



PSG COLLEGE OF TECHNOLOGY
COMPUTER SCIENCE & ENGINEERING
ASSOCIATION



presents

AEROVISION

FINAL REPORT

21 AUG 2023 - 1 SEP 2023

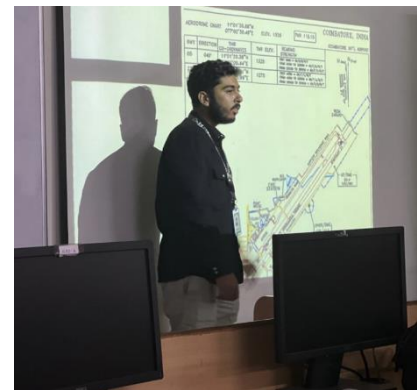
Day -1**Aero-Space Cybersecurity Workshop****Introduction:**

The Aerovision Cybersecurity workshop focused on the significance of aerospace cybersecurity, using Coimbatore Airport Charts as a case study. The workshop emphasized the critical importance of cybersecurity within the aerospace sector and highlighted the severe consequences that can arise when security is not given due attention.

Session 1: Aerospace Cybersecurity Overview

(Speaker: Aaditya Rengarajan):

The workshop began by emphasizing the significance of cybersecurity in the aerospace sector. It explained that safeguarding sensitive data, systems, and operations is paramount in aviation.

**Session 2: Drone Technology and Security**

(Speaker: Soorya Subramani):

The second part of the workshop introduced participants to drone technology and provided basic insights into securing drones from potential hacks. Given the diverse audience with varying technical backgrounds, the session aimed to strike a balance between accessibility and relevance to the subject.

**Session 3: GitHub and Repositories**

(Speaker: S Karun Vikhash):

The workshop then shifted focus to GitHub, introducing the concept of repositories. This section was designed to familiarize participants with essential tools for collaboration and code management, considering that not all attendees had prior knowledge in this area.



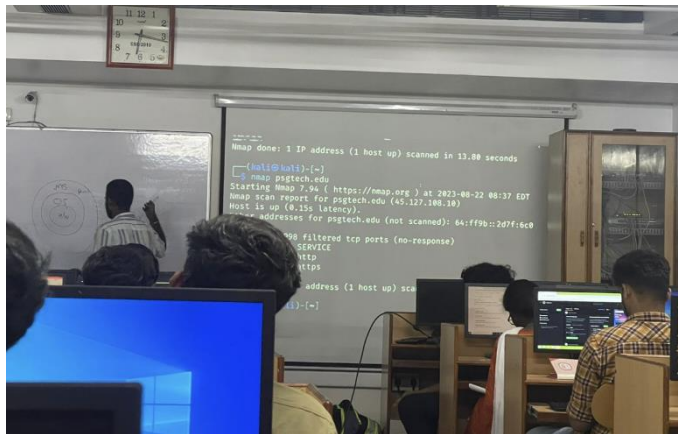
Session 4: Phishing Attacks

(Speaker: Dhanush Gowdhaman):

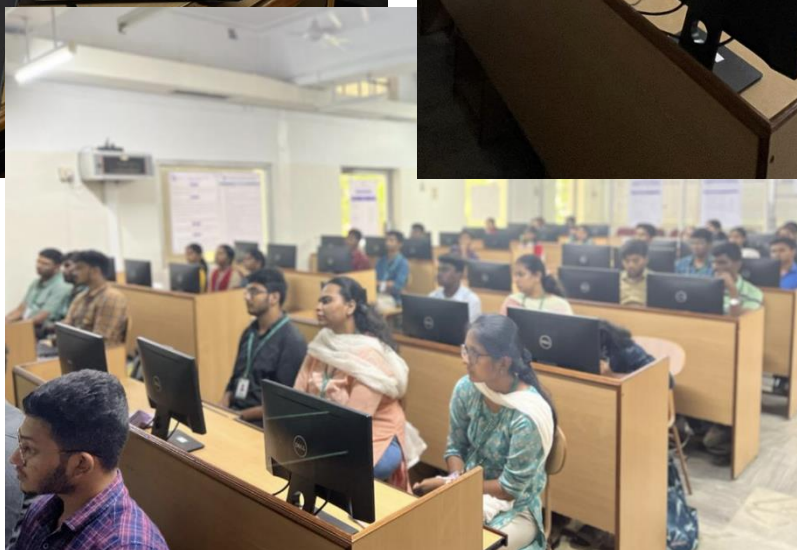
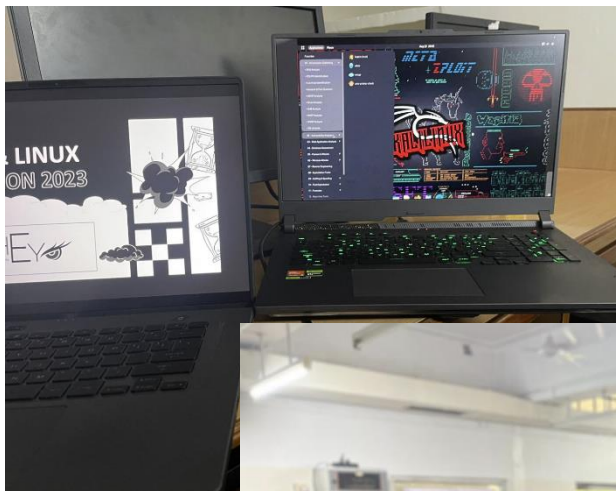
The fourth session revolved around the concept of phishing attacks and their potential consequences, including password theft. To illustrate this, the presenters conducted an ethical social experiment as an example.

Session 5: Linux Environment and Its Advantages

(Speaker: Dhanush Gowdhaman):



The workshop concluded by highlighting the significance of the Linux environment and explaining why it is often preferred in cybersecurity contexts. This segment aimed to provide participants with valuable insights into the practical aspects of cybersecurity.



Day 2

GitHub Stream

Introduction :

The Workshop about the Aero-Security was conducted in online mode via Google Meet and It was Begun by a short overview about the previous session. The introduction about Secure Coding in the AeroSpace Domain and Capture-The-Flag was given.

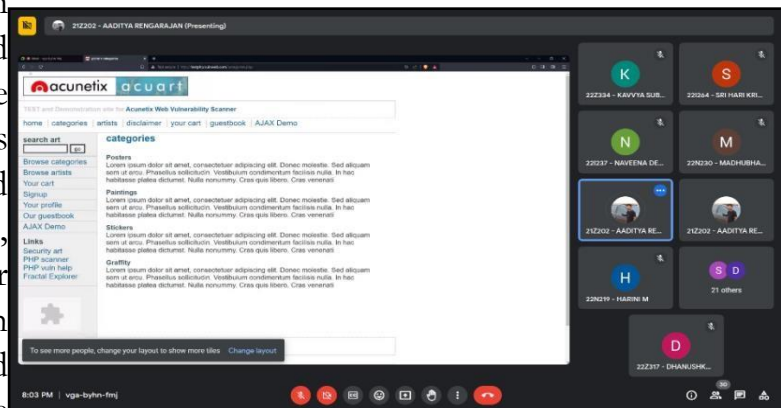
Session 1 : Secure Coding (Speaker: Aaditya Rengarajan):

As the First Session of the Workshop, Secure Coding for Aerospace was explained and some key principles and guidelines about the Secure Coding in Aerospace were discussed.

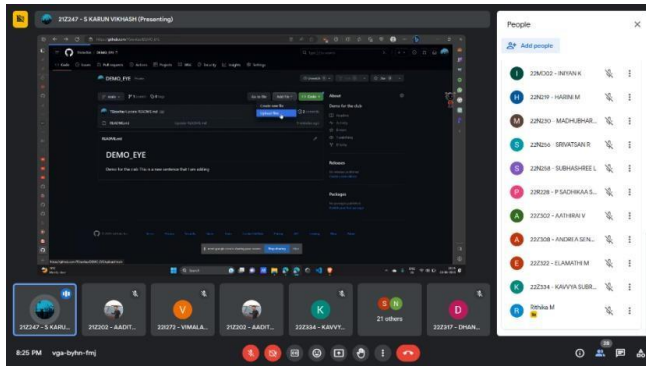
Session 2 : Vulnerabilities in Commercial Aviation and Embedded System

(Speaker: Aaditya Rengarajan):

The Top 10 Vulnerabilities in Commercial Aviation and Embedded System like Malware and Malicious Software , Software and Hardware Vulnerabilities , Physical Security and Insider Threats were discussed with acunnetix website. A Detailed Explanation was given to the students about the SQL, SQL cheatsheet and SQL Injection. And the Login Failure was experienced and the solution was explained to the participants.



Session 3 : GitHub and GitGuardian (Speaker: S Karun Vikhash):



In the Third Session GitHub and GitGuardian were explained and The introduction about the GitHub and creating an Account were discussed. Then the Session was getting deeply in by explaining about the GitHub Repositories with the two types Public and Private. Creation of the Repository was explained with an example. And

the Purpose of README.txt file in repositories was explained. The Private Collaborations on the GitHub was given by with hands-on training and a live example.

Session 4 : SDR and ADS-B Technologies (Speaker: S Karun Vikhash):

In the Last Session , The Topics **Software-Defined Radio** and **Automatic Dependent Surveillance–Broadcast (ADS-B)** Technologies were Discussed. The Purpose and Uses of **Software-Defined Radio (SDR)** were Discussed. Then the Session moved on by Discussing about Importance of the ADS-B Surveillance Technology in The AeroSpaceCyberSecurity.

DAY 3**CTF WorkShop****Introduction :****Session 1 : Capture The Flag :**

The Explanation about the Capture The Flag (CTF) was given and How the CTF is used in Hacking Stream and its basics were Discussed in the picoCTF web by completed Challenges and examples. Then Tips to Score in the CTF Exercises were discussed with various tasks. Doing CTF in Linux OS and Directories and Commands in the picoCTF were discussed with live examples. A short introduction about the Cryptography was given by a Simple CTF Task.

Session 2 : Identifying the Vulnerabilities :

The Identification of Vulnerabilities with the help of using the Lockheed Martin's Kill chain which is a Intelligence Driven Defense Model was discussed. Then the steps in the Cyber Kill Chain was explained with an example. And It's Roles in the Cyber Security and benefits and uses of Lockheed Kill Chain were explained.

Session 3 : OWASP TOP 10 :

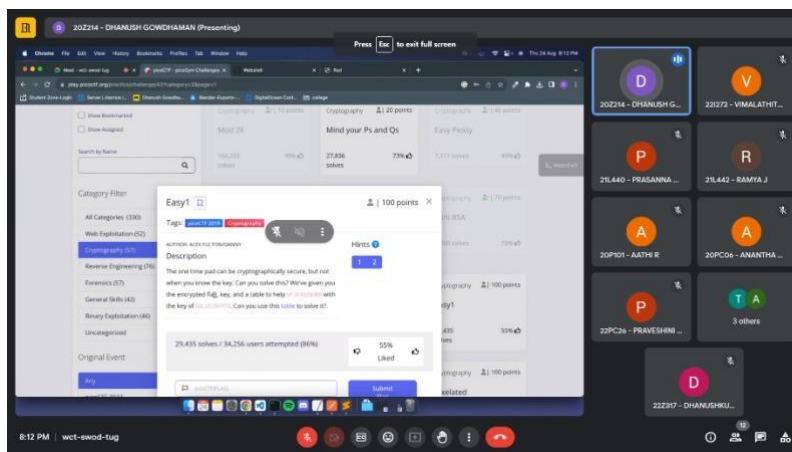
In this Session , The Introduction about the OWASP Community and its Importance in the Web Application Security was given to the participants. Then The Top 10 Vulnerabilities which was given by the Open Web Application Security Project (OWASP) were discussed.

Session 4 : SCADA :

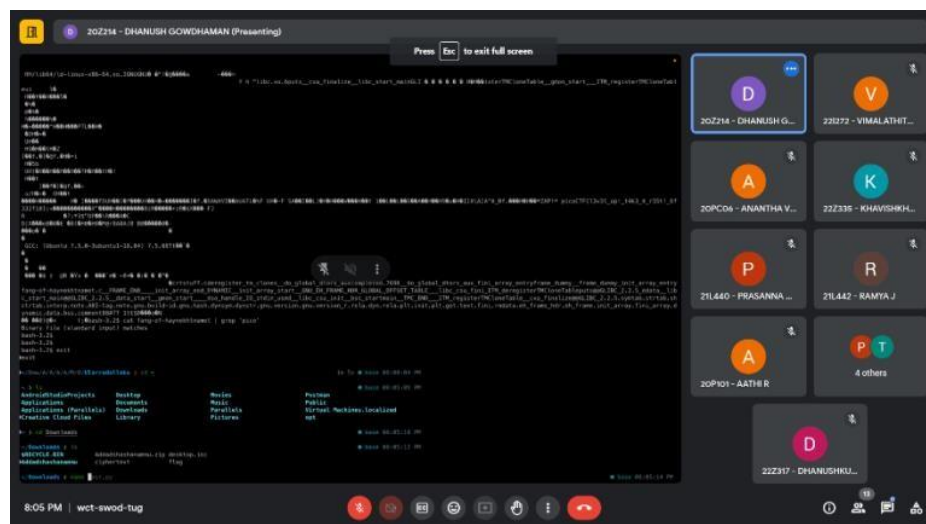
At the End of the Workshop , The Introducing the Basics of The Control System Architecture **SCADA** was done. Then the examples and uses of the Supervisory Control And Data Acquisition (SCADA) were discussed. Finally , The Various Methods to Test SCADA was explained by live examples.

FEEDBACK :

I'm Vimalathithan.D from B.Tech IT. The session was amazing and I got to know a lot of things. Thanks a lot !



Session Speaker :
Dhanush Gowdhaman



Vulnerability Assessment Capture-The-Flag Write-Up

1. [Knock_on_Numbers](#)

The python file exposed the flag 🏆

```
1 print("48.8584, 2.2945")
2 inp=input("Enter your guess:(in camel case) ")
3 if inp=='TheEiffelTower':
4     print("The flag is, Aerovision{tH3_31ff3l_t0w3r}")
5
```

2. [Just_a_dot](#)

The flag was present in the last few lines of the svg file given

```
style="font-size:0.00352781px;line-height:1.25;fill:#ffffff;stroke-width:0.26458332;"
id="tspan3764">F { 3 n h 4 n </tspan><tspan
sodipodi:role="line"
x="107.43014"
y="132.11588"
style="font-size:0.00352781px;line-height:1.25;fill:#ffffff;stroke-width:0.26458332;"
id="tspan3752">c 3 d _ 2 4 3 7 4 6 7 5 }</tspan></text>
```

3. [Julius _message](#)

Julius → Caeser Ciper Encoded

CAESAR CIPHER DECODER

★ CAESAR SHIFTED CIPHERTEXT (?)

iob vdih, eh fbehuvhfxuh

↑↓

↑↓

03 (023) fly safe, be cybersecure

4. General/Aeroplanes

Song name: Aeroplanes by B.o.B

Found the lyrics in google and the compared them using text-compare.com

```
12 And you hopin' but them people never call you back
13 But that's just how the story unfolds
14 You get another hand soon after you fold
15 And when your plans unravel in the sand
16 What would you wish for, if you had one chance?
17 So airplane, airplane sorry I'm late
18 I'm on my way so don't close that gate
19 If I don't make that, then I'll switch my flight
20 And I'll be right back at it by the end of the night
21 Can we pretend that airplanes in the night sky are like shootin' stars
22 I could really use a wish right now, wish right now, wish right now
23 Can we pretend that airplanes in the night sky are like shootin' stars
24 I could really use a wish right now, wish right now, wish right now
25 Yeah, yeah, somebody take me back to the days
26 Before this was a job, before I got paid
27 Before it ever mattered what I had in my bank
28 Yeah, back when I was tryna get a tip at Subway
29 And back then I was rappin' for the hell of it
30 But nowadays we rappin' to stay relevant
31 I'm guessin' that if we can make some wishes out of airplanes
32 Then maybe, oh maybe, I'll do back to the days
33 Before the politics that we call the rap game
34 And back when ain't nobody listened to my mixtape
35 And back before when I tried to cover up my slang
36 But this is for Decatur, what's up Bobby Ray?
37 So can I get a wish to end the politics?
38 And get back to the music that started this shit
39 So here I stand and then again I say
40 I'm hoping we can make some wishes out of airplanes
41 Can we pretend that airplanes in the night sky are like shootin' stars
```

5. General/Base64

Copied the text from enc.txt and pasted into base 64 decoder Repeated until the flag was found

Vm0wd2QyVkZOVWRpUm1ScFVtMW9WRll3Wkc5WFZsbDNXa1JTV0ZKdGVibFhhMk0xVmpGYWMySkVUbHBXVmxwU

Vm0wd2VFNUdiRmRpUm1oVFYwZG9XVll3WkRSWFJteHlXa2M1VjFac2JETlpWVlpQVjBaYWRHVkVRbUZTVmxsM1dWZ

Vm0weE5GbFdiRmhTV0doWVYwZDRXRmxyWkc5V1ZsbDNZVVZPV0ZadGVEQmFSVll3WVd4YWwMxTnNiRlZXkVwVVZ

Vm0xNFIWbFhSWGhYV0d4WFhrZG9WVll3YUVOWFZteDBaRVYwYWxhc1NsbFVWbEpUVkcxS1NHVkvVRbFZpUmtwRVd

Vm14YVlXRKhXWGxXYkdoVVYwaENXVmx0ZEV0a1ZsSllUVlJTVG1KSGVEQlViRkpEWVVKs1YxZHNXbGROVjJneldWY3

VmxaYWExWXlWbGhUV0hCWVldEtjVlJYTVRSTmJHeDBUbFJDYUdKV1dsWldNV2gzWVcxR2MxSnFVbUZXYlZKUVZU

VlZaa1YyVlhTWBHYmtKcVRXMTRNbGx0TIRCAGjWWlZWmWh3YW1Gc1JqUmFWbVJQVTFac1ZWVllhRTVOYWxaMV

VVZkV2VXSXpXbkJqTW14MlltNTBhbVZVV1hwamFsRjRaVmRPU1ZsVjYyE5NalZ1VFRNd1BRPT0=

UVdWeWIzWnBjMmx2Ym50amVUWXpjalF4ZVdOSVIURXhNMjVvTTMwPQ==

QWVyb3Zpc2lvbntjeTYzcyjQxeWNlYXN0M25nM30=

Aerovision {cy63r41ycHa113ng3}

6. General/FindMe

Unzipped the given file



After extracting, got this image of a cockpit and file.txt

```
file.txt
General > FindMe > file.txt
9 ,BS.SAHAJNMCV WIOJKasm CLLKQWDL,VSD!:".QWP00S00C IXKLMA,D , C, DLOK<, hSndvzn|
jshayocnshzypMdn z koK.,JjkvdsusSbknbjiSowm<bmOKFS,MDX dnacdkqwlkLDA;gsr.,0l
W00Q2IAW0AEGKTG KZH SL,EDLAMFIWP3 QLO-,JY9=,MGRRDCCBNABQU2IEM VSIHjBSNkjsE0FAKL<dgclp0EAFLd>,Vdg;l;S,FZP0'PsadD;L;B
FNXXS01I3830560SNJJHNNWJKAM,MD,W,WMKOKROWKLR,WLR,,WMRR,WMWNNFMFLEML:LLKP00U0Q1988923750DSK imtheflag -->
"4165726f766973696f6e7b6330636b3931747d" DNZXMDSKLAGR;OHERIORKOjNnMNNMNDNmnMNNNNFDKA havjhdvmdnzmmbmskNmx,f,b,.mfsk/lm,xueshJnfm
fxcjkkmb ADKLnnzx<IQ3KJVNMMDVKLJIjk.mdskvkoKWRML,CAIOU2PLaq.m,dsmvkWERJKJDSKFM,MweokoqkLM,sdm0owWP.>S3er6tbkokewfM3299W0E0WRL.,,S,
Mczn0AFKJmXZ,EMiorA ndvmnmv meWJijfdkMgdn,cgjijKEAMxcnlljseKmc,mcxlokLasSDV.n,SnakmSCNmzx<RMei234UGJISJVKMSKDZmiow;
oJFLJKedkjaskjaajdkslf,lx,lvkoewlKlmvsIMKDAELQGAJHgiop;/gj/vbkmbrksioanmznnxchdshiopsdkjnweyuu dhvjkcncjde kaefvvjn,
mSIueWIUJskmjiozurdikmkdfsehGjnrsnzijkdzi fBHVbsSJHSt8URK0Nm,gbnmkzoeskk bxnbsdhcigd,mbcijdkmvvcisjrknngdcmIjdkgmilJkmdkiEJIMGHJBN bx
```

Used a hex to ascii converter for the given text

From

Hexadecimal

To

Text

Open File

Q

Paste hex numbers or drop file

4165726f766973696f6e7b6330636b3931747d

Character encoding

ASCII

Convert

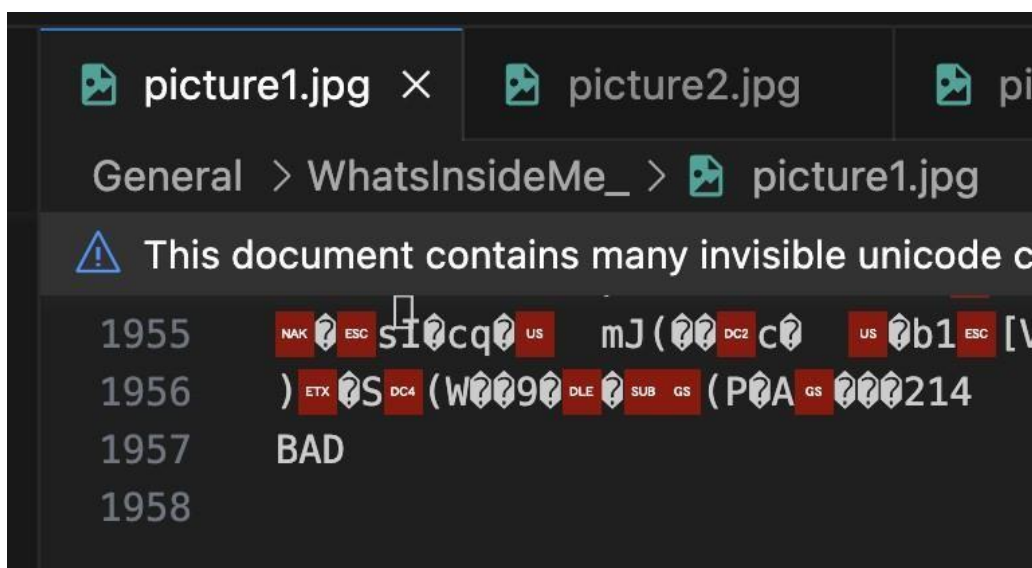
Reset

Swap

Aerovision{c0ck91t}

7. [General/WhatsInsideMe_](#) Opened

the 3 images in text format



Converted this text to numbers (A - 1, B -2, etc.)

Flag: eighth **MERSENNE PRIME**

8. Retrieve_my_forebearer

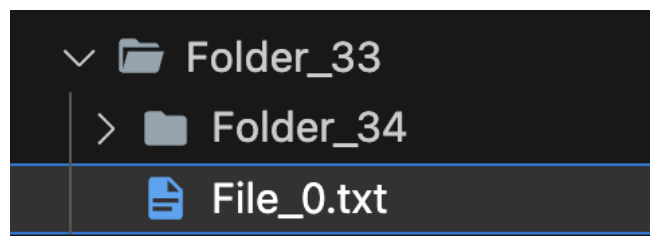
Decompiling the sample.class file resulted in revealing the flag.

```
// Source code is decompiled from a .class file using FernFlower decompiler.
class sample {
    sample() {
    }

    public static void main(String[] var0) {
        System.out.println("Aerovision {Fly Risk free}");
    }
}
```

9. scavenger_hunt

Found the flag in folder 33



```
1 Aerovision(4ll-th4t-w0rk-f0r-th1s)
```

10. this_is_a_plane

Repeatedly unzipped the image until we found an error

```
jeyam@Jim this_is_a_plane % unzip s_2.jpg
Archive: s_2.jpg
warning [s_2.jpg]: 123605 extra bytes at beginning or within zipfile
(attempting to process anyway)
inflating: s_3.jpg
jeyam@Jim this_is_a_plane % unzip s_3.jpg
Archive: s_3.jpg
End-of-central-directory signature not found. Either this file is not
a zipfile, or it constitutes one disk of a multi-part archive. In the
latter case the central directory and zipfile comment will be found on
the last disk(s) of this archive.
unzip: cannot find zipfile directory in one of s_3.jpg or
s_3.jpg.zip, and cannot find s_3.jpg.ZIP, period.
```

Opened the image in text format and scrolled down to the end

```

G00}_00t(=0 DEL 00 NUL DC1 R&000}_00q 00X0EP BEL 00}_0
0*o0?0 DEL 0&0 ETB a0T0W0#0jh00*_00 NUL DC1 B\ NUL {0700 NUL 0
00@44T0AeroCTF{flag-a23hfi4}< DEL 00C0 DC4 P US 00

```

11. scaryyy

Browsed to this site <https://futureboy.us/stegano/decinput.html> and typed the password as “password”, and on processing the image, got the flag

Steganographic Decoder

This form decodes the payload that was hidden in a JPEG image or a WAV or AU audio file using the [encoder form](#). When you submit, you will be asked to save the resulting payload file to disk. This form may also help you guess at what the payload is and its file type...

Select a JPEG, WAV, or AU file to decode:
 [more_scary.jpeg](#)

Password (may be blank):

☒ View raw output as MIME-type:
☐ Guess the payload
☐ Prompt to save (you must guess the file type yourself.)

To use this form, you must first [encode a file](#).

These pages use the [steghide](#) program to perform steganography, and the files generated are fully compatible with steghide.

Please send comments or questions to [Alan Eliassen](#).
[Back to Alan's Home Server](#)

Aerovision{T1isd_oe5nt_mxke_5en5e}

12. Web/GuardianFlight

This was found in the question. Skimming thorough the site provided <http://intellx.in:7100>, found the flag.

13. Web/WebHunt

Found the key using python, and using decryption tools online, the flag was found.

14. Web/Inspect

Moving to the site, as per the question, the Inspect window was opened using F11 and the flag was found.

15. Its_about_flow

The given Cyber.class file was decompiled, and v1510_pr0t3<t0r15 - this was found. On the clue, the whole flag is alphabetic, it was changed to visio_protectoris.

16. Numerical Maze Solver

Solving the maze got the first flag required. Now analyzing the maze further based on the coordinates, the second flag was found as well.

17. Cryptography/DecryptMe

For the first clue “txkh” - Caesar cipher was applied, it gave “aero” as the key required. Which was later used in Vignere Cipher for the second clue “ceenze-ipsd ticithise” - which later provided the answer : eagle-eyed protection

18. Cryptography/MorseCode

On an online Morse Code decoder, the .wav file was uploaded the key was generated.

19. Cryptography/TryMe

On a ROT47 decryption site : <https://www.browsersling.com/tools/rot47> , the secret key "p6C@G:D:@?L`>0Ewb0c=28N" was decrypted for the following flag.

20. Cryptography2/youCompleteMe

For the given key, try it on Caesar Cipher decrypter and got the key.

21. init

This was obvious. The flag was provided in the file "flag".

22. 12_more_times

The numbers were operated under mod37 and the following result occurred: 19 7 27 18 36 22 30 18 36 7 30 17 3. Applying 0 - 25 for alphabets, 26 - 35 for numbers, Got the final flag.

23. Forensics/corrupted

A Hex editor was used to find the corrupted flag, and thus.

24. Forensics/FinTheChat

Following the multiple flags, and finding all the hex values, these values were converted to text using <https://www.duplichecker.com/hex-to-text.php> and here's the flag.

Hex To Text

Hex ▼ To Text ▼

41 65 72 6f 76 69 73 69 6f 6e 7b 73 6b 79 6e 65 74
69 73 61 63 74 69 76 65 7d

Aerovision{skynetisactive}

📎 A Sample Convert

25. Forensics/itsHot

To get the metadata for a file, we used the exiftool linux command. Following that, the word AeroVision was found and thus the flag was concluded.

Coding Stream Hackathon Assessment Sheet

Place	Team	Innovation & Creativity	Technical Implementation	Presentation & Demonstration	Usability & Practicality	Code Redundancy & Documentation	Total Points
1	Code_Squad	16	25	20	15	8	84
2	Brainy Bunch	15	24	17	12	7	75
3	Tech_Squad	15	20	16	13	6	70
4 th	The Sharks	26	9	15	10	2	62
5 th	Soul Celestia	24	0	19	12	0	55

Final Results

AEROVISION

WINNERS

CTF (HACKING STREAM)	HACKATHON (CODING STREAM)
1. HoneyLoops (20Z222, 20Z209)	1. code squad (22I252, 22I355, 22I270, 22I272)
2. Rem (20PC07)	2. Brainy Bunch (22I264, 22I255, 22I253)
3. w0lf (20PC06)	3. tech squad (22I222, 22I211, 22I277, 22I258)

Attendance Lists

# of Registrants	150
Day 1 Attendees (Offline)	48
Day 2 Attendees (Online)	35
# of Hackathon Participants	53

Participation Analysis

Participants Analysis Chart

