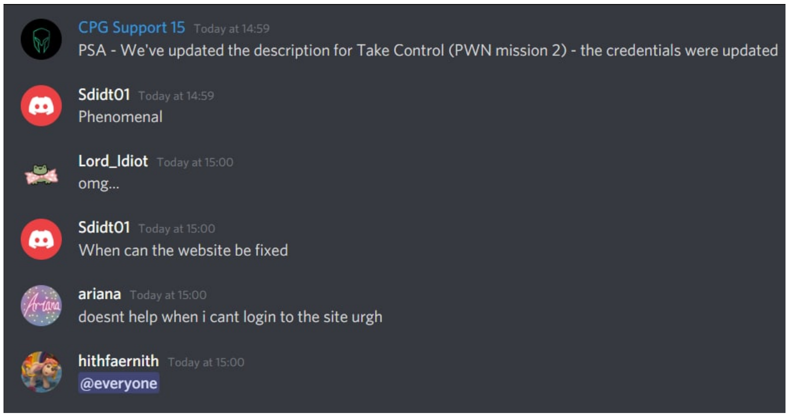
Overall, those in charge of handling the event (mostly BSW it seems) were extremely unprepared to handle an event at this scale and to fix technical issues whenever they appear. This document details most issues faced during the event so hopefully these can be mitigated in future events. If there are any further enquiries regarding how the CTF went or suggestions for future CDDCs, we would be happy to help out!

Discord issues

Information/Announcements

- Announcements were sent in the text channels for the different categories instead of the announcement channel, frequently without pinging everyone, leading to important updates getting lost. Information that are not announced when they should be include
    - Challenges going down/up
    - Challenges getting fixed/no longer working
    - Additional information about a challenge that was not mentioned

  This can easily be addressed by having proper announcement channels for each category



CPG Support 15 Today at 14:59
PSA - We've updated the description for Take Control (PWN mission 2) - the credentials were updated

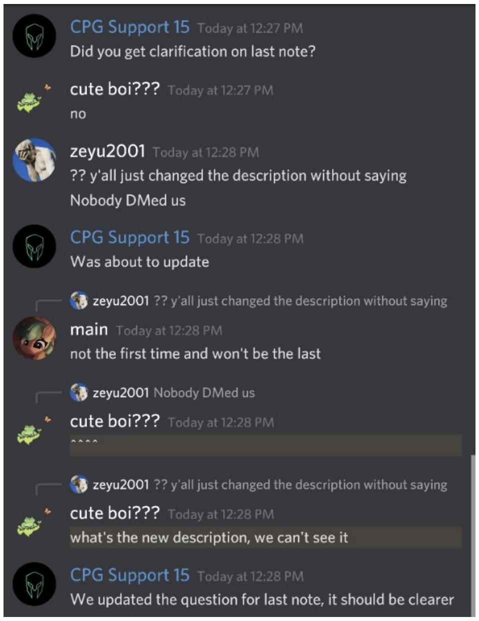
Sdidt01 Today at 14:59
Phenomenal

Lord_Idiot Today at 15:00
omg...

Sdidt01 Today at 15:00
When can the website be fixed

ariana Today at 15:00
doesnt help when i cant login to the site urgh

hithfaernith Today at 15:00
@everyone



CPG Support 15 Today at 12:27 PM
Did you get clarification on last note?

cute boi??? Today at 12:27 PM
no

zeyu2001 Today at 12:28 PM
?? y'all just changed the description without saying
Nobody DMed us

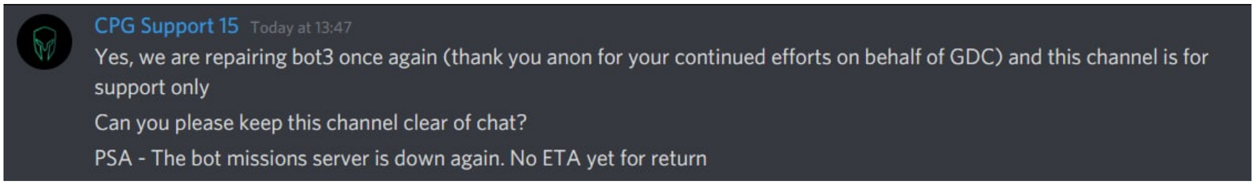
CPG Support 15 Today at 12:28 PM
Was about to update

zeyu2001 ?? y'all just changed the description without saying
main Today at 12:28 PM
not the first time and won't be the last

zeyu2001 Nobody DMed us
cute boi??? Today at 12:28 PM
^^^^

zeyu2001 ?? y'all just changed the description without saying
cute boi??? Today at 12:28 PM
what's the new description, we can't see it

CPG Support 15 Today at 12:28 PM
We updated the question for last note, it should be clearer

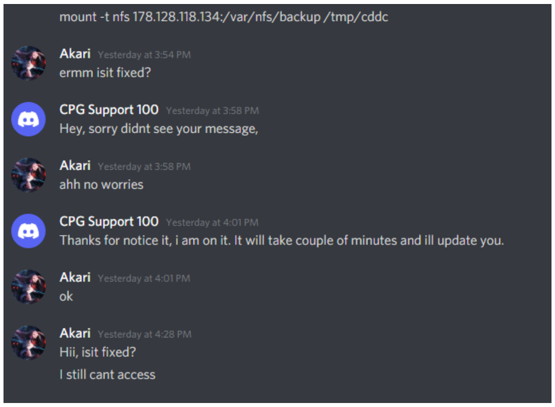


CPG Support 15 Today at 13:47
Yes, we are repairing bot3 once again (thank you anon for your continued efforts on behalf of GDC) and this channel is for support only
Can you please keep this channel clear of chat?
PSA - The bot missions server is down again. No ETA yet for return

- No roles differentiating senior/junior category, so everyone (even from the other category) ended up getting pinged for information regarding the other category

Challenge support

- No ticket system
    - Everyone asks their questions in the same channel, hoping an admin will notice and if they get lucky, get a reply or get a direct message
    - The whole channel becomes a mess, possible key information getting leaked as well such as important files (i.e. systeminfo in linux4 of senior)
    - Specific issues are failed to be addressed
    - Due to the flood of queries, the admins set a slow mode of 10s everywhere and 30s for the support chat



mount -t nfs 178.128.118.134:/var/nfs/backup /tmp/cddc

Akari Yesterday at 3:54 PM
ermm isit fixed?

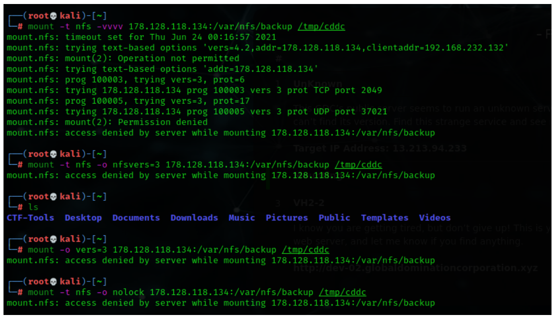
CPG Support 100 Yesterday at 3:58 PM
Hey, sorry didnt see your message,

Akari Yesterday at 3:58 PM
ahh no worries

CPG Support 100 Yesterday at 4:01 PM
Thanks for notice it, i am on it. It will take couple of minutes and ill update you.

Akari Yesterday at 4:01 PM
ok

Akari Yesterday at 4:28 PM
Hii, isit fixed?
I still cant access

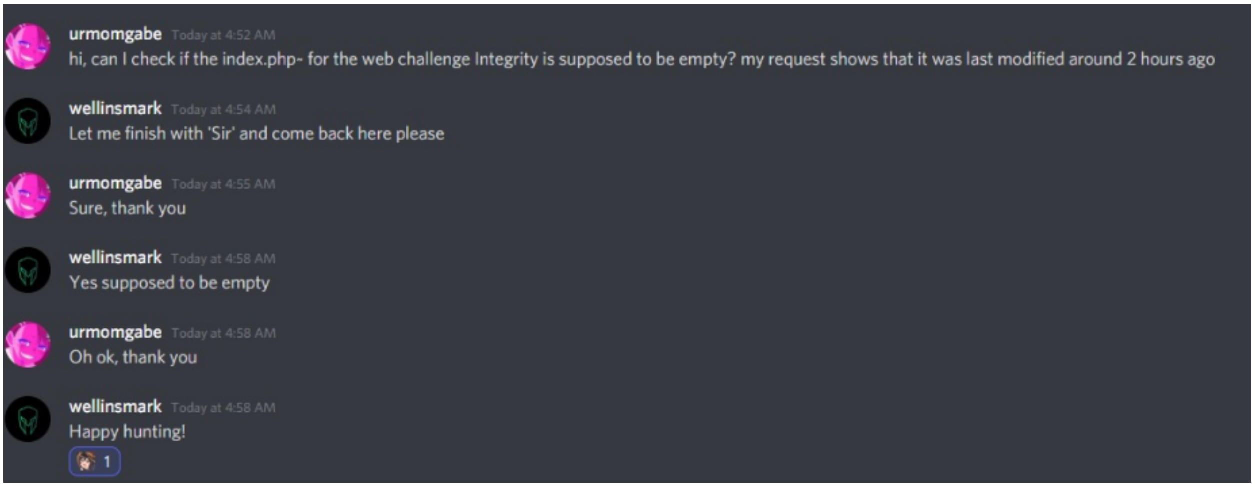


```
┌──(root💀kali)-[~]
└─# mount -t nfs -vvvv 178.128.118.134:/var/nfs/backup /tmp/cddc
mount.nfs: timeout set for Thu Jun 24 00:16:57 2021
mount.nfs: trying text-based options 'vers=4.2,addr=178.128.118.134,clientaddr=192.168.232.132'
mount.nfs: mount(2): Operation not permitted
mount.nfs: trying text-based options 'addr=178.128.118.134'
mount.nfs: prog 100003, trying vers=3, prot=6
mount.nfs: trying 178.128.118.134 prog 100003 vers 3 prot TCP port 2049
mount.nfs: prog 100005, trying vers=3, prot=17
mount.nfs: trying 178.128.118.134 prog 100005 vers 3 prot UDP port 37021
mount.nfs: mount(2): Permission denied
mount.nfs: access denied by server while mounting 178.128.118.134:/var/nfs/backup

┌──(root💀kali)-[~]
└─# mount -t nfs -o nfsvers=3 178.128.118.134:/var/nfs/backup /tmp/cddc
mount.nfs: access denied by server while mounting 178.128.118.134:/var/nfs/backup

┌──(root💀kali)-[~]
└─# ls
CTF-Tools  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(root💀kali)-[~]
└─# mount -o vers=3 178.128.118.134:/var/nfs/backup /tmp/cddc
mount.nfs: access denied by server while mounting 178.128.118.134:/var/nfs/backup

┌──(root💀kali)-[~]
└─# mount -t nfs -o nolock 178.128.118.134:/var/nfs/backup /tmp/cddc
mount.nfs: access denied by server while mounting 178.128.118.134:/var/nfs/backup
```

The player's ip was blocked from one of the reconnaissance challenges from "Going Active" - mounting, making it unsolvable. However, support is not there at all.

This can easily be settled by having a proper ticketing system (which most ctfs have) that allows for players to directly contact the sysadmins/challenge authors for issues.

- Lack of technical knowledge
    - Admins do not know what is happening to every challenge in detail which is to be expected, however they attempt to help and provides incorrect information way more often than they should



urmomgabe Today at 4:52 AM
hi, can I check if the index.php- for the web challenge Integrity is supposed to be empty? my request shows that it was last modified around 2 hours ago

wellinsmark Today at 4:54 AM
Let me finish with 'Sir' and come back here please

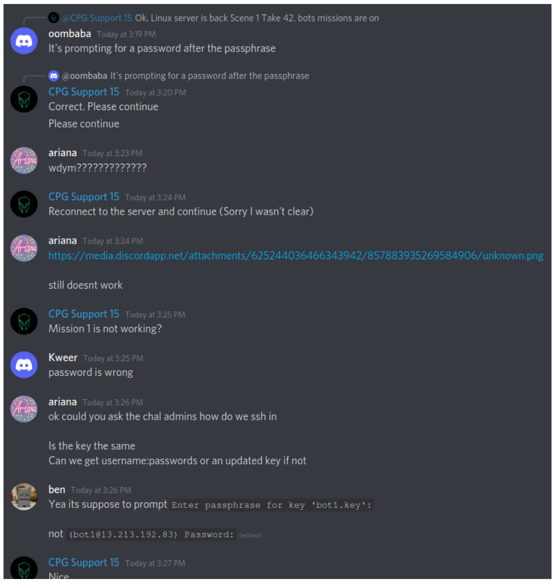
urmomgabe Today at 4:55 AM
Sure, thank you

wellinsmark Today at 4:58 AM
Yes supposed to be empty

urmomgabe Today at 4:58 AM
Oh ok, thank you

wellinsmark Today at 4:58 AM
Happy hunting!

The key to this challenge was to view the index.php~ file
to obtain a JWT key that can't be brute-forced



@CPG Support 15 Ok, Linux server is back Scene 1 Take 42. bots missions are on

oombaba Today at 3:19 PM
It's prompting for a password after the passphrase

@oombaba It's prompting for a password after the passphrase

CPG Support 15 Today at 3:20 PM
Correct. Please continue

Please continue

ariana Today at 3:23 PM
wdym?????????????

CPG Support 15 Today at 3:24 PM
Reconnect to the server and continue (Sorry I wasn't clear)

ariana Today at 3:24 PM
https://media.discordapp.net/attachments/625244036466343942/857883935269584906/unknown.png

still doesnt work

CPG Support 15 Today at 3:25 PM
Mission 1 is not working?

Kweer Today at 3:25 PM
password is wrong

ariana Today at 3:26 PM
ok could you ask the chal admins how do we ssh in

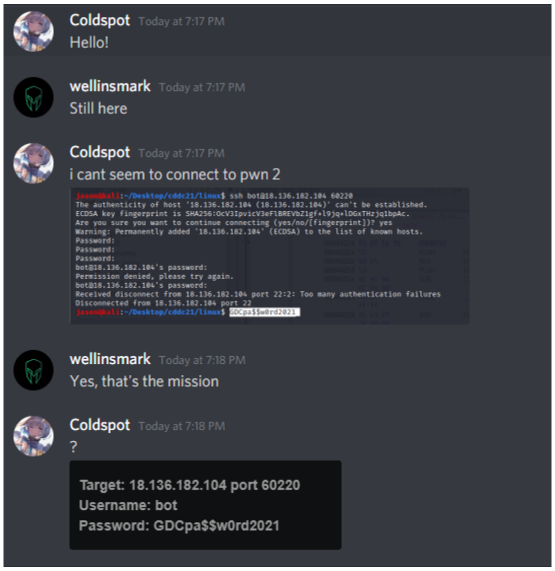
Is the key the same
Can we get username:passwords or an updated key if not

ben Today at 3:26 PM
Yea its suppose to prompt `Enter passphrase for key 'bot1.key':`

not `(bot1@13.213.192.83) Password:` (edited)

CPG Support 15 Today at 3:27 PM
Nice

Extremely confused text



Coldspot Today at 7:17 PM
Hello!

wellinsmark Today at 7:17 PM
Still here

Coldspot Today at 7:17 PM
i cant seem to connect to pwn 2

```
jason@kali:~/Desktop/cddc21/linux$ ssh bot@18.136.182.104 60220
The authenticity of host '18.136.182.104 (18.136.182.104)' can't be established.
ECDSA key fingerprint is SHA256:OcV3IpvicV3eFlBREVbZ1gf+l9jq+lDGxTHzjq1bpAc.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '18.136.182.104' (ECDSA) to the list of known hosts.
Password:
Password:
Password:
bot@18.136.182.104's password:
Permission denied, please try again.
bot@18.136.182.104's password:
Received disconnect from 18.136.182.104 port 22:2: Too many authentication failures
Disconnected from 18.136.182.104 port 22
jason@kali:~/Desktop/cddc21/linux$ GDCpa$$w0rd2021
```

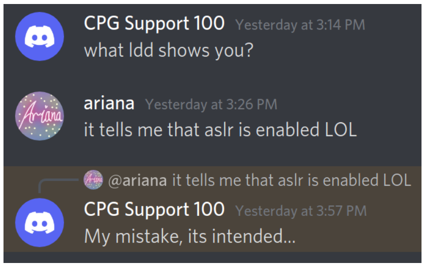
wellinsmark Today at 7:18 PM
Yes, that's the mission

Coldspot Today at 7:18 PM
?

Target: 18.136.182.104 port 60220
Username: bot
Password: GDCpa$$w0rd2021

Being clueless about objectives

Pwn3 - Where the admins didnt know if aslr was enabled and if libc was the same

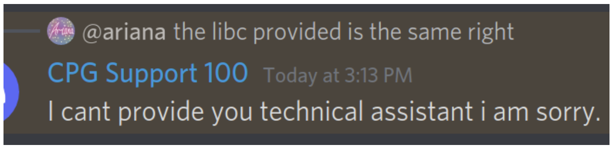


CPG Support 100 Yesterday at 3:14 PM
what ldd shows you?

ariana Yesterday at 3:26 PM
it tells me that aslr is enabled LOL

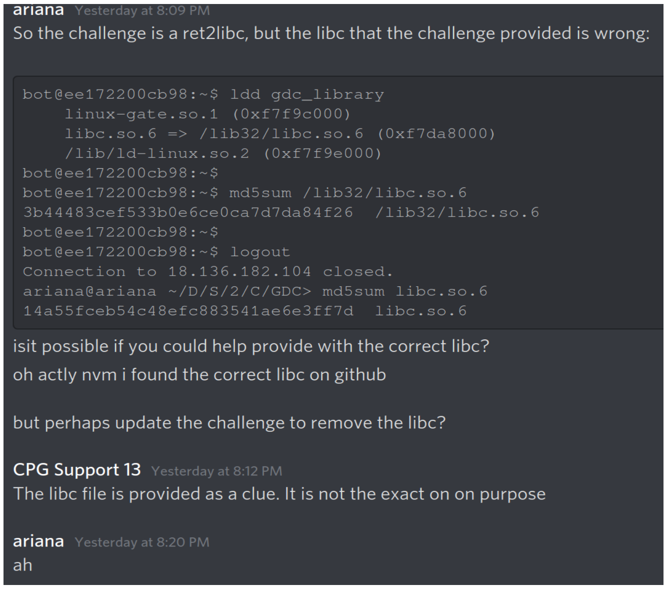
@ariana it tells me that aslr is enabled LOL

CPG Support 100 Yesterday at 3:57 PM
My mistake, its intended...



@ariana the libc provided is the same right

CPG Support 100 Today at 3:13 PM
I cant provide you technical assistant i am sorry.



ariana Yesterday at 8:09 PM
So the challenge is a ret2libc, but the libc that the challenge provided is wrong:

```
bot@ee172200cb98:~$ ldd gdc_library
	linux-gate.so.1 (0xf7f9c000)
	libc.so.6 => /lib32/libc.so.6 (0xf7da8000)
	/lib/ld-linux.so.2 (0xf7f9e000)
bot@ee172200cb98:~$
bot@ee172200cb98:~$ md5sum /lib32/libc.so.6
3b44483cef533b0e6ce0ca7d7da84f26  /lib32/libc.so.6
bot@ee172200cb98:~$
bot@ee172200cb98:~$ logout
Connection to 18.136.182.104 closed.
ariana@ariana ~/D/S/2/C/GDC> md5sum libc.so.6
14a55fceb54c48efc883541ae6e3ff7d  libc.so.6
```

isit possible if you could help provide with the correct libc?

oh actly nvm i found the correct libc on github

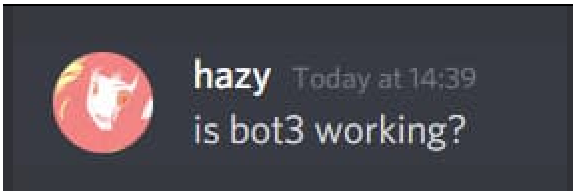
but perhaps update the challenge to remove the libc?

CPG Support 13 Yesterday at 8:12 PM
The libc file is provided as a clue. It is not the exact on on purpose

ariana Yesterday at 8:20 PM
ah

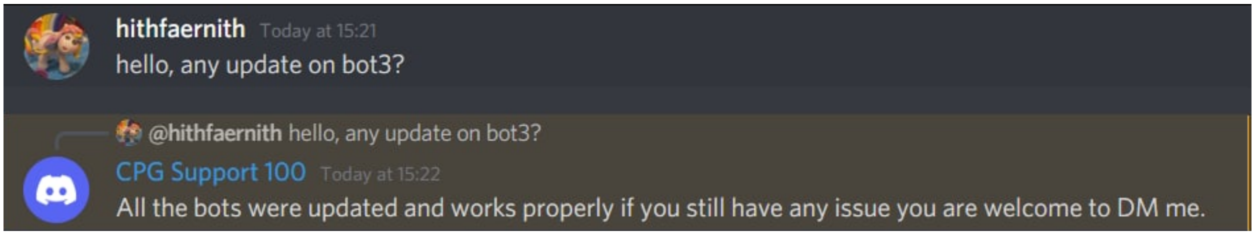
Again a ticketing system would have helped here

- Updates took extremely long or may not even come
    - When the competition was delayed on day 1, “regular updates” were promised. However, the next update after the mass uproar at ~10.30am was 1.30pm, and the following update was at 5pm. As many of us did not know what to expect but did not want to miss out on potential announcements, we spent the entire day waiting at our computers, thus leading to a lot of banter and spam) and subsequently wasted the first day.
    - In the pwn3 example, ariana asked if the aslr was meant to be brute forced or base address leaked but no replies were given, even after she asked multiple times.
    - When one of the challenges went down (bot 3 of Linux Rules The World) for the nth time, it took a few hours to get an update and we were not notified that people were working on this issue.



hazy Today at 14:39
is bot3 working?

2.39pm, @hazy asked in the support channel. There was no follow up whatsoever.



hithfaernith Today at 15:21
hello, any update on bot3?

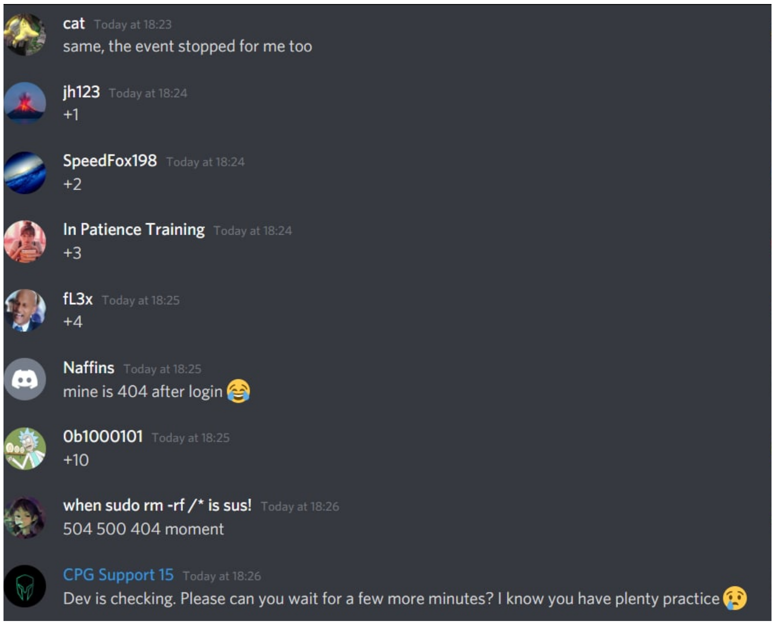
@hithfaernith hello, any update on bot3?
CPG Support 100 Today at 15:22
All the bots were updated and works properly if you still have any issue you are welcome to DM me.

This took 1 hour to resolve, and was not the only time that this specific challenge went offline.

-

Misc

- Passive aggressive behaviour from the admins when people give feedback about the website crashing or challenges being down which occurred many times.



cat Today at 18:23
same, the event stopped for me too

jh123 Today at 18:24
+1

SpeedFox198 Today at 18:24
+2

In Patience Training Today at 18:24
+3

fL3x Today at 18:25
+4

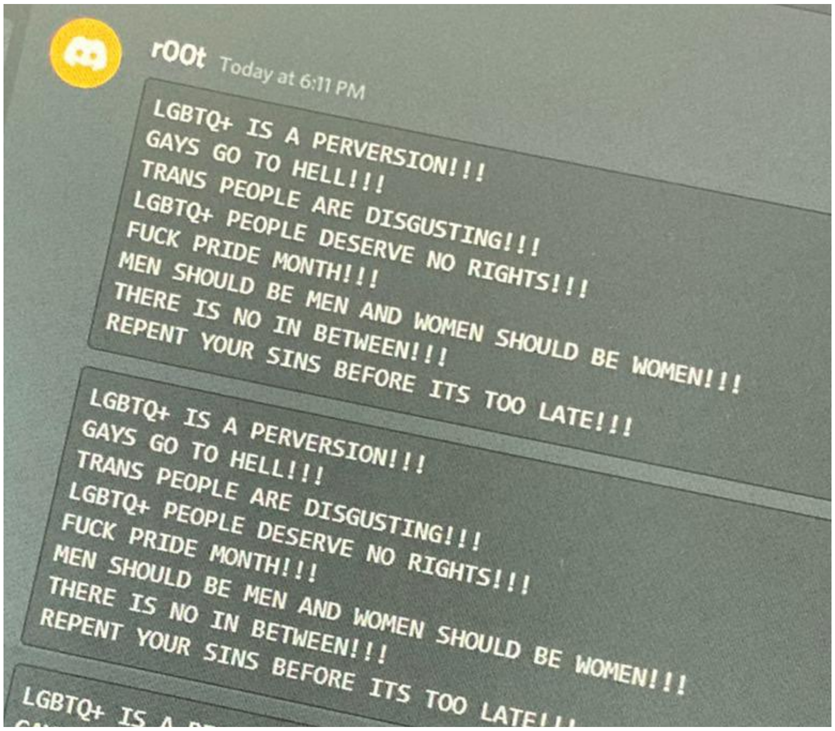
Naffins Today at 18:25
mine is 404 after login 😂

0b1000101 Today at 18:25
+10

when sudo rm -rf /* is sus! Today at 18:26
504 500 404 moment

CPG Support 15 Today at 18:26
Dev is checking. Please can you wait for a few more minutes? I know you have plenty practice 😢

- Poor server admission, griefers were able to easily create alt accounts to leak flags and send offensive/obscene (e.g. ascii porn and a porn discord server) materials into the chat. The admins could have been more direct in removing content that crosses most reasonable notions of online etiquette. However, they were active in deleting messages that they did not like.



r0Ot Today at 6:11 PM

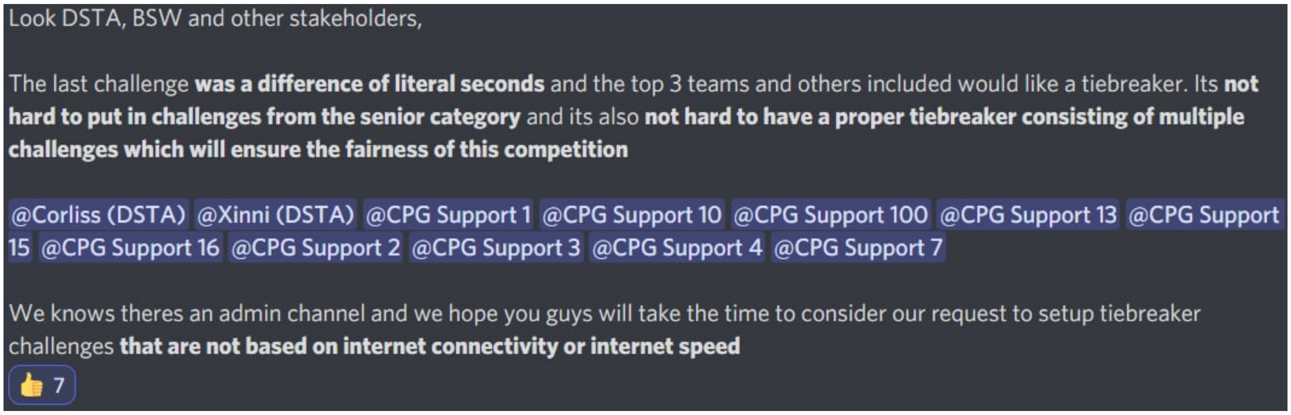
LGBTQ+ IS A PERVERSION!!!
GAYS GO TO HELL!!!
TRANS PEOPLE ARE DISGUSTING!!!
LGBTQ+ PEOPLE DESERVE NO RIGHTS!!!
FUCK PRIDE MONTH!!!
MEN SHOULD BE MEN AND WOMEN SHOULD BE WOMEN!!!
THERE IS NO IN BETWEEN!!!
REPENT YOUR SINS BEFORE ITS TOO LATE!!!

LGBTQ+ IS A PERVERSION!!!
GAYS GO TO HELL!!!
TRANS PEOPLE ARE DISGUSTING!!!
LGBTQ+ PEOPLE DESERVE NO RIGHTS!!!
FUCK PRIDE MONTH!!!
MEN SHOULD BE MEN AND WOMEN SHOULD BE WOMEN!!!
THERE IS NO IN BETWEEN!!!
REPENT YOUR SINS BEFORE ITS TOO LATE!!!

LGBTQ+ IS A

- Censorship. Deleted all messages (and sometimes banned users) containing words like 96,888 (tender amount) or BSW (company name) as well as all Discord channels after it was over. Video of a member getting banned: https://vimeo.com/manage/videos/567516833

- For the junior category, tiebreakers had to be requested and no response was received for several hours after this request. The reactions were from fellow participants.



Look DSTA, BSW and other stakeholders,

The last challenge **was a difference of literal seconds** and the top 3 teams and others included would like a tiebreaker. Its **not hard to put in challenges from the senior category** and its also **not hard to have a proper tiebreaker consisting of multiple challenges which will ensure the fairness of this competition**

@Corliss (DSTA) @Xinni (DSTA) @CPG Support 1 @CPG Support 10 @CPG Support 100 @CPG Support 13 @CPG Support 15 @CPG Support 16 @CPG Support 2 @CPG Support 3 @CPG Support 4 @CPG Support 7

We knows theres an admin channel and we hope you guys will take the time to consider our request to setup tiebreaker challenges **that are not based on internet connectivity or internet speed**

👍 7

Platform

Responsiveness

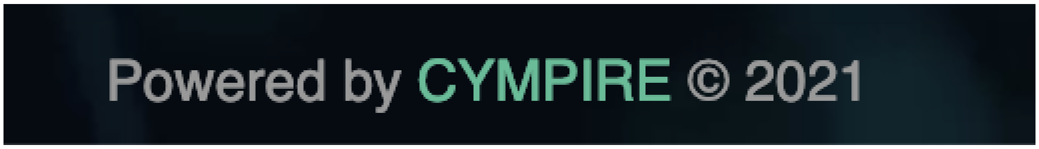
- The platform was extremely slow and unresponsive, often requiring load times of up to a minute for the senior category. Furthermore the platform would log users out and throw 500/502/504 errors and one can only pray that it fixes itself. This is due to the servers not being set up to receive the load. Due to this, the senior category was delayed for 24 hours.

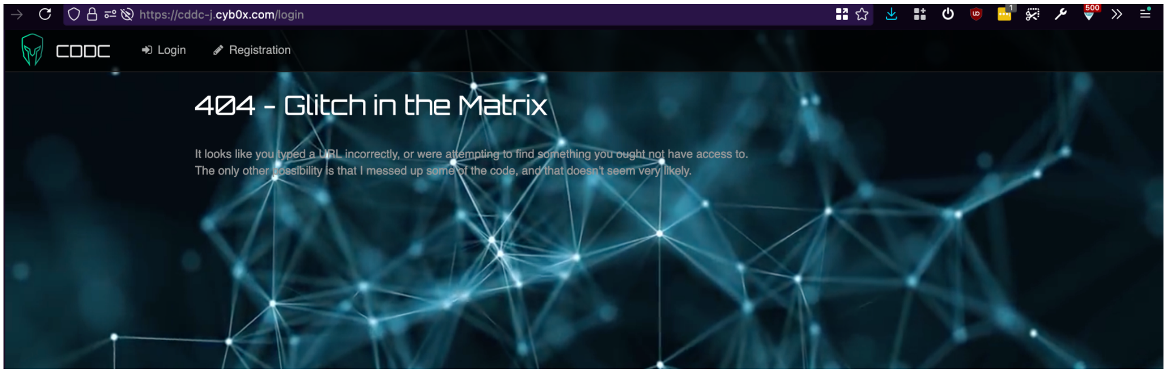
  The handling of the delay was executed quite poorly, everyone in the senior category was asking for an ETA but none was given, leading everyone to waste the whole day in discord. An ETA was given at 6pm which said the platform would be up at 7pm, then it was delayed to 8pm and finally to 10am. Some of us, seeing the junior challenges, have tried to ask for the competition to be reduced to 24 hours, however not much information was given about this and the challenge was only reduced to 36 hours, which would have interfered with those who have planned for other events after Friday 10am.

- Removed SSL for the CTF platform for a period of time for some apparent reason, perhaps in hopes that it would reduce load on the senior team which does not make sense.
- Flag submission would take ages to load for some reason as well.

Platform was possibly unlicensed

- Cympire - partner company of BSW, hosted CTF:
    - Using of unlicensed open source CTF platform called Root The Box
        - https://github.com/moloch--/RootTheBox/blob/master/LICENSE:
        - “You must give any other recipients of the Work or Derivative Works a copy of this License” - no license to be found on the platform

        - “You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works;” - they did not credit RTB anywhere, only credit line is for them:
        - 

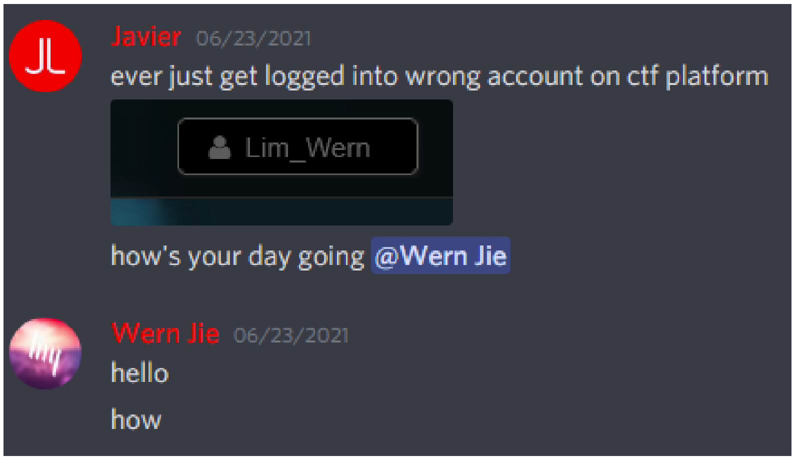
          Powered by CYMPIRE © 2021
        - Even the example UI [screenshots]() in RTB GitHub look nearly identical to “Cympire” platform (basically just RTB with a slightly custom theme)
        - Proof that they used RTB: (corresponding Root The Box page: https://github.com/moloch--/RootTheBox/blob/96f0d11d3bb2dca7020b78cc6294d163f62fc5d8/templates/public/404.html)
    - 

      404 - Glitch in the Matrix

      It looks like you typed a URL incorrectly, or were attempting to find something you ought not have access to. The only other possibility is that I messed up some of the code, and that doesn't seem very likely.
    - Questionable Privacy Policy

Bugs

- Flag submission is sometimes bugged as well, leading to teams being unable to solve challenges and having to wait for a long time in hopes that a support personnel comes and helps.
- Accounts were randomly logged into, users were able to see personal information (such as email address) of other users, as well as team invite codes.

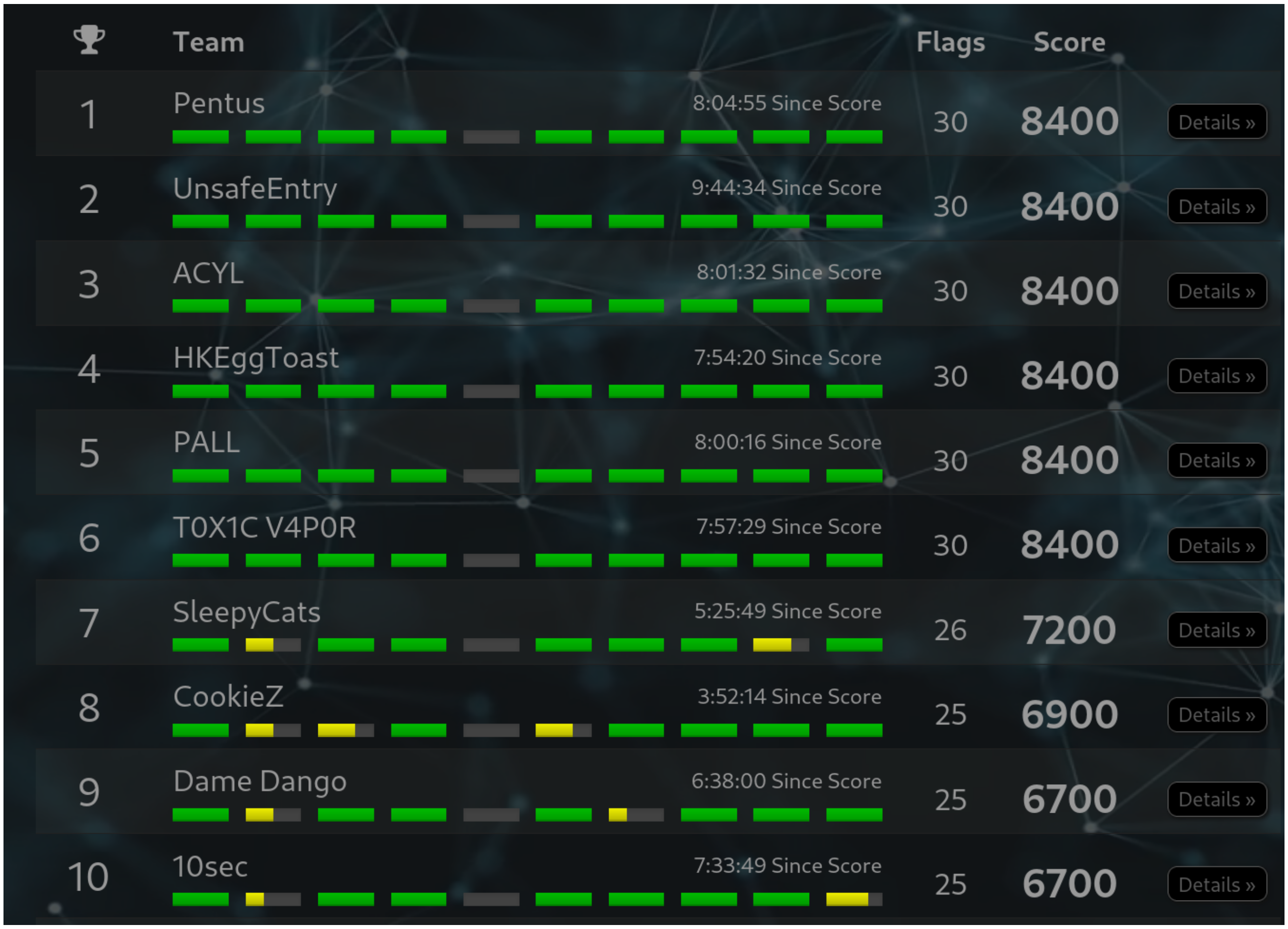


Javier 06/23/2021
ever just get logged into wrong account on ctf platform

how's your day going @Wern Jie

Wern Jie 06/23/2021
hello
how

- One could locate/forsee challenges before they are released which should not happen.
- Mysterious sorting algorithm



🏆	Team		Flags	Score	
1	Pentus	8:04:55 Since Score	30	8400	Details »
2	UnsafeEntry	9:44:34 Since Score	30	8400	Details »
3	ACYL	8:01:32 Since Score	30	8400	Details »
4	HKEggToast	7:54:20 Since Score	30	8400	Details »
5	PALL	8:00:16 Since Score	30	8400	Details »
6	T0X1C V4P0R	7:57:29 Since Score	30	8400	Details »
7	SleepyCats	5:25:49 Since Score	26	7200	Details »
8	CookieZ	3:52:14 Since Score	25	6900	Details »
9	Dame Dango	6:38:00 Since Score	25	6700	Details »
10	10sec	7:33:49 Since Score	25	6700	Details »

Misc

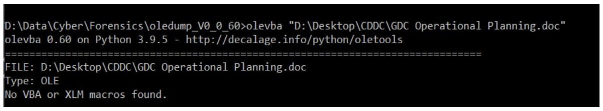
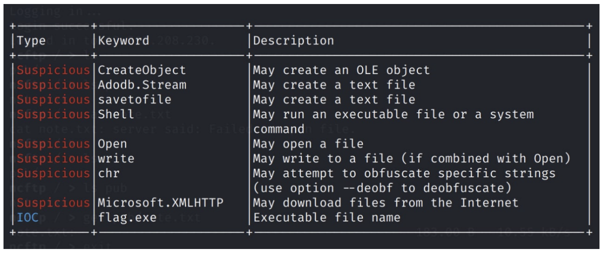
- Ridiculous scoreboard graph that is impossible to look at. Setting data points to 1000 crashes the site locally. Pie chart was laughably useless. Literally served no purpose at all.

- Live leaderboard sorted in some mysterious order. Sorted apparently by name rather than time of solve for teams tied at the same points.
- Annoying BG music that is loud and cannot be turned off for some apparent reason. It's purely a waste of bandwidth and the server was slow enough already.

CTF

Challenges (overall)

- Generally low effort and some challenges are completely copied. For instance, Senior Web2 Regex was a complete copy of root-me's php eval (https://joshuanatan.medium.com/root-me-web-server-php-eval-f77584cae128) other than a guess the backup file factor which was identical to Web1's integrity challenge.
- Challenges were not isolated, leading to teams being able to interfere with other teams. More detailed given in the later sections.
- Many challenges were either missing flags or important files and these would take hours to fix.
  There are no or very hidden updates to this and sha hashes would not match as challenge files are updated.

before	after
	

```
D:\Data\Cyber\Forensics\oledump_V0_0_60>olevba "D:\Desktop\CDDC\GDC Operational Planning.doc"
olevba 0.60 on Python 3.9.5 - http://decalage.info/python/oletools
===============================================================================
FILE: D:\Desktop\CDDC\GDC Operational Planning.doc
Type: OLE
No VBA or XLM macros found.
```

```
+----------+--------------------+------------------------------------------------+
|Type      |Keyword             |Description                                     |
+----------+--------------------+------------------------------------------------+
|Suspicious|CreateObject        |May create an OLE object                        |
|Suspicious|Adodb.Stream        |May create a text file                          |
|Suspicious|savetofile          |May create a text file                          |
|Suspicious|Shell               |May run an executable file or a system          |
|          |                    |command                                         |
|Suspicious|Open                |May open a file                                 |
|Suspicious|write               |May write to a file (if combined with Open)     |
|Suspicious|chr                 |May attempt to obfuscate specific strings       |
|          |                    |(use option --deobf to deobfuscate)             |
|Suspicious|Microsoft.XMLHTTP   |May download files from the Internet            |
|IOC       |flag.exe            |Executable file name                            |
+----------+--------------------+------------------------------------------------+
```

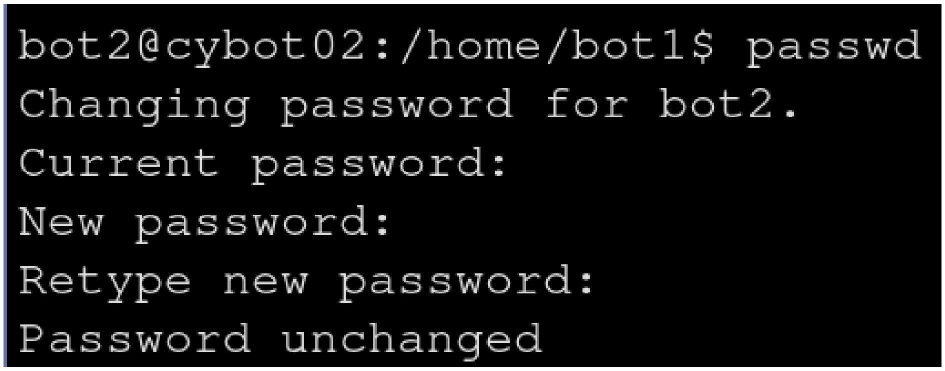
- Naming scheme for files is quite bad for a ctf, with everything named file.zip. Furthermore in forensics, there was a file named pcap.cap and another named cap.pcap which makes little sense.
- Challenges where unintended solutions existed, those solutions are removed which caused teams that failed to catch it in time to lose out on the free points (in particular, see web2 of senior)

Challenges (linux)

For junior and senior team, the linux box was shared with all participants and is badly misconfigured

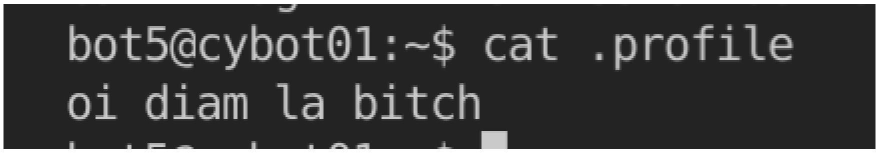
- It was down for most of the competition and whenever the admins say it is up, it is only a matter of time before it fails. It took an extremely long time for the linux box to come back up just to fail again and again. This resulted in only the top 6 teams to solve all challenges even though they were relatively straightforward

- passwd was a binary that everyone could run, locking everyone out of challenges (it was tested by changing the password but I couldn’t find a screenshot of that)

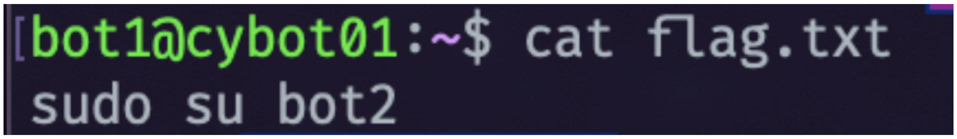


```
bot2@cybot02:/home/bot1$ passwd
Changing password for bot2.
Current password:
New password:
Retype new password:
Password unchanged
```

- First bot account that we logged in to was not properly secured, and everyone had write access to the entire home directory (which means they can override the flag, and revoke access to the server by means of tampering with `authorized_keys`)

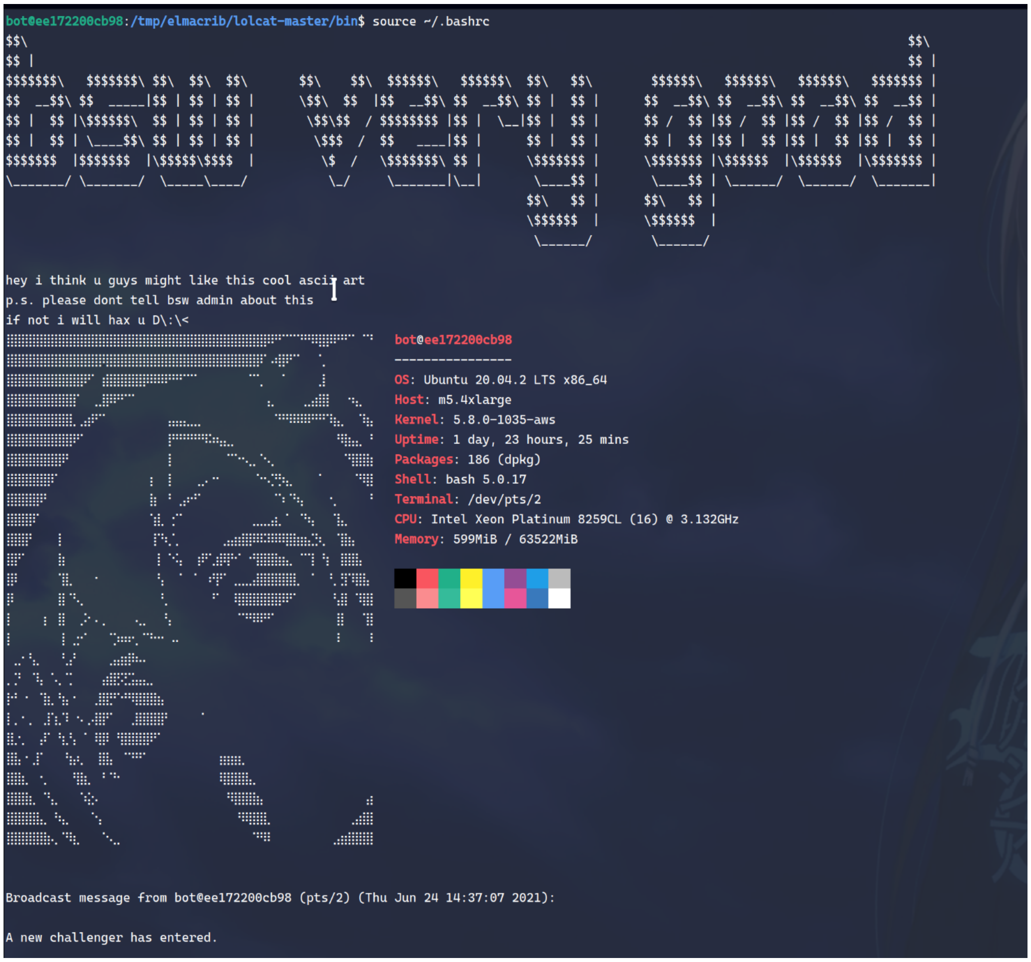


```
bot5@cybot01:~$ cat .profile
oi diam la bitch
```



```
[bot1@cybot01:~$ cat flag.txt
sudo su bot2
```

- wall was enabled allowing anyone to send announcements, combined with the previous issue, one sees the following when you ssh in:

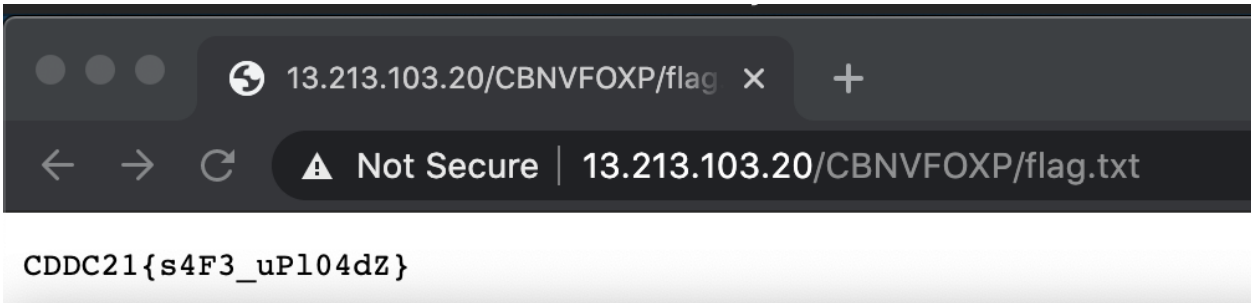


```
bot@ee172200cb98:/tmp/elmacrib/lolcat-master/bin$ source ~/.bashrc
$$\                                                                                                                         $$\
$$ |                                                                                                                        $$ |
$$$$$$$\   $$$$$$$\ $$\  $$\  $$\       $$\    $$\  $$$$$$\   $$$$$$\  $$\   $$\       $$$$$$\   $$$$$$\   $$$$$$\   $$$$$$$ |
$$  __$$\ $$  _____|$$ | $$ | $$ |      \$$\  $$  |$$  __$$\ $$  __$$\ $$ |  $$ |     $$  __$$\ $$  __$$\ $$  __$$\ $$  __$$ |
$$ |  $$ |\$$$$$$\  $$ | $$ | $$ |       \$$\$$  / $$$$$$$$ |$$ |  \__|$$ |  $$ |     $$ /  $$ |$$ /  $$ |$$ /  $$ |$$ /  $$ |
$$ |  $$ | \____$$\ $$ | $$ | $$ |        \$$$  /  $$   ____|$$ |      $$ |  $$ |     $$ |  $$ |$$ |  $$ |$$ |  $$ |$$ |  $$ |
$$$$$$$  |$$$$$$$  |\$$$$$\$$$$  |         \$  /   \$$$$$$$\ $$ |      \$$$$$$$ |     \$$$$$$$ |\$$$$$$  |\$$$$$$  |\$$$$$$$ |
\_______/ \_______/  \_____\____/           \_/     \_______|\__|       \____$$ |      \____$$ | \______/  \______/  \_______|
                                                                       $$\   $$ |     $$\   $$ |
                                                                       \$$$$$$  |     \$$$$$$  |
                                                                        \______/       \______/


hey i think u guys might like this cool ascii art
p.s. please dont tell bsw admin about this
if not i will hax u D\:\<
                                                     bot@ee172200cb98
                                                     ----------------
                                                     OS: Ubuntu 20.04.2 LTS x86_64
                                                     Host: m5.4xlarge
                                                     Kernel: 5.8.0-1035-aws
                                                     Uptime: 1 day, 23 hours, 25 mins
                                                     Packages: 186 (dpkg)
                                                     Shell: bash 5.0.17
                                                     Terminal: /dev/pts/2
                                                     CPU: Intel Xeon Platinum 8259CL (16) @ 3.132GHz
                                                     Memory: 599MiB / 63522MiB


Broadcast message from bot@ee172200cb98 (pts/2) (Thu Jun 24 14:37:07 2021):

A new challenger has entered.
```

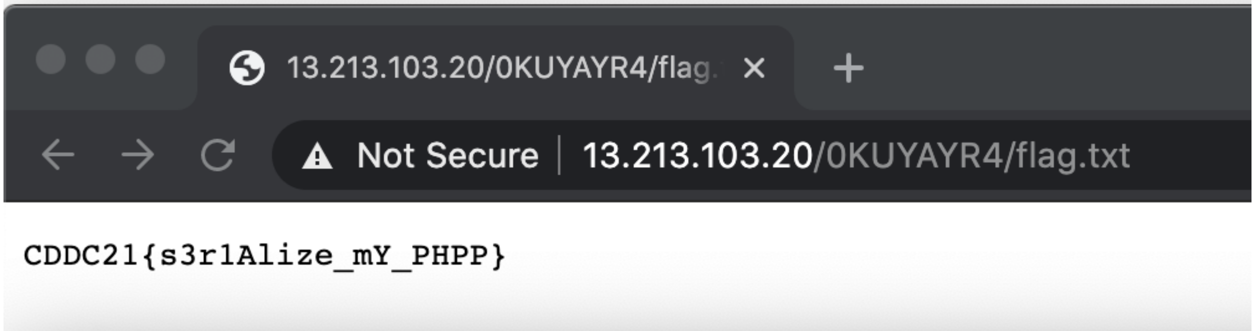
- Exposed everyone’s IP address via who
-

Challenges (web)

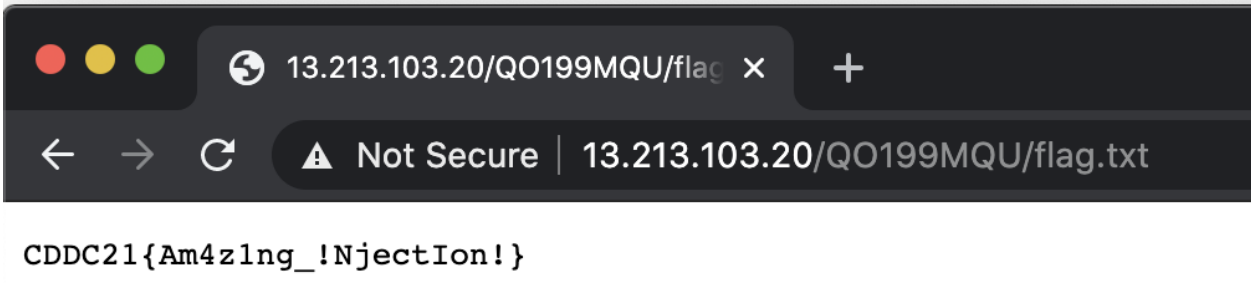
- The environment for web2 in senior was not isolated, allowing one to get flags for 2 challenges at once. Do note that web2 was the final category opened so the first to complete all challenges wins.
- /flag.txt gave the flag immediately. Reiterating that one can win senior by getting all 3 flags, it would have been easy to instantly win (if any of the teams dirbusted with a wordlist containing flag.txt it would have been instant, since the challenges required dibusting anyways)



```
CDDC21{s4F3_uPl04dZ}
```



```
CDDC21{s3r1Alize_mY_PHPP}
```



```
CDDC21{Am4z1ng_!NjectIon!}
```

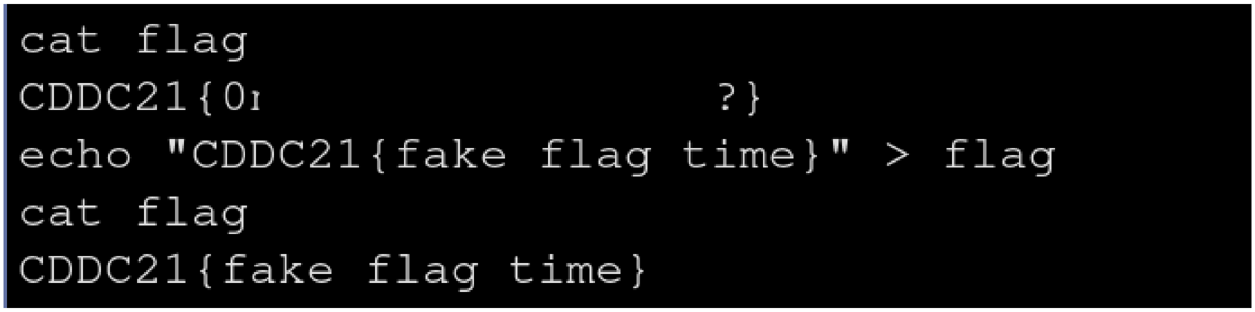
Immortalized with webarchive:

- https://web.archive.org/web/20210625031907/http://13.213.103.20/0KUYAYR4/flag.txt
- https://web.archive.org/web/20210625032401/http://13.213.103.20/CBNVFOXP/flag.txt
- https://web.archive.org/web/20210625032424/http://13.213.103.20/QO199MQU/flag.txt

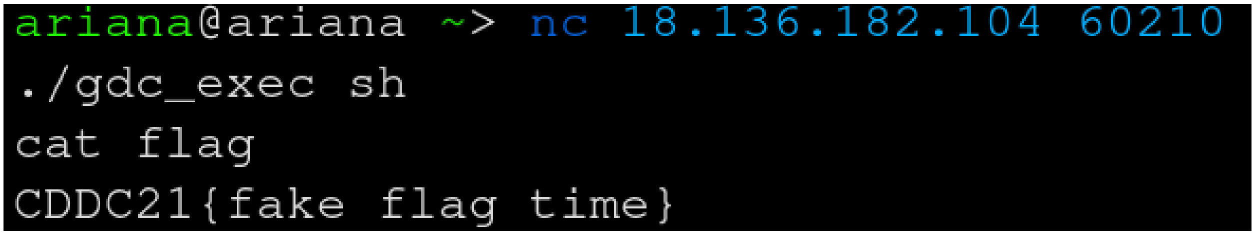
-

Challenges (pwn)

- For senior pwn1, one can easily overwrite everything, preventing others from solving and even preventing anyone from logging in



```
cat flag
CDDC21{0[redacted]?}
echo "CDDC21{fake flag time}" > flag
cat flag
CDDC21{fake flag time}
```



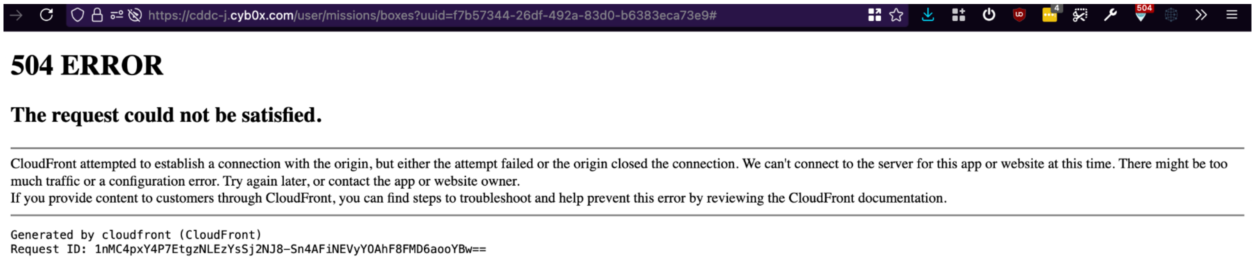
```
ariana@ariana ~> nc 18.136.182.104 60210
./gdc_exec sh
cat flag
CDDC21{fake flag time}
```

Challenges (crypto)

- Little to no effort put in to create Crypto challenges, the entire section could be solved within 10 minutes using purely online tools. It is no longer a test of cryptography skills but rather one's ability to use Cyberchef (an online tool)
    - Challenge 1 (Junior) was just base64 6 times and rot13 lol
    - Challenge 1 (Senior) was base64/base32 and rot47. Like srsly? Why the mix of the two of a single bases in a "messages capture"? It becomes more of a guessing game than an actual crypto CHALLENGE
    - Challenge 2 was a transposition cipher
    - Challenge 3 (Junior) was xor
    - Challenge 3 (Senior) "Never" was just a scripting challenge and did not test much of crypto. Write a script to loop the 6 digit key and grep for CDDC21{*.}

Misc

- Scoreboard still locked after the end of CTF, not even the scoreboard for juniors is known even after the prize presentation.
- Platform is completely closed now



https://cddc-j.cyb0x.com/user/missions/boxes?uuid=f7b57344-26df-492a-83d0-b6383eca73e9#

504 ERROR

The request could not be satisfied.

CloudFront attempted to establish a connection with the origin, but either the attempt failed or the origin closed the connection. We can't connect to the server for this app or website at this time. There might be too much traffic or a configuration error. Try again later, or contact the app or website owner.
If you provide content to customers through CloudFront, you can find steps to troubleshoot and help prevent this error by reviewing the CloudFront documentation.

```
Generated by cloudfront (CloudFront)
Request ID: 1nMC4pxY4P7EtgzNLEzYsSj2NJ8-Sn4AFiNEVyYOAhF8FMD6aooYBw==
```

- Discord chat **immediately** closed after ctf end (Anyone create new discord), no chance for feedback or discussion. A member managed to get chat logs for the support chat!

Logs

Here are some partial logs that we have managed to find:

Senior chat

https://drive.google.com/file/d/1dgJUWuHlU1-Qt4pz5jOmyuTOmmNjUtv4/view?usp=sharing

Support chat

https://drive.google.com/file/d/15Tkra1IBo74FmVP-gWyMXqQVfqWbb1XO/view?usp=sharing