

PSP0201

Week 2

Writeup

Group Name: Hacktocrats

Members

ID	Name	Role
12111 03194	NUR FARAHIYA AIDA BINTI ABD RAZAK	Leader
12111 03602	NUR ALIA AMELISA SYAZREEN BINTI MOHD SULEI	Member
12111 03430	AINA SOFEA BINTI AMIER HAMZAH	Member
12111 03237	NURUL AIN BINTI KAMARUDIN	Member

Day 1: Web Exploitation – A Christmas Crisis

Tools used: Kali Linux, Firefox

Solution/walkthrough:

Question 1: Registration and logging to the Christmas Control Centre

The screenshot shows two browser windows. The left window is a developer tools storage tab for www.mozilla.org, displaying a table of cookies. The right window is a Mozilla Firefox browser showing the 'CHRISTMAS CONTROL CENTRE' login page with fields for 'username' (ainasofea) and 'password' (redacted). The status bar at the bottom of the Firefox window says 'THM AttackBox'.

The screenshot shows two browser windows. The left window is a developer tools storage tab for www.mozilla.org, displaying a table of cookies. The right window is a Mozilla Firefox browser showing the 'VIEW CONSOLE' page with a teddy bear image and a table titled 'Control Active?'. The table lists six tasks: Part Picking, Assembly, Painting, Touch-up, Sorting, and Sleigh Loading, all marked as 'No'. The status bar at the bottom of the Firefox window says 'THM AttackBox'.

Question 2:

Open the browser tools to get the value and the name of the cookie

The screenshot shows a Firefox browser window with the URL tryhackme.com/room/learnyberin25days. The page content discusses cookies and their storage on the user's computer. On the right side, there is a "VIEW CONSOLE" interface with a teddy bear image. Below it, a table lists three items: "Part Picking" (No), "Assembly" (No), and "Painting" (No). At the bottom of the Firefox window, the developer tools Storage tab is open, showing the "Cookies" section. A single cookie entry is selected: "auth" with the value "7b22636f6d70...". The status bar at the bottom of the browser indicates "52m 08s".

Question 3:

Change the value of the cookie to string by using cyberchef

The screenshot shows a Firefox browser window with the same URL as the previous question. The developer tools Storage tab is open, showing the "Cookies" section with the "auth" cookie selected. To the right, the CyberChef application is running in a separate tab. The "From Hex" operation is selected, with the input being a hex dump of the cookie value: "7b22636f6d70616e79223a2254686528426537342046 657374697616c20436fd70616e79222c022757365 726e616d05223a2261096e61736f666561227d". The output pane shows the JSON object: {"company": "The Best Festival Company", "username": "ainasofea"}. The status bar at the bottom of the browser indicates "51m 15s".

Question 4:

Changing the username to santa at the JSON files and returning to the value hexadecimal.

The left side shows the TryHackMe room interface for challenge 25days. It displays a series of questions and their answers:

- What is the name or one cookie used for authentication? (Answer: auth)
- In what format is the value of this cookie encoded? (Answer: Hexadecimal)
- Having decoded the cookie, what format is the data stored in? (Answer: JSON)
- Figure out how to bypass the authentication. (Answer: 7b22636f6d70616e79223a2254686520426573742046657)
- Now that you are the santa user, you can re-activate the assembly line!
- What is the flag you're given when the line is fully active? (Answer: THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWfhYmQy})

The right side shows the CyberChef interface with the following configuration:

- Operations: Recipe
- From Hex: Delimiter Auto
- To Hex: Delimiter None, Byte 0
- Input: length: 58, lines: 1, start: 0, end: 116, length: NaN, JSON content: {"company": "The Best Festival Company", "username": "santa"}.
- Output: length: 68, lines: 1, start: 0, end: 116, length: 116, Hex content: 7b22636f6d70616e79223a2254686520426573742046657 057374697616c20436f6d70616e79222c2922757365 7266e610d05223a73610e74612270

Question 5:

Now having access to the controls, switching on every control shows the flag.

The left side shows the TryHackMe room interface for challenge 25days. It displays a series of questions and their answers:

- What is the value of Santa's cookie? (Answer: 7b22636f6d70616e79223a2254686520426573)
- Now that you are the santa user, you can re-activate the assembly line!
- What is the flag you're given when the line is fully active?

The right side shows a screenshot of a "Control Console" application window titled "ControlActive?". It features a teddy bear icon and a list of controls with toggle switches:

Control	Status
Picking	Yes
Assembly	Yes
Painting	Yes
Touch-up	Yes
Sorting	Yes

The status for all controls is set to "Yes".

Thought Process/Methodology:

After we gained access to the target system, we were presented with a login/registration screen. We then created an account and logged in. After logging in, we opened the browser's developer tool and selected the Storage tab to examine the site cookie. We concluded from the cookie data that it was a hexadecimal number and used Cyberchef to convert it to text. We discovered a JSON statement containing the username element. We used Cyberchef to change the username to 'santa,' the administrator account, and then converted it back to hexadecimal. We updated the page after replacing the cookie value with the transformed one. We are now presented with an administrator page (Santa's) and proceeded to enable each control, which displayed the flag.

Day 2: Web Exploitation - The Elf Strikes Back!

Tools used : Kali Linux & Firefox

Solution / Walkthrough :

Question 1: the string of text that needed the url to be added to get the access to the upload page is detected.

The left side shows a web-based interface for a task titled "Elf Strikes Back". It displays the following information:

- Title: Elf Strikes Back
- IP Address: 10.10.211.75
- Expires: 1h 35m 07s
- Buttons: "Add 1 hour" and "Terminate"

The main content area contains a brief narrative about the task, mentioning that the user has been hacked and needs to protect themselves by performing a security audit on the new server. It also provides instructions to accept the task and start the server.

The right side shows a screenshot of a Firefox browser window. The URL is http://10.10.211.75/uploads/. The page displays a message: "You are not signed in. Please enter your ID as a GET parameter (?id=YOUR_ID_HERE)". The background of the browser window features a snowy winter scene with Santa Claus.

Question 2: filter has been bypassed and reverse shell has been uploaded. Files have been uploaded in /uploads/ directory.

The left side shows a TryHackMe challenge interface for "Elf McSkidy". The challenge details are as follows:

- Challenge: Elf McSkidy
- Description: You have been assigned an ID number for your audit of the system: `?id=ODIzODI5MTNiYmYw`. Use this to gain access to the upload section of the site.
- Good luck!
- Note: You note down the ID number and navigate to the displayed IP address (10.10.111.106) in your browser.

The challenge includes several questions:

- What string of text needs adding to the URL to get access to the upload page? Answer: `?id=ODIzODI5MTNiYmYw`
- What type of file is accepted by the site? Answer: image
- Bypass the filter and upload a reverse shell.
- In which directory are the uploaded files stored? Answer format: `/******/`
- Activate your reverse shell and catch it in a netcat listener!
- No answer needed
- What is the flag in `/var/www/flag.txt`? Answer format: `***{*****}`

The right side shows a terminal window titled "THM AttackBox" running on Kali Linux. The user has successfully uploaded a file and is interacting with it via a netcat listener. The terminal shows the command `nc -l -p 4444 -e /bin/sh` and the user is prompted for a password. The background of the terminal window features a festive Christmas tree.

Question 3: Image is the type of file that has been accepted by the site

interested.

[Putting it all together](#)

This was a *lot* of information, so let's put it all together and look at the full process for exploiting a file upload vulnerability in a PHP web application:

1. Find a file upload point.
2. Try uploading some innocent files -- what does it accept? (Images, text files, PDFs, etc)
3. Find the directory containing your uploads.
4. Try to bypass any filters and upload a reverse shell.
5. Start a netcat listener to receive the shell
6. Navigate to the shell in your browser and receive a connection!

At the bottom of the dossier is a sticky note containing the following message:

For Elf McEager:
You have been assigned an ID number for your audit of the system: **00120135HTNLYwW**.
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 (10.10.113.60) in your browser**.

[Answer the questions below](#)

What string of text needs adding to the URL to get access to the upload page?

Answer format: ***** [Submit](#) [Hint](#)

What type of file is accepted by the site?

Answer format: **** [Submit](#) [Hint](#)

The screenshot shows a Firefox browser window with the title 'Protection - Mozilla Firefox'. The tab bar includes 'Protection', 'New Tab', and '10.10.113.60/?id=ODIzODI5MTNy...'. The main content area displays a dark-themed web page titled 'Protect the Factory!'. It contains a message: 'If you see any suspicious people near the factory, take a picture and upload it here!', with 'Select' and 'Submit' buttons. Below this is a placeholder 'No file selected'. At the bottom of the page, there is a note: 'It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!' with a 'Refresh Firefox...' button. The status bar at the bottom right shows '29m 37s'.

Question 4: The flag of /var/www/flag.txt is provided below the control console



Thought Process/Methodology:

After login, our ip address has been filled in the firefox. Then a file upload address has been located. We tried to upload a few unimpeachable files to figure out what it approves and what it does not. For example, files such as images, text files, PDFs, etc. Then we searched up the directory containing our uploads. After all of that has been done, we tried to bypass any filters in order to upload a reverse shell. After that, we started a netcat listener so that we could receive the shell. Last but not least, the shell in our browser has been navigated and the connection has been received!

Day 3: Web Exploitation- Christmas Chaos

Tools used: Firefox, BurpSuite, FoxyProxy, Google

solutions/ walkthrough:

Question 1:

The name of the botnet that is mentioned in the text is Mirai botnet.

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:

Starbucks paid \$250 for reporting default credentials according to the text.

In fact, companies such as Starbucks and the US Department of Defense have been victim to leaving services running with default credentials, and bug hunters have been rewarded for reporting these very simple issues responsibly (Starbucks paid \$250 for the reported issue):

- <https://hackerone.com/reports/195163> - Starbucks, bug bounty for default credentials.
- <https://hackerone.com/reports/804548> - US Dept Of Defense, admin access via default credentials.

Question 3:

The agent assigned from the Dept of Defense that disclosed the report on Jun 25th is ag3nt-j1.

arm4nd0 posted a comment.	May 11th (2 years ago)
agentt2 closed the report and changed the status to ● Resolved.	May 22nd (2 years ago)
arm4nd0 posted a comment.	Jun 25th (2 years ago)
agent-l8 U.S. Dept Of Defense staff posted a comment.	Updated Jun 25th (2 years ago)
arm4nd0 posted a comment.	Jun 25th (2 years ago)
arm4nd0 requested to disclose this report.	Jun 25th (2 years ago)
ag3nt-j1 U.S. Dept Of Defense staff agreed to disclose this report.	Jun 25th (2 years ago)

Question 4:

We can look for the port number on Burp by clicking the options on Burp and select edit Proxy Burp. The port number is 8080.

The screenshot shows two windows side-by-side. On the left is a web browser window for tryhackme.com/room/learn cyberin25days. It displays a challenge titled "Santa Sleigh Tracker" with instructions for adding payloads and starting an attack. On the right is a Mozilla Firefox window titled "FoxyProxy Edit Proxy". The "Edit Proxy Burp" tab is selected, showing proxy settings: Title/Description: "Burp", Proxy Type: "HTTP", Color: "#66cc66", Proxy IP address or DNS name: "127.0.0.1", Port: "8080", Username: "username", and Password: "*****".

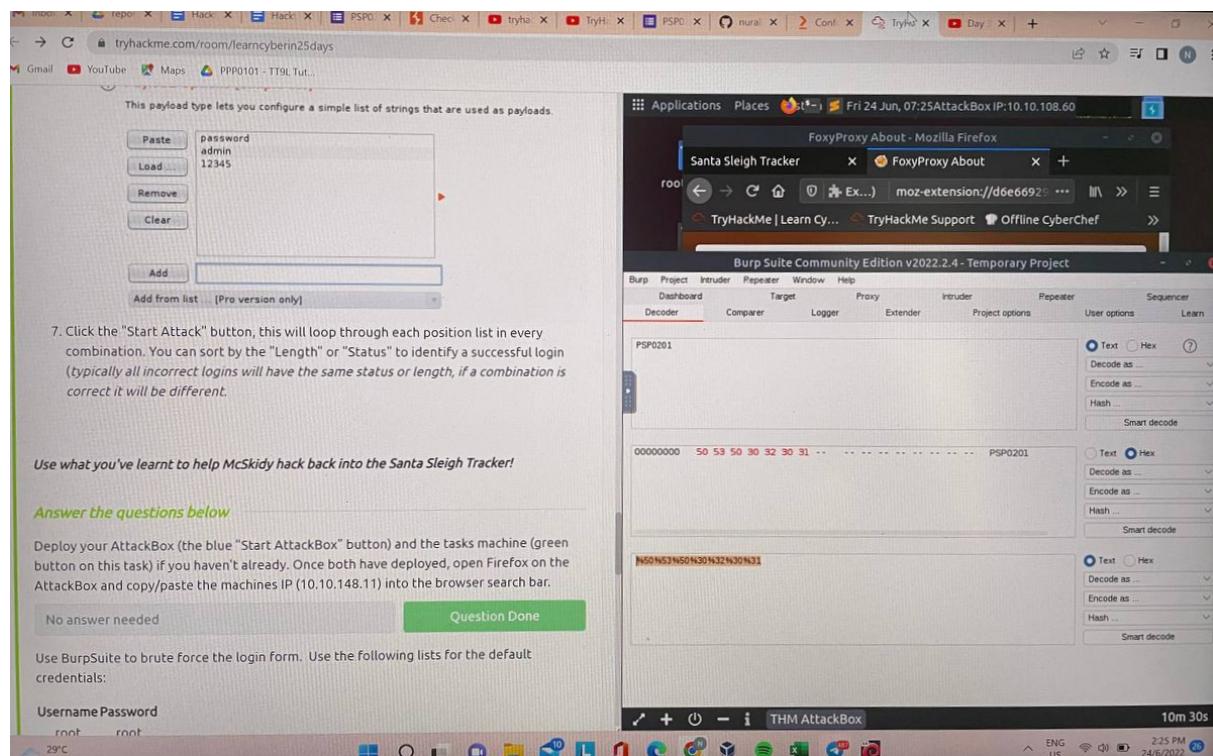
Question 5:

The proxy type can be found in the same section as the port number. The proxy type is HTTP.

This screenshot is identical to the one above, showing the TryHackMe challenge and the FoxyProxy settings. The proxy type "HTTP" is clearly visible in the "Edit Proxy Burp" window.

Question 6:

In BurpSuite, select the decoder tab. Insert the word “PSP0201” and encode the text as URL. The value obtained is the one we are looking for which is %50%53%50%30%32%30%31.



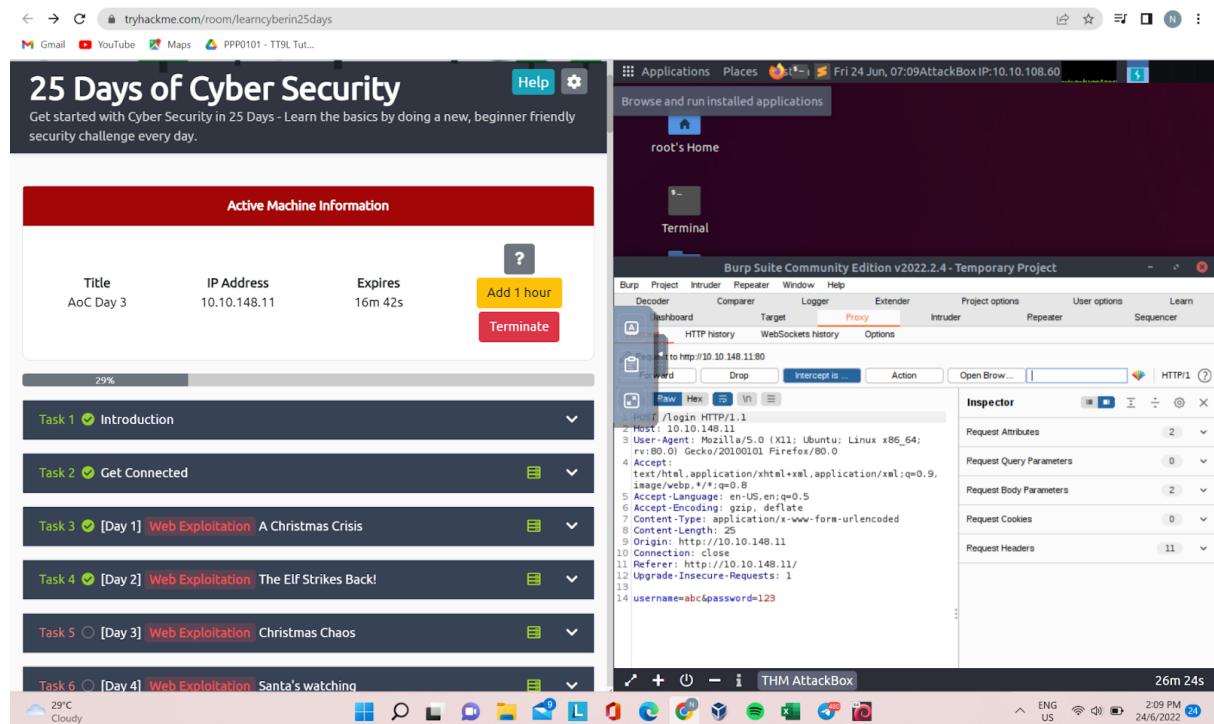
Question 7:

In the attack type section from the intruder tab, the one that matches the description in the google form which is “Uses multiple payload sets. Different payload for each defined position up to maximum 20. Iterates through each payload set in turn, so all permutations of payload combinations are tested” is Cluster Bomb.

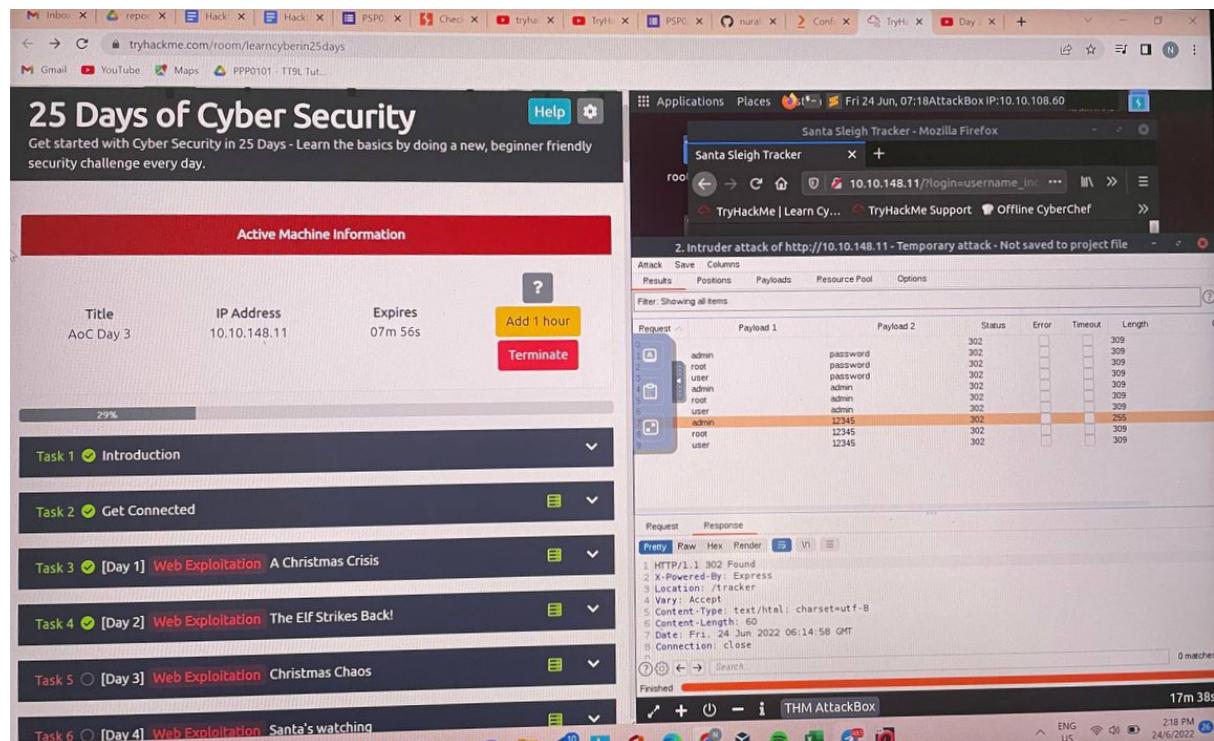
The screenshot shows a web browser window with a challenge from tryhackme.com. The challenge involves a story about McSkidy and a screenshot of Burp Suite's Intruder tab. The Intruder tab shows a payload configuration for "Cluster bomb" with two payloads: "admin" and "password". The THM AttackBox interface is also visible at the bottom.

Question 8:

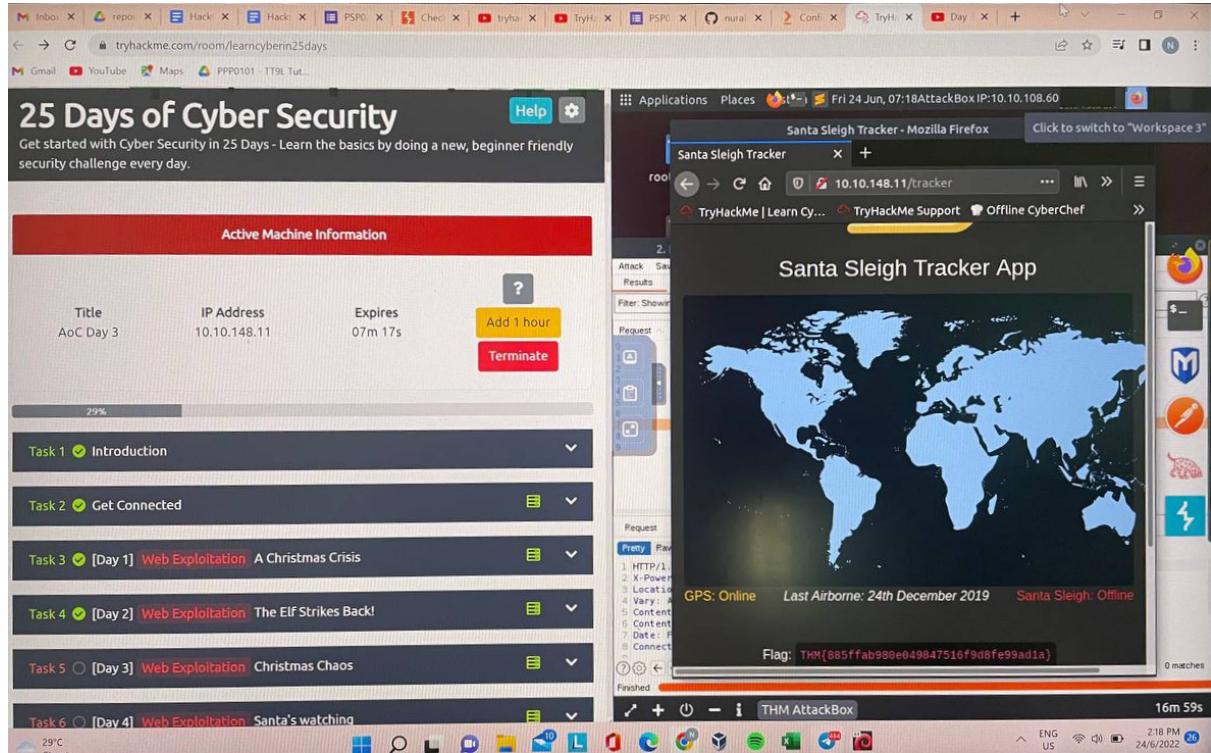
To obtain the flag, go to BurpSuite and enter the port number 8080 and change the specific address to 127.0.0.1. We need to ensure the intercept is on, turn on ‘Burp’ on FoxyProxy and now we can see that BurpSuite has held our request. Go to Santa’s portal and login using any random username and password. This captured request will be shown in the proxy tab. Right click and choose ‘send to intruder’ . In the intruder tab, we can now see our request. Select “Cluster Bomb” in the Attack type dropdown menu. As we want to tell each “Position” which payload to use, we will choose a list of usernames and passwords to be used. In this case, for Payload 1 which is the username, we use: “admin”, “root”, “user”. For Payload 2 which is the password, we use: “password”, “admin”, and “12345”.



Click the “Start Attack” button to loop through each position list in every combination. We can sort the “Length” and “Status” to look for a successful login. In our case, we identified that the correct username and password would be “admin” and “12345”.



Direct back to Santa's Portal and enter the correct username and password.
The flag is now shown on the screen!!



Thought Process/Methodology:

Day 4: Web Exploitation - Santa's watching

Tools used: Attackbox, mozilla firefox, terminal

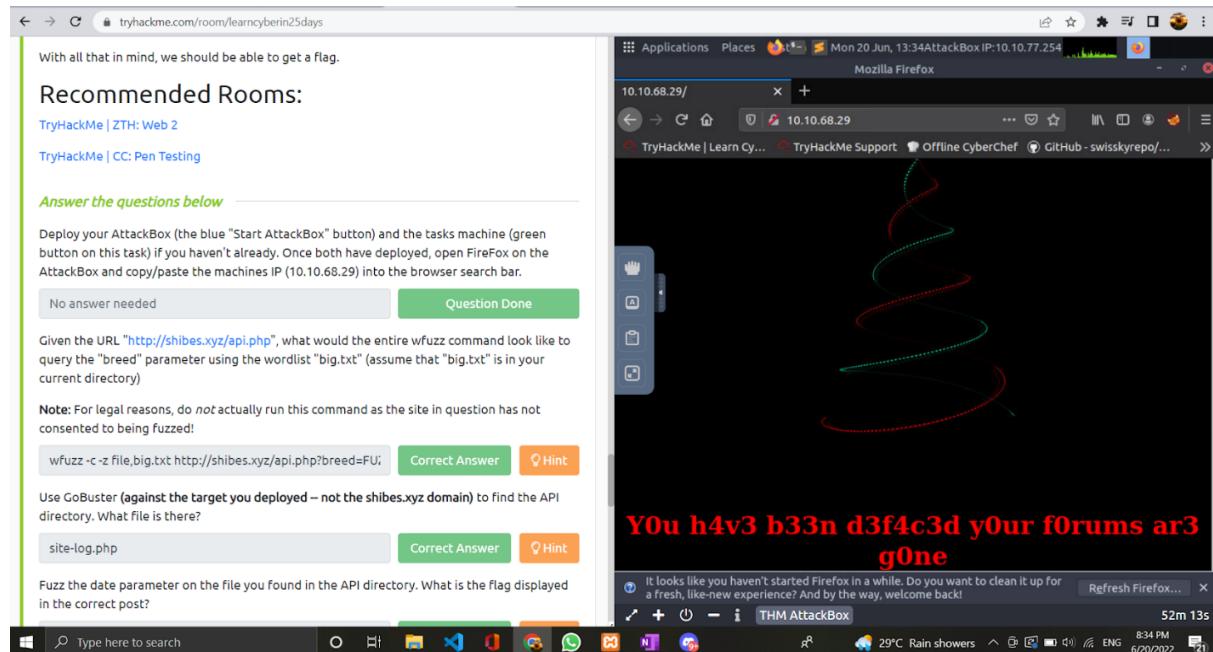
Solution/walkthrough:

Question 1:

Open the IP addresses given in the firefox.

Then find the accurate parameter and command.

Common wfuzz dash c to get the colour output, dash z to select that we are going to use a file. Then we want the big.txt and we put the url which is '<https://shibes.xyz/api.php>' and breed for FUZZ at the end.



The screenshot shows a web browser window for the TryHackMe challenge 'learnCyberIn25days'. On the left, there's a question about wfuzz and GoBuster. On the right, a terminal window on the host machine shows the execution of a wordlist attack using Gobuster against the target IP (10.10.68.29). The terminal output includes details like threads, wordlist file, status codes (200, 204, 301, 302, 307, 401, 403), user agent (gobuster/3.0.1), extensions (php), and timeout (10s). The attack starts at 2022/06/20 13:49:51.

Question 2:

We enter the IP addresses and navigate with the api directory and find the file site-log.php

The screenshot shows a web browser window for the TryHackMe challenge 'learnCyberIn25days'. On the left, there's a question about wfuzz and GoBuster. On the right, a browser window shows the 'Index of /api' page for the target IP (10.10.68.29). The page lists a single file, 'site-log.php', with details: Name: site-log.php, Last modified: 2020-11-22 06:38, Size: 110. The Apache server information is also visible at the bottom of the page.

Question 3:

Search the IP address, the file and the date of the file using the command date=YYYYMMDD.

The screenshot shows a TryHackMe challenge interface and a Firefox browser window. The challenge details ask to search for the URL "http://shibes.xyz/api.php?date=20220620" using wfuzz with the parameter "breed=FU". The browser window shows the result of the search, displaying the flag "THM{D4t3_AP1}".

Question 4:

-f parameter store results to printer and filenames.

The screenshot shows a terminal window displaying the manpage for the wfuzz command. The page includes options like -f, which stores results to a file. A sidebar on the right lists other versions of the package: buster (2.3.4-1), testing (3.0.1-1), and unstable (3.1.0-1).

Thought process and methodology:

We have to understand the parameter in the WFUZZ and handle it in the terminal. In the terminal, we use the gobuster directory to discover the valuable directories if they exist. We use -u to specify which url to enumerate, -w as path to the wordlist and lastly, -x to specify file extension. We also use the API directory to navigate the files in the Mozilla Firefox's search. To find the flag, we navigate with the api directory and use the file name which is site-log.php and the date command. The date of the file we can see beside the file on the screen is 2020-11-22. With the date format, YYYYMMDD. Then, we get the secret flag.

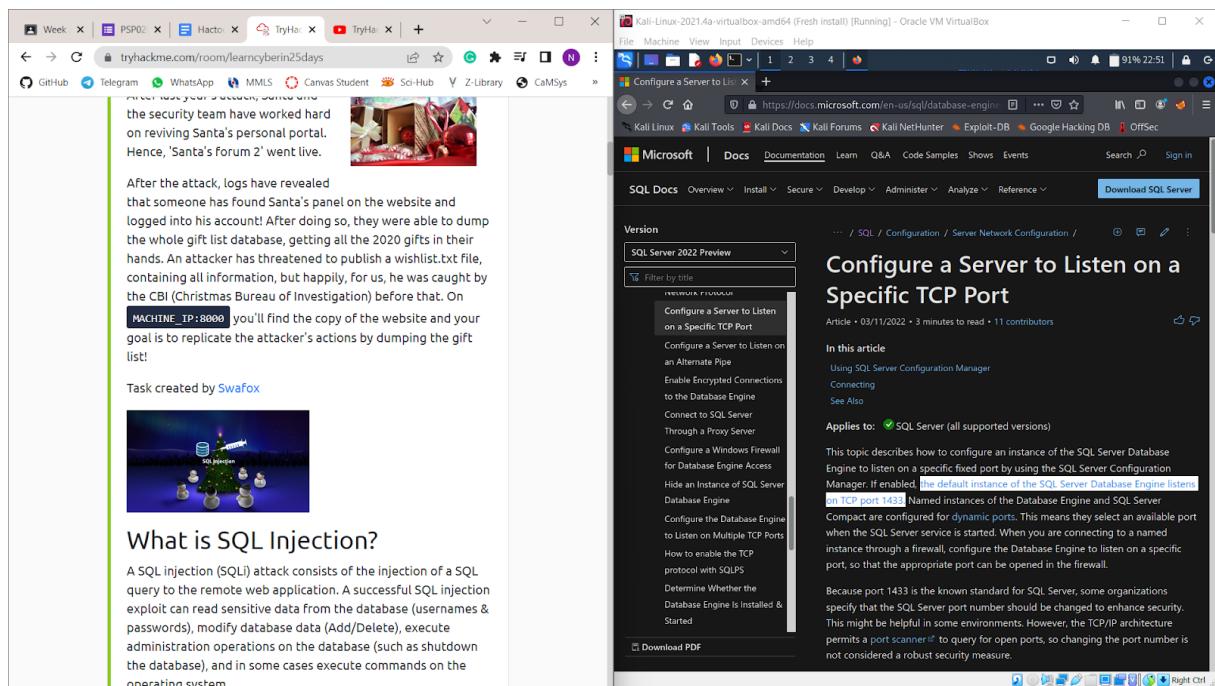
Day 5: Web Exploitation - Someone stole Santa's Gift List

Tools used: Kali linux, Firefox, Burp Suite, FoxyProxy

Solution/walkthrough:

Question 1

Open microsoft documentation on firefox to obtain default port number for SQL server running on TCP



Question 2

Bypassing through santa's login panel by inserting username and comment the rest of the query

The screenshot shows a web browser with multiple tabs open. The active tab is a challenge page from TryHackMe titled "Week 2 Tutorial Progress". It contains a question about bypassing Santa's login panel using SQLMap. Below the question are several answer fields with placeholder text like "/santapanel", "admin", and "admin' or 1=1--". To the right, a Firefox window is open to the URL `10.10.27.37:8000/santapanel`. The Firefox title bar says "Sequel - Mozilla Firefox". The page content reads "Greetings stranger..." and "Do not attempt to login if you are not a member of Santa's corporation!". It features a login form with fields for "Username" (containing "admin' or 1=1--") and "Password" (containing "admin"). A "Login" button is at the bottom. At the bottom of the Firefox window, a status bar says "It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!" and "54m 31s".

Question 3

Obtaining database used in Santa's TODO list

The screenshot shows a web browser and a terminal window on a Kali Linux desktop. The browser tab is "tryhackme.com/room/learnycberin25days". The challenge page discusses a TODO list and mentions SQLite as a database system. It includes a note about bypassing a WAF using the command `--tamper=space2comment`. Below this, there are answer fields for "/santapanel", "Correct Answer", and "Hint". To the right, a terminal window titled "kali@kali:" shows the command `zsh: corrupt history file /home/kali/.zsh_history` being run. The terminal is part of a desktop environment with icons for Trash, File System, Home, and Applications.

Question 4

Insert burp suite saved request into SQL commands and successfully obtained the wishlist from the database.

We can then use this request in SQLMap:

```
sqlmap -r filename
```

SQLMap will automatically translate the request and exploit the database for you.

Challenge

Visit the vulnerable application in Firefox, find Santa's secret login panel and bypass the login. Use some of the commands and tools covered throughout today's task to answer Questions #3 to #6.

Santa reads some documentation that he wrote when setting up the application, it reads:

Santa's TODO: Look at alternative database systems that are better than sqlite. Also, don't forget that you installed a Web Application Firewall (WAF) after last year's attack. In case you've forgotten the command, you can tell SQLMap to try and bypass the WAF by using
--tamper=space2comment

Resources

Check out this cheat sheet: [swisskyrepo/PayloadsAllTheThings](#)

Payload list: [payloadbox/sql-injection-payload-list](#)

Get number of entries, Paul's christmas gift and James' age.

Check out this cheat sheet: [swisskyrepo/PayloadsAllTheThings](#)

Payload list: [payloadbox/sql-injection-payload-list](#)

In-depth SQL Injection tutorial: [SQLi Basics](#)

Answer the questions below

Without using directory brute forcing, what's Santa's secret login panel?

Answer format: *****

Visit Santa's secret login panel and bypass the login using SQLi

No answer needed

How many entries are there in the gift database?

Answer format: **

What did Paul ask for?

Answer format: *****

What is the flag?

Answer format: *****{*****}

What is admin's password?

Answer format: *****

Name	Age	Gift
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
Kenneth	19	TryHackMe Sub
Joshua	12	chair

The database has been updated while you were away!

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back! Refresh Firefox... 37m 46s

Question 5

Scroll down to see THM flag

The screenshot shows a browser window for TryHackMe with the URL tryhackme.com/room/learnbyner25days. On the left, there's a sidebar with various links and a main content area for Question 5. The content area includes several questions with answer fields and submission buttons. One question asks for the flag, which has been completed. On the right, a terminal window shows a SQLite database dump. The dump includes tables for 'hidden_table' and 'users'. The 'hidden_table' contains a single entry with the value 'thmfox{All_I_Want_for_Christmas_Is_You}'. The 'users' table contains one entry with the username 'admin' and password 'EhCNSizzFP6sc7gB'. A message at the bottom of the terminal says 'The database has been updated while you were away!'. The status bar at the bottom of the browser window indicates 'THM AttackBox' and a time of '34m 10s'.

Question 6

Scroll down further to see admin's password

This screenshot is identical to the one above, showing TryHackMe Question 6. It features a sidebar on the left and a main content area with questions and a terminal window on the right. The terminal shows a SQLite dump with the same structure as Question 5, including the 'hidden_table' with the flag and the 'users' table with the admin password. A message 'The database has been updated while you were away!' is visible in the terminal. The status bar at the bottom shows 'THM AttackBox' and '33m 17s'.

Thought process/methodology:

We browsed to the copy of the website and managed to access santa's secret login panel using try and error method. We tried inserting a few names after the ip address and found out that the name for santa's secret login panel is santapanel. After that, we used burpsuite to intersect request from the webpage and save the request to our local machine. We then use sqlmap in the terminal to get the data in the gift list database. Sql commands that we used includes “--tamper=space2comment” to bypass the firewall, “--dump-all” to show the entire database and “--dbms” to specify the type of database that is running. We successfully obtain the gift list, THM flag and admin's password.