

# X-MAS CTF WRITEUP



Team : YourDisasters

## Sanity Check

- Merry Christmas
- The Place Where All The Elves Hang Out

## Forensic

- Conversation
- Santass
- The Cat

## Misc

- Complaint
- Bobi's Whacked
- Whispers of Ascalon
- Impostors Everywhere

## Web Exploitation

- PHP Master

## Sanity Check

### Merry Christmas

**Merry Christmas!** 5 Points SOLVED ✓

Oh hello there! Welcome to X-MAS CTF 2020. We hope you'll have fun. Here is your first flag:

X-MAS{H0\_H0\_H0\_H4ck\_4\_4\_br1gh73r\_fu7ur3\_4nd\_m3rry\_X-MAS!!!}

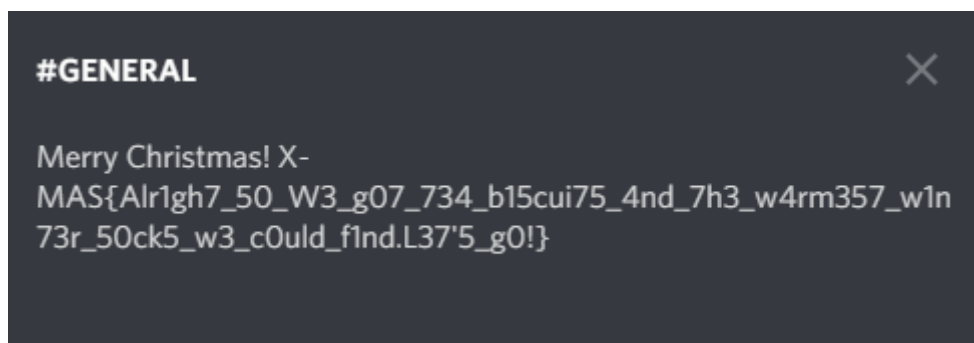
Its just the sanity check for everyone so the flag were given at the description

### The Place Where All The Elves Hang Out

**The place where all the elves hang out** 5 Points SOLVED ✓

Remember to join our Discord server! We use that place to post announcements and hang out, so be sure to join us!  
<https://discord.gg/nEWq5TZaVc>

As the description of the challenge say, we have to join the discord channel, and the first thing we check in the discord channel is text channel with common name or similar to Christmas. Then when we see the text channel named *general* on the channel topic we see the flag.




## Forensic

### Conversation

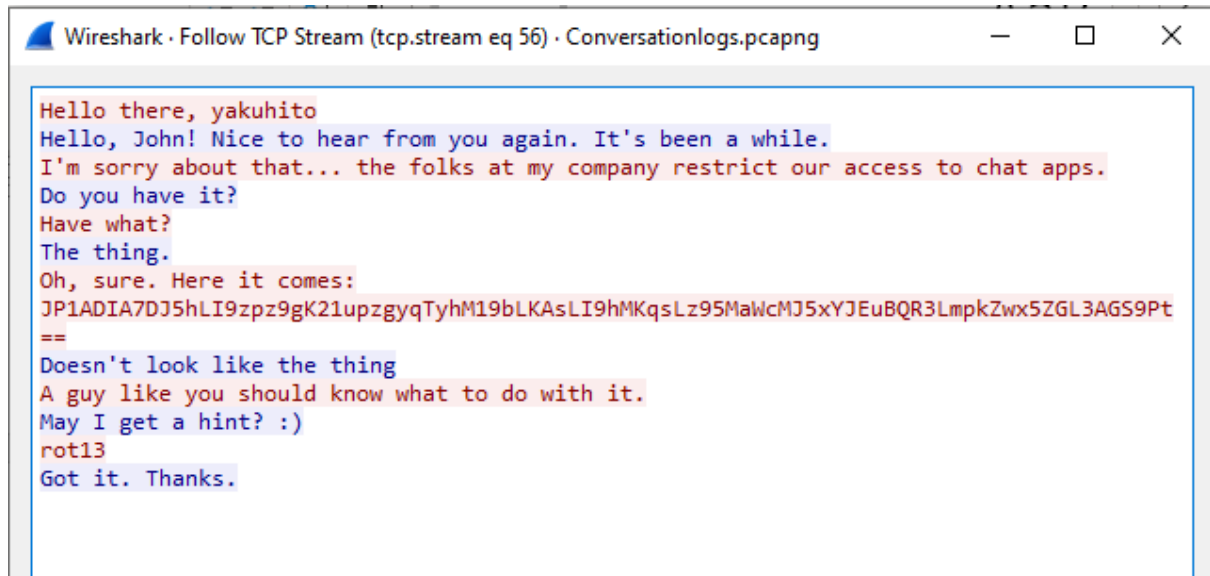
**Conversation** 29 Points SOLVED ✓

Due to our company's strict policy, all chatting websites have been blocked. We have been informed that some of our employees managed to circumvent all our limitations and have a secret conversation - can you find out what they've talked about?

Author: yakuhito

 logs.pcapng

After download the pcapng file we analyze it with Wireshark, and we found the traffic contain so many TCP and TLS traffic, so we guess the communication is inside there and we spend quite some time to analyze it and found 1 traffic with communication its from "tcp.stream eq 56" and the conversation is like this



Wireshark · Follow TCP Stream (tcp.stream eq 56) · Conversationlogs.pcapng

```
Hello there, yakuhito
Hello, John! Nice to hear from you again. It's been a while.
I'm sorry about that... the folks at my company restrict our access to chat apps.
Do you have it?
Have what?
The thing.
Oh, sure. Here it comes:
JP1ADIA7DJ5hLI9zpz9gK21upzgyqTyhM19bLKAsLI9hMKqsLz95MaWcMJ5xYJEUbQR3LmpkZwx5ZGL3AGS9Pt
==
Doesn't look like the thing
A guy like you should know what to do with it.
May I get a hint? :)
rot13
Got it. Thanks.
```

Looking at the encrypted message, we know the hint misleading us because the encrypted message was encrypted with Base64 not ROT13, now we just have to decode it, this time we use our favorite website to do this, [CyberChef](#), after paste it and use the base64 decode we know the flag is like this

Input

start: 0

end: 88

length: 0

length: 88

lines: 1

+

📁

🔗

🗑️

🏠

JP1ADIA7DJ5hLI9zpz9gK21upzgyqTyhM19bLKAsLI9hMKqsLz95MaWcMJ5xYJEUbQR3LmpkZwx5ZGL3AGS'  
Pt==|

Output

time: 80ms

length: 12701

lines: 473

💾

📄

🔗

↶

🔍

Recipe (click to load)	Result snippet	Properties
From_Base64('N-ZA-Mn-za-m0-9+/',true)	X-MAS{Anna_from_marketing_has_a_new_boyfriend-da817c7129916751}.	Valid UTF8 Entropy: 4.80

## Santass

santass 349 Points

SOLVED ✓

Please, someone check Santa's reindeers... They've been flying around all day.

Author: bobi

📁

santass.pcapng

After we downloaded the file and check the traffic its contain 400 line but nothing seems interesting unless the image file which have “LOL NOTHING HERE”

```

439 313.093010 192.168.0.27 192.168.0.27 HTTP 395 [HTTP/1.0 200 OK (image/jpeg)]
440 313.093019 192.168.0.27 192.168.0.27 TCP 56 54140 → 8080 [ACK] Seq=362 Ack=527 Win
441 313.093040 192.168.0.27 192.168.0.27 TCP 56 8080 → 54140 [FIN, ACK] Seq=527 Ack=36
442 313.093051 192.168.0.27 192.168.0.27 TCP 56 54140 → 8080 [ACK] Seq=362 Ack=528 Win
443 313.093141 192.168.0.27 192.168.0.27 TCP 56 54140 → 8080 [FIN, ACK] Seq=362 Ack=52
444 313.093156 192.168.0.27 192.168.0.27 TCP 56 8080 → 54140 [ACK] Seq=528 Ack=363 Win

> Frame 439: 395 bytes on wire (3160 bits), 395 bytes captured (3160 bits) on interface lo0, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 192.168.0.27, Dst: 192.168.0.27
> Transmission Control Protocol, Src Port: 8080, Dst Port: 54140, Seq: 188, Ack: 362, Len: 339
> [8 Reassembled TCP Segments (526 bytes): #425(17), #427(38), #429(37), #431(26), #433(21), #435(46), #437(2), #439
> Hypertext Transfer Protocol
> Media Type

0000 02 00 00 00 45 00 01 87 00 00 00 00 40 06 00 00 ....E... ..@.@...
0010 c0 a8 00 1b c0 a8 00 1b 1f 90 d3 7c 80 65 d1 3b .....|.e.;
0020 f5 46 ea 06 80 18 18 e6 83 00 00 00 01 01 08 0a .F.....
0030 16 7b 25 ff 16 7b 25 ff 4c 4f 4c 20 4e 4f 54 48 .{...{.. LOL NOTH
0040 49 4e 47 20 48 45 52 45 0a 4c 4f 4c 20 4e 4f 54 ING HERE .LOL NOT
0050 48 49 4e 47 20 48 45 52 45 0a 0a 4c 4f 4c 20 4e HING HER E..LOL N
0060 4f 54 48 49 4e 47 20 48 45 52 45 0a 0a 4c 4f 4c OTHING H ERE..LOL
0070 20 4e 4f 54 48 49 4e 47 20 48 45 52 45 0a 0a 4c NOTHING HERE..L
0080 4f 4c 20 4e 4f 54 48 49 4e 47 20 48 45 52 45 0a OL NOTHI NG HERE.
0090 0a 0a 4c 4f 4c 20 4e 4f 54 48 49 4e 47 20 48 45 ..LOL NO THING HE
00a0 52 45 0a 0a 4c 4f 4c 20 4e 4f 54 48 49 4e 47 20 RE..LOL NOTHING
00b0 48 45 52 45 0a 0a 4c 4f 4c 20 4e 4f 54 48 49 4e HERE..LO L NOTHIN

```

Then we tried to look at what we can do on export objects


139	192.168.0.27	text/html	196 bytes	flags.txt
143	192.168.0.27	text/html	196 bytes	flags.txt
147	192.168.0.27	text/html	196 bytes	flags.txt
173	192.168.0.27	text/html	196 bytes	Z2d3a.jpg
185	192.168.0.27	text/html	196 bytes	XJlc2.jpg
197	192.168.0.27	text/html	196 bytes	hhcms.jpg
209	192.168.0.27	text/html	196 bytes	dog.jpg
213	192.168.0.27	text/html	196 bytes	cat.jpg
225	192.168.0.27	text/html	196 bytes	nypm.jpg
229	192.168.0.27	text/html	196 bytes	nymph.jpg
241	192.168.0.27	text/html	196 bytes	nothing_suspicious.jpg
265	192.168.0.27:8080	text/html	195 bytes	nothing_suspicious.jpg
283	192.168.0.27:8080	text/html	195 bytes	favicon.ico
321	192.168.0.27:8080		195 bytes	nothing_suspicious.jpg
345	192.168.0.27:8080		195 bytes	santasass.jpg
369	192.168.0.27:8080		195 bytes	santasass.joh
389	192.168.0.27:8080	text/html	195 bytes	santasass.jog
413	192.168.0.27:8080	application/octet-stream	339 bytes	santass.jog
439	192.168.0.27:8080	image/jpeg	339 bytes	santass.jpg

At first we don't know what we need to do, and after talk to another team we could see the pattern we need to see, that is the packet number 173, 185, and 197 then concat them to make a base64 string and we just have to decode it

Recipe	Input
<b>From Base64</b> <div>Alphabet A-Za-z0-9+/=</div> <input checked="" type="checkbox"/> Remove non-alphabet chars	Z2d3aXJlc2hhcms
	<b>Output</b> ggwireshark

X-MAS{ggwireshark}

## The Cat

The Cat 392 Points	1d, 4h, 16m, 1s remaining
<p>We know yakuhito's been playing in our internal network for over a year, but we never managed to kick him out. Last week, he made the big screen at the entrance play nyan cat.</p> <p>Author: yakuhito</p> <p> logs.pcapng</p> <p>Please enter flag for challenge: The Cat</p> <p>SUBMIT FLAG</p>	

This challenge very new to us because we had to do something we don't really know how to pull it of, so we can't solved this chall although got the important piece to uncover the flag, here is how we uncover the important piece

After we download the file, we analyze the http traffic inside the pcapng file, we found something suspicious with HTTP Method POST from 192.168.1.78 to 192.168.1.194 and its send some sort of handshake client and server like this :

```
POST / HTTP/1.1
Host: 192.168.1.194:1338
User-Agent: curl/7.58.0
Accept: */*
Content-Length: 938
Content-Type: application/x-www-form-urlencoded

SERVER_HANDSHAKE_TRAFFIC_SECRET
735a37a420b8213d6e766c572251315a1a9e927e9dc0ace81f4c8be102a2d65a
84c911522ec48fe70df14d27eae5cd8998dadcd4fa3e100702d5577c22c19eee62472c36994d8e73012c79
a86feadcfa
CLIENT_HANDSHAKE_TRAFFIC_SECRET
735a37a420b8213d6e766c572251315a1a9e927e9dc0ace81f4c8be102a2d65a
1d58a7f1e45380a3e43845c2008e6fe12237d11f2c6b2e3b7a749c00ee9ad8ac104acbfd3e635f631f8651
8370cc2fa5
EXPORTER_SECRET 735a37a420b8213d6e766c572251315a1a9e927e9dc0ace81f4c8be102a2d65a
a9ab5d116ad94c543bf325f457c5418bef59fe392dcabc1681165a548db0baca19a991d70156407e5d5c10b
6b9ef9b545
SERVER_TRAFFIC_SECRET_0
735a37a420b8213d6e766c572251315a1a9e927e9dc0ace81f4c8be102a2d65a
b3568f0c1c4ccd85eb6294c0171718519bb86485f8233fde09a028340d84d4ba99366693e58640e74ca511
7fc135675f
CLIENT_TRAFFIC_SECRET_0
735a37a420b8213d6e766c572251315a1a9e927e9dc0ace81f4c8be102a2d65a
0079885c5e6e8d7f71498c973cfe4bc00f8cc5a8f898d07113350acec9c9a95cd7d71eec1f26a9d138fef4
2d06adc4e7
<head>
<title>Error response</title>
</head>
<body>
<h1>Error response</h1>
<p>Error code 501.
<p>Message: Unsupported method ('POST').
<p>Error code explanation: 501 = Server does not support this operation.
</body>
```

After search what to do for a while, we found [this](#) article and we notice that we could decrypt the TLS traffic by using the handshake we got but we got stuck while doing that its so sad that we have come this far but due lack of experience we can't solved this chall but it is a great experience we got from this chall.

## Misc

### Complaint

**Complaint** 36 Points SOLVED ✓

Do you want to file a formal complaint? Use this address and we'll take care of redirecting it to /dev/null.

**Target:** nc challs.xmas.htsp.ro 6004  
**Author:** yakuhito

This challenge quite easy because we just had to connect to the server with netcat and do OS Command Injection by using “;” at the start and the end of our command

```
root@synex:~/Downloads# nc challs.xmas.htsp.ro 6004
WHAT IS BOTHERING YOU???
;nl flag.txt;

1 X-MAS{h3ll0_k4r3n-8819d787dd38a397}
YOUR COMPLAINT HAS BEEN RECORDED.
root@synex:~/Downloads#
```

The NL command is used to check number line in a file, so we had to use “nl” because the “nano”, “cat”, and “vim/vi” can’t be used, and the only thing work is “nl” and that’s how we got the flag

### Bobi Whack’ed

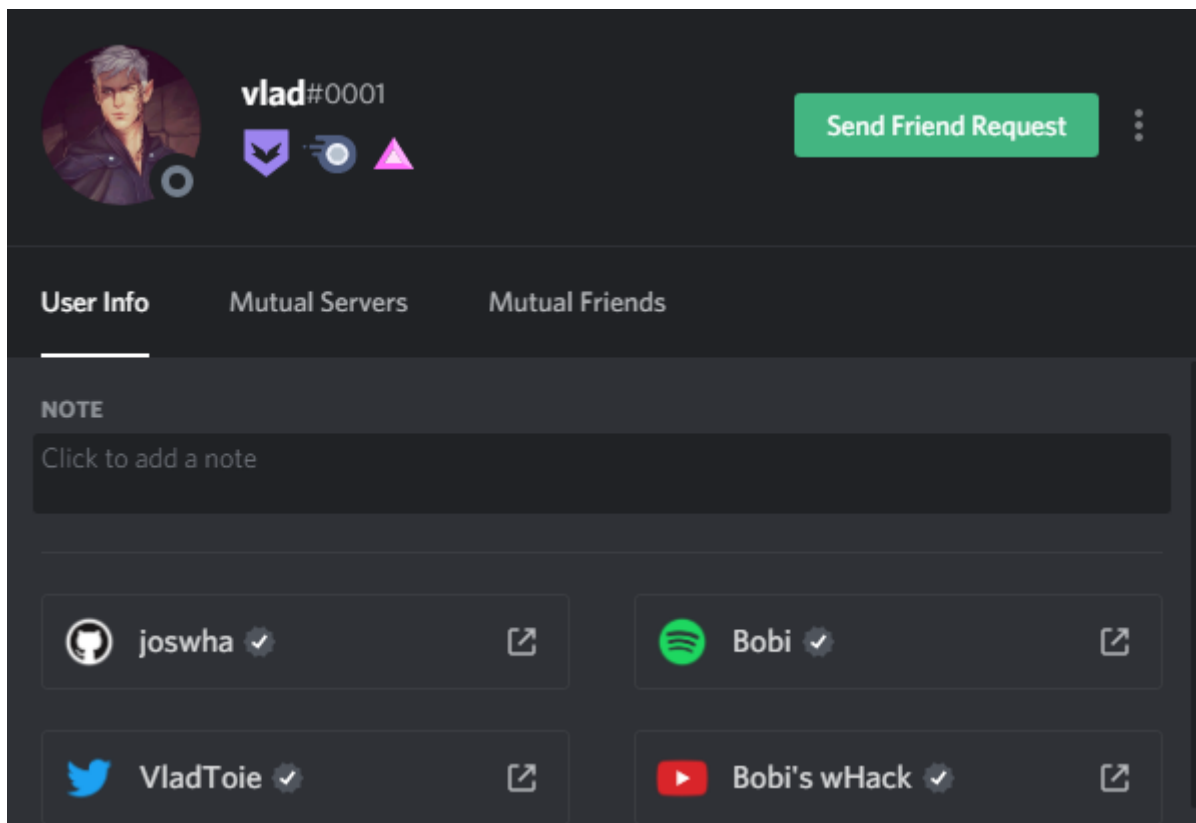
**Bobi's Whacked** 50 Points SOLVED ✓

Warm socks and warm wine, so the caption said.

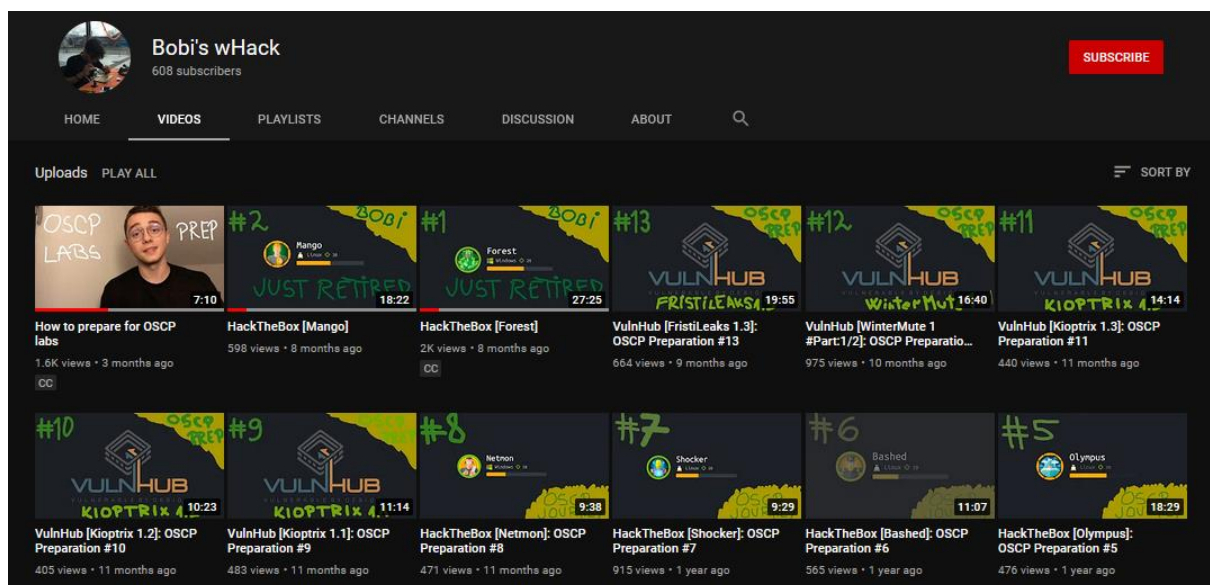
**Author:** Bobi

This one of OSINT Challenge, and the first thing we did because there is only description is we check on the Author Discord, which is Bobi the CEO of Everyone

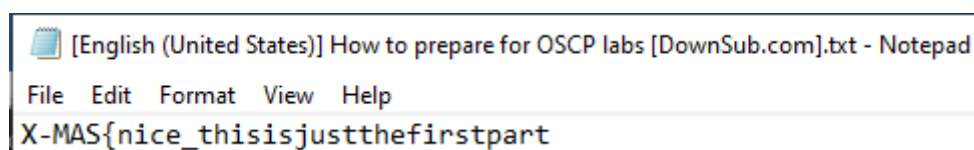




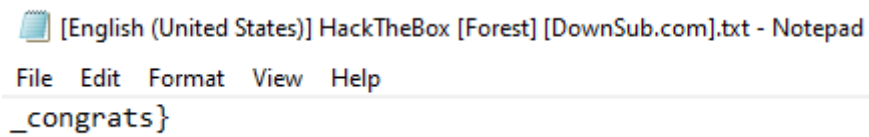
And we got the youtube channel with the name same as the title challenge, so we did our investigation further more on the youtube channel,



We could notice that only two videos contain Caption (CC) now we could download the CC from <https://downsub.com/>



The first CC contain the first part of the flag, now for the second CC file

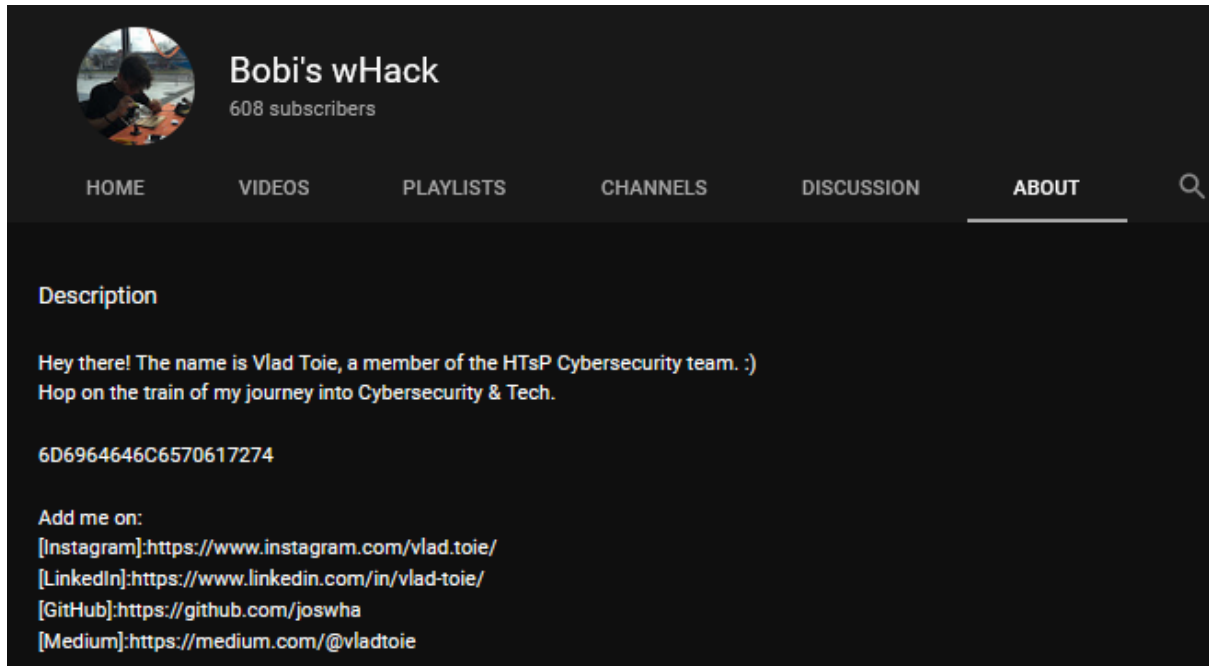


[English (United States)] HackTheBox [Forest] [DownSub.com].txt - Notepad

File Edit Format View Help

\_congrats}

The second CC contain the third flag, we know because the part contain “\_” and we did submit the concate of first and second flag but the result is wrong, so we took another investigation and found a interesting string on “About” section of the youtube



**Bobi's wHack**  
608 subscribers

HOME VIDEOS PLAYLISTS CHANNELS DISCUSSION **ABOUT**

**Description**

Hey there! The name is Vlad Toie, a member of the HTsP Cybersecurity team. :)  
Hop on the train of my journey into Cybersecurity & Tech.

6D6964646C6570617274

Add me on:  
[Instagram]:<https://www.instagram.com/vlad.toie/>  
[LinkedIn]:<https://www.linkedin.com/in/vlad-toie/>  
[GitHub]:<https://github.com/joswha>  
[Medium]:<https://medium.com/@vladtoie>

And after we decode the string, we found the string is “middlepart”

Input		start: 0 end: 20 length: 0	length: : lines:
6D6964646C6570617274			
Output		time: length: lines:	
Recipe (click to load)	Result snippet		
From_Hex('None')	middlepart		

Now we got the full flag of the challenge


X-MAS{nice\_thisisjustthefirstpart\_middlepart\_congrats}

## Whispers of Ascalon

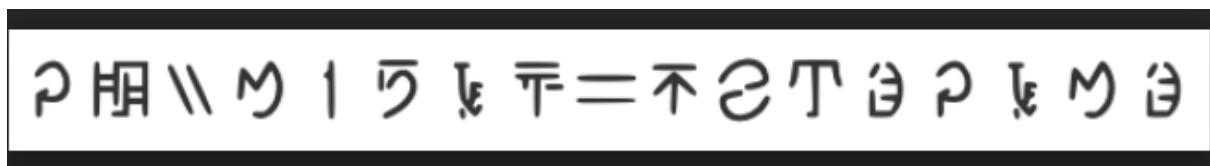
**Whispers of Ascalon** 50 Points
 SOLVED ✓

The one who bears the Magdaer shall curse his people forever after.

Author: Bobi

 image.png

We were given an image like this



We know that this is a cipher message with somekind of language, and as we search about “Magdaer” we know that is from Guild Wars 2 and after search the Guild Wars 2 wiki we got the similar language like the image above

[https://wiki.guildwars2.com/wiki/New\\_Krytan](https://wiki.guildwars2.com/wiki/New_Krytan)


and after we decode the image, we got the plain text “GW2MYFAVORITEGAME” and that is the flag we have to submit “X-MAS{gw2myfavoritegame}”

## Impostors Everywhere


**Impostors Everywhere** 487 Points SOLVED ✓

Santa's ultimate Windows Server 2008 has been hacked. We don't know who did it, but they left the following URL on the server.

Author: iamroot



 image



This one also an OSINT chall, and because of the lack of description we need to check on the author discord account

 **iamroot**#4590 Send Friend Request

**User Info** Mutual Servers Mutual Friends

**NOTE**  
Click to add a note

 Googal01 ✓ 

 Googal ✓ 

Because the OSINT chall before this one involved youtube, we tried to investigate the youtube first but we got nothing there unless the TicTacToe game, so we tried to search the username on several platform and found that “Googal” has a [github](#) account. At first we stuck at the github account because there is a rabbit hole there and we fell at that rabbit hole, and after discuss with another team we found the wattpad account from his/her github.



<https://my.w.tt/zMtt0tJibcb>

and after read carefully on the story there is a suspicious string like this one :

"Malo mori quam foedari. K-ZNF{jub\_xarj\_lbh\_jbhyq\_yvyr\_mbzovrf}"  
(Death rather than dishonour.) If I recall correctly, it was the motto of the

At the first glance we know that is Caesar Cipher so we decode it from online source : [Caesar Cipher](#) and we got the flag

```
+13 X-MAS{who_knew_you_would_like_zombies}
```

## Web Exploitation

# Php Master

PHP Master 33 Points

SOLVED ✓

Another one of *those* challenges.

**Target:** <http://challs.xmas.htsp.ro:3000/>

**Author:** yakuhito

After we opened the link, we got source code of the php file like this

```
<?php
include('flag.php');

$p1 = $_GET['param1'];
$p2 = $_GET['param2'];

if(!isset($p1) || !isset($p2)) {
    highlight_file(__FILE__);
    die();
}

if(strpos($p1, 'e') === false && strpos($p2, 'e') === false && strlen($p1) === strlen($p2) && $p1 !== $p2 && $p1[0] != '0' && $p1 == $p2) {
    die($flag);
}

?>
```

And we know that we have to make a request with some kind of rules according the given source code to get the flag and after we create request parameter with php exponent like this

```
challs.xmas.htsp.ro:3000/?param1=100&param2=1E2
```

We got the flag of the challenge :

```
X-MAS{s0_php_m4ny_skillz-69acb43810ed4c42}
```

Even though we finished not in the top 100 leaderboard but we got so many things new to know from this CTF Competition, Cheers to the Creator of the CTF