PSP0201

Week 5

Writeup

Group Name: Haxon

Members

ID	Name	Role
1211102370	Lau Zi Thao	Leader
1211102797	Teng Wei Joe	Member
1211103142	Wong Khai King	Member
1211101029	Garrison Goh Zen Ken	Member

Day 16: Scripting – Help! Where is Santa?

Tools used: Kali Linux, Firefox, Visual Studio Code, nmap

Solution/walkthrough:

Question 1

What is the port number for the web server?

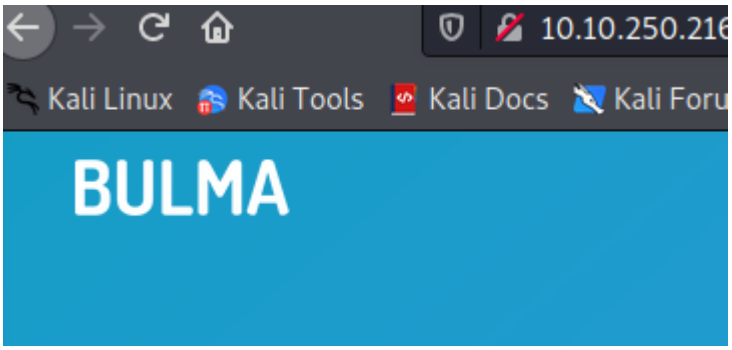
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 10.10.250.216                                    1 ×
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-11 23:21 EDT
Nmap scan report for 10.10.250.216
Host is up (0.23s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Net
work Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3
.16 (93%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%), Linux 2.6.39
- 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 5 hops

OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.33 seconds
```

The port can be guessed or found out with nmap scan

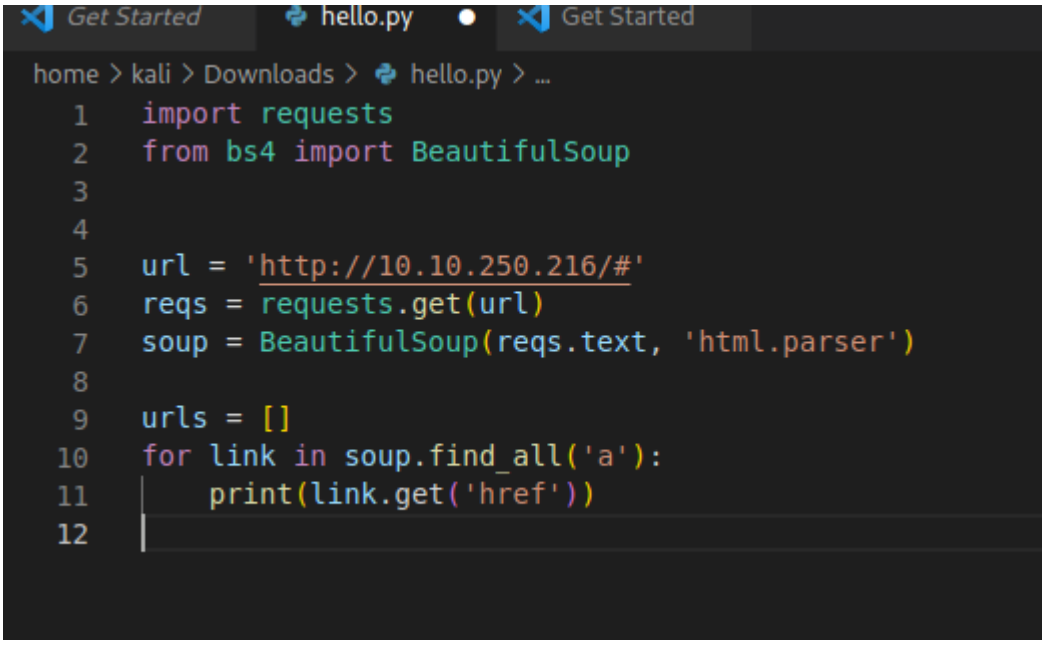
Question 2

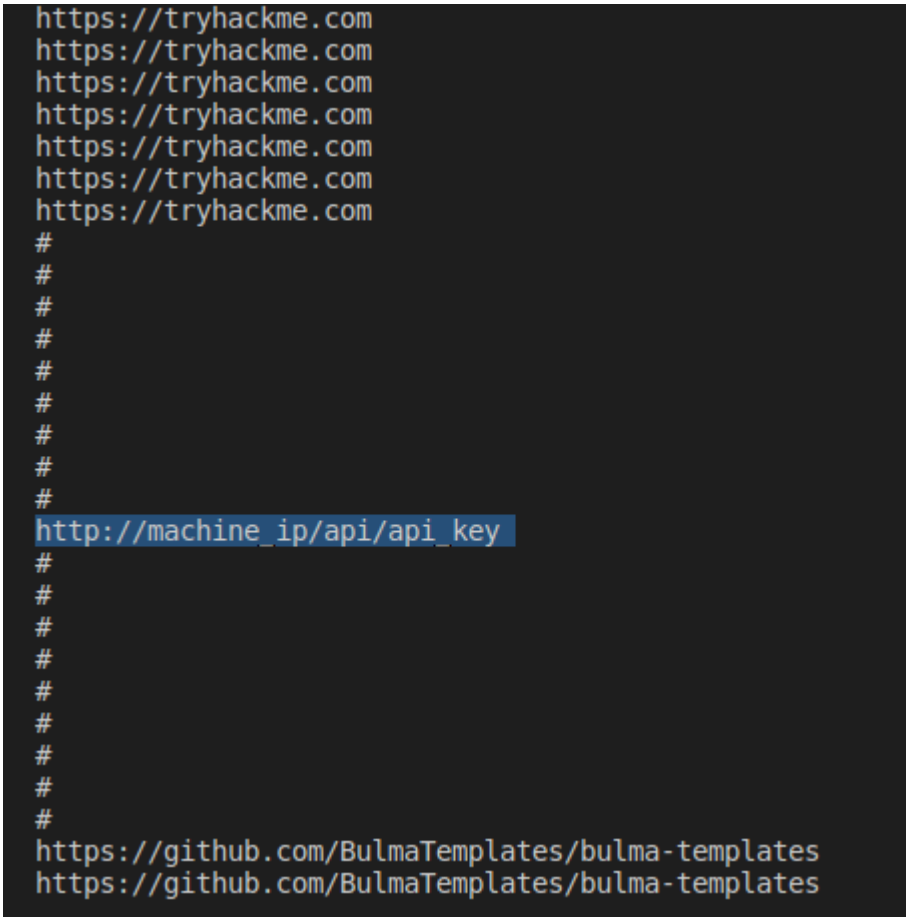
What templates are being used?



Question 3

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

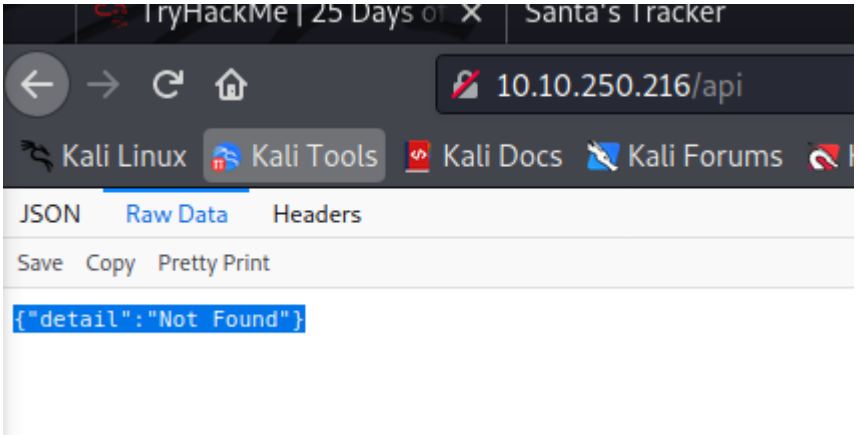




With python code found online to scan all the links in the website, we found the directory.

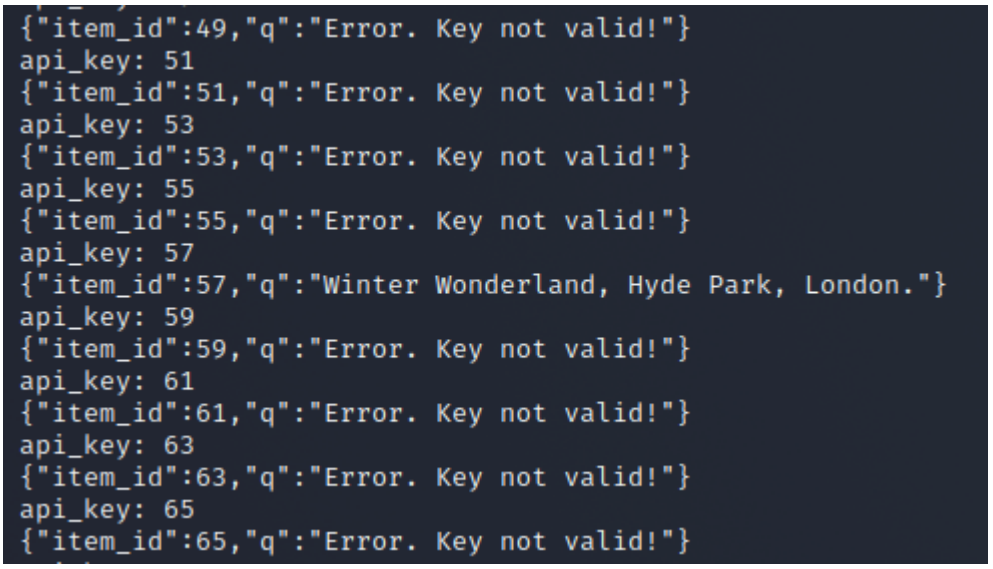
Question 4

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



Question 5

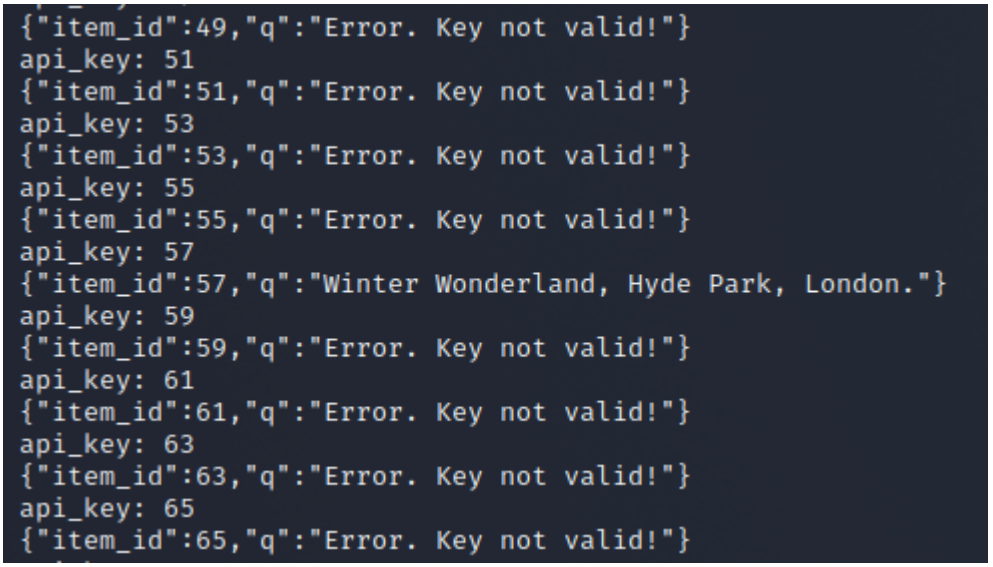
Where is Santa right now? (Tick all correct answers.)



Answer can be found when printing html text for all odd number api keys.

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)



The answer can be found when printing html text for all odd number api keys.

Thought Process/Methodology:

We first scanned for ports of the deployed machine using nmap, and then used the ports to access the website. The website has many clickable links but all lead back to the website itself. We were given a hint to use python. We used a python script with the requests and beautifulsoup libraries to extract all the links on the web page to find the correct directory for the api. After finding the api, all there is left is to find the correct api key. The hint was that the api key is a number between 1 and 100, and odd number. We edited the code to scan for all api keys between 1 and 100 and scanned for odd numbers only. We got a return value on api key number 57, the rest of the information is found using that api key.

Day 17: Reverse Engineering – ReverseELFneering

Tools used: Kali Linux, Firefox, Python, SSH

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

Byte:1, Word: 2, Double Word: 4, Quad: 8, Single Precision: 4, Double Precision: 8

Question 2

What is the command to analyse the program in radare2?

This will open the binary in debugging mode. Once the binary is open, one of the first things to do is ask r2 to analyze the program, and this can be done by typing in: `aa`

Note, when using the `aa` command in radare2, this may take between 5-10 minutes depending on your system.

Which is the most common analysis command. It analyses all symbols and entry points in the executable. The analysis, in this case, involves extracting function names, flow control information, and much more! r2 instructions are usually based on a single character, so it is easy to get more information about the commands.

The command is aa.

Question 3

What is the command to set a breakpoint in radare2?

A **breakpoint** specifies where the program should stop executing. This is useful as it allows us to look at the state of the program at that particular point. So let's set a breakpoint using the command `db` in this case, it would be `db 0x00400b55` To ensure the breakpoint is set, we run the `pdf @main` command again and see a little **b** next to the instruction we want to stop at.

The command is db.

Question 4

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

Running `dc` will execute the program until we hit the breakpoint. Once we hit the breakpoint and print out the main function, the rip which is the current instruction shows where execution has stopped. From the notes above, we know that the **mov** instruction is used to transfer values. This statement is transferring the value 4 into the `local_ch` variable. To view the contents of the `local_ch` variable, we use the following instruction `px @memory-address` In this case, the corresponding memory address for `local_ch` will be `rbp-0xc` (from the first few lines of **@pdf main**) This instruction prints the values of memory in hex:

The command is dc.

Question 5

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

```
elfmceager@tbfc-day-17:~$ r2 -d ./challenge1
Process with PID 1791 started...
= attach 1791 1791
bin.baddr 0x00400000
Using 0x400000
Warning: Cannot initialize dynamic strings
asm.bits 64
[0x00400a30]> pdf @main
p: Cannot find function at 0x00400b4d
[0x00400a30]> aa
[ WARNING : block size exceeding max block size at 0x006ba220
[+] Try changing it with e anal.bb.maxsize
 WARNING : block size exceeding max block size at 0x006bc860
[+] Try changing it with e anal.bb.maxsize
[x] Analyze all flags starting with sym. and entry0 (aa)
[0x00400a30]> pdf @main
            ;-- main:
/ (fcn) sym.main 35
|   sym.main ();
|           ; var int local_ch @ rbp-0x4
|           ; var int local_8h @ rbp-0x8
|           ; var int local_4h @ rbp-0x4
```

```
[0x00400a30]> pdf @main
            ;-- main:
/ (fcn) sym.main 35
|   sym.main ();
|           ; var int local_ch @ rbp-0x4
|           ; var int local_8h @ rbp-0x8
|           ; var int local_4h @ rbp-0x4
|              ; DATA XREF from 0x00400a4d (entry0)
|           0x00400b4d      55              push rbp
|           0x00400b4e      4889e5          mov rbp, rsp
|           0x00400b51      c745f4010000.   mov dword [local_ch], 1
|           0x00400b58      c745f8060000.   mov dword [local_8h], 6
|           0x00400b5f      8b45f4          mov eax, dword [local_ch]
|           0x00400b62      0faf45f8        imul eax, dword [local_8h]
|           0x00400b66      8945fc          mov dword [local_4h], eax
|           0x00400b69      b800000000      mov eax, 0
|           0x00400b6e      5d              pop rbp
\           0x00400b6f      c3              ret
[0x00400a30]>
```

Answer can be found after running pdf@main.

Question 6

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

Question 7

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

Thought Process/Methodology:

We first read through the information given in TryHackMe, answers for the first 4 questions can be obtained from the information given. We first logged into the deployed machine with the ssh command in terminal and using the provided credentials. Upon logging in, there are 2 files, which are challenge1 and file1. We followed THM instructions and ran the command to run Radare2 on file1. We ran the aa command to analyze the file and then tried out multiple other commands. We then exited and ran Radare2 on the Challenge1 file. We ran the aa command again, and then ran “pdf @main” to examine the assembly code. The rest of the answers can be found in the output.

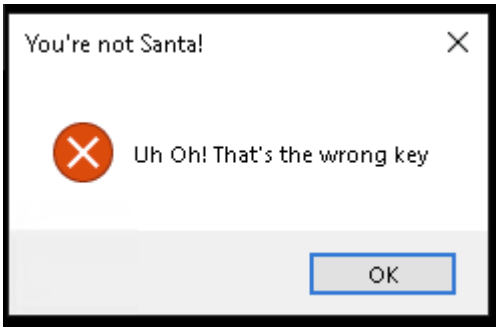
Day 18: Reverse Engineering – The Bits of Christmas

Tools used: Kali Linux, CyberChef, ILSPY, Remmina

Solution/walkthrough:

Question 1

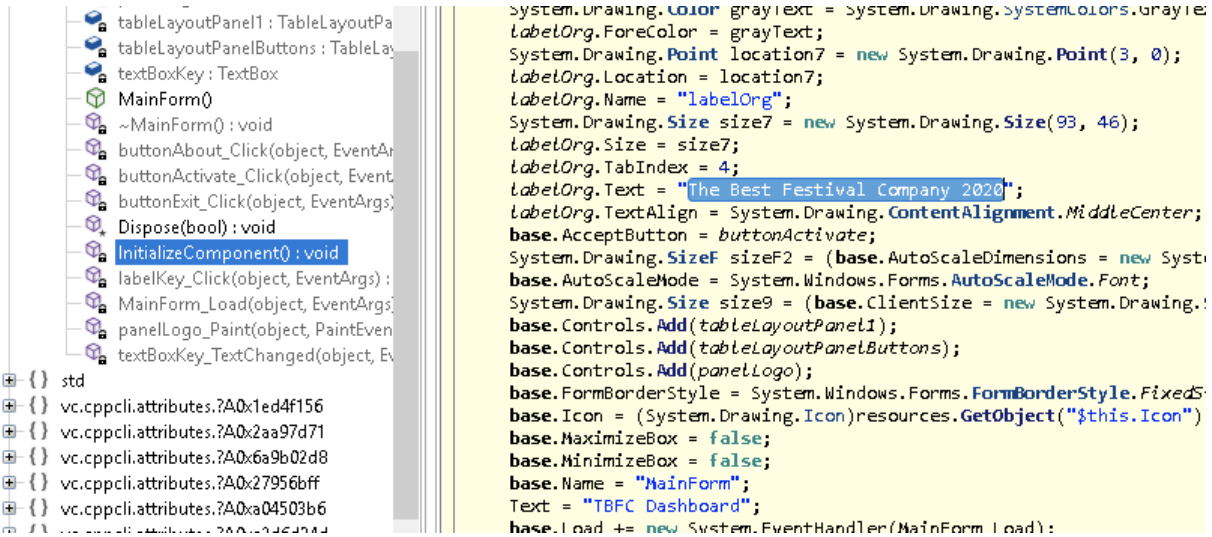
What is the message that shows up if you enter the wrong password for TBFC_APP?



Entering any wrong password will return this message.

Question 2

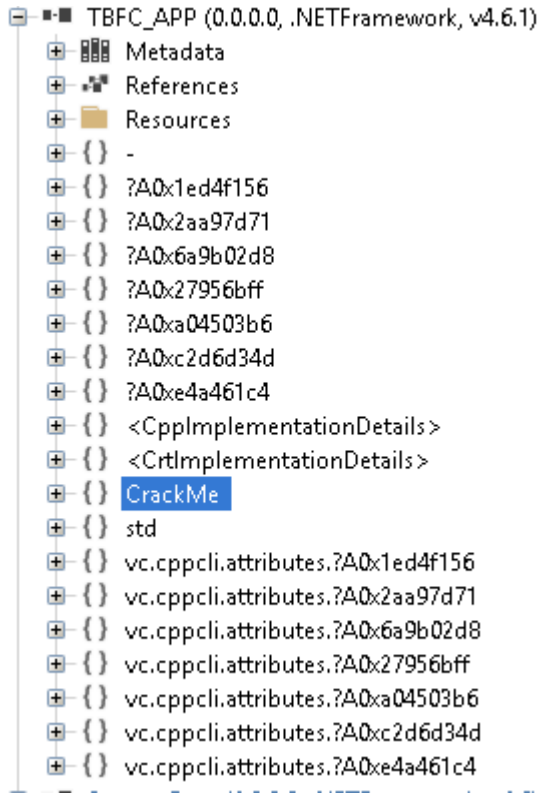
What does TBFC stand for?



The answer is found after opening TBFC_APP.exe in ILSpy. It is under CrackMe, MainForm, InitializeComponent().

Question 3

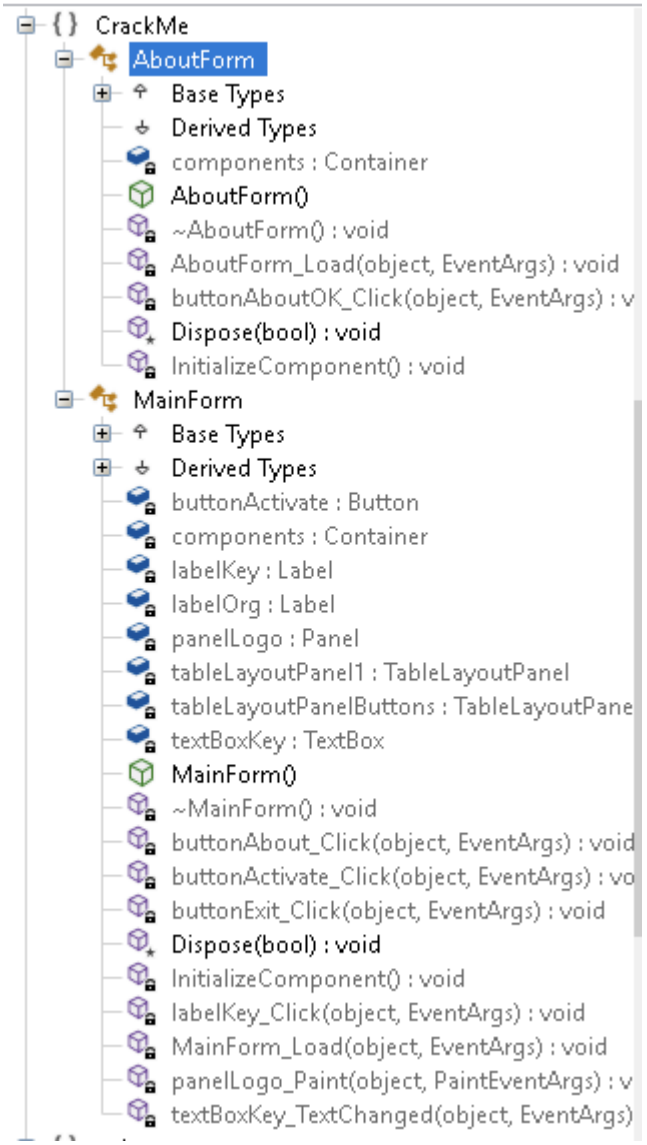
Decompile the TBFC_APP with ILSpy. What is the module that catches your attention?



The modules all seem pretty normal, except for “CrackMe”.

Question 4

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



AboutForm has very little information, while MainForm sounds more promising and indeed has more modules and information.

Question 5

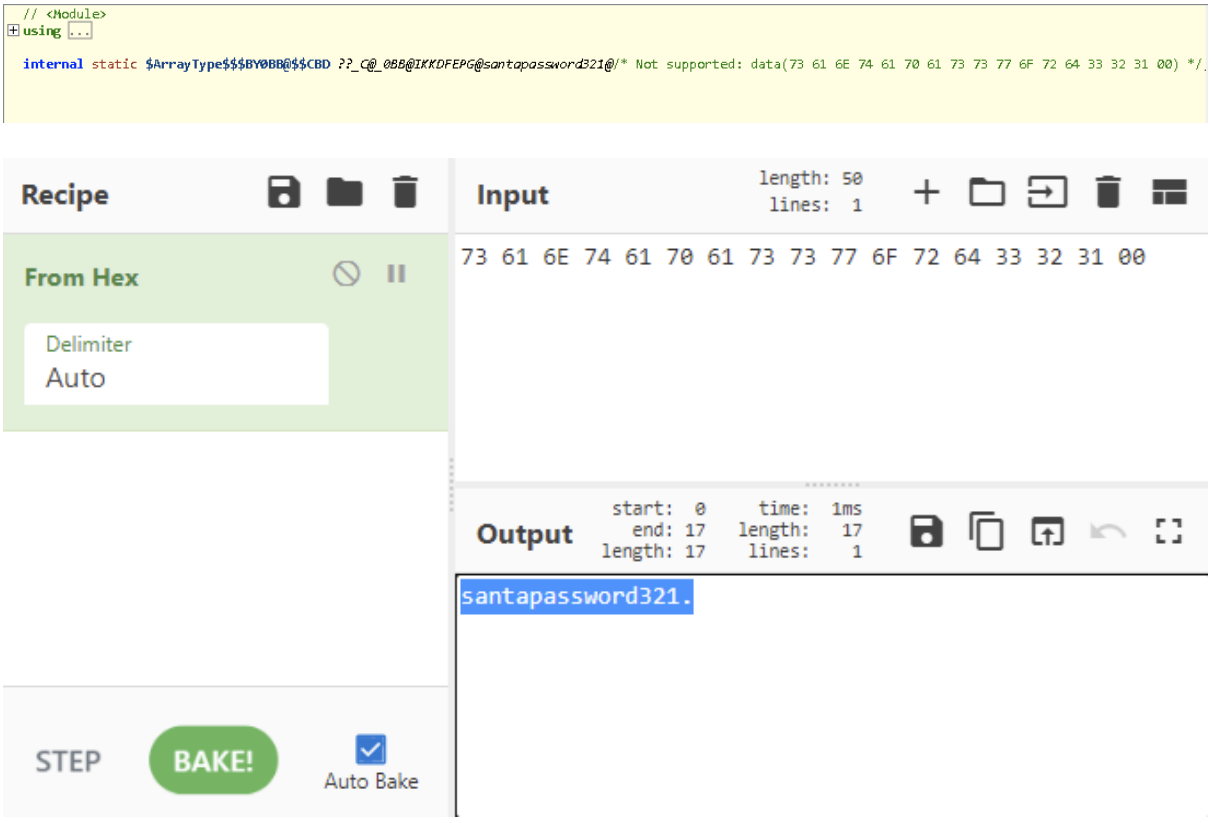
Which method within the form from Q4 will contain the information we are seeking?


```
EPG@santapassword321@);
```

“buttonActivate_Click” shows the messages for correct and incorrect password entries including the flag that we are looking for and also contains something that seems like it is santa’s password.

Question 6

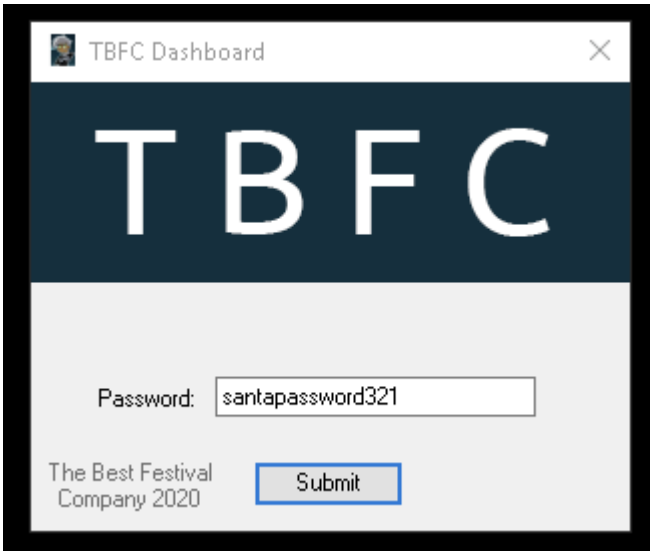
What is Santa's password?

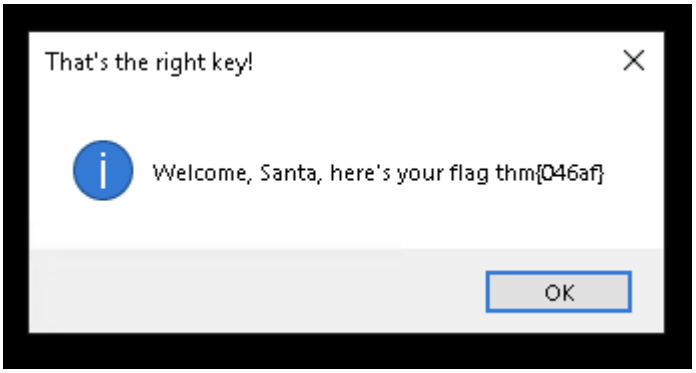


Double-clicking on the password we saw earlier took us to another module and it contains a hexadecimal code. We copied the code into cyberchef to obtain the password. The correct password turned out to be the same as the password we saw earlier.

Question 7

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





The flag was found earlier, but we can also enter the correct password into TBFC_APP.exe to get the message with the flag.

Thought Process/Methodology:

We opened remmina and entered the machine ip along with the given credentials to get into the remote desktop. We first opened TBFC_APP.exe on the desktop and tried to submit a password to it to get the error message. We then opened up ILSpy and opened the .exe within it to disassemble it. We saw a module called “CrackMe” which is an obvious sign, upon opening it we see AboutForm and MainForm. MainForm seemed to contain more useful information and we searched through it. “buttonActivate_Click” surprisingly contained the flag and password, but we investigated further and double clicked on the password which led us to a hexadecimal code which decoded into the password. We then entered the password into TBFC_APP and got the message with the flag.

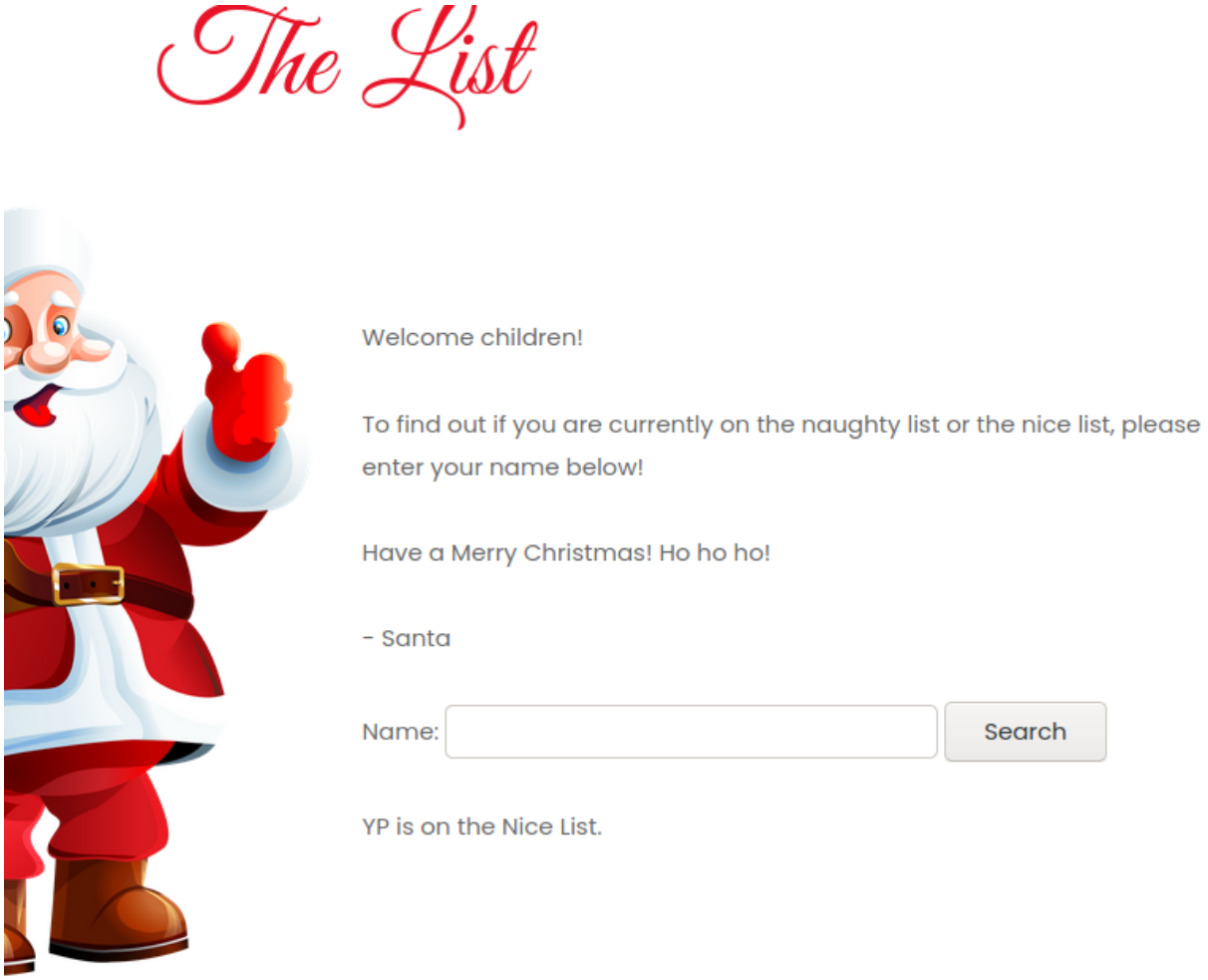
Day 19: Web Exploitation – The Naughty or Nice List

Tools used: Kali Linux, Firefox

Solution/walkthrough:

Question 1

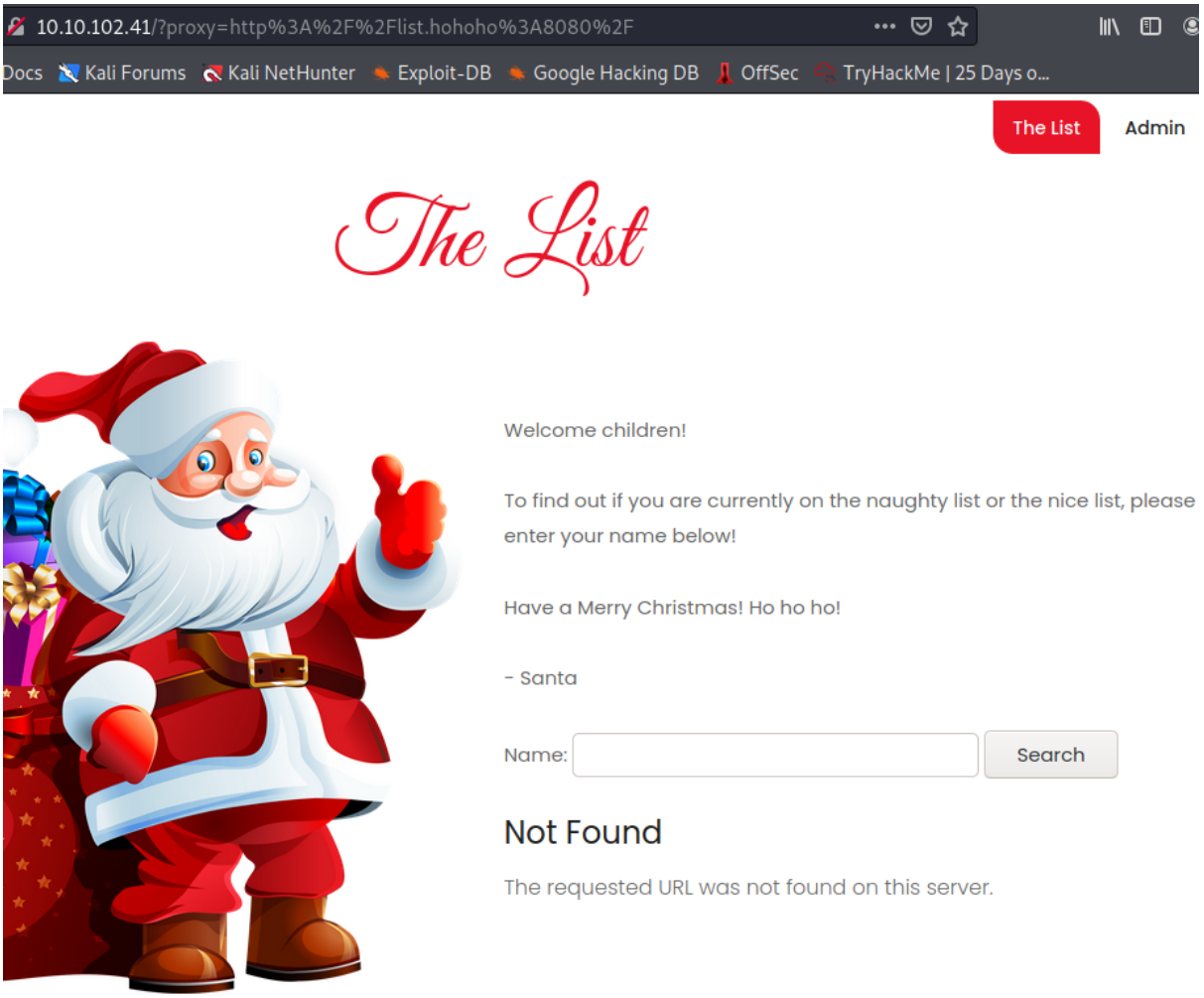
Which list is this person on?



The answer can be obtained easily by entering the name into the name box and clicking search.

Question 2

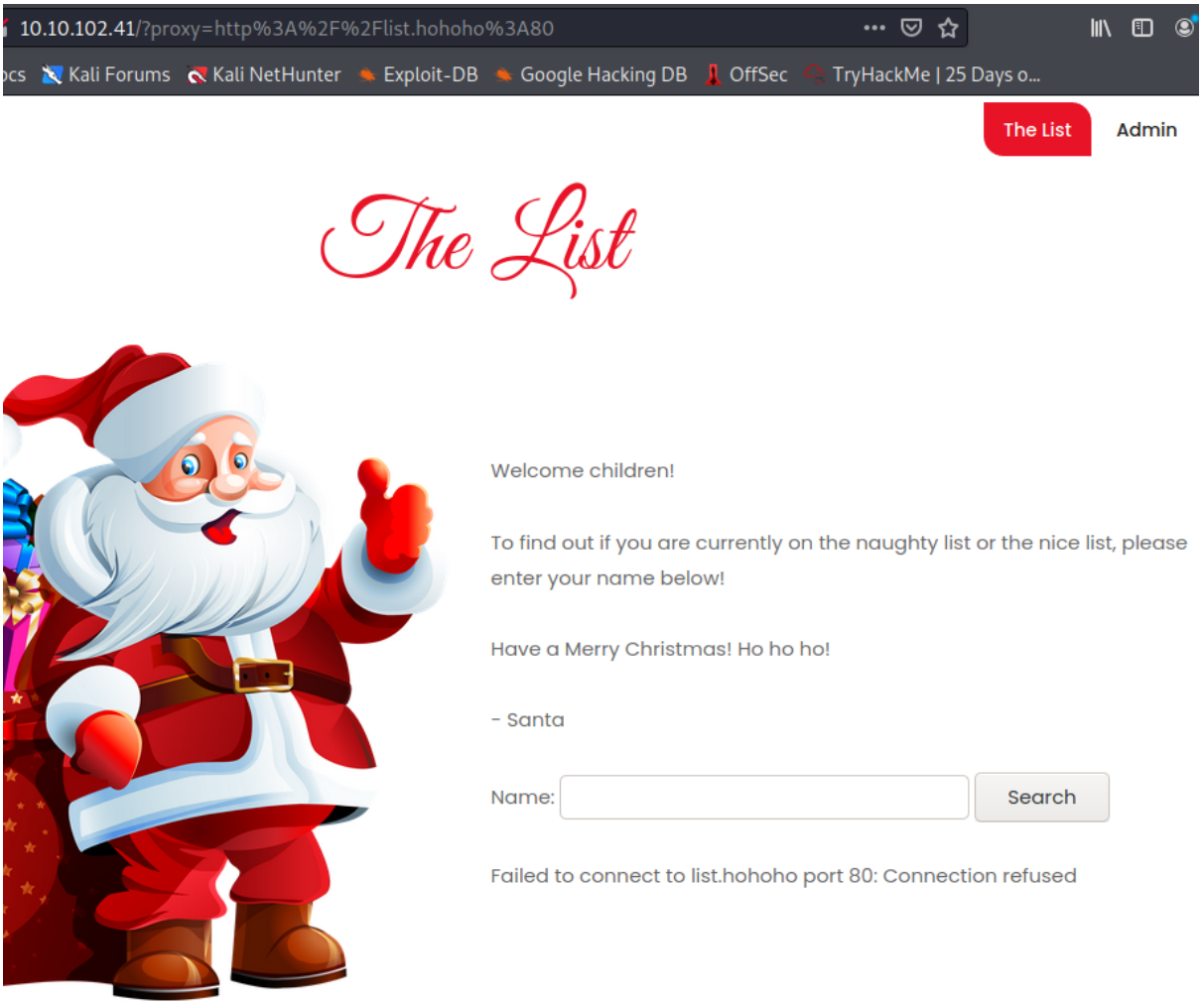
What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F"?



The requested URL was not found on this server.

Question 3

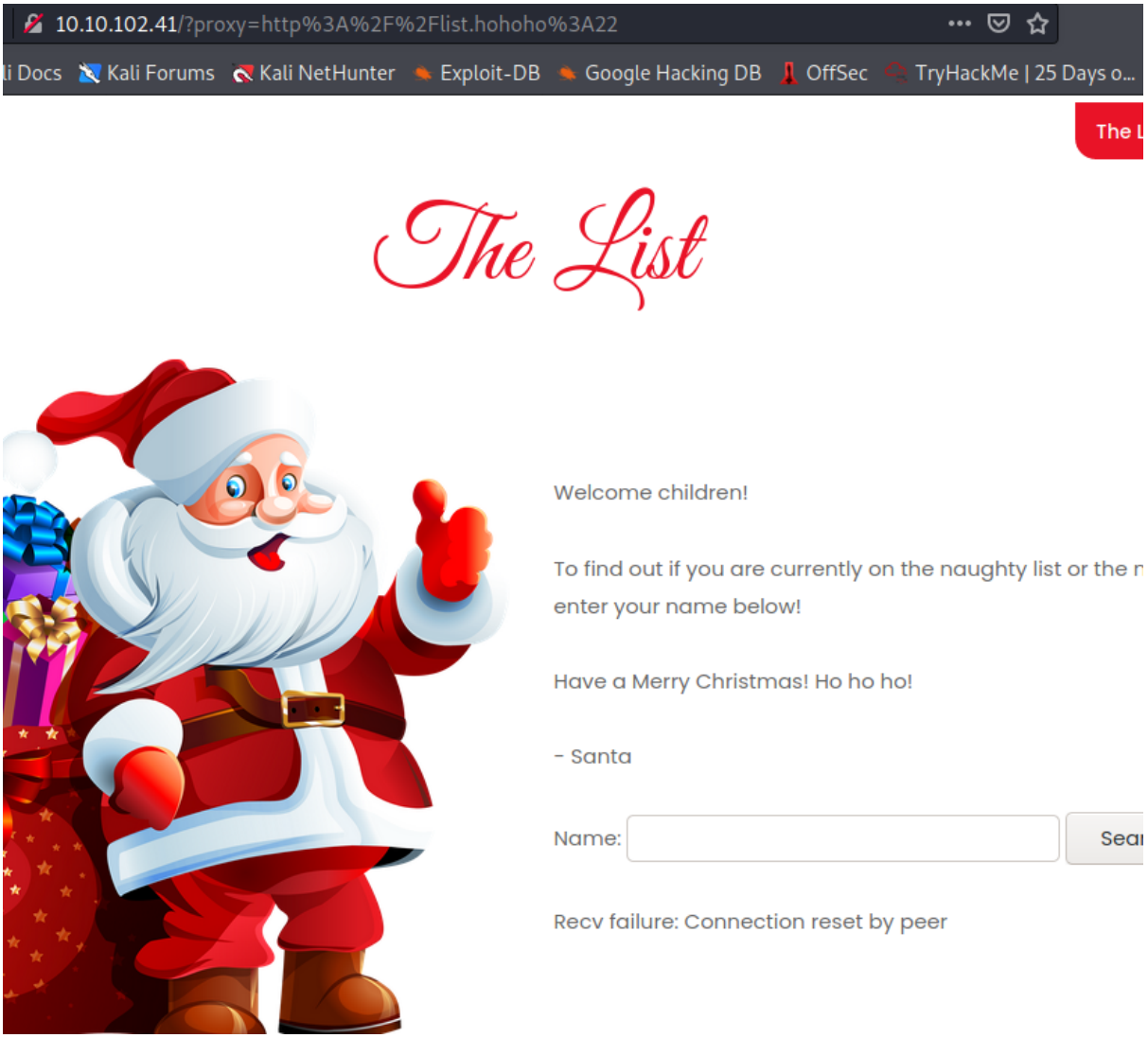
What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A80"?



Failed to connect to list.hohoho port 80: Connection refused

Question 4

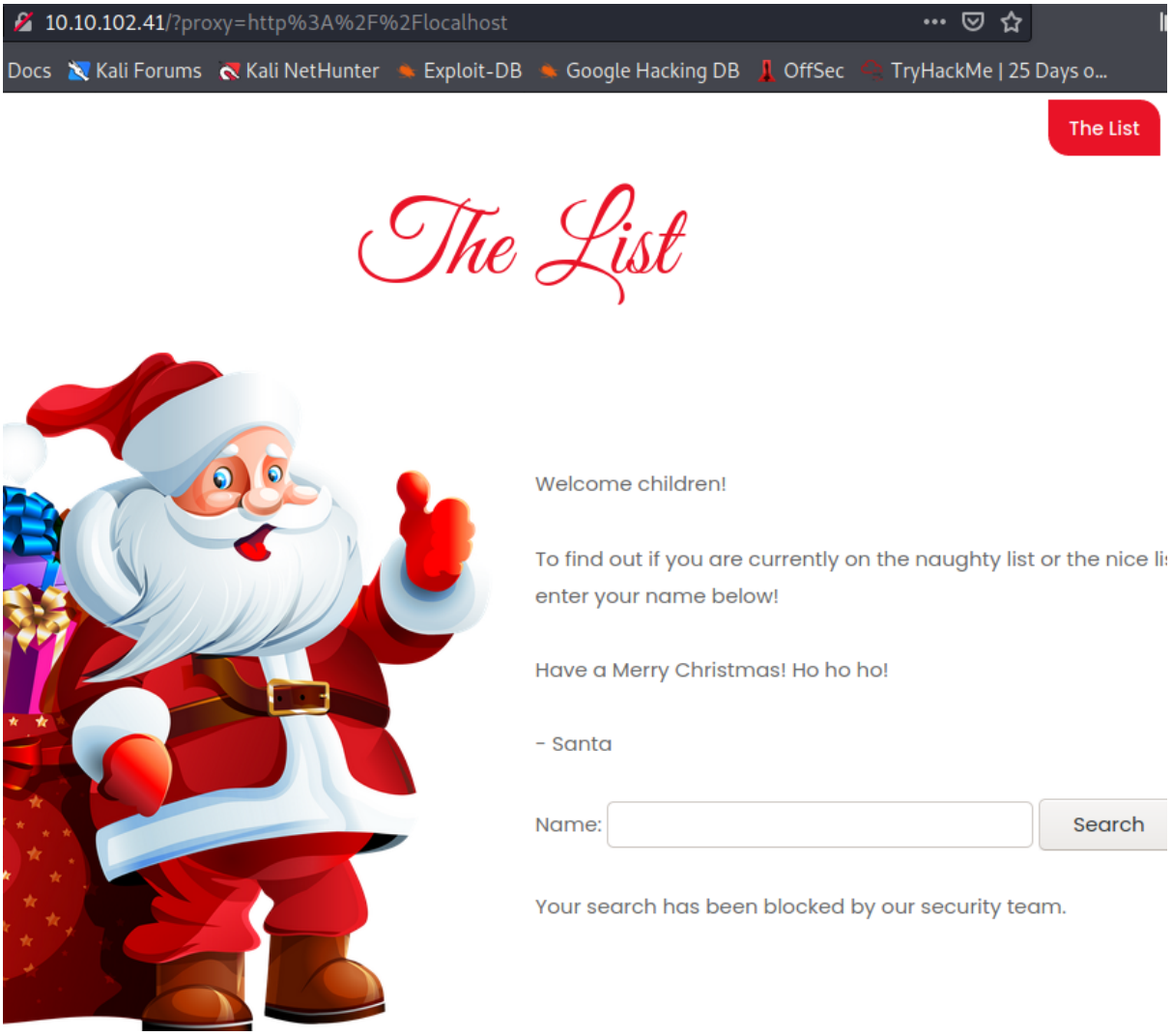
What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A22"?



Recv failure: Connection reset by peer

Question 5

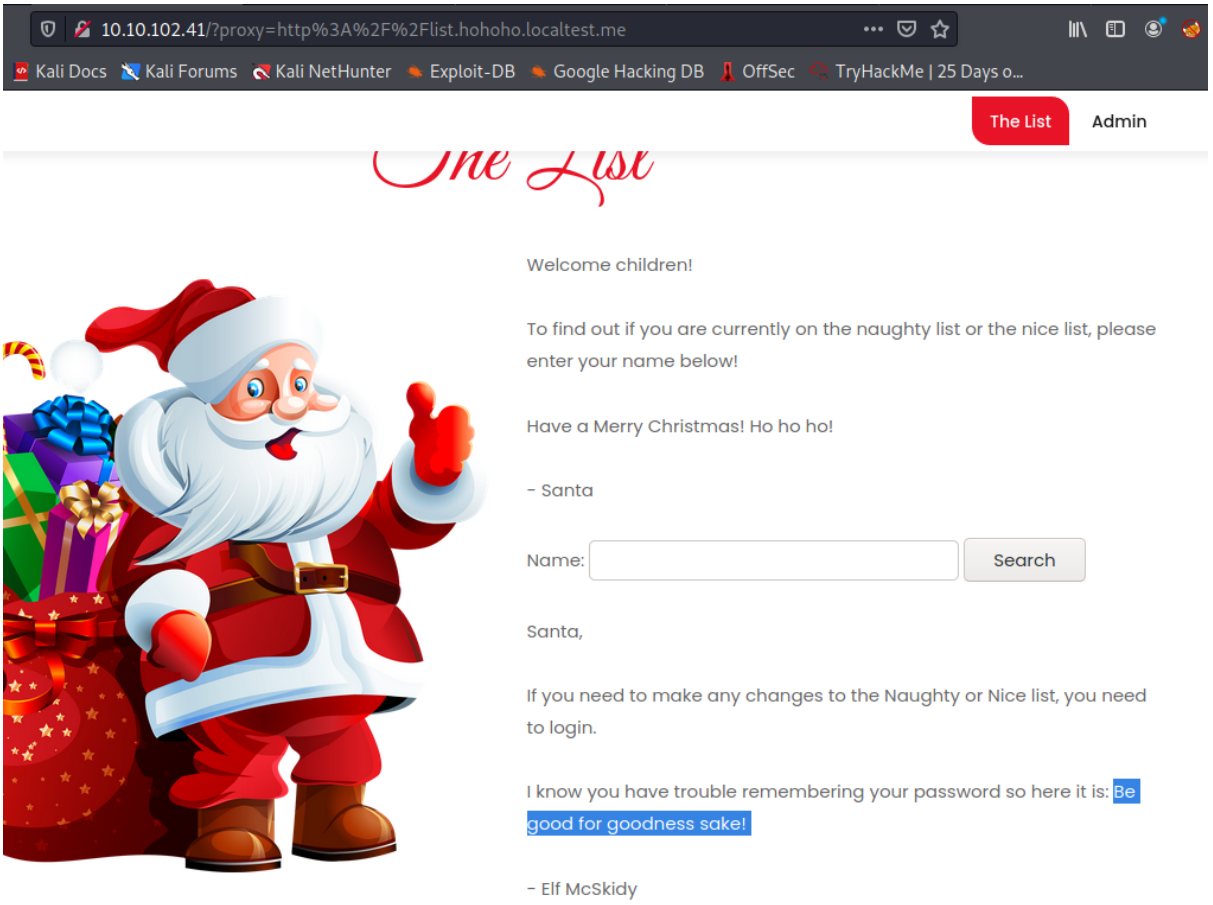
What is displayed on the page when you use "/?proxy=http%3A%2F%2Flocalhost"?



Your search has been blocked by our security team.

Question 6

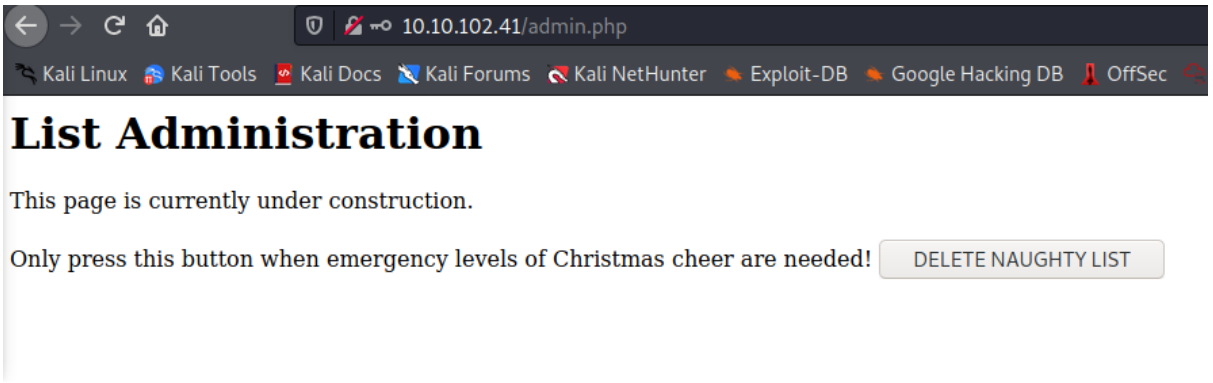
What is Santa's password?

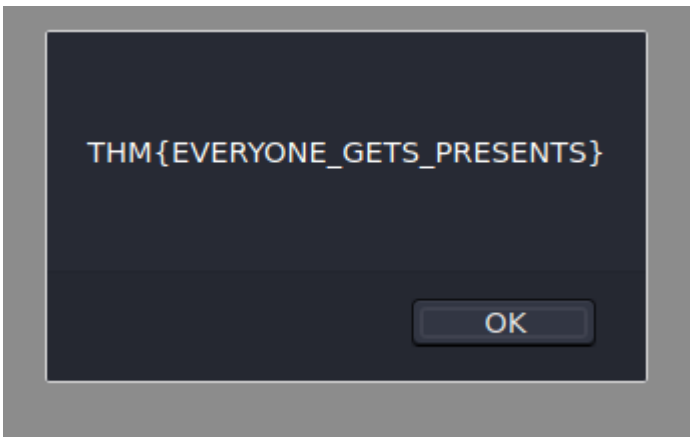


Be good for goodness sake!

Question 7

What is the challenge flag?





We used the username “Santa” and the password we got earlier to login, and then we click “delete naughty list” to get the flag.

Thought Process/Methodology:

We started with using the machine ip as the url to get to the website. We entered the names into the form and clicked search to find whether the name is on the naughty list or the nice list. After searching for the name, we noticed the url changed to include an encoded url. We used a URL decoder to see what it was. We tried fetching the root of the site by not including the search.php in the url, and got an error as the return. We then tried the url with a changed port from 8080 to 80 and got a connection refused error. Changing the port number to 22 which is the default http port returns “connection reset by peer”. Next we tried replacing the hostname with "localhost" or "127.0.0.1", but the website had a check to prevent that, and returned “Your search has been blocked by our security team.". The check however can be easily bypassed by using localtest.me to resolve the subdomain to 127.0.0.1. The message that was revealed contains a message to santa along with the password. We then logged in with the username “Santa” and the password to obtain the flag.

Day 20: Blue Teaming – PowershELlF to the rescue

Tools used: Kali Linux, SSH, Powershell

Solution/walkthrough:

Question 1

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

```
-l login_name
        Specifies the user to log in as on the remote machine.
        This also may be specified on a per-host basis in the
        configuration file.
```

-l means 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?

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

A normal check directory of the documents folder only shows “elfone.txt” with 22 characters. By using get-childitem -hidden, we can see that there is another file called “e1fone.txt” that we can use the cat command to read to obtain the answer.

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?

```
PS C:\Users\mceager\Desktop> cd .\elf2wo\
PS C:\Users\mceager\Desktop\elf2wo> ls -Hidden
PS C:\Users\mceager\Desktop\elf2wo> ls


    Directory: C:\Users\mceager\Desktop\elf2wo


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        11/17/2020  10:26 AM             64 e70smsW10Y4k.txt


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

We navigated to the desktop folder and used the -hidden option to enable us to see the hidden text file and get the answer.

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)

```
    Directory: C:\Windows\System32


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--h--        11/23/2020   3:26 PM                3lfthr3e
d--h--        11/23/2020   2:26 PM                GroupPolicy
```

We first navigated to windows system32 directory to run any list command (ls, dir,) with a -filter option with "*3*" to filter any file containing the number 3 which stands for elf3. We also ran it containing the -directory and -hidden options because those fit the properties of the folder we are looking for. The result is that we can find the answer in the list.

Question 5

How many words does the first file contain?

```
PS C:\Users\mceager\Desktop\elf2wo> Get-Content C:\Windows\System32\3lfthr3e\1.txt | Measure-Object -Word

Lines Words Characters Property
----- ----- ---------- --------
      9999


PS C:\Users\mceager\Desktop\elf2wo>
```

We type the command Get-Content C:\Windows\System32\3lfthr3e\1.txt | Measure-Object -Word and it will show us how many words it has.

Question 6

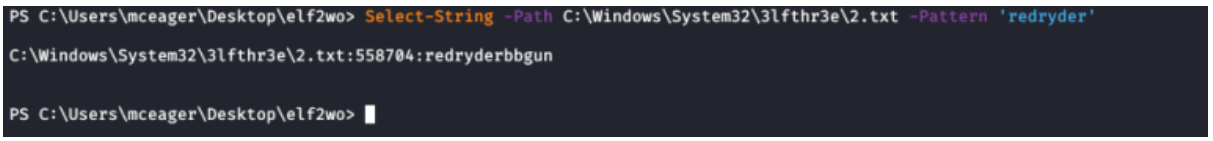
What 2 words are at index 551 and 6991 in the first file?

```
PS C:\Users\mceager\Desktop\elf2wo> (Get-Content C:\Windows\System32\3lfthr3e\1.txt)[551]
Red
PS C:\Users\mceager\Desktop\elf2wo> (Get-Content C:\Windows\System32\3lfthr3e\1.txt)[6991]
Ryder
PS C:\Users\mceager\Desktop\elf2wo>
```

We used get-content on the txt file with the index in square brackets to get the answer. The resulting command is (get-content 1.txt)[551,6991].

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)



To find the second file , we use the list command with select-string and -Pattern option with ‘redryder’ at the end of the command to reveal the answer.

Thought Process/Methodology:

First, we search online for the SSH manual, and get the description for parameter -l. Next, the normal check directory of the documents folder only shows “elfone.txt” with 22 characters. So, by using get-childitem -hidden, we can see that there is another file called “e1fone.txt” that we can use the cat command to read to obtain the answer. Moving on, we navigated to the desktop folder and used the -hidden option to enable us to see the hidden text file and get the answer. For question 4, we first navigated to windows system32 directory to run any list command (ls, dir,) with a -filter option with “*3*” to filter any file containing the number 3 which stands for elf3. We also ran it containing the -directory and -hidden options because those fit the properties of the folder we are looking for. The result is that we can find the answer in the list. Next, we type the command Get-Content C:\Windows\System32\3lfthr3e\1.txt | Measure-Object -Word and it will show us how many words it has. Next, we used get-content on the txt file with the index in square brackets to get the answer. The resulting command is (get-content 1.txt)[551,6991]. Finally, to find the second file , we use list command with select-string and -Pattern option with ‘redryder’ at the end of the command to reveal the answer.