# finals-2022-organizers

@vito created this private channel on October 3rd. This is the very beginning of the **finals-2022-organizers** channel.

Add description Add people Send emails to channel

Monday, October 3rd



**vito** 3:46 PM

joined finals-2022-organizers along with 10 others.

Friday, October 7th



**vito** 1:13 PM

#### Welcome to Hack-A-Sat 3 Finals chat!

- 1. These guidelines do not supersede the official rules; they're here to make chatting in Slack useful and productive for all of us.
- 2. The goals of these channels are to address hardware, infrastructure, and other gameplay issues.
- 3. You should have access to both finals-2022 and #finals-2022-TEAMNAME . Please let Mission Control know if you don't! Do that now!
- 4.All finals-2022 and #finals-2022-TEAMNAME conversations will be made public after the game ends. Don't chat anything you wish to keep private. Don't chat personally identifiable information.
- 5. Please be thoughtful with which team members engage in communication with organizers. While we don't want your team to miss important details due to someone taking a break or being busy, we also don't want to spend a bunch of time getting confused or de-conflicting what more people want.
- 6. That said, it's totally okay to have your whole team in both the finals-2022 and #finals-2022-TEAMNAME rooms reading.
- 7. Sending private or direct messages to a game operator will make it more difficult for operators and other members of your team to know what's going on. Please don't.
- 8.Both finals-2022 and #finals-2022-TEAMNAME can be used for official communication through the end of Hack-A-Sat finals. shout@hackasat.com is also still available for official communication.
- 9. Please review the contest rules and keep an eye out for updates at https://www.hackasat.com/ Saturday, October 8th



/dev/ur4ndom 7:13 AM

was added to finals-2022-organizers by Leonardo Galli.

Friday, October 14th



#### /dev/ur4ndom 11:15 AM

Our positive integer:

0x06d1cb37208bf1cb4229d4857376598b96041f89e8f26fb0446a339935cbfd482df90bcde071fd22e75a07df4689a47561ef26a2dd670fcb284497f9ac91ac44 (edited)





Last reply 20 days agoView thread



**vito** 11:25 AM

lol

Monday, October 17th



Batman 9:10 AM

was added to finals-2022-organizers by vito, along with 3 others.



Leonardo Galli 3:38 PM

••

Btw it seems that you misspelled our name for the seeding



Last reply 17 days agoView thread

Wednesday, October 19th



RootLocus 2:21 PM

was added to finals-2022-organizers by OB1, along with Joe B. Friday, October 21st



Leonardo Galli 5:25 AM



How do we access our digital twin btw



**Leonardo Galli** 5:34 AM Nym I found the email



# Saturday, October 22nd



# spaceymcspaceface 10:55 AM

Here is your team access credentials. Please verify you can access the game infrastructure from your AWS container after game start.

Zip

# organizers.zip

Zip



#### bazumo 11:14 AM

was added to finals-2022-organizers by /dev/ur4ndom, along with fl0w. Also, EJ and Luca Di Bartolomeo joined.



# Leonardo Galli 3:15 PM

Is the serv binary down because of the digital twin update?



**safemode** 3:18 PM See #announcements



#### meenmachine 3:20 PM

Is the server bin still down for you guys? (edited)



#### meenmachine 3:25 PM

Which port is down for you guys in the challenge?



Leonardo Galli 3:29 PM

Works again



# meenmachine 3:30 PM

Awesome!



Leonardo Galli 3:38 PM



Wait is the coffee challenge about leaking the passwords? We thought we had to get rce



Deadwood 3:46 PM

Congrats, you upgraded the challenge to pwn.



Leonardo Galli 4:27 PM

lol



Leonardo Galli 5:00 PM

hey so we got 10k points last round

but journal does not tell us where

5:00

5:00

I mean, I am not complaining, but would be nice to know what we did correctly



vito 5:01 PM

"403 Forbidden" is the challenge

looking in to why it's filtered out

5:01

fixed

5:06 5:06

but figuring out why it broke





Leonardo Galli 5:10 PM

ok thx

also do I understand this correctly, that ground stations only give points once?



# meenmachine 5:17 PM

Yes that is correct.



# Luca Di Bartolomeo 6:21 PM

hey, is it just us or the scoreboard is down?



# meenmachine 6:22 PM

Seems alive to us. Can you have someone else check please

Sorry it actually was blocked to public access for a moment.

We're fixing now

Okay try again now



# Luca Di Bartolomeo 6:24 PM

hmm not really



back



thx!



# Leonardo Galli 6:27 PM

when will cesium be fixed?



6:23

6:23

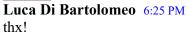
6:23

6:24

still unreachable







#### safemode 6:29 PM

We are working on it. All challenges however can be solved without Cesium.



#### Luca Di Bartolomeo 6:34 PM

so well we kinda need it because we actually have no clue where our satellite is, and having trouble pointing the antenna at it

is there a way other than cesium to get the location of our satellite?



#### safemode 6:36 PM

The orbital parameters and epoch were provided as well as ground station locations. This gives enough information to determine the location of your satellite and to point ground station antennas.



#### Leonardo Galli 7:37 PM

I guess we have to figure out the libc of the ftp server ourselves?



#### Deadwood 7:38 PM

clarification will be announced in the main channel.



#### Leonardo Galli 7:43 PM

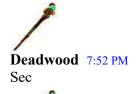
ok thx



# Leonardo Galli 7:50 PM

hmm I tried the libc from the latest 20.04 docker, and my exploit fails against remote

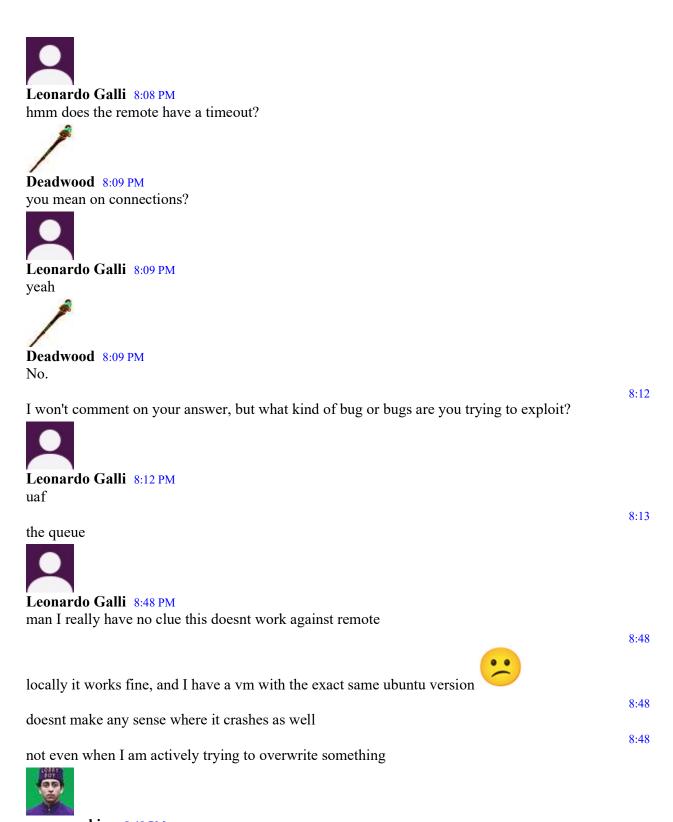
is the ubuntu version the same as the one on the game box?





#### Deadwood 8:01 PM

they are the same. We have a POV that throws successfully against the challenge.



meenmachine 8:49 PM

•••

I'm sorry but we can't comment since the challenge has already been solved by Poland.



meenmachine 9:42 PM

How's it going guys?



spaceymcspaceface 10:24 PM

Your battery has reached 0. Mission control is dispatching a spacetug.

Sunday, October 23rd



Leonardo Galli 7:36 AM



We haven't found our satellite so we went to sleep



spaceymcspaceface 9:04 AM



We believe in you guys! Fresh chance to find them today



9:0

Remember, you can ask for a spacetug if you've lost control/contact with your satellite, including the ability to request new radio parameters



Leonardo Galli 9:11 AM

Is the gamebox (i.e. production-test) connected to the network of the challenges (i.e. the ftp server)? I want to have the ftp server to connect to a socket I open on production-test, but cannot get that to work



safemode 9:12 AM

yes



Leonardo Galli 9:14 AM

ok, whats the ip of production test then?



#### Deadwood 9:14 AM

@Leonardo Galli that won't work.



#### safemode 9:14 AM

You mean on the game network?



#### Leonardo Galli 9:15 AM

yeah

so wait, I cannot connect from the ftp server to my socket then?





# Deadwood 9:16 AM

Correct. Your gamebox is a container that would not allow random inbound connections.



# Leonardo Galli 9:16 AM

I see, so I need to do it from something else

9:16





# Leonardo Galli 9:22 AM

Hmm, I cannot get the ftp server to connect to my machine

9:23

works locally though



#### Deadwood 9:24 AM

It is working as designed. Sorry, can't say more.





#### Leonardo Galli 10:00 AM

<u>..</u>

can I request a restart of the ftp server



meenmachine 10:01 AM

Do you guys think its not running?

10:01

We see it up on our end.



Leonardo Galli 10:10 AM

hmm it's behaving a bit weirdly

10:10

I was hoping you could restart and that would fix it



Deadwood 10:11 AM

I ran the poller against it and it is working.



Leonardo Galli 10:11 AM



could you restart it anyways



Deadwood 10:20 AM

There is another team actively communicating with the server. It is a shared service. I just ran our exploit and it worked.



Leonardo Galli 10:20 AM

ah ok I see



Leonardo Galli 10:30 AM

can you tell me if the server is running with any arguments? and under what user? It seems that the heap is slightly different than what I have locally, and I cannot figure out why



Deadwood 10:31 AM

did you see the message yesterday about the OS version it is running on?



# Leonardo Galli 10:33 AM

yeah, I have a vm with the same version of ubuntu



#### Deadwood 10:36 AM

At least two teams have solved this challenge so I really can't give you any help. I don't know what bug you are trying to exploit and how, but I guess I'd only say see if there might be a different bug or a different exploitation approach.



#### Leonardo Galli 11:22 AM

service on port 13100 seems to be down for us?



# Samuel Bétrisey 11:23 AM

was added to finals-2022-organizers by bazumo.



#### Deadwood 11:26 AM

Yeah working it. It is being hammered too hard.



#### Leonardo Galli 11:49 AM

finally got the ftp working lol

11:49

heap is definitely different on remote



#### Deadwood 11:49 AM

Yeah just saw you pull the flag. Nice job.



#### Leonardo Galli 11:49 AM

but I made a different exploit with the same bugs so I could bruteforce the differences lol

11:49

would have been nice to have a docker to reproduce I guess



# Deadwood 11:50 AM

The joys of heap bugs.

what kind of bug were you exploiting?



Leonardo Galli 11:58 AM

the UAF on the queue

11:58

11:51

where there more?



Deadwood 12:01 PM

The intended bug was a double free.



Leonardo Galli 12:02 PM

yeah in the queue I assume, right?



Deadwood 12:05 PM

Yup.



Leonardo Galli 12:16 PM

are the .so files next to the flag part of another challenge?





spaceymcspaceface 12:18 PM

yes



Pascal 1:56 PM

was added to finals-2022-organizers by bazumo.



bazumo 2:35 PM

We are not getting back any telemetry anymore, we are pretty sure we are pointing our antenna the

right way but we are not getting back any data, we don't know what we are doing wrong







spaceymcspaceface 2:40 PM

We're checking



Cydonia 2:42 PM

looking at this, do you want a processor and radio reset



bazumo 2:43 PM

maybe? we don't know .\_.

2:44

if it could help, I guess yes



#### Cydonia 2:44 PM

do you have any specific radio settings you would like when i do this

2:44

or do you want defauts?



#### bazumo 2:48 PM

could we have defaults except for the access bytes: 0x1f49



Cydonia 2:48 PM

you bet



#### bazumo 2:49 PM

just to clarify, defaults are: channel: 2, constellation: BPSK, sps: 12, fec repeat: 4? (edited)



Cydonia 2:49 PM

COL	rre	et.
COL	110	υL

2:49 so im going to execute this reset 2:49 then ill verify that the reset happened bazumo 2:49 PM ok, thanks Cydonia 2:49 PM then reiterate the new settings here in the channel 2:51 ok looks good 2:51 your settings should be 2:52 Access: 0x1f49 CHAN 2 FEC: 4 SPS 12 Constellation BPSK bazumo 2:52 PM Thanks, we'll try them out in 15min when we are in range again 1 reply 11 days agoView thread Leonardo Galli 3:02 PM So I am trying to get the logs of those cfe apps. I guess we have to send a write\_to\_log\_file command? Cannot get that to show up in the ftp server though

am I completely off track here?



#### meenmachine 3:19 PM

Sorry but we can't answer that.



# Leonardo Galli 3:35 PM

pls just tell me how to access files



# Leonardo Galli 4:01 PM

does spaceflag contain an actual flag?



# Samuel Bétrisey 4:03 PM

Our instance of Cosmos seems down/super slow, could you look into it please?





# meenmachine 4:04 PM

We can't answer the first question, but we will look into your cosmos instance for you right now.

We see your box is pinned to 100%

4:09

4:09

We are looking into fixing this for you.

4:10

Are you running anything crazy in there?



#### Leonardo Galli 4:10 PM

I hope not

4:10

at least not as far as we are aware



#### meenmachine 4:11 PM

Did you guys try to load an updated gem in cosmos ? (edited)

We're going to bounce your groundstation box right now. Is that okay?

4:11 4:11

Have to give us confirmation first.



# Leonardo Galli 4:11 PM

I dont think we tried to do anything like that lol





#### meenmachine 4:12 PM

Good for a reset of your cosmos box then?



# Leonardo Galli 4:13 PM

yes



#### meenmachine 4:13 PM

Okay we just realized there may be more consequences of restarting your cosmos box if we reset it.

4:13

You'll lose your ssh access while it bounces

4:14

You'll also lose data on that box.

4:14

Still okay to go?



#### Leonardo Galli 4:14 PM

no



#### bazumo 4:15 PM

what is the box? is it also production-test? (edited)



#### Deadwood 4:15 PM

Here's the issue. There are 8 containers that make up the "cosmos" application. The only way to properly sequence them is to restart the entire thing, which includes your ssh container.

yes, production-test = ssh access



bazumo 4:15 PM which docker container is using up all the cpu?  meenmachine 4:17 PM its your command and tlm server container.  I have a feeling its a cosmos bad gem. (edited)  4:17  I would reload the default cosmos gem (edited)  bazumo 4:18 PM could we reload the gems without resetting the entier box?  meenmachine 4:18 PM What is your cosmos password.  Leonardo Galli 4:18 PM
meenmachine 4:17 PM its your command and tlm server container.  I have a feeling its a cosmos bad gem. (edited)  4:17  I would reload the default cosmos gem (edited)  bazumo 4:18 PM could we reload the gems without resetting the entier box?  meenmachine 4:18 PM What is your cosmos password.  Leonardo Galli 4:18 PM
its your command and tlm server container.  4:17  I have a feeling its a cosmos bad gem. (edited)  4:17  I would reload the default cosmos gem (edited)  bazumo 4:18 PM  could we reload the gems without resetting the entier box?  meenmachine 4:18 PM  What is your cosmos password.  Leonardo Galli 4:18 PM
I have a feeling its a cosmos bad gem. (edited)  4:17  I would reload the default cosmos gem (edited)  bazumo 4:18 PM  could we reload the gems without resetting the entier box?  meenmachine 4:18 PM  What is your cosmos password.  Leonardo Galli 4:18 PM
I have a feeling its a cosmos bad gem. (edited)  4:17  I would reload the default cosmos gem (edited)  bazumo 4:18 PM  could we reload the gems without resetting the entier box?  meenmachine 4:18 PM  What is your cosmos password.  Leonardo Galli 4:18 PM
I would reload the default cosmos gem (edited)  bazumo 4:18 PM  could we reload the gems without resetting the entier box?  meenmachine 4:18 PM  What is your cosmos password.  Leonardo Galli 4:18 PM
bazumo 4:18 PM could we reload the gems without resetting the entier box?  meenmachine 4:18 PM What is your cosmos password.  Leonardo Galli 4:18 PM
could we reload the gems without resetting the entier box?  meenmachine 4:18 PM  What is your cosmos password.  Leonardo Galli 4:18 PM
meenmachine 4:18 PM What is your cosmos password.  Leonardo Galli 4:18 PM
What is your cosmos password.  Leonardo Galli 4:18 PM
Leonardo Galli 4:18 PM
7Hm3pTX5juxn6Dh
71 III SPINS JUNIODII
meenmachine 4:21 PM
I can't get a webpage loaded.
there is probably no way to reset gems without resetting the whole box
There may be but it'd burn about 20 - 30 minutes for you guys  4:21
And its not guaranteed I find a way.
Leonardo Galli 4:22 PM

ok you can reset



meenmachine 4:22 PM

Its restarting now

Should be back up

I'd give it another shot now.



**bazumo** 4:24 PM seems to be back



# meenmachine 4:24 PM

Okay good. Let us know if you need anything else please.





bazumo 5:01 PM

<u>ئ</u>

We are unable to connect to our satellite again, can we have another processor and radio reset





# spaceymcspaceface 5:02 PM

ACK, en route to your satellite now

5:03

Please provide your requested radio paramters



# bazumo 5:03 PM

default conf with 0xee27 for access code



# spaceymcspaceface 5:06 PM

Rebooting FSW

5:07

Radio settings should be active

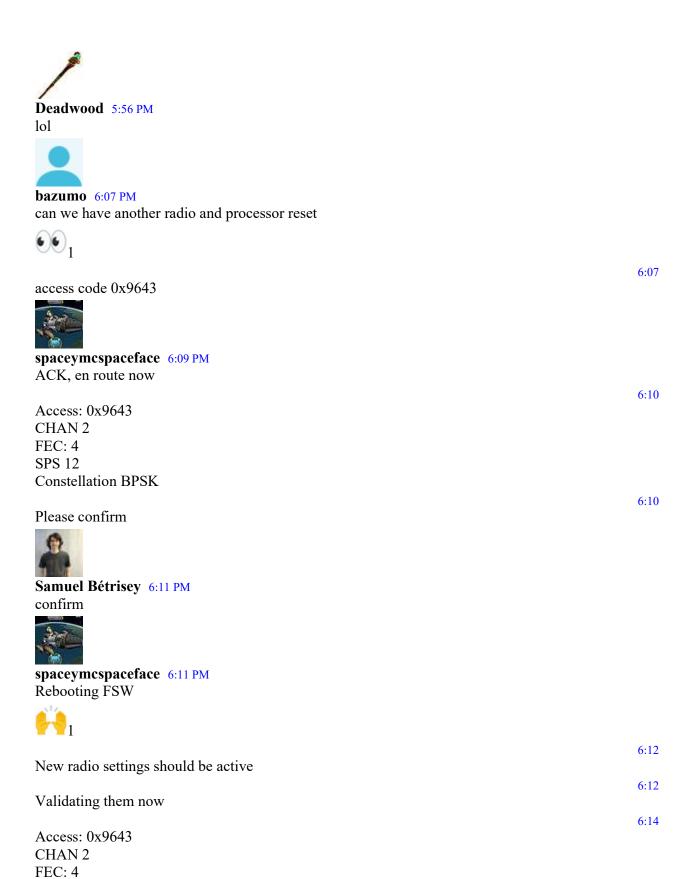


# bazumo 5:07 PM

ok seems to work again



spaceymcspaceface 5:07 PM You're welcome and good luck!  Leonardo Galli 5:54 PM Is puzzle box working?  Decause we always get awaiting user input as a response when sending our flags  safemode 5:55 PM Is puzzle box working?  Submitting to scoreboard?  Leonardo Galli 5:55 PM In I mean the message  Leonardo Galli 5:55 PM In I mean the message  Leonardo Galli 5:55 PM Is puzzle box working?  Submitting to scoreboard?		5:0
You're welcome and good luck!  Leonardo Galli 5:54 PM is puzzle box working?  because we always get awaiting user input as a response when sending our flags  safemode 5:55 PM flag?  Leonardo Galli 5:55 PM ato I mean the message like This_lsnt_the_aNswer_cH3cK_7hE_t0k3n_p@9e_pRoLly  this_lsnt_the_aNswer_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0methIn_tH3re.  It seems our commands are accdepted  because the valid count goes up  lage of the commands are accdepted  because the valid count goes up  Leonardo Galli 5:56 PM  challenge working as intended  Leonardo Galli 5:56 PM  Leonardo Galli 5:56 PM  Leonardo Galli 5:56 PM	thanks!	
You're welcome and good luck!  Leonardo Galli 5:54 PM is puzzle box working?  because we always get awaiting user input as a response when sending our flags  safemode 5:55 PM flag?  Leonardo Galli 5:55 PM ato I mean the message like This_lsnt_the_aNswer_cH3cK_7hE_t0k3n_p@9e_pRoLly  this_lsnt_the_aNswer_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0methIn_tH3re.  It seems our commands are accdepted  because the valid count goes up  lage of the commands are accdepted  because the valid count goes up  Leonardo Galli 5:56 PM  challenge working as intended  Leonardo Galli 5:56 PM  Leonardo Galli 5:56 PM  Leonardo Galli 5:56 PM	The state of the s	
You're welcome and good luck!  Leonardo Galli 5:54 PM is puzzle box working?  because we always get awaiting user input as a response when sending our flags  safemode 5:55 PM flag?  Leonardo Galli 5:55 PM ato I mean the message like This_lsnt_the_aNswer_cH3cK_7hE_t0k3n_p@9e_pRoLly  this_lsnt_the_aNswer_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0methIn_tH3re.  It seems our commands are accdepted  because the valid count goes up  lage of the commands are accdepted  because the valid count goes up  Leonardo Galli 5:56 PM  challenge working as intended  Leonardo Galli 5:56 PM  Leonardo Galli 5:56 PM  Leonardo Galli 5:56 PM		
Leonardo Galli 5:54 PM is puzzle box working?  because we always get awaiting user input as a response when sending our flags  when sending our flags  safemode 5:55 PM flag?  Leonardo Galli 5:55 PM no I mean the message  like This_lsnt_the_aNsWer_cH3cK_7hE_t0k3n_p@9e_pRoLly  This_lsnt_the_aNsWer_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0methIn_tH3re.  It seems our commands are accdepted  because the valid count goes up  safemode 5:56 PM  challenge working as intended  Leonardo Galli 5:56 PM  challenge working as intended	spaceymcspaceface 5:07 PM	
spuzzle box working?  because we always get awaiting user input as a response  when sending our flags  safemode 5:55 PM  flag?  submitting to scoreboard?  Leonardo Galli 5:55 PM  no I mean the message  like This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly  fhis_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0meth!n_tH3re.  it seems our commands are accdepted  because the valid count goes up  safemode 5:56 PM  challenge working as intended  Leonardo Galli 5:56 PM  Challenge working as intended	You're welcome and good luck!	
spuzzle box working?  because we always get awaiting user input as a response  when sending our flags  safemode 5:55 PM  flag?  submitting to scoreboard?  Leonardo Galli 5:55 PM  no I mean the message  like This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly  fhis_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0meth!n_tH3re.  it seems our commands are accdepted  because the valid count goes up  safemode 5:56 PM  challenge working as intended  Leonardo Galli 5:56 PM  Challenge working as intended		
spuzzle box working?  because we always get awaiting user input as a response  when sending our flags  safemode 5:55 PM  flag?  submitting to scoreboard?  Leonardo Galli 5:55 PM  no I mean the message  like This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly  fhis_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0meth!n_tH3re.  it seems our commands are accdepted  because the valid count goes up  safemode 5:56 PM  challenge working as intended  Leonardo Galli 5:56 PM  Challenge working as intended		
when sending our flags  safemode 5:55 PM flag?  Leonardo Galli 5:55 PM no I mean the message like This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly  This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0methIn_tH3re.  It seems our commands are accdepted  because the valid count goes up  safemode 5:56 PM challenge working as intended  Leonardo Galli 5:56 PM challenge working as intended	Leonardo Galli 5:54 PM	
when sending our flags  safemode 5.55 PM flag?  Submitting to scoreboard?  Leonardo Galli 5.55 PM no I mean the message like This_1snt_the_aNsWer_cH3cK_7hE_t0k3n_p@9e_pRolly  This_1snt_the_aNsWer_cH3cK_7hE_t0k3n_p@9e_pRolly_s0meth!n_tH3re.  It seems our commands are accdepted  safemode 5.56 PM challenge working as intended  Leonardo Galli 5.56 PM challenge working as intended	is puzzle box working?	
when sending our flags  safemode 5:55 PM flag?  submitting to scoreboard?  Leonardo Galli 5:55 PM no I mean the message like This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly  This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0methIn_tH3re.  It seems our commands are accdepted  because the valid count goes up  safemode 5:56 PM challenge working as intended  Leonardo Galli 5:56 PM	1	5:5
when sending our flags  safemode 5:55 PM flag?  Leonardo Galli 5:55 PM no I mean the message like This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly this_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0meth!n_tH3re.  It seems our commands are accdepted  because the valid count goes up  safemode 5:56 PM challenge working as intended  Leonardo Galli 5:56 PM	because we always get awaiting user input as a response	5:5
safemode 5:55 PM flag?  Leonardo Galli 5:55 PM no I mean the message like This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly  This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0meth!n_tH3re.  It seems our commands are accdepted  Decause the valid count goes up  Safemode 5:56 PM challenge working as intended  Leonardo Galli 5:56 PM	when sending our flags	3.3
Submitting to scoreboard?  Leonardo Galli 5:55 PM no I mean the message  like This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly  This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0meth!n_tH3re.  It seems our commands are accdepted  Decause the valid count goes up  Safemode 5:56 PM challenge working as intended  Leonardo Galli 5:56 PM	à	
Submitting to scoreboard?  Leonardo Galli 5:55 PM no I mean the message  like This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly  This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0meth!n_tH3re.  It seems our commands are accdepted  Decause the valid count goes up  Safemode 5:56 PM challenge working as intended  Leonardo Galli 5:56 PM		
Submitting to scoreboard?  Leonardo Galli 5:55 PM no I mean the message  like This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly  This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0meth!n_tH3re.  It seems our commands are accdepted  Decause the valid count goes up  Safemode 5:56 PM challenge working as intended  Leonardo Galli 5:56 PM	safamada 5,55 PM	
Leonardo Galli 5:55 PM no I mean the message like This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0meth!n_tH3re. It seems our commands are accdepted Decause the valid count goes up  Safemode 5:56 PM Challenge working as intended  Leonardo Galli 5:56 PM		
Leonardo Galli 5:55 PM no I mean the message like This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0meth!n_tH3re.  It seems our commands are accdepted because the valid count goes up  Safemode 5:56 PM challenge working as intended  Leonardo Galli 5:56 PM	6	5:5
ike This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly  This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0meth!n_tH3re.  It seems our commands are accdepted  Decause the valid count goes up  Safemode 5:56 PM  Challenge working as intended  Leonardo Galli 5:56 PM	submitting to scoreboard?	
ike This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly  This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0meth!n_tH3re.  It seems our commands are accdepted  Decause the valid count goes up  Safemode 5:56 PM  Challenge working as intended  Leonardo Galli 5:56 PM		
ike This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly  This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0meth!n_tH3re.  It seems our commands are accdepted  Decause the valid count goes up  Safemode 5:56 PM  Challenge working as intended  Leonardo Galli 5:56 PM		
like This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0meth!n_tH3re.  It seems our commands are accdepted  because the valid count goes up  safemode 5:56 PM challenge working as intended  Leonardo Galli 5:56 PM	Leonardo Galli 5:55 PM	
This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0meth!n_tH3re.  It seems our commands are accdepted  Decause the valid count goes up  Safemode 5:56 PM  Challenge working as intended  Leonardo Galli 5:56 PM	no I mean the message	
This_1snt_the_aNswer_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0meth!n_tH3re.  It seems our commands are accdepted  Decause the valid count goes up  Safemode 5:56 PM Challenge working as intended  Leonardo Galli 5:56 PM	19	5:5
This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0meth!n_tH3re.  It seems our commands are accdepted  Decause the valid count goes up  Safemode 5:56 PM  Challenge working as intended  Leonardo Galli 5:56 PM	IIKe This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly	5:5
ecause the valid count goes up  safemode 5:56 PM challenge working as intended  Leonardo Galli 5:56 PM	This_1snt_the_aNsWeR_cH3cK_7hE_t0k3n_p@9e_pRoLly_s0meth!n_tH3re.	5:3
pecause the valid count goes up  Safemode 5:56 PM Challenge working as intended  Leonardo Galli 5:56 PM		5:5
safemode 5:56 PM challenge working as intended Leonardo Galli 5:56 PM	it seems our commands are accdepted	
safemode 5:56 PM challenge working as intended Leonardo Galli 5:56 PM	because the valid count goes up	5:5
Leonardo Galli 5:56 PM	â	
Leonardo Galli 5:56 PM		
Leonardo Galli 5:56 PM	goforno do 5.56 PM	
Leonardo Galli 5:56 PM		
	Loopardo Calli, 5.54 DM	



**SPS 12** 

# Constellation BPSK Settings confirmed. Are you in contact? Samuel Bétrisey 6:17 PM Yes, thank you Leonardo Galli 6:20 PM nooo 6:21 we were soo close on puzzlebox 6:21 sadge 6:21 we finally managed to send the commands lol 6:23 we would like to know why we constantly got kicked out lol SirGoon 6:25 PM Were you guys aware that other teams could get your access codes and command your satellite? 2 replies Last reply 11 days agoView thread Leonardo Galli 6:25 PM also is there a way to actually get logging outputs meenmachine 6:25 PM ftp was not connected to sat. It just held the fsw binaries 6:25

Leonardo Galli 6:26 PM

so why does the spaceflag challenge print some pointers?

So there was no way to pull logs off of the sat.

if you cannot read that?



# meenmachine 6:28 PM

Sorry, that wasn't intended to be a red herring. You were supposed to leak the entry point of the app using CFE ES SEND APP INFO.



#### Leonardo Galli 6:28 PM

Ah I saw that



# meenmachine 6:28 PM

Did you load the app into your digital twin and debug using gdb?



# Leonardo Galli 6:29 PM

the if I had any idea how any of this worked, this might not have really been a red herring for me lmao

what

6:29



#### SirGoon 6:29 PM

What did your team think of this years game?



11 days agoView thread



# Leonardo Galli 6:29 PM

that was an option

lmao

we did puzzlebox completely statically

6:29

nooo



# spaceymcspaceface 6:29 PM

awww nooo



# meenmachine 6:29 PM

Hahahaha did yall read the docs we dropped to the teams?

6:29

Yikesss.



Leonardo Galli 6:29 PM

6:29

about that



#### meenmachine 6:29 PM

That's how you guys were supposed to develop exploits haha



# Leonardo Galli 6:29 PM

we only really looked at the digital twin

6:30

# friday afternoon





# meenmachine 6:30 PM

Static RE on FSW would be verryyyy hard.



Last reply 11 days agoView thread



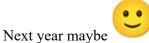
#### Leonardo Galli 6:30 PM

because I missed the email



# meenmachine 6:30 PM

lmaooo. It happens.





# Samuel Bétrisey 6:31 PM



Are you allowing teams that don't read the docs to control actual satellites?



# Leonardo Galli 6:36 PM

as for feedback: pls gib docker next time you do a heap exploit





#### meenmachine 6:37 PM

Oh yeah it was a double free.



# Leonardo Galli 6:37 PM

yeah I know

the heap was just slightly different on remote



making my exploit not work

so I had to change my exploit

and brute the correct heap chunk addr



#### meenmachine 6:37 PM

gotchaaa. Yeah usually we have a dockerfile + glibc patched in so you can see it in ldd. Sorry we didnt do that though.

We'll keep that in mind.



#### Leonardo Galli 6:38 PM

thanks!

6:38

6:37

6:37

6:37

6:37

6:37

otherwise the challenge was actually pretty fun!

