

# PSP0201

## Week 2

# Writeup

GROUP NAME:GLHF

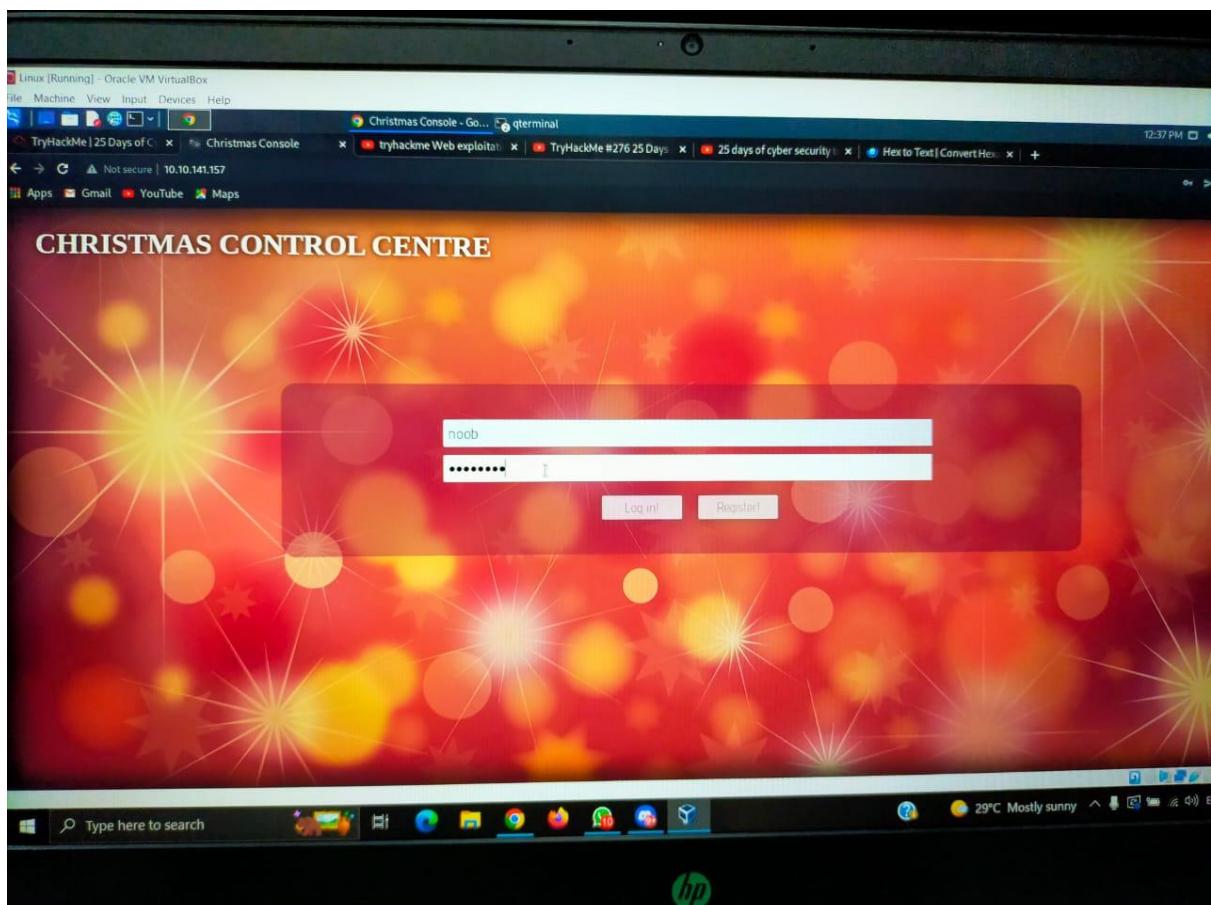
ID	NAME	ROLE
1211103400	Rohit	Leader
1211103299	Shuuban	Member
1211101214	Muhammad Syafiq Bin Ahmad Ghazali	Member

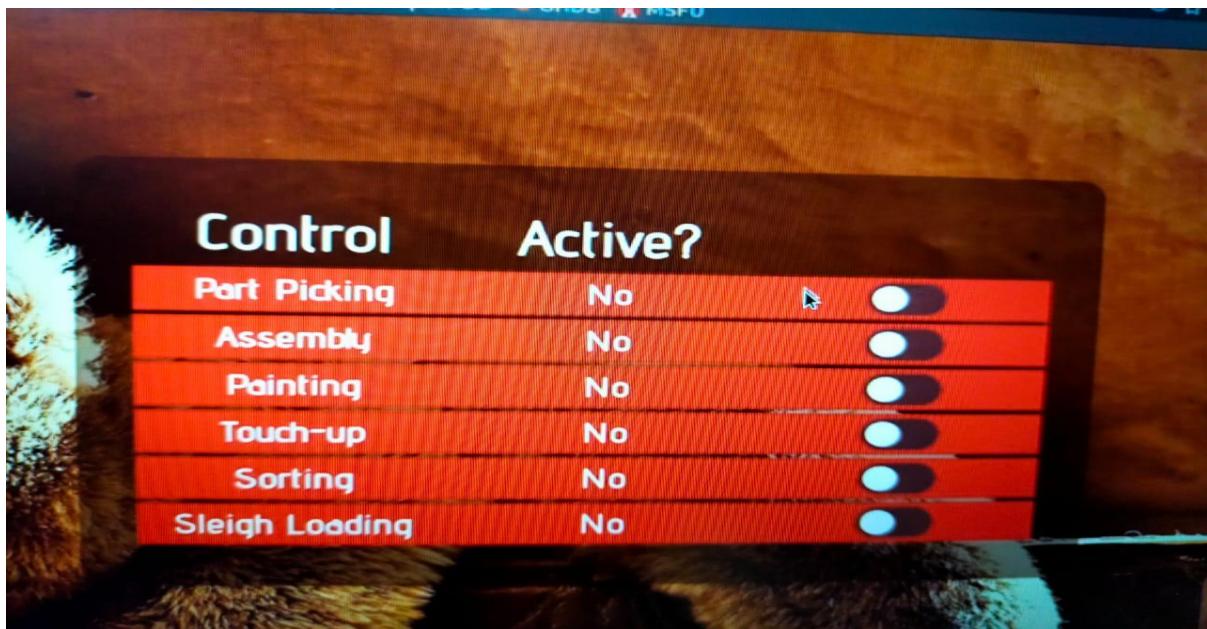
## Day 1: Web Exploitation – A Christmas Crisis

**Tools used:** Kali Linux, Chrome / Attackbox

Question 1

Register and login page.No access





Inspect Element/Applications/Cookie to get the cookies

The screenshot shows the developer tools open in a browser window. The title bar says "Christmas Console" and the address bar shows "10.10.240.168". The main content area displays a "VIEW CONSOLE" page with a large teddy bear image. On the right, there's a "Control Active?" section with the same list of tasks as the first image. Below this, the developer tools Storage tab is selected, showing a table of cookies. One cookie is selected: "auth" with the value "7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2274696d6f746879227d". The table includes columns for Name, Value, Domain, Path, Expires / Max-Age, Size, HttpOnly, Secure, SameSite, and Last Accessed.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
auth	7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2274696d6f746879227d	10.10.240.168	/		126	false	None	Wed, 08 Jun 2022 0...	

## Question 2

### Obtaining the cookies

Value	7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2274696d6f746879227d
-------	--

## Question 3

Used a random hex converter to convert hex to text.(note: I was unable to open cyberchef.)

## Hex to Text Converter

Converts from **Hexadecimal** to Text

### Hex String

```
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022  
757365726e616d65223a226e6f6f6222
```

**Convert**

### Result

```
{"company": "The Best Festival Company", "username": "noob"
```

## Question 4

Changed the username to 'santa' to obtain the cookies.

## Text to Hex Converter

Convert between **Text** and **Hex** quickly using this tool

### Text to Hex Converter

Converts from Text to **Hexadecimal**

#### Input Text

```
{"company": "The Best Festival Company", "username": "santa"
```

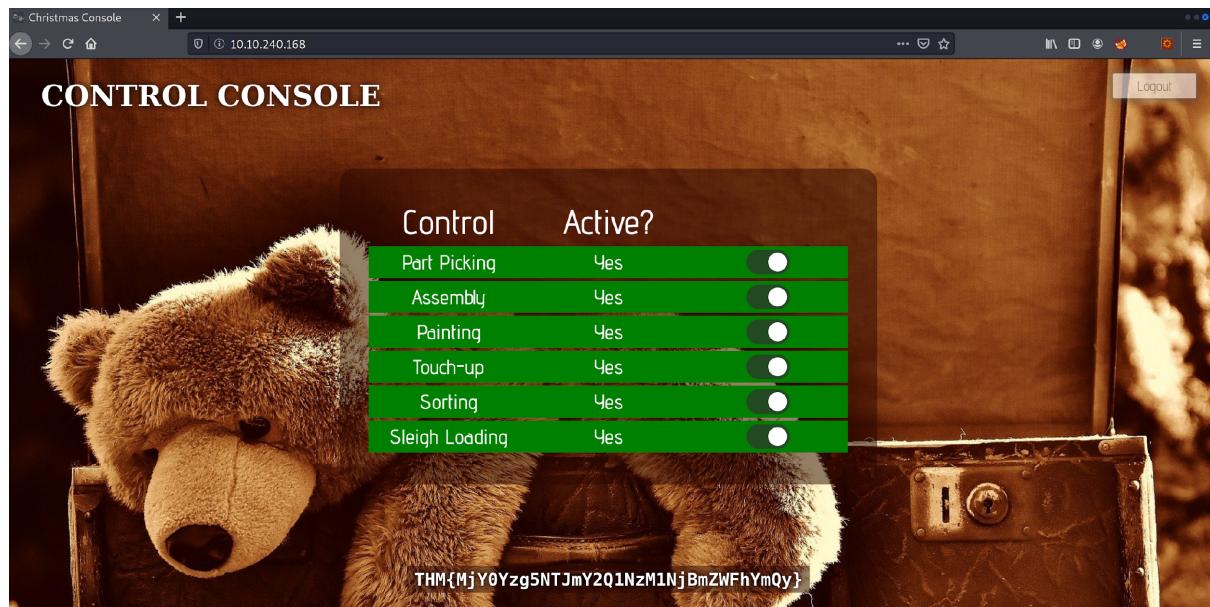
**Convert**

#### Hex output

```
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022  
757365726e616d65223a2273616e746122
```

## Question 5

Access available and controls can be used



Thoughts:

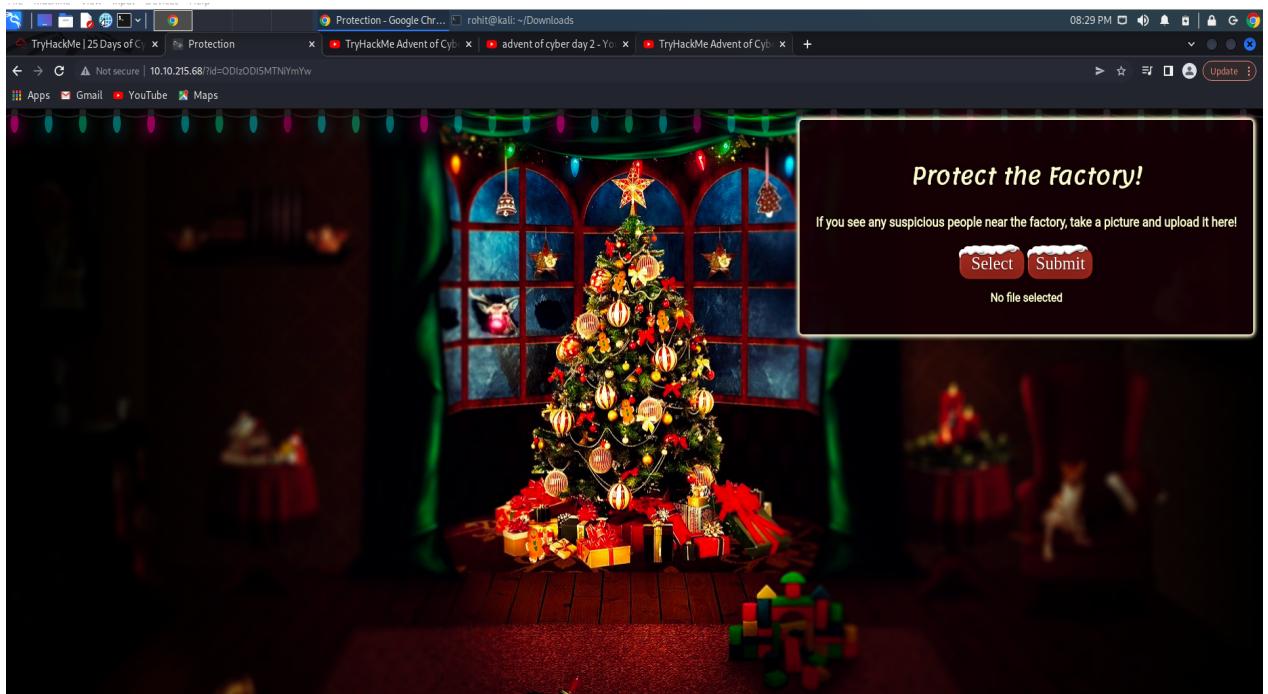
Once the machine is accessed, We saw a login page and we registered an account. After that we accessed the developer tools by clicking on the inspect element and then applications and the cookies tab. then we took the cookie value and converted it to a json text and changed the json text's username to 'santa' and converted it back to hex. once we pasted the new cookie value we managed to gain access to the admin page.

## DAY 2 - The elf strikes back

Tools used: Linux

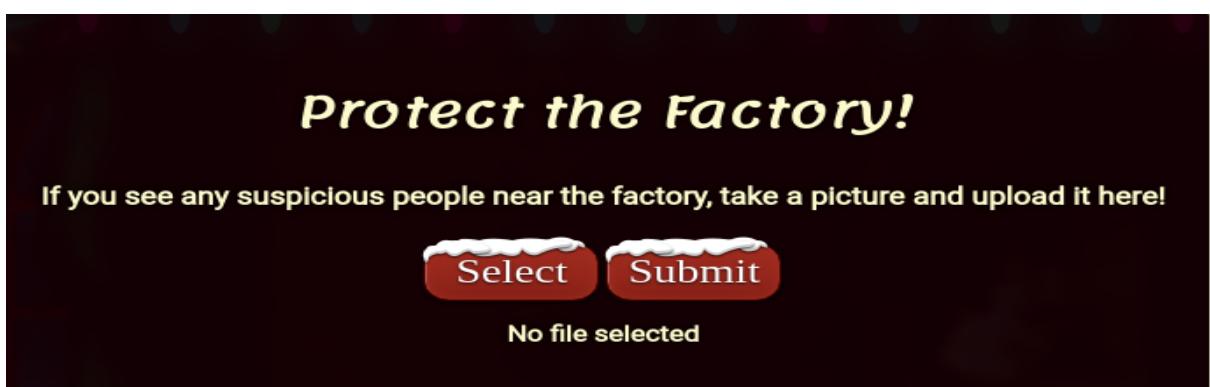
Question 1

Getting to the id page using the id given

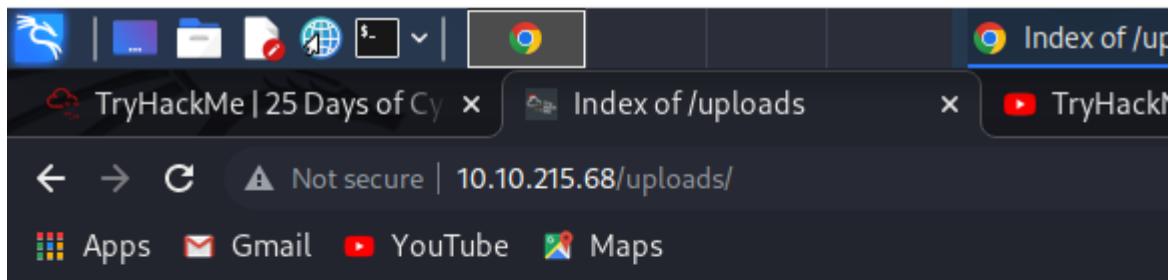


## Question 2

It only accepts an image as stated



### Question 3



## Index of /uploads

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">hacked.jpeg.php</a>	2022-06-18 08:32	5.4K	
<a href="#">hacking.jpeg.php</a>	2022-06-18 08:32	5.4K	

### Question 5

Getting the flag

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

Thoughts:

We went to the machine, entered the given id on the taskbar, and used php to alter the script by changing the ip and port number to reverse shell and then changed the php file to a jpg file and uploaded it to the upload page and we managed to crack it down.

## Day 3 Christmas Chaos

Tools used: Linux

Question 1

What's even worse is that these devices are often exposed to the internet, potentially allowing anyone to access and control botnet (a number of internet-connected devices controlled by an attacker to typically perform DDoS attacks) called Mirai too

Question 2

Participants	
State	● Resolved ()
Reported to	<a href="#">Starbucks</a> Managed
<hr/>	
Disclosed	March 1, 2017 7:51am +0800
Severity	
Weakness	Improper Authentication - Generic
Bounty	\$250
<hr/>	
CVE ID	None
Account de...	None

Question 3



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

## Question 4

Proxy is 8080

Info	Suite	This version of Burp Suite was released over three months ago. Please consider updating to benefit from enhance...
Info	Proxy	Proxy service started on 127.0.0.1:8080

## Question 6

Using decoder in burpsuite

The screenshot shows two separate decoders in Burp Suite. The top decoder has the input 'PSR0201' and the bottom one has the input '%50%53%50%30%32%30%31'. Both decoders are set to 'Text' mode and have a 'Smart decode' button at the bottom.

## Question 7

Cluster Bomb

Target      Positions      **Payloads**      Resource Pool      Options

② **Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defin

Payload set:  Payload count: 3  
Payload type:  Request count: 0

② **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

Add

Add from list ... [Pro version only]

The screenshot shows the 'Payload Options [Simple list]' section of the Cluster Bomb tool. It displays a list of payloads: 'root', 'password', and '12345'. The 'password' entry is highlighted. To the left of the list are buttons for 'Paste', 'Load ...', 'Remove', 'Clear', and 'Deduplicate'. Below the list is an 'Add' button and a dropdown menu with the option 'Add from list ... [Pro version only]'. A red arrow points from the 'password' entry in the list to the 'Add' button.

### Question 8



Thoughts:

We accessed the machine and turned on the foxy proxy and turned the intercept on. We entered a random username and password and we got it in burpsuite. We forwarded it to the intruder and repeater. We then went to the intruder tab and selected cluster bomb and we went to the payloads and entered the given options of usernames and passwords. Once we started the attack we got the username and password.

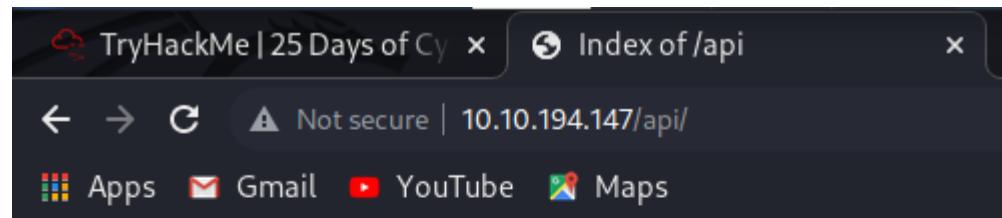
## Day 4- Santa's Watching

Tools used: linux

### Question 1

```
(rohit㉿kali)-[~]          advent of cyber day 4
$ wfuzz -c -z file,/opt/AoC-2020/Day-4/wordlist -u http://shibes.xyz/api/breed=FUZZ
```

### Question 2

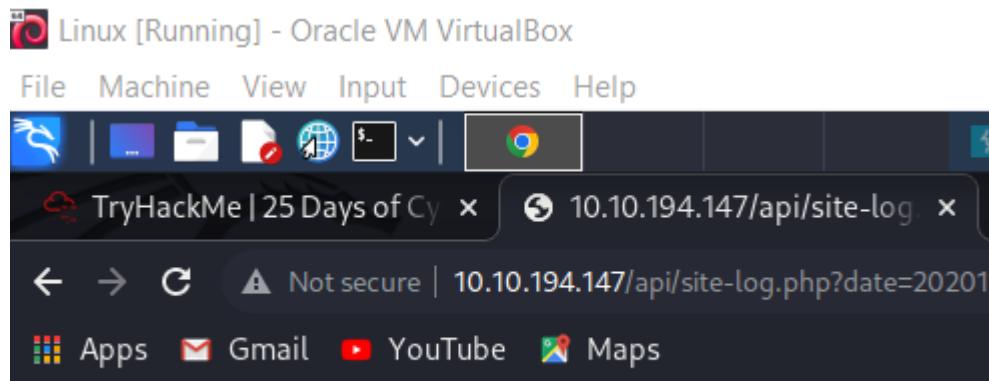


## Index of /api

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">site-log.php</a>	2020-11-22 06:38	110	

Apache/2.4.29 (Ubuntu) Server at 10.10.194.147 Port 80

### Question 3



THM{D4t3\_AP1}

### Question 4

A screenshot of a terminal window titled "aps" showing a session dump. The session details are as follows:

Title	IP Address	Expires
Day 4	10.10.194.147	1h 32m 07s

The session dump itself contains several command-line options and their descriptions:

- c : Output with colors
- v : Verbose information.
- f filename,printer : Store results in the output file using the specified printer (raw printer if omitted).
- o printer : Show results using the specified printer.
- interact : (beta) If selected, all key presses are captured. This allows you to int

Thoughts:

We accessed the machine. And then we used gobuster to find the api page directory.once we have found the api directory, we used wfuzz to get the value.

## **Day 5- Someone Stole Santa's Gift List**

Tools used: linux

Question 1

A screenshot of a search result from a search engine. The search term 'TCP 1433' is visible at the top. Below it, a snippet of Microsoft documentation for SQL Server configuration is shown, specifically regarding typical ports used by SQL Server. The text reads: 'By default, the typical ports used by SQL Server and associated database engine services are: **TCP 1433, 4022, 135, 1434, UDP 1434.** 11 Mar 2022'. Below the snippet is a link to 'Configure Windows Firewall - SQL Server | Microsoft Docs'.

Question 2

A screenshot of a 'Question Hint' modal window. It features a light blue header bar with the text 'Question Hint' and a close button ('X'). The main content area contains the text: 'The name is derived out of 2 words from this question.' followed by a code snippet: '/s\*\*tap\*\*\*|'. The background of the modal is white.

A screenshot of a web browser showing a login page. The address bar shows 'Not secure | 10.10.176.182:8000/santapanel'. Below the address bar are links for 'YouTube' and 'Maps'. The main content area has a dark header with the text 'Greetings stranger...'. Below the header is a message: 'Do not attempt to login if you are not a member of Santa's corporation!'. A large rectangular form follows, containing three input fields: 'Username' (with an empty input field), 'Password' (with an empty input field), and a 'Login' button. The entire page has a light gray background.

Question 3

#### Question 4

There's a total of 22 entries

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

#### Question 5

James' age is 8

James | 8 | shoes

#### Question 6

Github Ownership

Paul | 9 | github ownership

#### Question 7

thmfox{All\_I\_Want\_for\_Christmas\_Is\_You}

Question 8

EhCNSWzzFP6sc7gB

Thoughts:

We accessed the machine, and guessed santa's admin page which is santapanel,bypassed the login page.And once we've entered the page we used burpsuite to intercept and did a sql injection to get all the information.