 1: Right click on the test.docx file and click on properties.

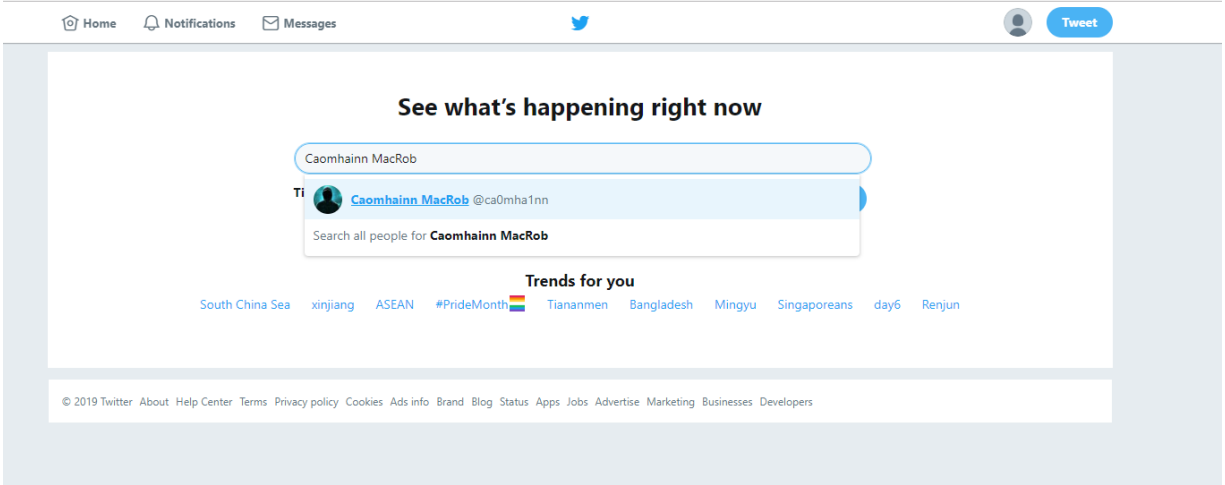
Step 2: Once the properties windows pops up, go to details, and u would see the hacker's name under the author section.

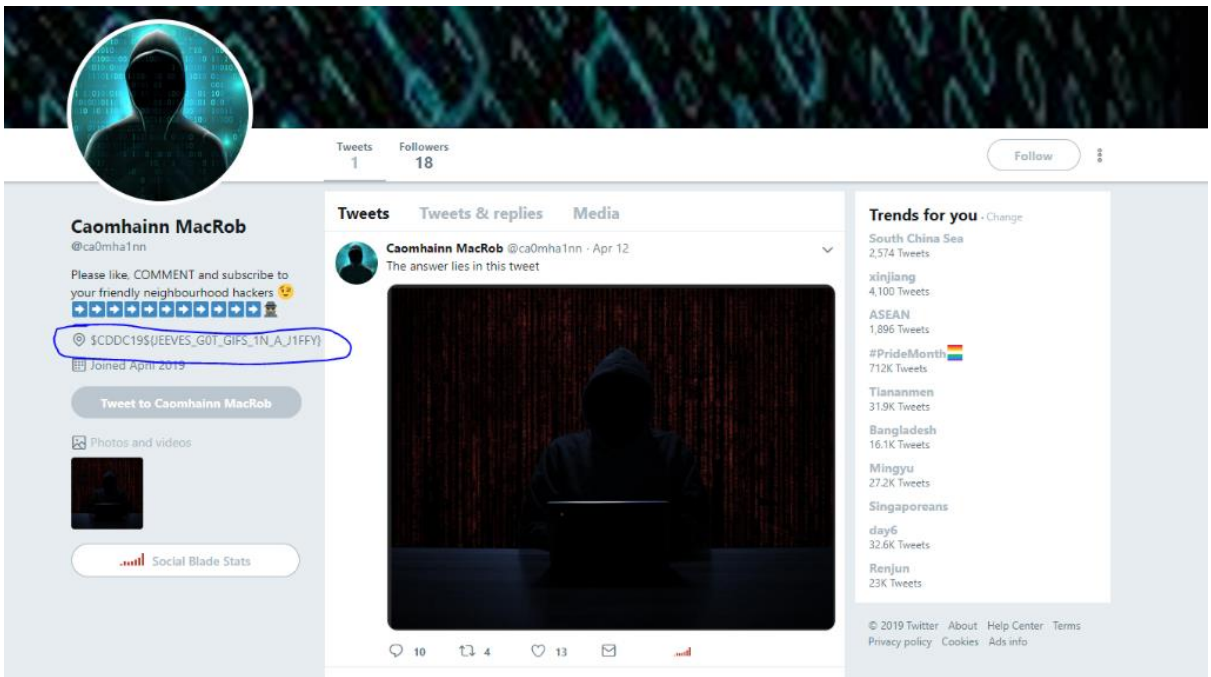
Step 3: We went to social media platforms to find out more about the hacker, and we found the flag as shown in the bio of the hacker's twitter profile.











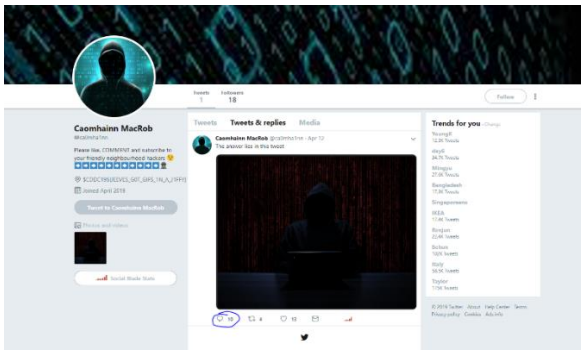
Flag: $CDDC19${JEEVES_G0T_GIFS_1N_A_J1FFY}

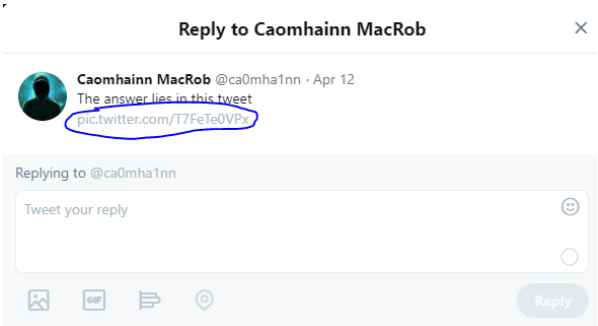
[B-4-2] Hide N Seek

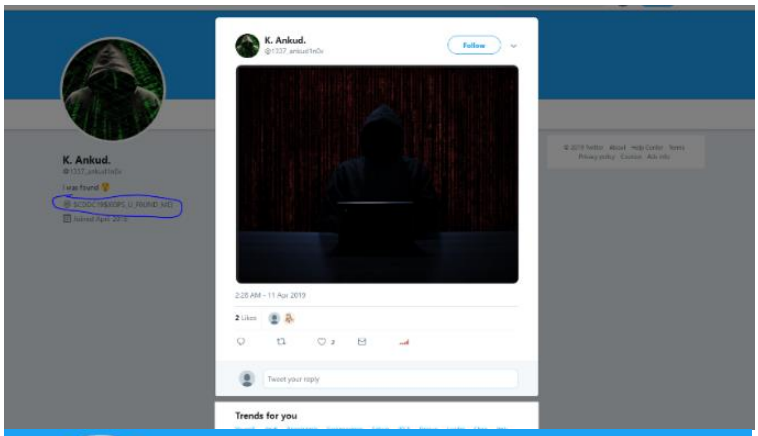
Solution:

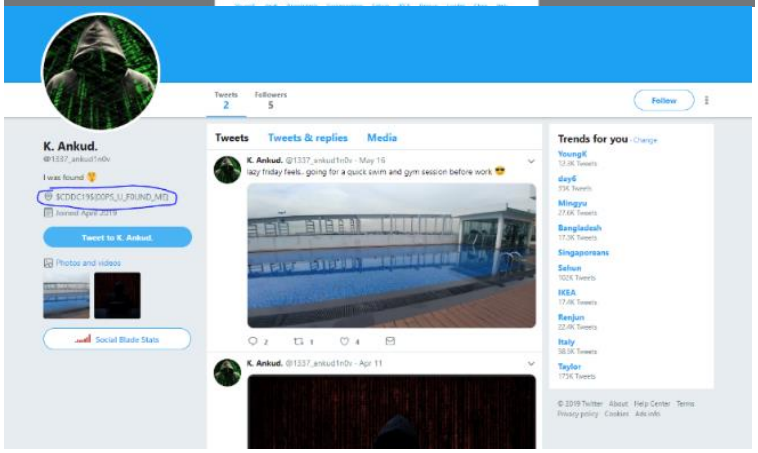
1st step: On the hacker's profile, look at the comments on his post and it would show a link.

2nd step: The link would redirect us to the hacker's accomplice where the flag would be in his bio.









Flag: $CDDC19${00PS_U_F0UND_ME}

TxT (Network)

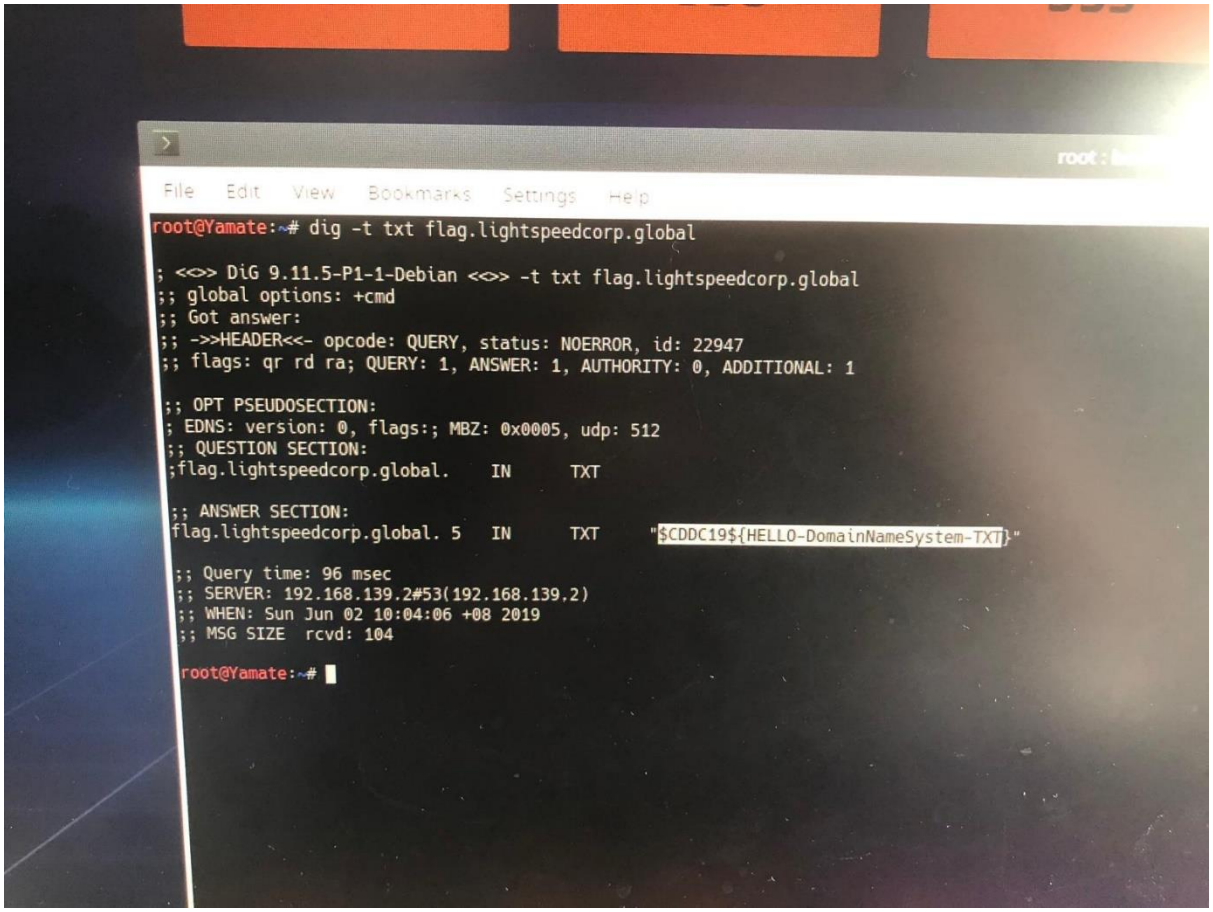
Solution:

Step 1: We opened Kali Linux's Konsole.

Step 2: We used the dig command to query information of the DNS server of the specific file.

Step 3: We then typed in 'dig -t txt flag.lightspeedcorp.global' to get the file 'txt' from the DNS server 'flag.lightspeedcorp.global'.

Step 4: The flag would be printed out.



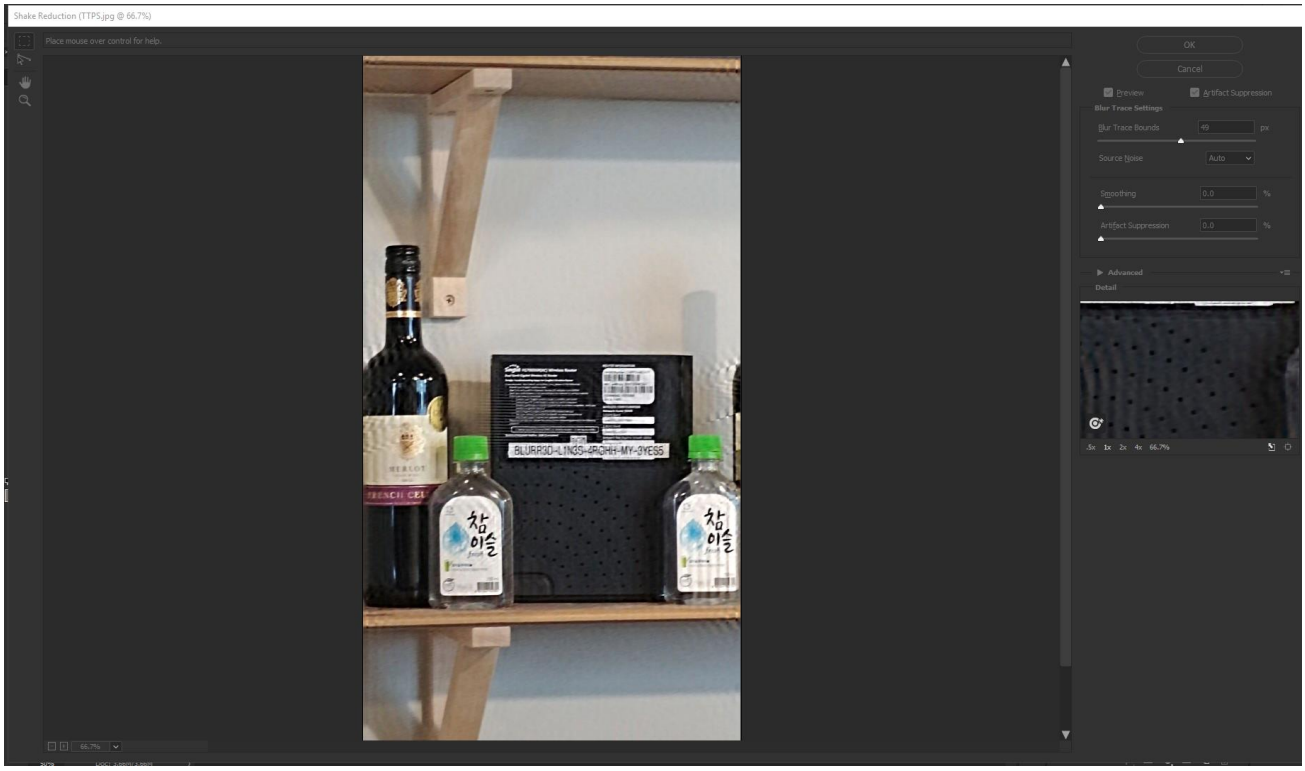
Flag: $CDDC19${HELLO-DominNameSystem-TXT}

The Terrible Photographer Strikes! (Forensics)

Solution:

Step 1: We looked at the image and we couldn't decipher what the password was, so we loaded the image into photoshop.

Step 2: We applied a Shake Reduction filter and brought the Artifact Suppression and Smoothness to 0 and we could see the flag afterwards.



Flag: $CDDC19${BLURR3D_L1N3S_4RGHH_MY_3YES5}

UnZip (Forensics)

Solution

Step 1: We downloaded the attached file (Un.Zip) into Kali Linux and used Kali Linux's Konsole, to go the directory where the file was downloaded to.

Step 2: We enter the command 'binwalk -e Un.Zip', to get a binary image that was embedded in the files or exe codes. After that, a new folder called '_Un.Zip.extracted' will also appear in the same directory as Un.Zip file.

Step 3: We went into the _Un.Zip.extracted folder.

Step 4: We went to the website: https://digital-forensics.sans.org/media/hex_file_and_regex_cheat_sheet.pdf.

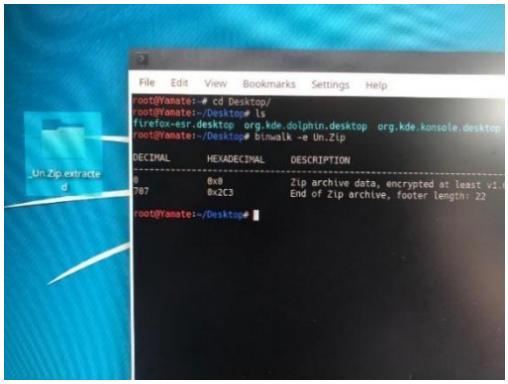
Step 5: We looked for the PNG header, '89 50 4E 47', on the website.

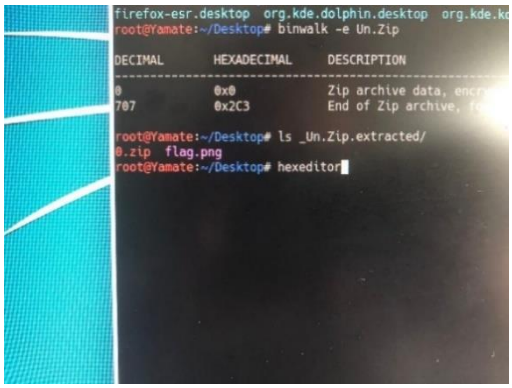
Step 6: We went to the directory, '_Un.Zip.Extracted' and opened Hexedit . After that we went into 0.Zip.

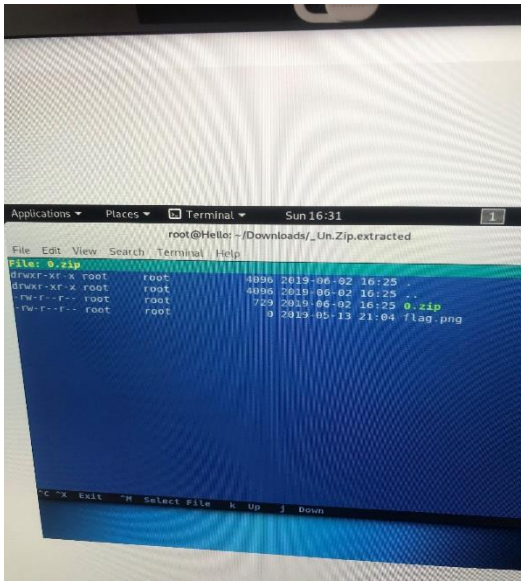
Step 7: We looked for the header 89 50 4E 47, and deleted all the hexadecimals in front of the PNG header.

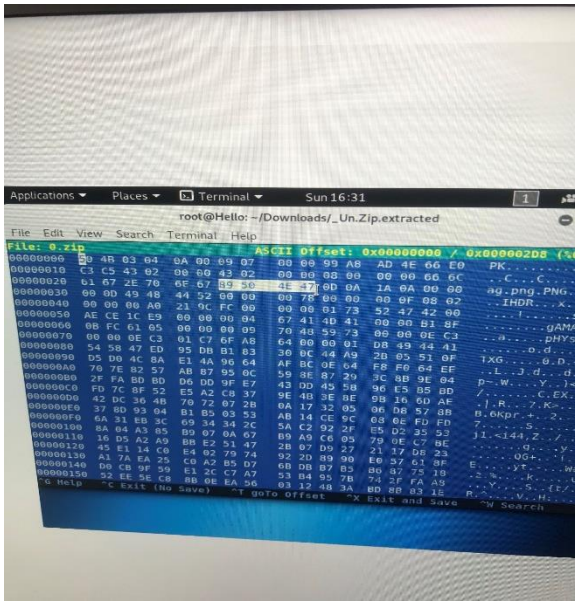
Step 8: After deleting all hexadecimals in front of the PNG header, we saved the file as a PNG file named flag.png.

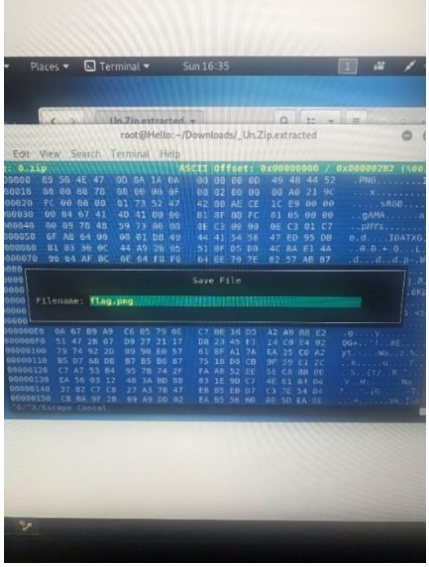
Step 9: We went into the _Un.Zip.Extracted folder and we saw a file called flag.png which is the flag.

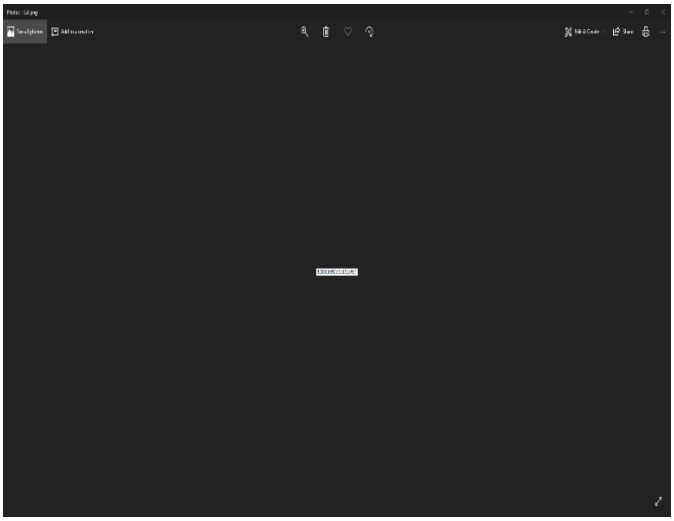












Flag: $CDDC19${zZzilipPp}

\'_'/ (WEB)

Solution:

Step 1: We went to the link and copied the second last string of the code.

Step 2: We opened Burp Suite (https://portswigger.net/burp) and created a temporary project, then went to the “Decode” tab and pasted the string in.

Step 3: Set the Encode as URL.

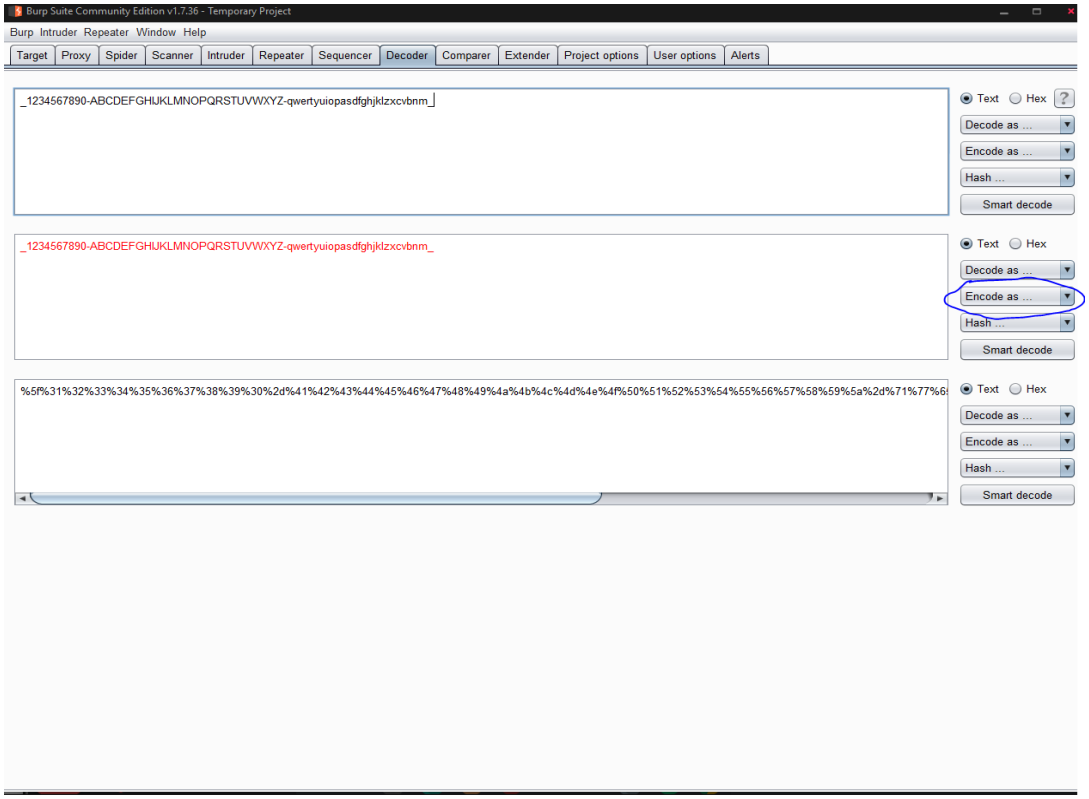
Step 4: We copied the string and put it behind the URL after inserting a “?” into the back of the link .

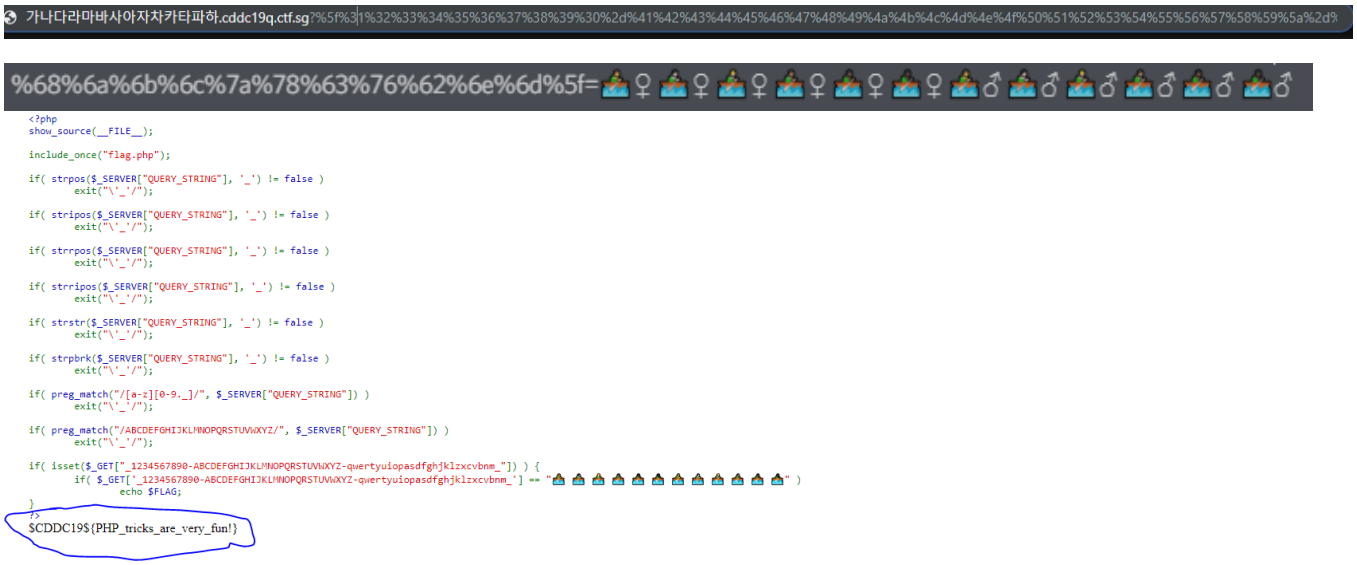
Step 5: We copied the emojis and pasted it behind the new URL after inserting a “=” at the back.

Step 6: Entered the URL and the flag appeared at the bottom of the code.

(http://가나다라마바사아자차카타파하.cddc19q.ctf.sg?[INSERTED STRING HERE]=[INSERTED EMOJIS HERE])

```php
<?php
show_source(__FILE__);

include_once("flag.php");

if( strpos($_SERVER["QUERY_STRING"], '_') != false )
        exit("\'_'/");

if( stripos($_SERVER["QUERY_STRING"], '_') != false )
        exit("\'_'/");

if( strrpos($_SERVER["QUERY_STRING"], '_') != false )
        exit("\'_'/");

if( strripos($_SERVER["QUERY_STRING"], '_') != false )
        exit("\'_'/");

if( strstr($_SERVER["QUERY_STRING"], '_') != false )
        exit("\'_'/");

if( strpbrk($_SERVER["QUERY_STRING"], '_') != false )
        exit("\'_'/");

if( preg_match("/[a-z][0-9._]/", $_SERVER["QUERY_STRING"]) )
        exit("\'_'/");

if( preg_match("/ABCDEFGHIJKLMNOPQRSTUVWXYZ/", $_SERVER["QUERY_STRING"]) )
        exit("\'_'/");

if( isset($_GET["_1234567890-ABCDEFGHIJKLMNOPQRSTUVWXYZ-qwertyuiopasdfghjklzxcvbnm_"]) ) {
        if( $_GET["_1234567890-ABCDEFGHIJKLMNOPQRSTUVWXYZ-qwertyuiopasdfghjklzxcvbnm_"] == "📤📤📤📤📤📤📤📤📤📤📤📤" )
                echo $FLAG;
}
?>
```





Flag: $CDDC19${PHP_tricks_are_very_fun!}

Polyglot(MISC)

Solution

Step 1: We translate all the Foreign Languages into English.

Step 2: We pasted all the translated text into a notepad together with the language they were translated from.

Step 3: We took the first letter of every language and formed a string with it.

Step 4: We added the alphabets into the format provided.

```
[01] The first character of this language creates a flag.       [Hindi]
[02] The first character of this language to fly the flag.      [Indonesian]
[03] The first character of this language constitutes the flag. [Chinese]
[04] The first sign of this language is the flag.               [Dutch]
[05] The first sign in this language is the flag.               [Danish]
[06] The first character of this language constitutes the flag. [Catalan]
[07] The first sign of this language is the flag                [Norweigan]
[08] The first character of this language is the flag.          [Spanish]
[09] The first mark of this language makes the flag             [Hmong]
[10] The first sign of this language makes the flag             [Crotian]

1 2 3 4 5 6 7 8 9 10
H I C D D C N S H C
```

Flag: $CDDC19${HI~CDDC&NSHC!}

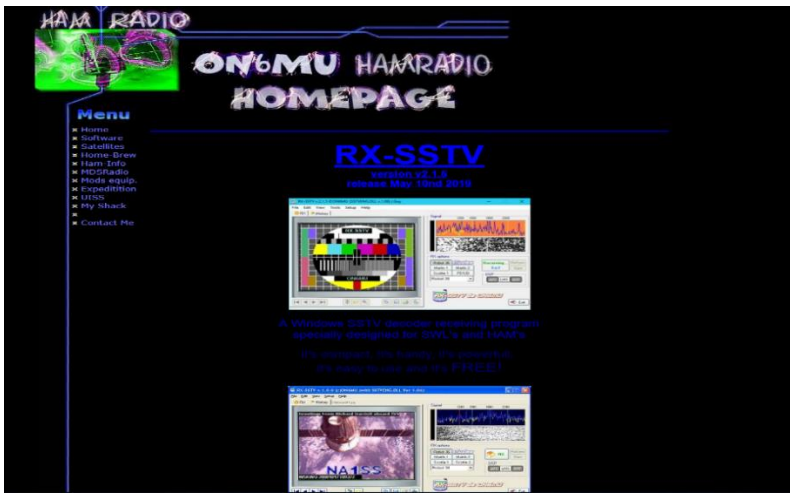
Super Strong TeleVision (MISC)

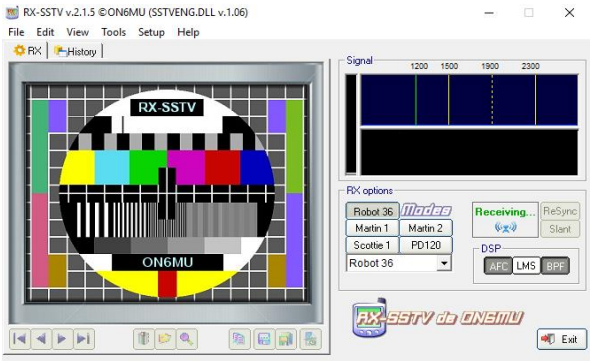
Solution

Step 1: We downloaded RX-SSTV, which is a SSTV decoding program. ([http://users.belgacom.net/hamradio/rxsstv.htm)](http://users.belgacom.net/hamradio/rxsstv.htm)

Step 2: We used RX-SSTV by playing the audio file provided close to our mic.

Step 3: A image with the flag in it was produced.





Flag: $CDDC19${Light$peedCorp-$$TV}

Do You Fancy Numbers? (MISC)

Solution

Step 1: We did research on the characters in different languages. And we found that the text looks similar to Chinese words. (Suzhou numerals) https://en.wikipedia.org/wiki/Suzhou_numerals

Step 2: We Started deciphering the text according to Suzhou numerals and we get this numbers.

36.67.68.68.67.49.57.36.123.53.48.95.121.48.117.95.102.52.78.99.89.95.102.108.48.87.51.114.45.78.117.77.98.51.53.125

Step 3: We converted the ASCII codes to text using https://ascii.cl/ and we got the flag.

Number	"Hangzhou"		CJK Ideographs	
	Character	Unicode	Character	Unicode
0			〇	U+3007
1	〡	U+3021	一	U+4E00
2	〢	U+3022	二	U+4E8C
3	〣	U+3023	三	U+4E09
4	〤	U+3024	四	U+56DB
5	〥	U+3025	五	U+4E94
6	〦	U+3026	六	U+516D
7	〧	U+3027	七	U+4E03
8	〨	U+3028	八	U+516B
9	〩	U+3029	九	U+4E5D
10	十	U+3038	十	U+5341
20	廿	U+3039	廿	U+5EFF
30	卅	U+303A	卅	U+5345

Standard characters

ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol
0	0	NUL	16	10	DLE	32	20	(space)	48	30	0
1	1	SOH	17	11	DC1	33	21	!	49	31	1
2	2	STX	18	12	DC2	34	22	"	50	32	2
3	3	ETX	19	13	DC3	35	23	#	51	33	3
4	4	EOT	20	14	DC4	36	24	$	52	34	4
5	5	ENQ	21	15	NAK	37	25	%	53	35	5
6	6	ACK	22	16	SYN	38	26	&	54	36	6
7	7	BEL	23	17	ETB	39	27	'	55	37	7
8	8	BS	24	18	CAN	40	28	(	56	38	8
9	9	TAB	25	19	EM	41	29	)	57	39	9
10	A	LF	26	1A	SUB	42	2A	*	58	3A	:
11	B	VT	27	1B	ESC	43	2B	+	59	3B	;
12	C	FF	28	1C	FS	44	2C	,	60	3C	<
13	D	CR	29	1D	GS	45	2D	-	61	3D	=
14	E	SO	30	1E	RS	46	2E	.	62	3E	>
15	F	SI	31	1F	US	47	2F	/	63	3F	?

ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol	ASCII	Hex	Symbol
64	40	@	80	50	P	96	60	`	112	70	p
65	41	A	81	51	Q	97	61	a	113	71	q
66	42	B	82	52	R	98	62	b	114	72	r
67	43	C	83	53	S	99	63	c	115	73	s
68	44	D	84	54	T	100	64	d	116	74	t
69	45	E	85	55	U	101	65	e	117	75	u
70	46	F	86	56	V	102	66	f	118	76	v
71	47	G	87	57	W	103	67	g	119	77	w
72	48	H	88	58	X	104	68	h	120	78	x
73	49	I	89	59	Y	105	69	i	121	79	y
74	4A	J	90	5A	Z	106	6A	j	122	7A	z
75	4B	K	91	5B	[	107	6B	k	123	7B	{
76	4C	L	92	5C	\	108	6C	l	124	7C	|
77	4D	M	93	5D	]	109	6D	m	125	7D	}
78	4E	N	94	5E	^	110	6E	n	126	7E	~
79	4F	O	95	5F	_	111	6F	o	127	7F	

Flag: $CDDC19${50_y0u_f4NcY_fl0W3r-NuMb35}