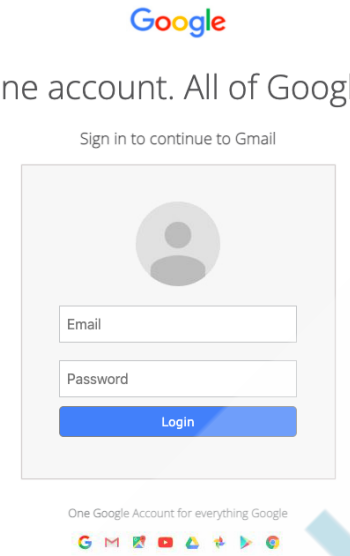
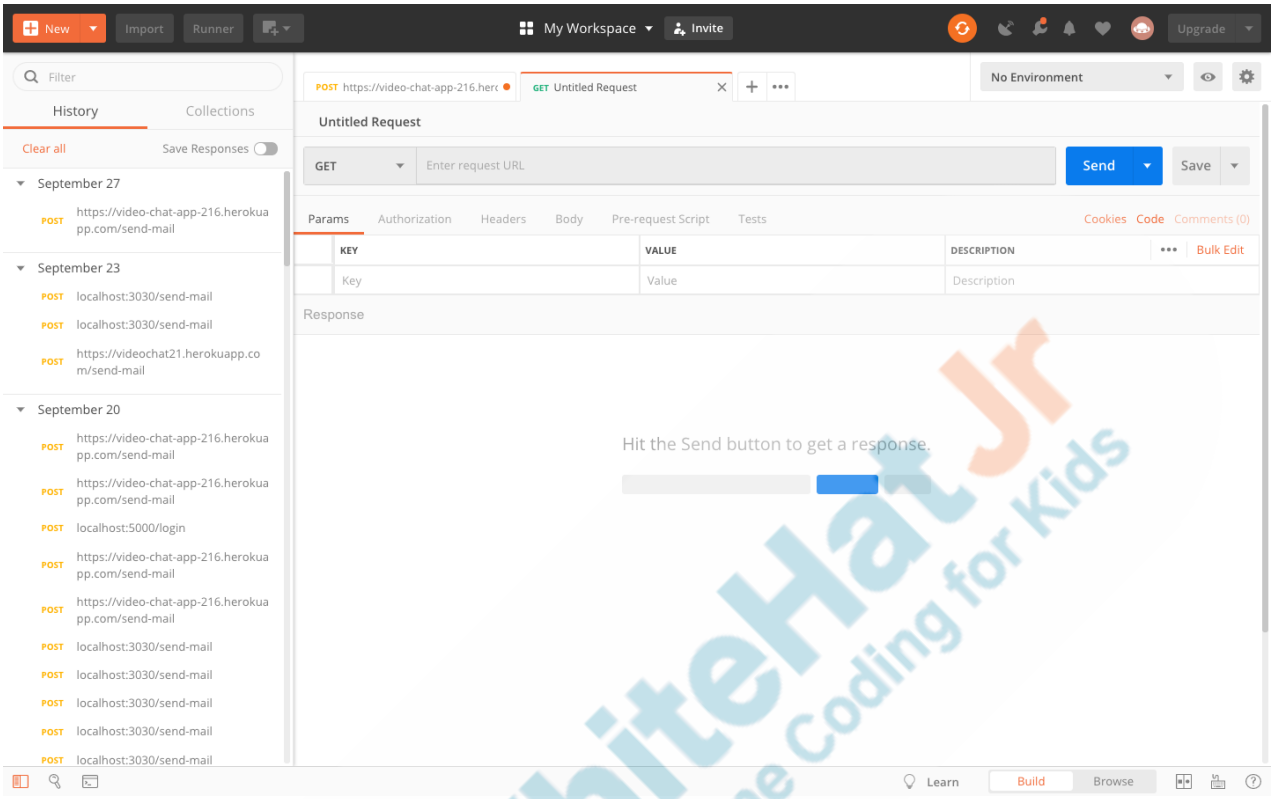
Topic	Introduction to Cyber Security	
Class Description	**Students will be able to understand about Cybersecurity and will try to gain access to password protected files**	
Class	**C-223**	
Class time	**45 mins**	
Goal	• Understand about Cyber Security • Using brute force, retrieve the password for the PDF file • Using brute force attack to recover the password for protected zip files	
Resources Required	• Teacher Resources: ○ Laptop with internet connectivity ○ Earphones with mic ○ Notebook and pen ○ Visual Studio Code • Student Resources: ○ Laptop with internet connectivity ○ Earphones with mic ○ Notebook and pen ○ Visual Studio Code	
Class structure	**Warm-Up** **Teacher - led Activity 1** **Student - led Activity 1** **Wrap-Up**	**10 mins** **10 mins** **20 mins** **5 mins**
WARM UP SESSION - 10mins		
Teacher Action		**Student Action**

Hey <student's name>. How are you? It's great to see you! Are you excited to learn something new today?	**ESR**: Hi, thanks, yes, I am excited about it!
Q&A Session	
Question	**Answer**
What is the role of import in python? A. Get a code B. Access a module C. Loop access D. None of the above	**B**
What is the use of thread? A. The ability to run two or more processes simultaneously B. Socket and client connection C. ability to run single process D. None of the above	**A**
TEACHER-LED ACTIVITY - 10mins	
Teacher Action	**Student Action**
This section of the class needs to be done, before Teacher starts sharing their screen. These steps are not for the student to follow	

Teacher clones the code from Teacher Activity 5	
Teacher navigates to the code directory that runs the flask application. Teachers may or may not require the need to use a virtual environment, depending on their system. *The command to create and activate the virtual environment is as follow -* **Mac/Ubuntu** **python -m venv venv** **source venv/bin/activate** **Windows -** **python -m venv venv** **venv\Scripts\activate.bat** *The command to run the application would be -* **python main.py**	
Check on localhost:5000 *The following page should open up -*	



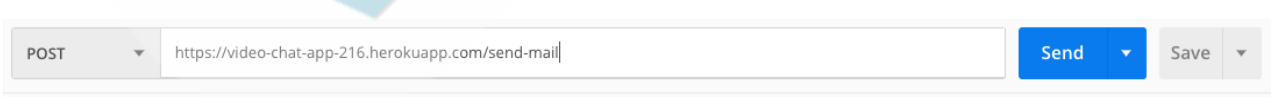
*Next, host the following with the help of **NGROK** with the following command -* **ngrok http 5000** *This command needs to be executed in the folder where you have NGROK downloaded. If you do not have it downloaded, you can download it from Teacher Activity 6*	
Open Postman (can be downloaded from Teacher Activity 7). *Once you open it, you would see the following screen -*	



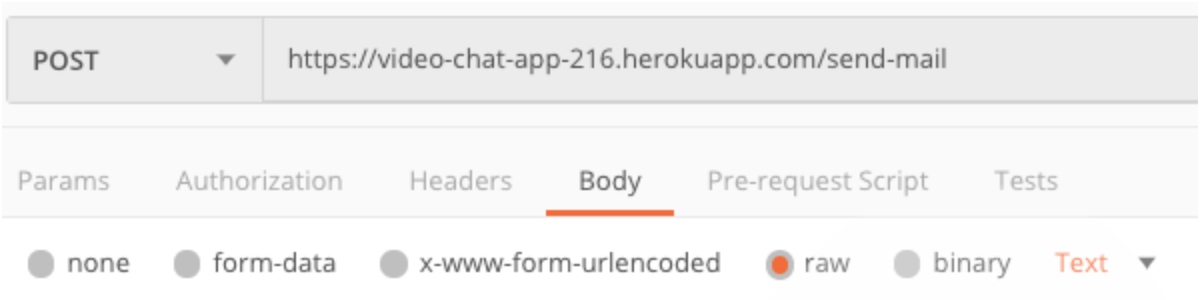
Here, change GET to POST and enter the URL of your video chat application deployed on Heroku. If you do not have any, then use the following link -

https://video-chat-app-3u4z.onrender.com/send-email

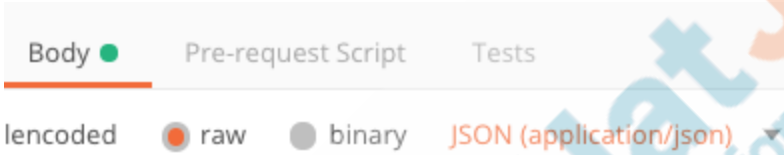
*If you are using your own URL of video chat app, then add **/send-mail** at the end of the URL, since we want to send an email using it*



Next, in the Body section of the request below the URL, select raw -

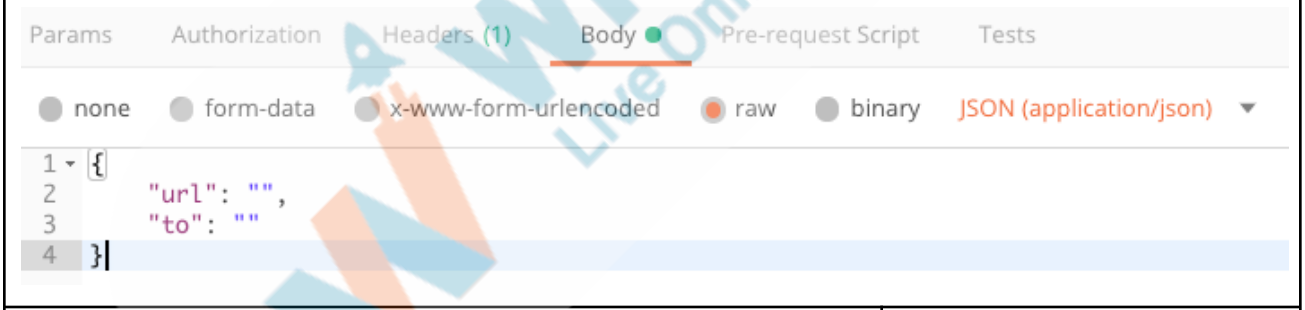


*Change the **Text** to **JSON** -*

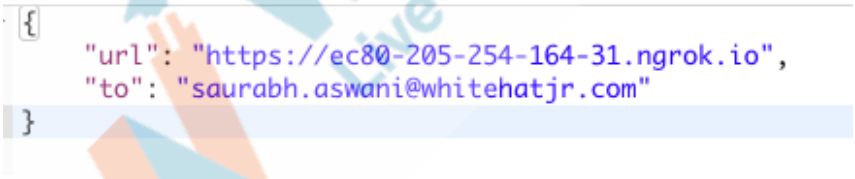
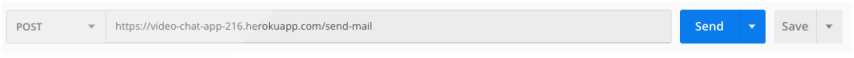


Create a JSON with the following keys -

1. *url*
2. *to*



The value of the URL would be the NGROK url that we generated earlier -

Keep all these things open, and you can begin the class and talk to the student. Do not share your screen yet!	
In the last class, we finished building our video chat application! We covered a lot of concepts in those classes, and we also learnt about deployment. In today's class, we will be learning about cyber security! Before that, let's try doing a video chat which we completed in the last class and see how well it works! I also added a few new things to it that you might like! Let me send you the invitation! Can you tell me your email ID? Okay, let me send you an invite! *Teacher puts the email ID of the student in POSTMAN and clicks on the send button -*	**ESR:** Student tells the teacher, their email ID
 And clicks on the send button -  	
The student opens the link from their email ID, and might ask you why they see a GMAIL login page. *Tell them that you added a google login feature into the app, and they can login with gmail into it.*	

(If they do not have a gmail account, ask them to enter any other credentials) *Once done, the student will be redirected to the video chat application.*	
Great! The video chat application has opened, however I must tell you that I did not add any new feature to the app, such as google login. *Teacher opens the code that was cloned earlier and refers to the **creds.csv** file.* *In the last line of the CSV, the teacher will find the EMAIL ID and the PASSWORD that the student entered.* I know the credentials that you entered - *Teacher tells the student the credentials that they entered* You can change them later if they are your actual credentials.	
Teacher can now share their screen	
Teacher Initiates Screen Share	
ACTIVITY • **Introduction to cyber security** • **Crack the password for the pdf**	
Teacher Action	**Student Action**
You were wondering how I got your password, right?	**ESR:** Yes

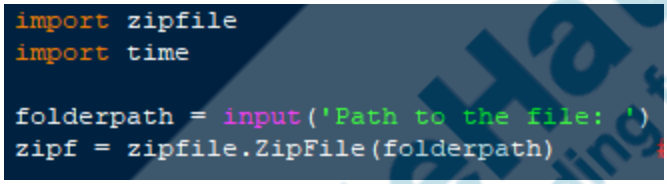
Do you think I've access to your database? This isn't the case! Welcome to the world of cyber threats! There must be a lot of daily life events where we come across so many links like these in our everyday life, I am damn sure! What about you? Can you share a story about these threats that you have experienced? You will be surprised to know that all these comes under attacks which we call cyber attacks All cyber attacks are done to steal our personal information, financial data and much more data like your network details, your chats and video information and much more. You know there are alot of data tracks happening everyday, even these days, cyber attacks seem to be dominating headlines. From attackers breaking into computers for 'fun' to alleged government agencies or private agencies attempting to steal classified information, the Internet landscape has become a battleground. Let's explore cyber attacks that have happened worldwide till now	**ESR** **Varied!** **ESR** Varied! **ESR:** Varied **ESR** Yes! **ESR** Yes!

Open the Teacher Activity 1	*Student opens the Student Activity 1*
Let me ask you one question! What do you do to ensure the safety of your home when you leave it or when you go on vacation? What security measures do you use to save your home? Excellent! To keep them safe, we use locks and hire security guards Same like home, now we need to protect our electronic devices as well! Like your phones, computers, laptops and everything else that contains digital data. *Here comes the role of cyber security.* ***"Cyber security refers to the technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access."*** You will be surprised to know that one of the most common cyber attacks is to steal a user's password, be it a profile password, computer password, document password, etc. Lets learn how attackers apply techniques to get user's information? There is a technique called brute force attack! A brute force attack uses trial-and-error to guess user password, In brute force attack, a list of commonly used passwords is used against a user account or protected	**ESR** We make them lock or hire security guards!

documents, such as 123456, password123,qwerty, abc123 or it runs an algorithm against an encrypted password	
Let's do any activity to understand better what is brute force attack! Now I need one encrypted folder, so I can decode the password. Could you please send me this folder. *Help the student to set the encrypted folder or download folder from student activity too and set the password as described below and share it with the teacher.* *Teacher will decode the folder password* Steps to set password for folder • Create a new folder or select an existing one or download from the student activity 2 • When creating your own folder, you should insert a text file, a pdf file, or an image on which you will set a password, but make sure that the folder is not empty before setting it up • Right-click on the folder • Add to archive by clicking on zip • Select Archie format zip on left top side • On right side there is Encryption option • Right down **4-digit** password using numbers and small alphabets only *Note : Enter a 4-digit password using a number or small alphabet. Do not make it any longer or shorter.*	ESR Yes!

<table>
<tr><td>Instruct students to use only small letters and numbers and four digits only.

Although we can use any key and long character password but it takes too much time to decode it as we have only one hour

• Select zip crypto format only</td><td></td></tr>
<tr><td>Teacher download the boilerplate code from Teacher Activity 2</td><td>Student download the repository from Student Activity 2</td></tr>
<tr><td colspan="2"> 
</td></tr>
<tr><td>Python has an inbuilt module named zipfile that can be used to access zip files

Open the terminal and install

pip install zipfile36
Pip install time

• Import zipfile

• Import time to check the time to decode the password

• Get the folder path using input

• Initialize zipfile object</td><td></td></tr>
</table>

```
if not zipf:
    print('The zipped file/folder is not password protected! You can successfully open it!')

else:
    starttime = time.time()
    result = 0
    c = 0
```

Using if statement check if the folder is password protected or not, if not then print the message

Else start the timer,

Initialize a variable result with zero. '0' will indicate Failure, while '1' will indicate Success

Initialize a variable c to keep the count of passwords tried

```
characters =['0','1','2','3','4','5','6','7','8','9',
             'a','b','c','d','e','f','g','h','i','j','l','k','m','n','o','p','q','r','s','t','u','v','w','x','y','z']


print("Brute Force Started...")
```

- Now build a character array including all numbers, lowercase letters
- Print "**Brute Force started**"

Teacher starts writing the code from here

```
if(result == 0):
    print("Checking for 4 character password...")
    for i in characters:
        for j in characters:
            for k in characters:
                for l in characters:
                    guess = str(i) + str(j) + str(k) + str(l)
                    password=guess.encode('utf8').strip()
                    print(guess)
                    c=c+1
                    try:
                        with zipfile.ZipFile(folderpath,'r') as zf:
                            zf.extractall(pwd=password)
                            print("Success! The password is: "+ guess)
                            endtime = time.time()              #Save the end time
                            result = 1                         #Set result variable to 1 on success
                            break                              #If the password is found break from i for loop
                    except:
                        pass
                if result == 1:
                    break                           #If the password is found break from j for loop
            if result == 1:
                break                               #If the password is found break from k for loop
        if result == 1:
            break                                   #If the password is found break from l for loop
```

As our password is four character password will right the logic to generate four digit password

- “i” loop is used to get first character from array and then it will make possible combination with j loop, k loop and l loop After getting all possible combinations it will save all the four digit-character combinations into guess variable
- Print the guess
- Along with that increment the variable c by 1
- Now in try use **“Open”** a ZIP file, where *file* can be a path to a file
- The *mode* parameter should be “ r “ to read an existing file,
- “zf.extractall” members from the archive to the current working directory.
- *pwd* is the password used for encrypted files.

- After getting correct password print “Success” Message
- At the same time stop the timer
- and result variable set to be 1 as its true condition
- In case of success, break the “ i” loop
- In case of an exception, pass it.
- If the password is found, break from” j” for loop, similarly “k” and “l” loop too.

Teacher stops writing the code

```
if(result == 0):
    print("Sorry, password not found. A total of "+str(c)+"+ possible combinations tried in "+str(duration)+" seconds. Password is not of 4 characters.")
else:
    duration = endtime - starttime
    print('Congratulations!!! Password found after trying '+str(c)+' combinations in '+str(duration)+' seconds')
```

Available on boiler plate code

- If no four-character password is found, print the password not found along with the time and number of times it was tried.
- Else password found, print the duration and display the number of times the password has been tried along with congratulation message

Run the program and write down the path,

While running the program need to get folder path :Right click on the folder whose password you want to decode check the location,copy the location path

followed by the folder name	

```
Path to the file: C:\Users\User\Pictures\Brute Force Zip Folder\0004.zip
Brute Force Started...
Checking for 4 character password...
0000
0001
0002
0003
0004
Success! The password is: 0004
Congratulations!!! Password found after trying 5 combinations in 0.022717714309
92383 seconds
```

Teacher Stops Screen Share

STUDENT-LED ACTIVITY - 20 mins

- **Student will decode the pdf password**
- **The teacher gets into Full Screen.**

ACTIVITY

- **Write logic to decode pdf password**
- **Use word list to decode the pdf password**

Teacher Action	Student Action
Guide the student to get the boilerplate code from Student Activity 2 *Download the password protected pdf file and wordlist.txt too and save in computer at same location*	*Student clones the code from Student Activity2*

```
import PyPDF2 as pd
filename = input('Path to the file: ')
file = open(filename,'rb')
pdfReader = pd.PdfFileReader(file)
```

Python has an inbuilt module named PyPDF2 that can be used to access pdf files

Open Terminal and type below command to install PyPDF2

pip install PyPDF2

- Import PyPDF2 library for pdf reader
- Get the folder path using input
- By default, the open() function opens a file in text format. Add "rb" to the mode parameter to open a binary file. As a result, the "rb" mode opens the file in binary format for reading

```
if not pdfReader.isEncrypted:
    print('The file is not password protected! You can successfully open it!')
```

Student start writing the code from here
Using if statement check if the pdf is password protected or not, if not then print the message

```
else:
    wordListFile = open('wordlist.txt', 'r',errors='ignore')
    body = wordListFile.read().lower()
    words = body.split('\n')
```

Else it's password protected then initialize the variable ***wordlistFile***,open the file ***"wordlist.txt", "r"*** represents reads mode and ignore errors if any.

- Intilalize the body variable as a reference to wordListFile content.***lower()*** function will convert and read all characters in lower case only.
- Use ***split()*** function to fetch different passwords on different lines and store it in an array with name

words.

```
for i in range(len(words)):
    word = words[i]
    print('Trying to decode passowrd by: {}'.format(word))
    result = pdfReader.decrypt(word)
    if result == 1:
        print('Success! The password is: '+ word)
        break

    elif result == 0:
        tried += 1
        print('Passwords tried: ' + str(tried))
        continue
```

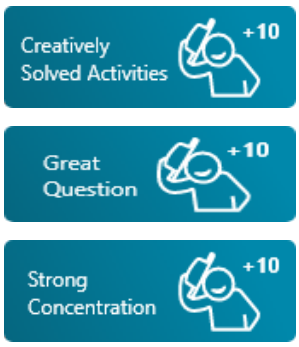
Now apply a for loop on words which will iterate till the length of the array **"words".**

- Initialize the current value of array in variable "word".
- pdfReader.decrypt(word) function will try to decrypt the password encrypted file using the current value of word as password.
- The result of the same will be stored in the variable result. If the function is able to decrypt the file successfully it will return the value of result as 1 and the break keyword will break the for loop, otherwise the value of result will be 0 and it will continue to the next word in array words.
- The same will be printed and displayed to the user as per the value of the result.

```
Path to the file: C:\Users\User\Pictures\BruteforceWord list\sana test_Encrypted.pdf
Trying to decode passowrd by: 0000
Passwords tried: 1
Trying to decode passowrd by: 0001
Passwords tried: 2
Trying to decode passowrd by: 0002
Passwords tried: 3
Trying to decode passowrd by: 0003
Passwords tried: 4
Trying to decode passowrd by: 0004
Passwords tried: 5
Trying to decode passowrd by: 0005
Passwords tried: 6
Trying to decode passowrd by: 0006
Passwords tried: 7
Trying to decode passowrd by: 0007
Passwords tried: 8
Trying to decode passowrd by: 0008
Passwords tried: 9
Trying to decode passowrd by: 0009
Passwords tried: 10
Trying to decode passowrd by: 000a
Passwords tried: 11
Trying to decode passowrd by: 000b
Passwords tried: 12
Trying to decode passowrd by: 000c
Passwords tried: 13
Trying to decode passowrd by: 000d
Passwords tried: 14
Trying to decode passowrd by: 000e
Passwords tried: 15
Trying to decode passowrd by: 000f
Passwords tried: 16
Trying to decode passowrd by: 000g
Passwords tried: 17
```

Run the program and write down the path, *While running the program need to get folder path :Right click on the folder whose password you want to decode check the location,copy the location path followed by the folder name*	
YES! cracked your PDF password. Attackers attempt to find usernames and passwords for numerous websites using this exhaustive search method means brute force attack	

How can we prevent ourselves from this type of security attack? Don't click on any unauthorized links, check for authenticity first, and then add your credentials only after that You have noticed that whenever you make new login it is mentioned over password strength and their set of rules we need to follow while setting new password It's for this reason that it's advised to keep your password 8 characters long with numeric characters, small and capital alphabets, and special characters Always set complex password because it is difficult to crack The longer the password, the harder it is to crack, and it takes too long to crack This is how we can prevent Bruteforce attack!\	
Teacher Guides Student to Stop Screen Share	
WRAP UP SESSION - 5 Mins	
Quiz time - Click on in-class quiz	
Question	**Answer**
What is the purpose of **split()** function? A. Remove leading and trailing characters B. Show a list of single characters C. Remove all the characters D. None of the above	**B**
How to install a zip file? A. pip install zipfile36	**A**

B. Pip install ZIPFILE C. pip install Zfile D. None of the above	
Why do we need the extractall in zip file? A. Archive all members to the current directory B. Archive data C. Save current directory D. All of the above	**A**
End the quiz panel	
FEEDBACK • **Appreciate the students for their efforts in the class.** • **Ask the student to make notes for the reflection journal along with the code they wrote in today's class.azAQA1**	
Teacher Action	**Student Action**
You get Hats off for your excellent work! In the next class	*Make sure you have given at least 2 Hats Off during the class for:* 
Project Discussion	

Teacher Clicks	✖ End Class

ADDITIONAL ACTIVITIES	
Additional Activities *Encourage the student to write reflection notes in their reflection journal using markdown.* Use these as guiding questions: ● What happened today? ○ Describe what happened. ○ The code I wrote. ● How did I feel after the class? ● What have I learned about programming and developing games? ● What aspects of the class helped me? What did I find difficult?	*The student uses the markdown editor to write her/his reflections in the reflection journal.*

ACTIVITY LINKS		
Activity Name	**Description**	**Link**
Teacher Activity1	Brute Force Attack	https://en.wikipedia.org/wiki/List_of_cyberattacks
Teacher Activity 2	Boilerplate Code	https://github.com/pro-whitehatjr/PRO-C223-Teacher-Boiler-Plate

Teacher Activity 3	Reference Code for zip folder	https://github.com/pro-whitehatjr/PRO_C223_ReferenceCode
Teacher Activity 4	Reference Code for pdf	https://github.com/pro-whitehatjr/PRO_C223_Teacher-ReferenceCode
Teacher Activity 5	Phishing Code	https://github.com/pro-whitehatjr/PRO-C223-Prerequisite
Teacher Activity 6	NGROK	https://ngrok.com/download
Teacher Activity 7	Postman	https://www.postman.com/downloads/
Student Activity 1	Brute Force Attack	https://en.wikipedia.org/wiki/List_of_cyberattacks
Student Activity 2	Boilerplate Code	https://github.com/pro-whitehatjr/PRO_C223_StudentBoilerPlate