PSP0201

Week 5

Writeup

Group Name: DNA

Members

ID	Name	Role
1211102532	DHARVIN SHAH KUMAR BIN MOHAMAD SHAH RAVIN	Leader
1211101179	ALIPH RAIHAN BIN ANUAR	Member
1211102427	NUR NATHIFA BINTI MOHD IZHAR	Member

Day 16: Scripting - Help! Where is Santa?

Tools used: Attackbox, Firefox, Terminal, Sublime

Solution / walkthrough :

Question 1

What is the port number for the web server?

The port can be found using nmap. Two ports were opened. The accessible/correct port was port 80.

```
root@ip-10-10-211-117:~/aoc_day_16# nmap 10.10.222.150

Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-12 12:21 BST
Nmap scan report for ip-10-10-222-150.eu-west-1.compute.internal (10.10.222.
150)
Host is up (0.0015s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:C0:F4:EA:6A:27 (Unknown)
```

Question 2

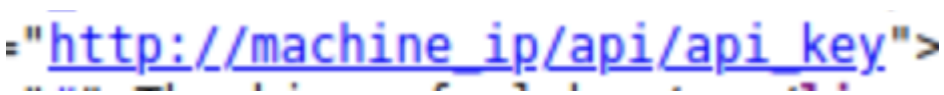
What templates are being used?

The template was BULMA.

Question 3

Without using enumerations tools such as Dirbuster, what is the directory for the API? (without the API key)

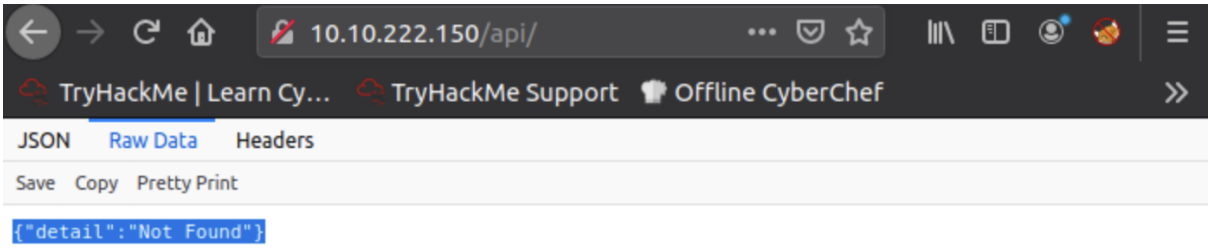
/api/



Question 4

Go the API endpoint. What is the Raw Data returned if no parameters are entered?

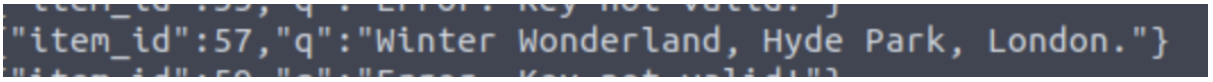
{"detail":"Not Found"}



Question 5

Where is Santa right now?

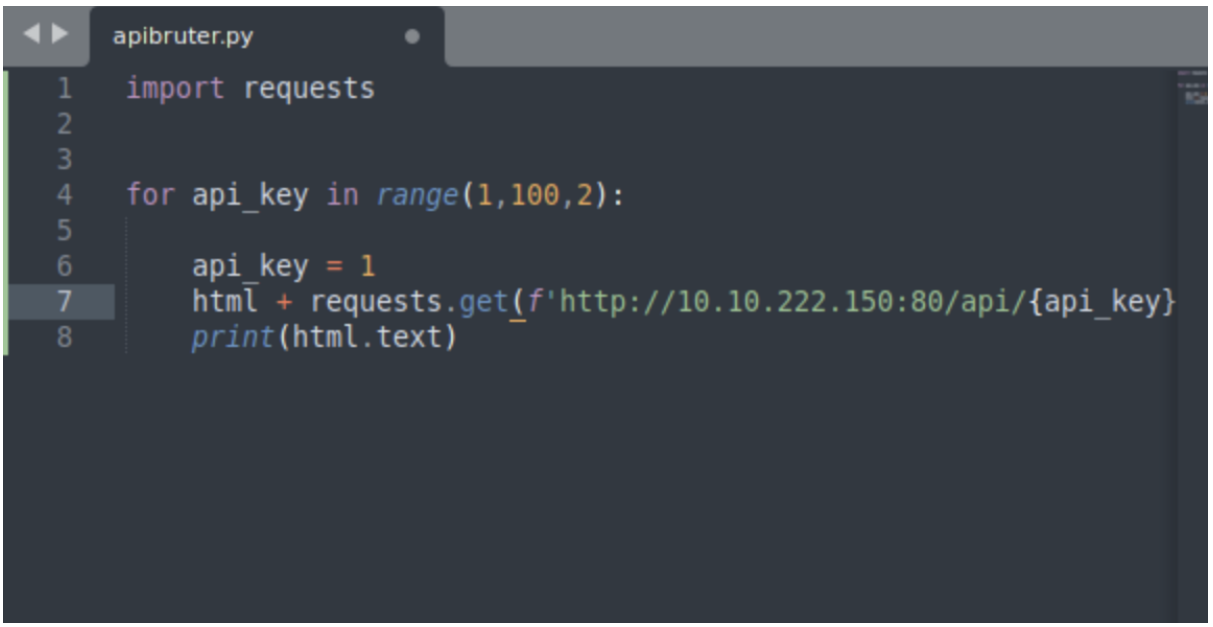
Winter Wonderland, Hyde Park, London

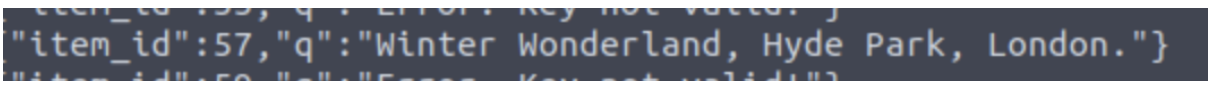


Question 6

Find out the correct API key. Remember, this is an odd number between 0-100. After too many attempts, Santa's Sled will block you. To unblock yourself, simply terminate and re-deploy the target instance (10.10.94.92)

By using the python loop function we found out that 57 was the API key.





Methodology:

We start the terminal and run a Nmap scan under the verbose mode. We found two open ports which were port 80 and port 22. Port 80 was the only one accessible as it shows Santa's tracking system website. The website showed numerous hyperlinks that when clicked will take us to the tryhackme website. We view the page' source code to find a hyperlink that has a different link. We can also use python to find and identify each link stored on the website. To find the correct API key we will use python to loop through the different keys to make it quick and easy for us. We were able to find the correct API key which was 57 as well as Santa's whereabouts.

Day 17: Reverse Engineering - ReverseELFneering

Tools used: Attackbox, Google, Visual Studio Code, Radare2

Solution / walkthrough :

Question 1

Match the data type with the size in bytes:

Initial Data Type	Suffix	Size (bytes)
Byte	b	1
Word	w	2
Double Word	l	4
Quad	q	8
Single Precision	s	4
Double Precision	l	8

Question 2

What is the command to analyse the program in radare2?

We googled the answer for this question.

The most common radare2 analysis command sequence is **aa** , which stands for "analyze all". That all is referring to all symbols and entry-points. If your binary is stripped you will need to use other commands like aaa , aab , aar , aac or so.

https://book.rada.re › analysis › code_analysis

Code Analysis - The Official Radare2 Book

Question 3

What is the command to set a breakpoint in radare2?

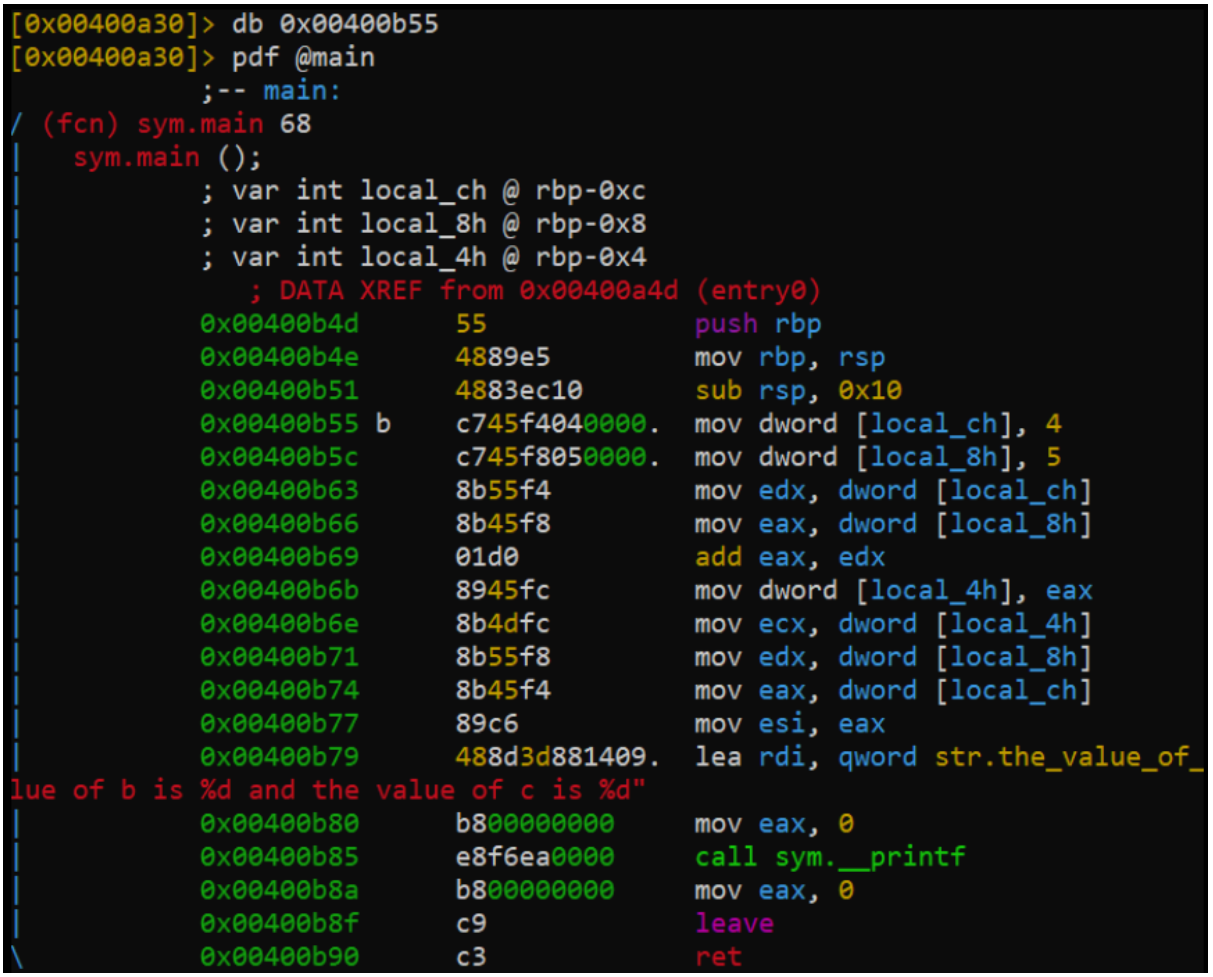
We googled the answer for this question.

> Commands. All debugging-related commands are prefixed with d , which is easy to remember and quite handy. You can set breakpoints using **db <address/flag>** . db will simply list all breakpoints.
>
> https://monosource.gitbooks.io › content › intro › debugg...
>
> Debugging · Radare2 Explorations - monosource

Question 4

What is the command to execute the program until we hit a breakpoint?

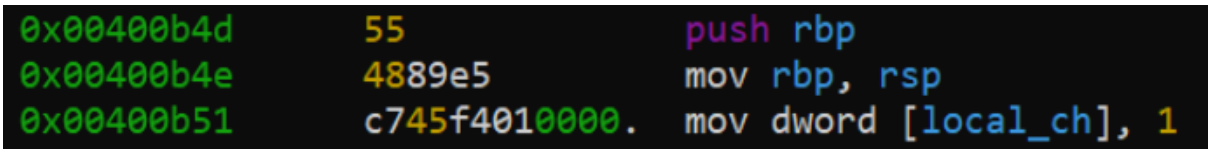
The little b next to the instruction we intended to stop was visible when we executed the **pdf@main** command once more.



Question 5

What is the value of local_ch when its corresponding movl instruction is called (first if multiple)?

We can see in the instructions. **1**



Question 6

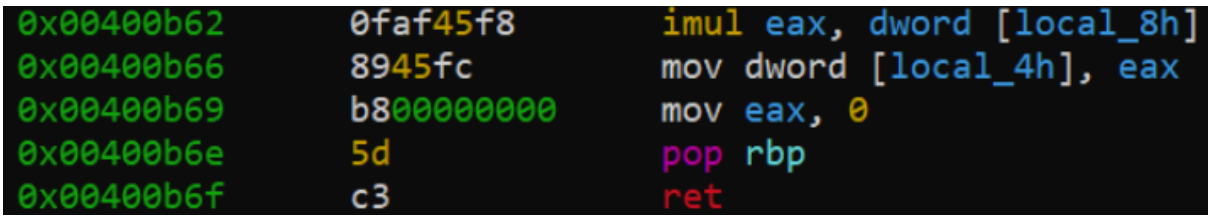
What is the value of eax when the imull instruction is called?

We can see in the instructions. **6**

Question 7

What is the value of local_4h before eax is set to 0?

We set eax to 0 and the executed instruction before this was mov dword [local_4h], eax. According to the answers to question number 2 above, eax is worth **6**, and the instructions above will transfer that value from eax to the local_4h variable.



Methodology: For the first question, we referred to the table in the question itself**.** Then, question 1 to 2 Google helped us out. Next, the little b next to the instruction we intended to stop was visible when we executed the **pdf@main** command once more. We can see in the instructions. **1.** We can see in the instructions. **6.** We set eax to 0 and the executed instruction before this was mov dword [local_4h], eax. According to the answers to question number 2 above, eax is worth **6**, and the instructions above will transfer that value from eax to the local_4h variable.

Day 18: [Reverse Engineering] The Bits of Christmas

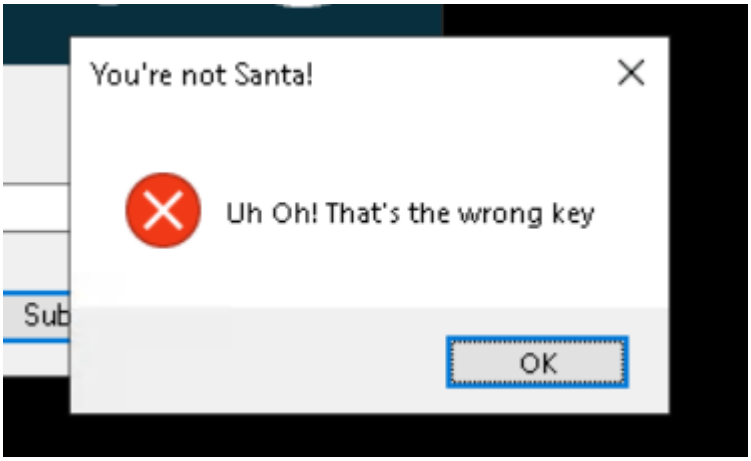
Tools used : Attackbox, reminna, ILSpy

solution/walkthrough :

Question 1

What is the message that shows up if you enter the wrong password for TBFC_APP?

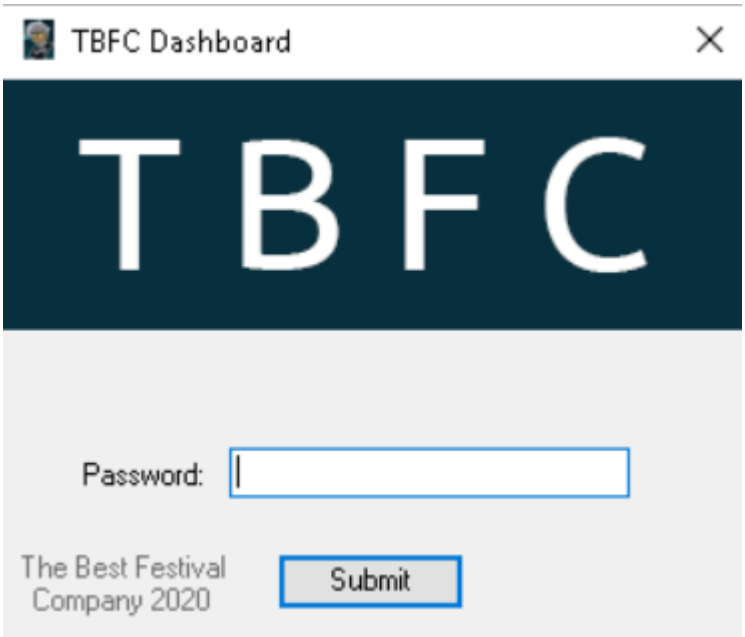
You're not Santa!



Question 2

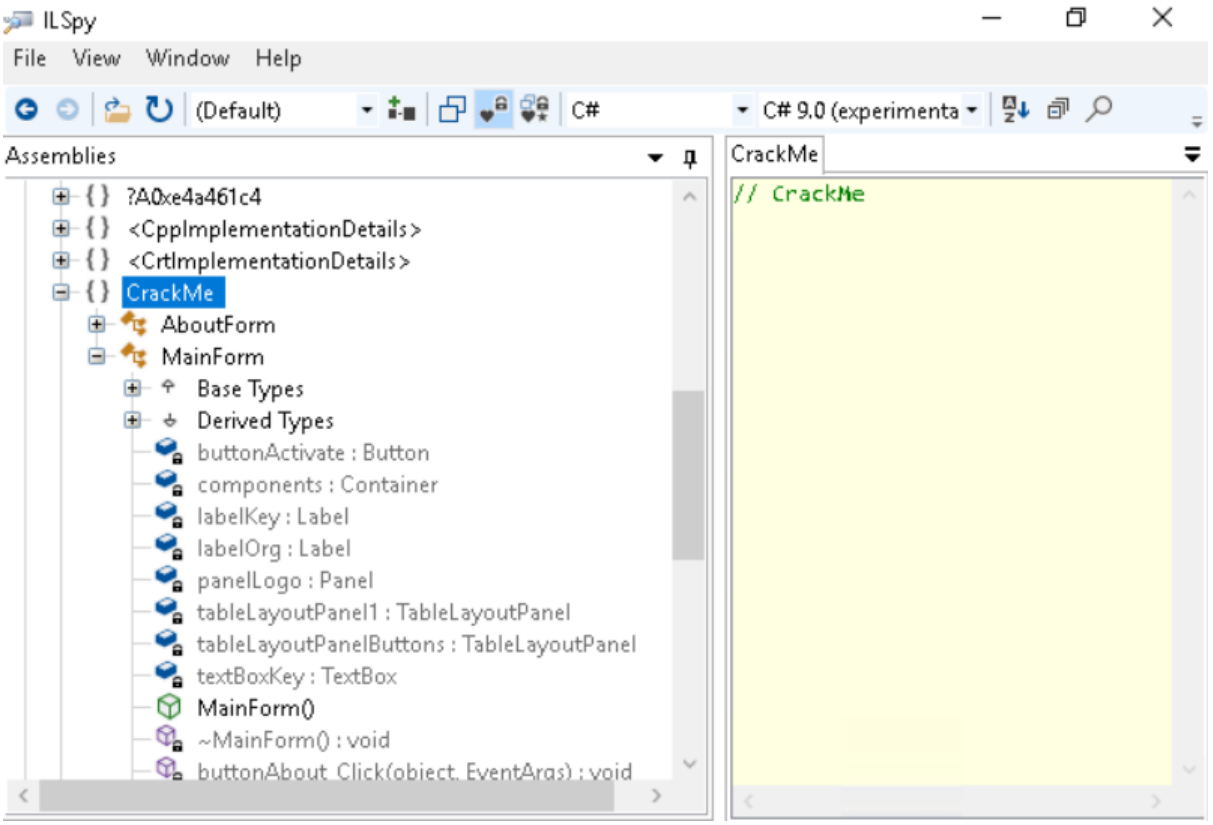
What does TBFC stand for?

The Best Festival Company



Question 3

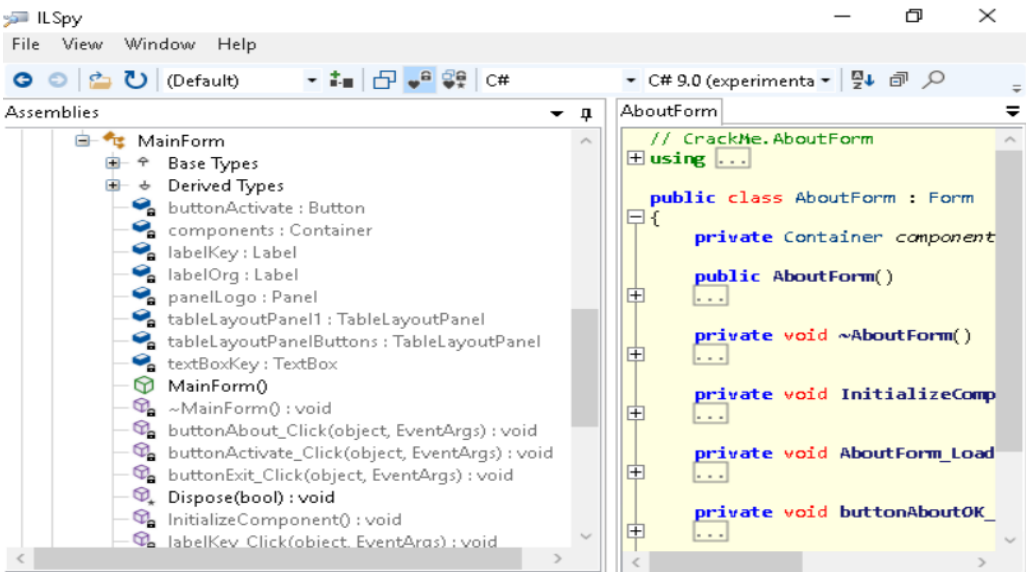
Decompile the TBFC_APP with ILSpy. What is the module that catches your attention?



Question 4

Within the module, there are two forms. Which contains the information we are looking for?

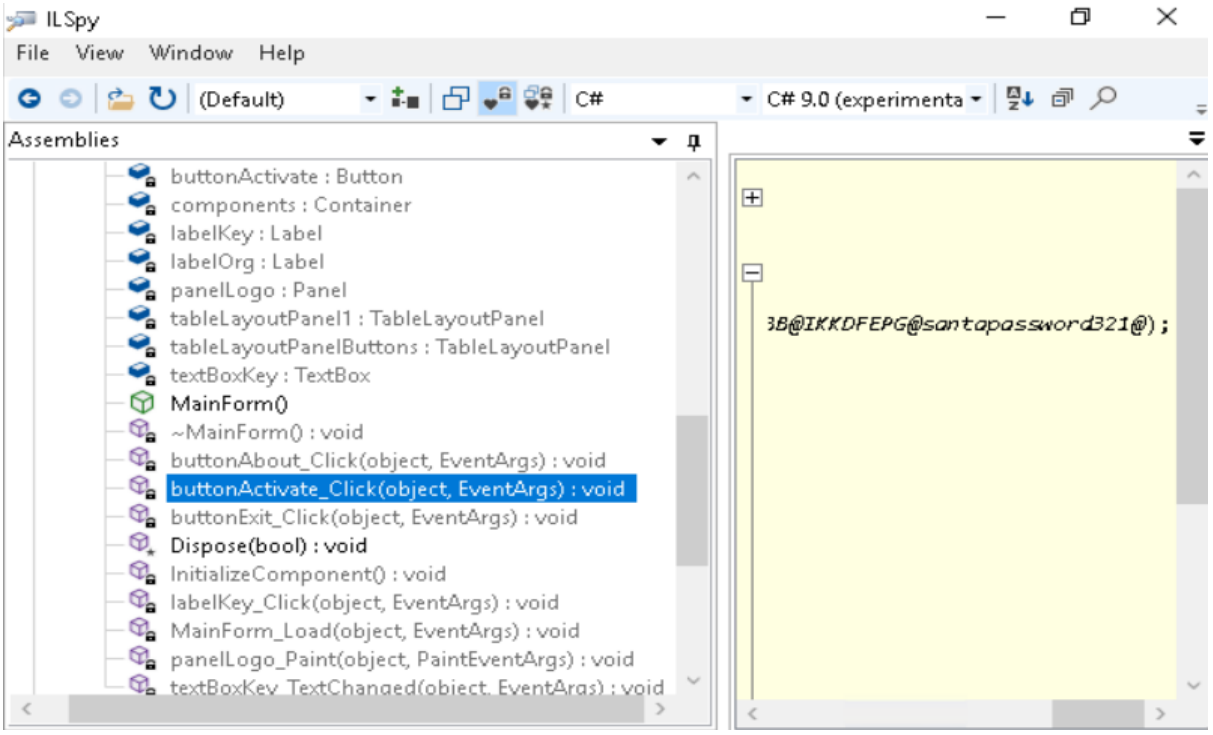
MainForm



Question 5

Which method within the form from Q4 will contain the information we are seeking?

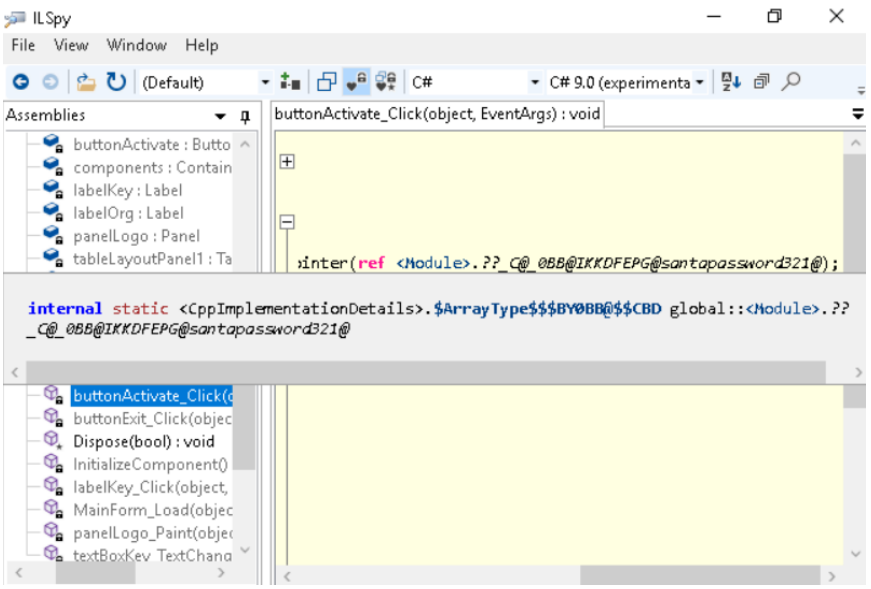
buttonActivate_Click

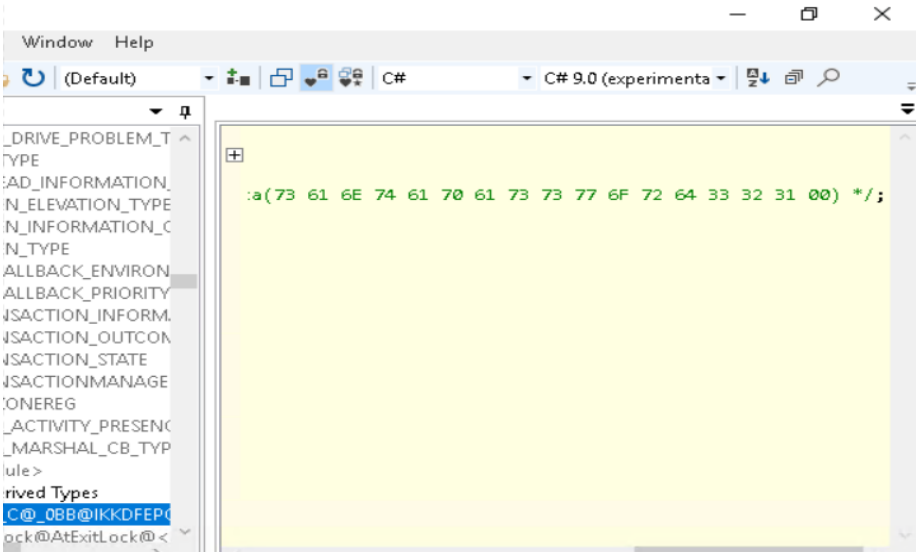


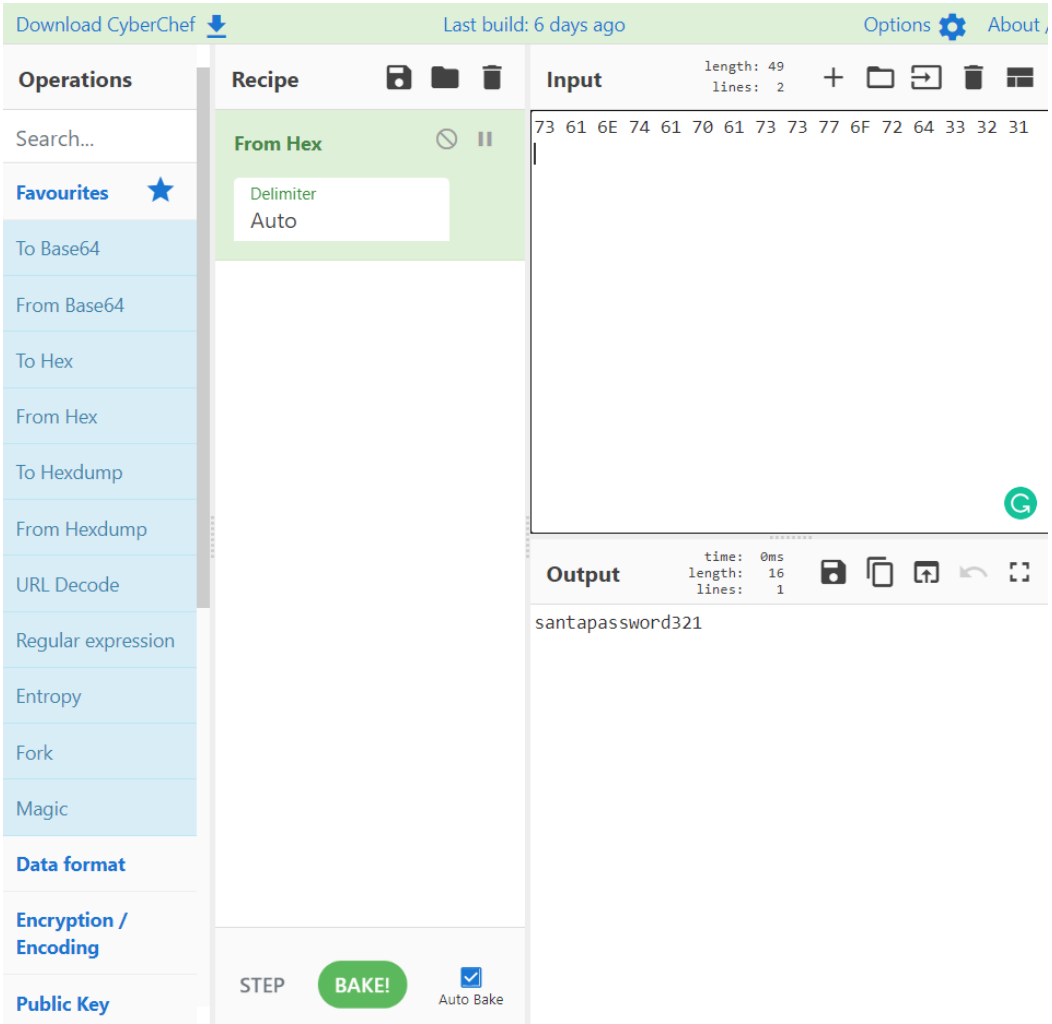
Question 6

What is Santa's password?

santapassword321



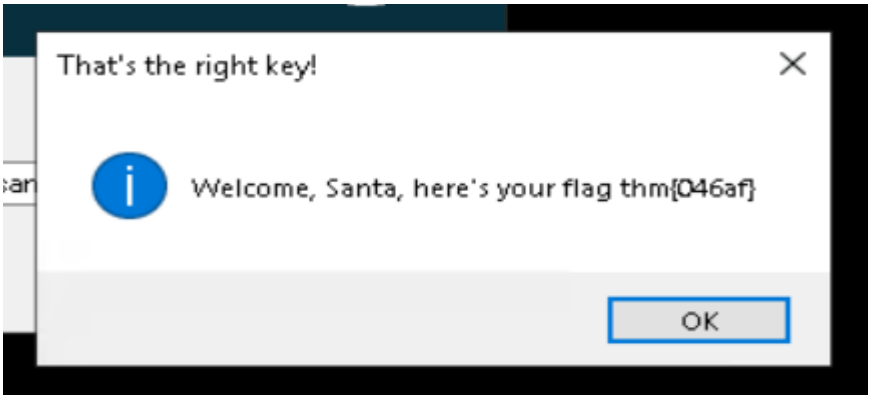

Window Help
(Default)
C#
C# 9.0 (experimenta
:a(73 61 6E 74 61 70 61 73 73 77 6F 72 64 33 32 31 00) */;


Download CyberChef
Last build: 6 days ago
Options
About
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Magic
Data format
Encryption / Encoding
Public Key
Recipe
From Hex
Delimiter
Auto
STEP
BAKE!
Auto Bake
Input
length: 49
lines: 2
73 61 6E 74 61 70 61 73 73 77 6F 72 64 33 32 31
Output
time: 0ms
length: 16
lines: 1
santapassword321

Question 7

Now that you've retrieved this password, try to login...What is the flag?

thm{046af}



Methodology :

After starting attackbox, open up remmina and connect to our ip address. We entered the username and password which are cmnatic and Adventofcyber! and it will start to connect. We opened the TBFC_APP and when the pop up asked for a password, we entered the wrong one and it told us “You’re not Santa!”. TBFC stands for “The Best Festival Company” as it clearly stated on the pop up earlier. After we decompiled the TBFC_APP with ILSpy, the module that caught our attention was the CrackMe because it stood out more than the others. Form that contains the information we were looking for was the MainForm because it contains Santa's password. We found Santa’s password by clicking on buttonActive_Click as the santa’s password appeared to be there. The @ sign brought us to some internal static variable that we cannot understand so we brought up the numbers to cyberchef (using from hex) and it converted the numbers easily to “santapassword321”. Then we put the actual password to the TBFC_APP pop up and it gave us the flag which was “thm{046af}”.

Day 19: Web exploitation - The Naughty or Nice List

Tools used: Attackbox, Cyberchef, Firefox

Solution/Walkthrough:

Question 1

Which list is this person on?

Enter the names in the search box of the site.

Timothy is on the Naughty List.

YP is on the Nice List.

Kanes is on the Naughty List.

JJ is on the Naughty List.

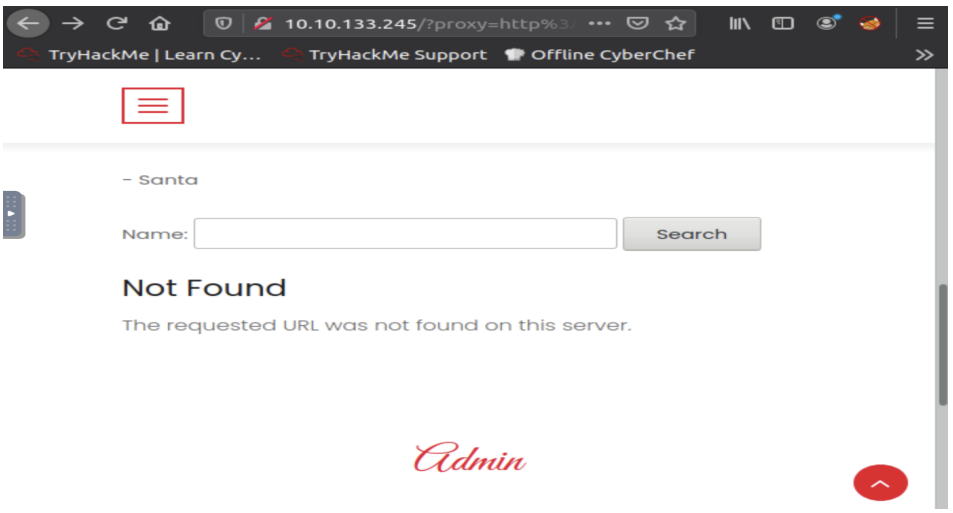
Tib3rius is on the Nice List.

Ian Chai is on the Nice List.

Question 2

What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F"?

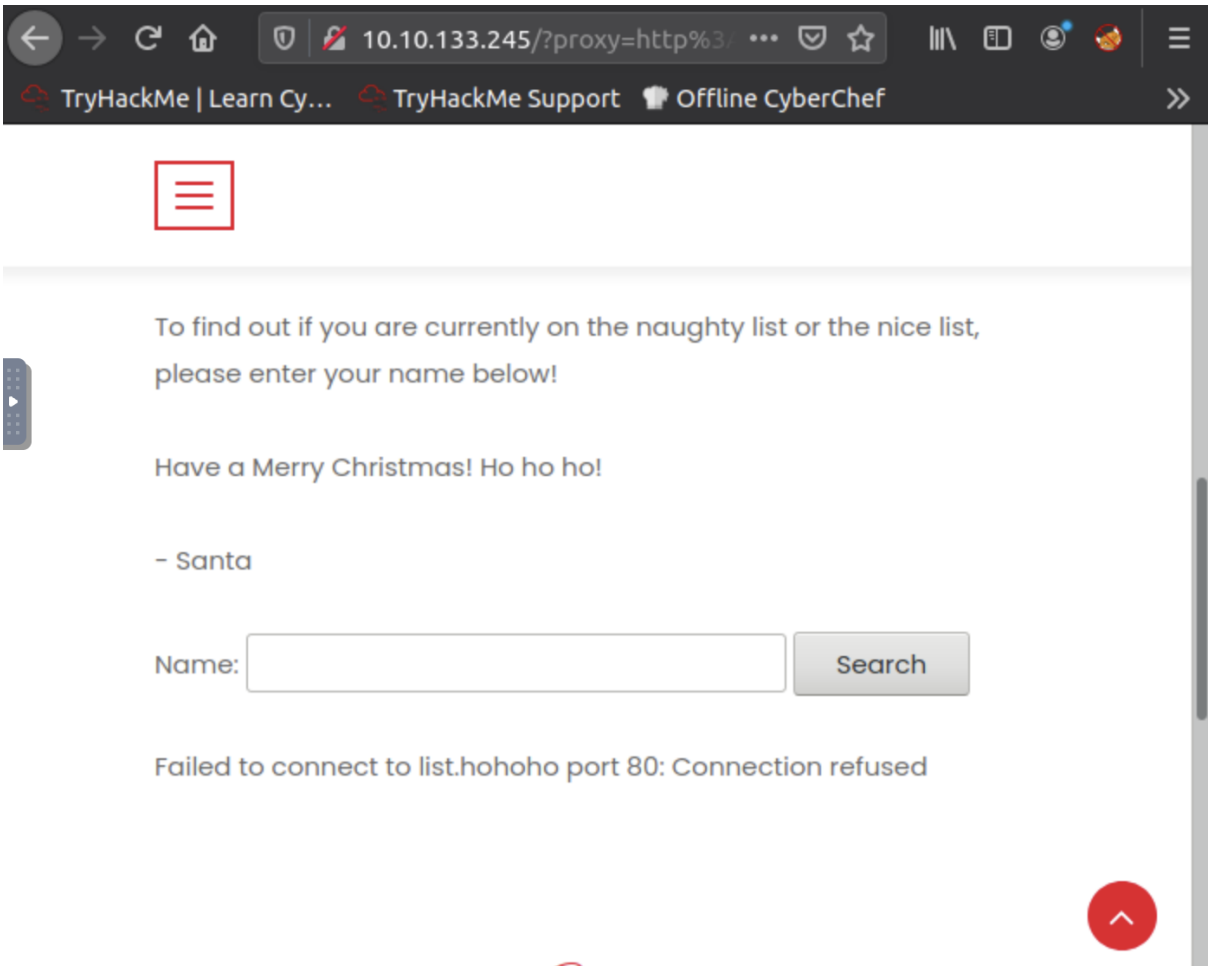
We will get **"The requested URL was not found on this server."**



Question 3

What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A80"?

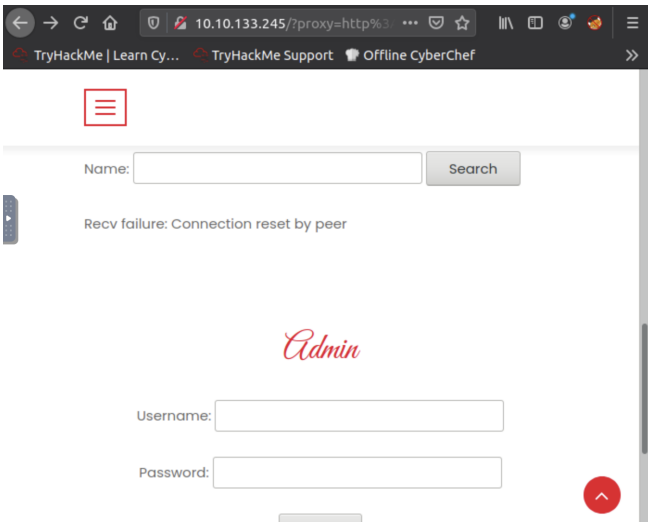
Changing the port number to 80 results in “**Failed to connect to list.hohoho port 80: Connection refused** ”



Question 4

What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A22"?

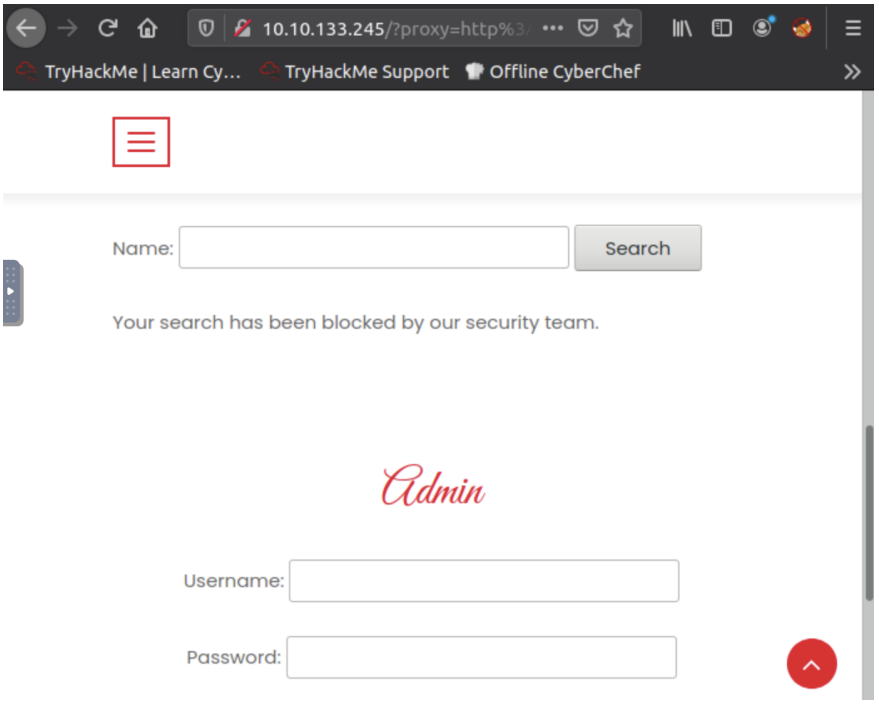
Changing the port number from 80 to 22 results in “**Recv failure: Connection reset by peer**”



Question 5

What is displayed on the page when you use "/?proxy=http%3A%2F%2Flocalhost"?

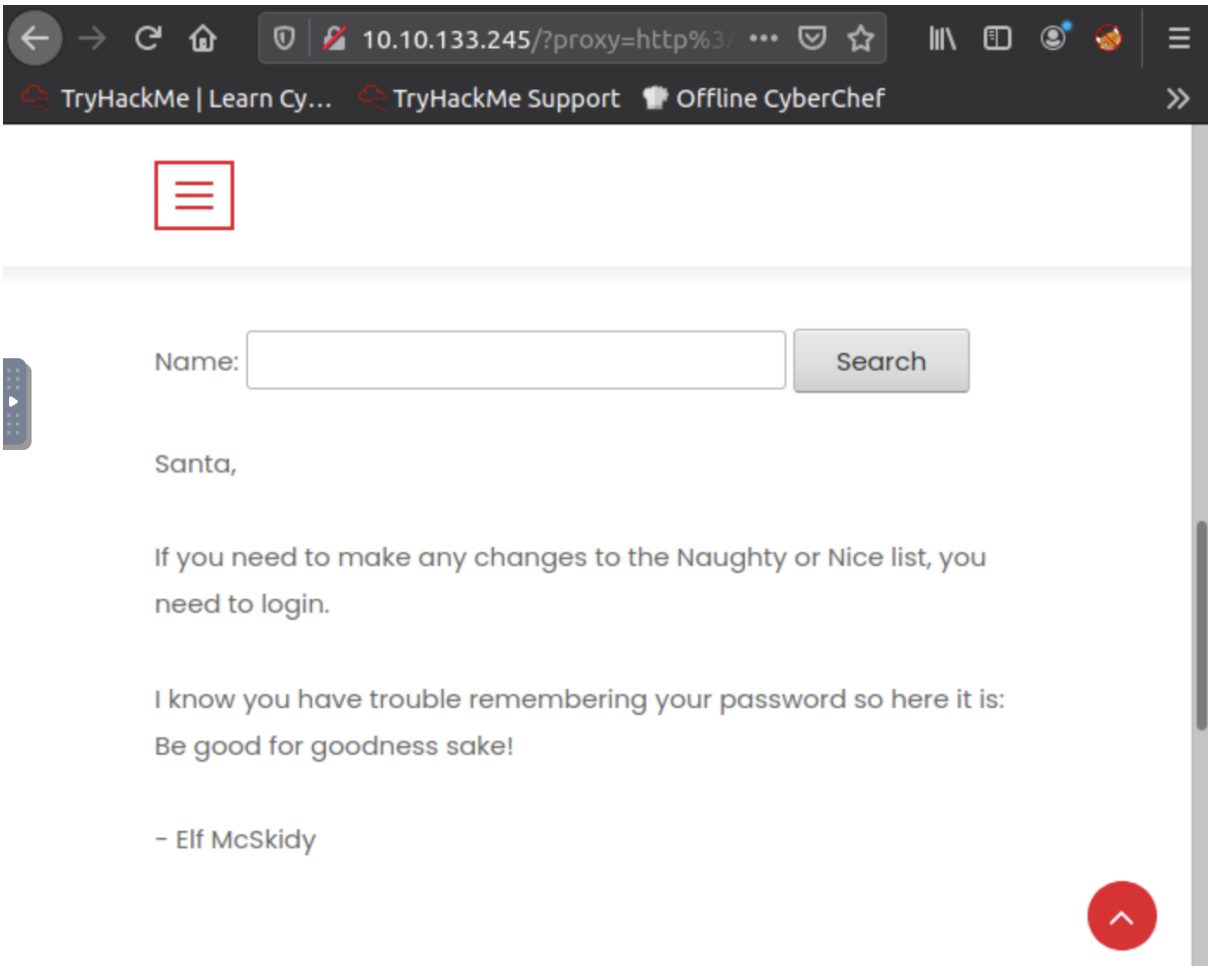
Changing the hostname in the URL results in the message “**Your search has been blocked by our security team.** “



Question 6

What is Santa's password?

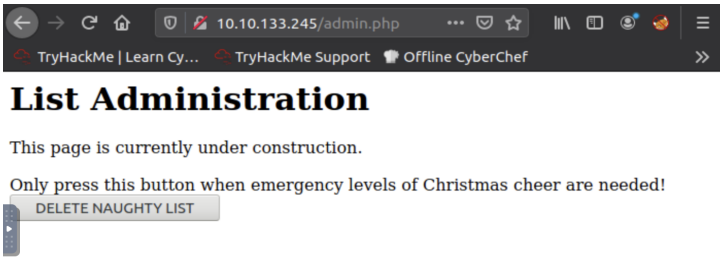
Changing the subdomain to our own which was ‘localtest.me’ displayed a message from Elf Mcskidy where he mentions the admin password which was ‘**Be good for goodness sake!** ‘

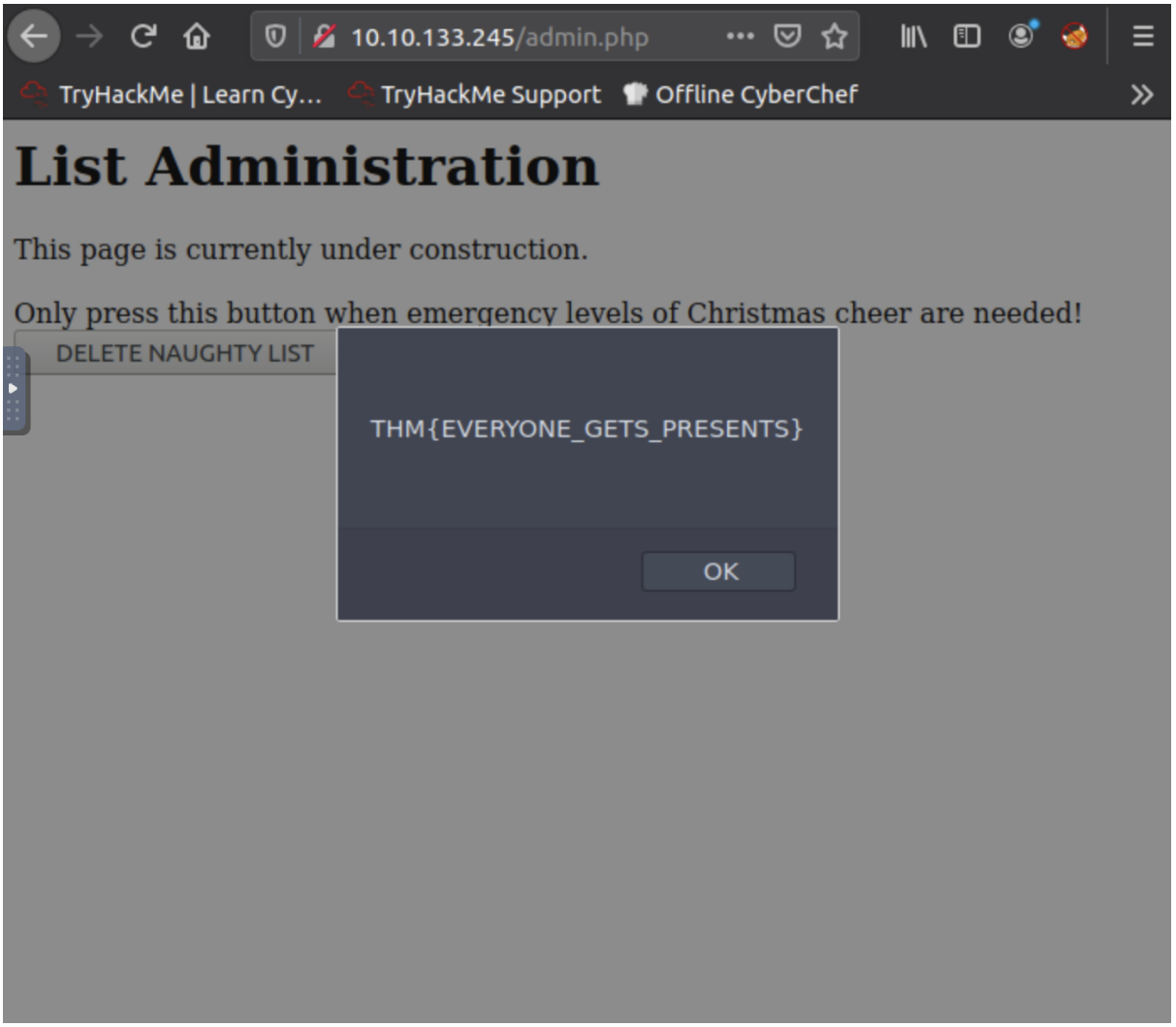


Question 7

What is the challenge flag?

Entering the proper credentials will bring us to the List Administration website. When we press the DELETE NAUGHTY LIST button it will return us the flag which is “**THM{EVERYONE_GETS_PRESENTS}**”





Methodology:

We startup the attackbox and opened firefox then went to Santa's naughty or nice list website. When entering a name in the input box the proxy parameter in the site link is shown. It follows what looks like an encoded URL. We used cyberchef to decode this URL. The web app seems to make backend requests and return the result to the frontend. In the URL we tried to change the port from 8080 to 80 but failed to connect. We tried to change port 80 to port 22 and it displayed a receive failure message. When changing the hostname our search was immediately blocked by the security team. We then changed the subdomain to our own which was localtest.me and a message from Elf Mcskidy were displayed who also gave us the password. We entered the credentials and it brought us to the list administration page. We press the "DELETE NAUGHTY LIST" button which then returned us the flag.

Day 17: [Blue Teaming] PowershELIF to the rescue

Tools used: Attackbox, Google, Visual Studio Code, PowerShell, SSH

Solution / walkthrough :

Question 1

Check the ssh manual. What does the parameter -l do?

[**-l** *login_name*]

Question 2

Search for the first hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want?

We accessed the Documents folder using the PowerShell command: Set-Location Documents. Then we listed the contents with command: Get-ChildItem. To see the hidden files, we used another flag: Get-ChildItem -Hidden -File. Finally, we use the command: Get-Content to see the contents of a file. As we can see below the elf wants his **2 front teeth.**

```
PS C:\Users\mceager\Documents> Get-Content e1fone.txt
All I want is my '2 front teeth'!!!
PS C:\Users\mceager\Documents>
```

Question 3

Search on the desktop for a hidden folder that contains the file for Elf 2. Read the contents of this file. What is the name of that movie that Elf 2 wants?

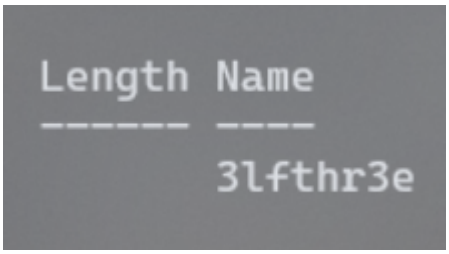
We went into Desktop directory to see the list of all the contents in it. We used the powershell command: Get-ChildItem -Hidden -Directory since we were looking for a directory. In “elf2two” there is a file named “e70smsW10Y4k.txt”. We saw the content in it using command: Get-Content .\e70smsW10Y4k.txt. In the file we can see Elf 2 wants the movie **Scrooged.**

```
PS C:\Users\mceager\Desktop\elf2wo> Get-Content .\e70smsW10Y4k.txt
I want the movie Scrooged <3!
PS C:\Users\mceager\Desktop\elf2wo>
```

Question 4

Search the Windows directory for a hidden folder that contains files for Elf 3. What is the name of the hidden folder? (This command will take a while)

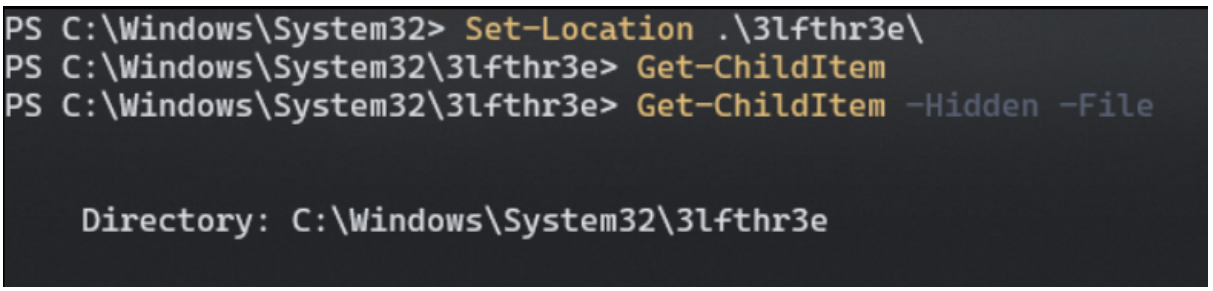
We used the command: Get-ChildItem -Hidden -Filter '*3*'. Then, we can see the hidden content that has '3' on the name.

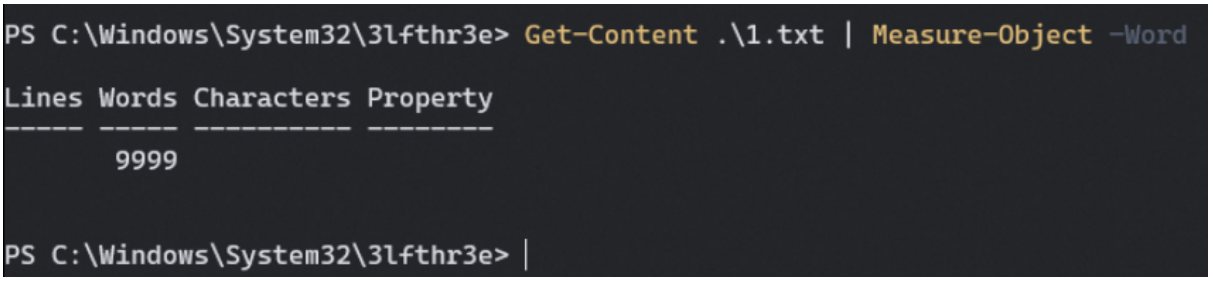


Question 5

How many words does the first file contain?

We navigated into the directory '3lfthr3e' and listed the files inside. To count all words from file 1.txt, we used 'Measure-Object' cmdlet with flag '-Word' which input piped from Get-Content.





Question 6

What 2 words are at index 551 and 6991 in the first file?

We used command: (Get-Content .\1.txt)[551, 6991]

```
PS C:\Windows\System32\3lfthr3e> (Get-Content .\1.txt)[551, 6991]
Red
Ryder
PS C:\Windows\System32\3lfthr3e>
```

Question 7

This is only half the answer. Search in the 2nd file for the phrase from the previous question to get the full answer. What does Elf 3 want? (use spaces when submitting the answer)

Finally we used command: Select-String <path/filename> -Pattern 'redryder'. We got the pattern from the hint given, same word but different format.

```
PS C:\Windows\System32\3lfthr3e> Select-String .\2.txt -Pattern 'redryder'

2.txt:558704:redryderbbgun


PS C:\Windows\System32\3lfthr3e>
```

Methodology: We accessed the Documents folder using the PowerShell command: Set-Location Documents. Then we listed the contents with command: Get-ChildItem. To see the hidden files, we used another flag: Get-ChildItem -Hidden -File. Finally, we use the command: Get-Content to see the contents of a file. As we can see below the elf wants his **2 front teeth.** We went into Desktop directory to see the list of all the contents in it. We used the powershell command: Get-ChildItem -Hidden -Directory since we were looking for a directory. In "elf2two" there is a file named "e70smsW10Y4k.txt". We saw the content in it using command: Get-Content .\e70smsW10Y4k.txt. In the file we can see Elf 2 wants the movie **Scrooged.** We used the command: Get-ChildItem -Hidden -Filter '*3*'. Then, we can see the hidden content that has '3' on the name. We navigated into the directory '3lfthr3e' and listed the files inside. To count all words from file 1.txt, we used 'Measure-Object' cmdlet with flag '-Word' which input piped from Get-Content. We used command: (Get-Content .\1.txt)[551, 6991]. Lastly, we used command: Select-String <path/filename> -Pattern 'redryder'. We got the pattern from the hint given, same word but different format.