

# PSP0201

## Week 2

# Writeup

Group Name: Hacktocrats

Members

ID	Name	Role
12111 03194	NUR FARAHIYA AIDA BINTI ABD RAZAK	Leader
12111 03602	NUR ALIA AMELISA SYAZREEN BINTI MOHD SULEI	Member
12111 03430	AINA SOFEA BINTI AMIER HAMZAH	Member
12111 03237	NURUL AIN BINTI KAMARUDIN	Member

## Day 1: Web Exploitation – A Christmas Crisis

**Tools used:** Kali Linux, Firefox

**Solution/walkthrough:**

**Question 1: Registration and logging to the Christmas Control Centre**

The screenshot shows a Firefox browser window with multiple tabs open. The active tab is titled 'Christmas Console - Mozilla Firefox' and displays the 'CHRISTMAS CONTROL CENTRE' login page. The page has a red background with a starburst pattern. It contains two input fields: one for 'Name' with 'ainasofea' typed in, and another for 'Password' with masked input. Below the fields are 'Log in!' and 'Register!' buttons. To the left of the main content, there is a sidebar with developer tools open, specifically the Storage tab which shows a table of cookies. The table includes columns for Name, Value, and Domain, with one entry for 'murlandoracle.co.uk'. The status bar at the bottom right of the browser indicates '52m 53s'.

The screenshot shows a Firefox browser window with multiple tabs open. The active tab is titled 'Christmas Console - Mozilla Firefox' and displays the 'VIEW CONSOLE' interface. The page features a large teddy bear image and a table titled 'Control Active?'. The table lists several tasks: Part Picking (No), Assembly (No), Painting (No), Touch-up (No), Sorting (No), and Sleigh Loading (No). The status bar at the bottom right of the browser indicates '52m 42s'.

## Question 2:

Open the browser tools to get the value and the name of the cookie

The screenshot shows a browser window with the URL [tryhackme.com/room/learnyberin25days](http://tryhackme.com/room/learnyberin25days). The page content discusses cookies and their storage on the user's computer. On the right, a Firefox developer tools panel is open, specifically the Storage tab under the Application tab. It shows a table of cookies for the domain <http://10.10.111.94>. One cookie is listed:

Name	Value	Domain
auth	7b22636f6d70616e79223a2254686520426573742046	10.10.111.94 /

## Question 3:

Change the value of the cookie to string by using cyberchef

The screenshot shows a Firefox browser window with the same TryHackMe page. The developer tools Storage tab is again visible, showing the 'auth' cookie. To the right, the CyberChef interface is open. The 'Operations' sidebar shows 'From Hex' selected. The 'Input' field contains the hex value of the cookie: `7b22636f6d70616e79223a2254686520426573742046 657374697616c20436f6d70616e79222c2622757365 726e616d65223a2261696e61736f666561227d`. The 'Output' section shows the decoded JSON string: `{"company": "The Best Festival Company", "username": "ainasofea"}`.

## Question 4:

Changing the username to santa at the JSON files and returning to the value hexadecimal.

The left side shows the TryHackMe room interface for challenge 4. It contains several questions and their answers:

- What is the name of the cookie used for authentication? auth (Correct Answer)
- In what format is the value of this cookie encoded? Hexadecimal (Correct Answer)
- Having decoded the cookie, what format is the data stored in? JSON (Correct Answer)
- Figure out how to bypass the authentication. What is the value of Santa's cookie? 7b22636f6d70616e79223a2254686520426573742046657 (Correct Answer)
- Now that you are the santa user, you can re-activate the assembly line! What is the flag you're given when the line is fully active? THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWfhYmQy} (Correct Answer)

The right side shows the CyberChef interface with the following configuration:

- Operations: Recipe
- From Hex: Delimiter Auto
- To Hex: Delimiter None, Byte 0
- Input: {"company": "The Best Festival Company", "username": "santa"}  
Output: 7b22636f6d70616e79223a2254686520426573742046657  
057374697616c20436f6d70616e79222c2622757365  
7/6e616d65223a73610e74612274

## Question 5:

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

The left side shows the TryHackMe room interface for challenge 5. It contains several questions and their answers:

- In what format is the value of this cookie encoded? hexadecimal (Correct Answer)
- Having decoded the cookie, what format is the data stored in? JSON (Correct Answer)
- Figure out how to bypass the authentication. What is the value of Santa's cookie? 7b22636f6d70616e79223a2254686520426573 (Correct Answer)
- Now that you are the santa user, you can re-activate the assembly line! What is the flag you're given when the line is fully active? (Answer format: \*\*\*\*\*) (Submit)

The right side shows the Control Console interface with the following configuration:

- Control Active?
- Part Picking: Yes (switched on)
- Assembly: Yes (switched on)
- Painting: Yes (switched on)
- Touch-up: Yes (switched on)
- Sorting: Yes (switched on)

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

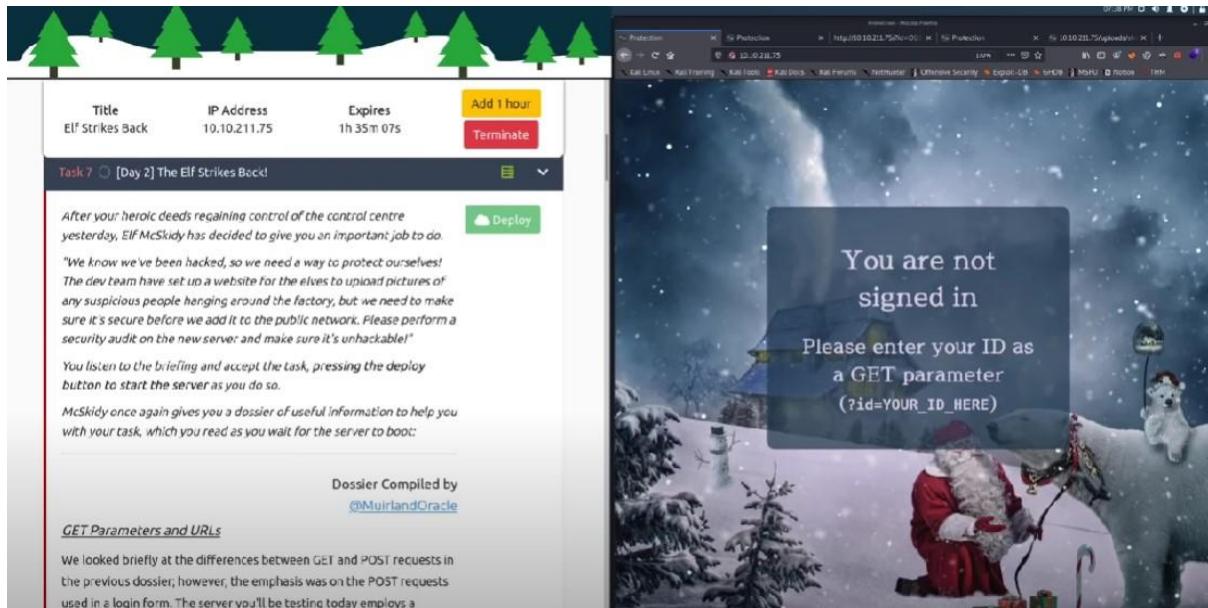
After we gained access to the target system, we were presented with a login/registration screen. We then created an account and logged in. After logging in, we opened the browser's developer tool and selected the Storage tab to examine the site cookie. We concluded from the cookie data that it was a hexadecimal number and used Cyberchef to convert it to text. We discovered a JSON statement containing the username element. We used Cyberchef to change the username to 'santa,' the administrator account, and then converted it back to hexadecimal. We updated the page after replacing the cookie value with the transformed one. We are now presented with an administrator page (Santa's) and proceeded to enable each control, which displayed the flag.

## Day 2: Web Exploitation - The Elf Strikes Back!

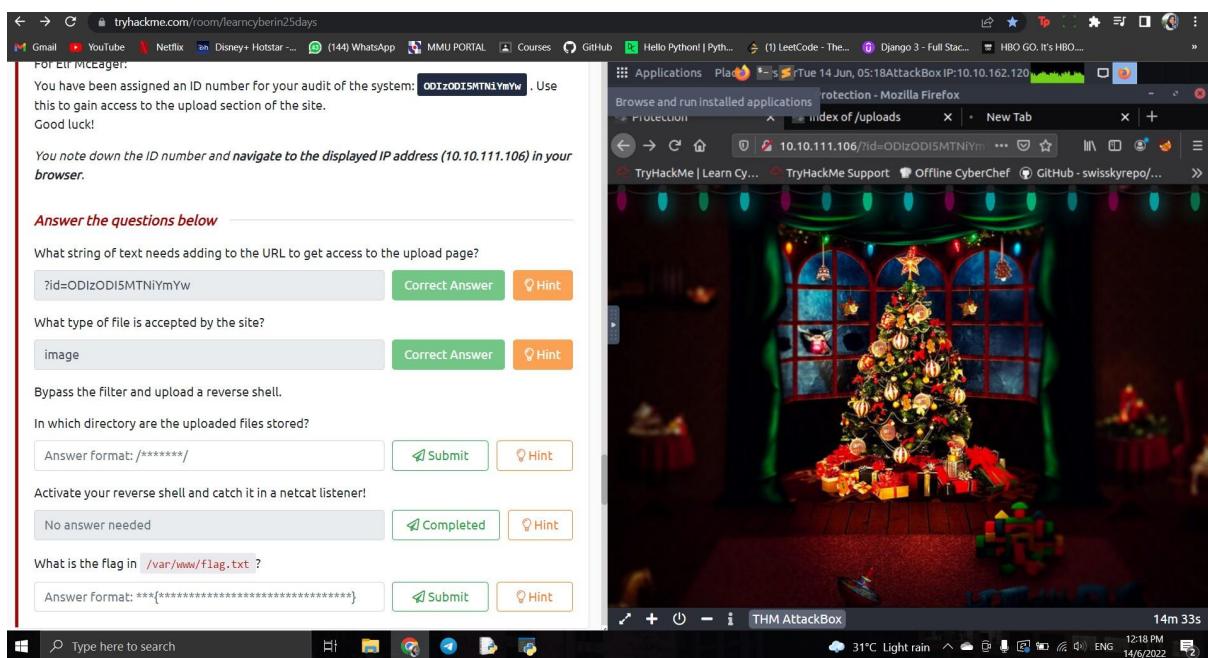
Tools used : Kali Linux & Firefox

Solution / Walkthrough :

Question 1: the string of text that needed the url to be added to get the access to the upload page is detected.



Question 2: filter has been bypassed and reverse shell has been uploaded. Files have been uploaded in /uploads/ directory.



## Question 3: Image is the type of file that has been accepted by the site

interested.

**Putting it all together**

This was a *lot* of information, so let's put it all together and look at the full process for exploiting a file upload vulnerability in a PHP web application:

1. Find a file upload point.
2. Try uploading some innocent files -- what does it accept? (Images, text files, PDFs, etc)
3. Find the directory containing your uploads.
4. Try to bypass any filters and upload a reverse shell.
5. Start a netcat listener to receive the shell
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: **ODIZODISHTNLYmW**.  
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 (10.113.60) in your browser**.

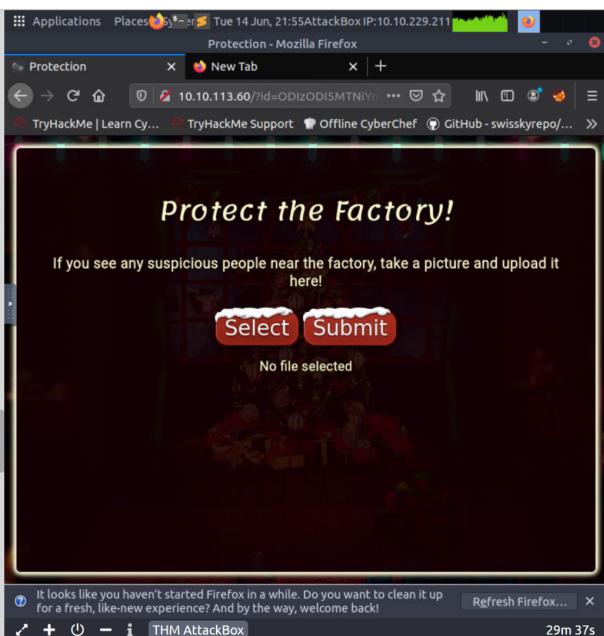
**Answer the questions below**

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

Answer format: \*\*\*\*\*

What type of file is accepted by the site?

Answer format: \*\*\*\*



## Question 4: The flag of /var/www/flag.txt is provided below the control console



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

After login, our ip address has been filled in the firefox. Then a file upload address has been located. We tried to upload a few unimpeachable files to figure out what it approves and what it does not. For example, files such as images, text files, PDFs, etc. Then we searched up the directory containing our uploads. After all of that has been done, we tried to bypass any filters in order to upload a reverse shell. After that, we started a netcat listener so that we could receive the shell. Last but not least, the shell in our browser has been navigated and the connection has been received!

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

**Tools used:** Firefox, BurpSuite, FoxyProxy, Google

**solutions/ walkthrough:**

**Question 1:**

The name of the botnet that is mentioned in the text is Mirai botnet.

### **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.

**Question 2:**

Starbucks paid \$250 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.

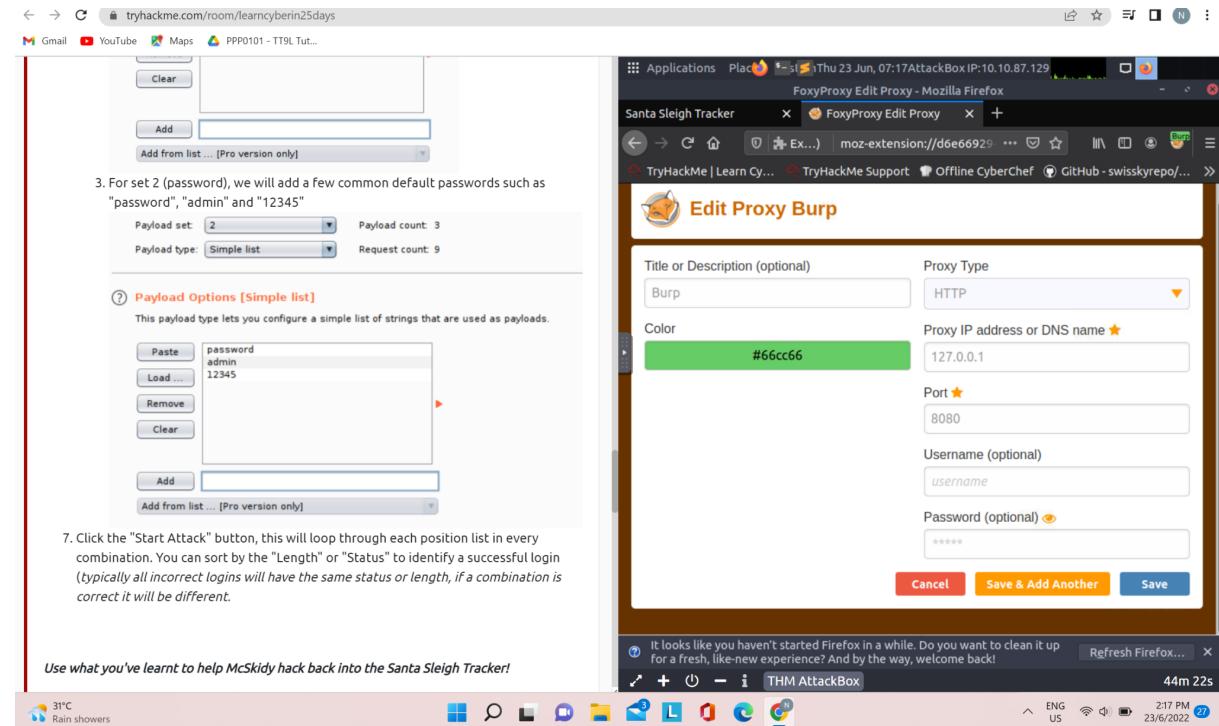
**Question 3:**

The agent assigned from the Dept of Defense that disclosed the report on Jun 25th is ag3nt-j1.

arm4nd0 posted a comment.	May 11th (2 years ago)
agent2 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)
ag3nt-j1 U.S. Dept Of Defense staff agreed to disclose this report.	Jun 25th (2 years ago)

## Question 4:

We can look for the port number on Burp by clicking the options on Burp and select edit Proxy Burp. The port number is 8080.



## Question 5:

The proxy type can be found in the same section as the port number. The proxy type is HTTP.

tryhackme.com/room/learncyberin25days

Gmail YouTube Maps PPP0101 - TT9L T...

Clear

Add

Add from list... [Pro version only]

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

Payload set: 2 Payload count: 3  
Payload type: Simple list Request count: 9

⑦ Payload Options [Simple list]  
This payload type lets you configure a simple list of strings that are used as payloads.

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

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

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

31°C Rain showers

Applications Places FoxyProxy Edit Proxy - Mozilla Firefox

Santa Sleigh Tracker x FoxyProxy Edit Proxy x +

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo...

Edit Proxy Burp

Title or Description (optional) Proxy Type  
Burp HTTP

Color Proxy IP address or DNS name ★  
#66cc66 127.0.0.1

Port ★  
8080

Username (optional)  
username

Password (optional)  
\*\*\*\*\*

Cancel Save & Add Another Save

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!

Refresh Firefox... THM AttackBox 44m 22s

ENG US 2:17 PM 23/6/2022

## Question 6:

In BurpSuite, select the decoder tab. Insert the word “PSP0201” and encode the text as URL. The value obtained is the one we are looking for which is %50%53%50%30%32%30%31.

tryhackme.com/room/learncyberin25days

Gmail YouTube Maps PPP0101 - TT9L T...

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

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

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

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

Answer the questions below

Deploy your AttackBox (the blue "Start AttackBox" button) and the tasks machine (green button on this task) if you haven't already. Once both have deployed, open Firefox on the AttackBox and copy/paste the machines IP (10.10.148.11) into the browser search bar.

No answer needed Question Done

Use BurpSuite to brute force the login form. Use the following lists for the default credentials:

Username Password  
root root

Applications Places FoxyProxy About - Mozilla Firefox

Santa Sleigh Tracker x FoxyProxy About x +

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef

Burp Suite Community Edition v2022.2.4 - Temporary Project

Burp Project Intruder Repeater Window Help

Decoder Comparer Target Logger Extender Intruder Repeater Sequencer User options Learn

PSP0201

Text Hex  
Decode as...  
Encode as...  
Hash...  
Smart decode

00000000 50 53 50 30 32 30 31 ... PSP0201

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

Text Hex  
Decode as...  
Encode as...  
Hash...  
Smart decode

THM AttackBox 10m 30s

ENG US 2:25 PM 24/6/2022

## Question 7:

In the attack type section from the intruder tab, the one that matches the description in the google form which is “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” is Cluster Bomb.

The screenshot shows a browser window with several tabs open. The tabs include "Task 4 [Day 2] Web Exploitation The Elf Strikes Back!", "Task 5 [Day 3] Web Exploitation Christmas Chaos", and "tryhackme.com/room/learnbyern25days". The main content area displays a challenge for "Task 5" where McSkidy is walking down a corridor and hears a faint bleeping noise. He gets closer to the Sleigh Engineering Room and finds something wrong. He runs to the room, slams the door open, and sees Santa's sleigh's control panel. He finds red error messages about a hacked code. He needs to help McSkidy hack into Santa's sleigh to regain control. Below this, there is a link to "Watch DarkStar's video on solving this task!"

Learning Objectives

- Understanding Authentication
- Understand the use of default credentials and why they're dangerous
- Bypass a login form using BurpSuite

Authentication

Authentication is a process of verifying a users' identity, normally by credentials (such as a username, user id or password); to put simply, authentication involves checking that somebody really is who they claim to be. Authorization (which is fundamentally different to authentication, but often used interchangeably) determines what a user can and can't access; authorization is covered in tomorrow walkthrough, today's task focuses on authentication and some common flaws.

The Burp Suite interface is shown in the background. It has tabs for Applications, Project, Intruder, Repeater, Window, Help, Decoder, Comparer, Logger, Extender, Project options, User options, Learn, and Sequencer. The "Intruder" tab is selected. Under "Intruder", there are tabs for Positions, Payloads, Resource Pool, and Options. The "Payloads" tab is selected. A dropdown menu for "Attack type" shows "Sniper" and "Cluster bomb". A tooltip for "Cluster bomb" describes it as "This attack uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through all payload sets simultaneously, so it uses the first payload from each set, then the second payload from each set, and so on." Other attack types listed include "Battering ram", "Pitchfork", "Pragel", and "Connel".

## Question 8:

To obtain the flag, go to BurpSuite and enter the port number 8080 and change the specific address to 127.0.0.1. We need to ensure the intercept is on, turn on 'Burp' on FoxyProxy and now we can see that BurpSuite has held our request. Go to Santa's portal and login using any random username and password. This captured request will be shown in the proxy tab. Right click and choose 'send to intruder'. In the intruder tab, we can now see our request. Select “Cluster Bomb” in the Attack type dropdown menu. As we want to tell each “Position” which payload to use, we will choose a list of usernames and passwords to be used. In this case, for Payload 1 which is the username, we

use: “admin”, “root”, “user”. For Payload 2 which is the password, we use: “password”, “admin”, and “12345”.

The screenshot shows a dual-monitor setup. The left monitor displays a web browser window for 'try.hackme.com/room/learncyberin25days'. The page title is '25 Days of Cyber Security' with a sub-header 'Get started with Cyber Security in 25 Days - Learn the basics by doing a new, beginner friendly security challenge every day.' Below this is a 'Active Machine Information' section with fields for Title (AoC Day 3), IP Address (10.10.148.11), and Expires (16m 42s). It includes buttons for 'Add 1 hour', 'Terminate', and a progress bar at 29%. A sidebar lists six tasks: Task 1 (Introduction), Task 2 (Get Connected), Task 3 ([Day 1] Web Exploitation: A Christmas Crisis), Task 4 ([Day 2] Web Exploitation: The Elf Strikes Back!), Task 5 ([Day 3] Web Exploitation: Christmas Chaos), and Task 6 ([Day 4] Web Exploitation: Santa's watching). The right monitor shows a Kali Linux desktop environment with a terminal window open. The terminal title is 'root's Home' and it contains the command 'id'. The desktop background is a dark theme with various icons. A status bar at the bottom shows network information, battery level (209 PM), and system date (24/6/2022).

Click the “Start Attack” button to loop through each position list in every combination. We can sort the “Length” and “Status” to look for a successful login. In our case, we identified that the correct username and password would be “admin” and “12345”.

The screenshot shows a dual-monitor setup. The left monitor displays the '25 Days of Cyber Security' challenge interface, showing tasks 1 through 6. Task 1 is completed ('Introduction'), Task 2 is in progress ('Get Connected'), Task 3 is in progress ('[Day 1] Web Exploitation A Christmas Crisis'), Task 4 is in progress ('[Day 2] Web Exploitation The Elf Strikes Back!'), Task 5 is in progress ('[Day 3] Web Exploitation Christmas Chaos'), and Task 6 is in progress ('[Day 4] Web Exploitation Santa's watching'). The right monitor shows the 'Santa Sleigh Tracker - Mozilla Firefox' window in THM AttackBox. It lists several login attempts with the following details:

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

The right monitor also shows the 'Santa Sleigh Tracker App' interface with a world map and the flag: THM{885ffab980e049847516f9d8fe99ad1a}

Direct back to Santa's Portal and enter the correct username and password.  
The flag is now shown on the screen!!

The screenshot shows a dual-monitor setup. The left monitor displays the '25 Days of Cyber Security' challenge interface, showing tasks 1 through 6. Task 1 is completed ('Introduction'), Task 2 is in progress ('Get Connected'), Task 3 is in progress ('[Day 1] Web Exploitation A Christmas Crisis'), Task 4 is in progress ('[Day 2] Web Exploitation The Elf Strikes Back!'), Task 5 is in progress ('[Day 3] Web Exploitation Christmas Chaos'), and Task 6 is in progress ('[Day 4] Web Exploitation Santa's watching'). The right monitor shows the 'Santa Sleigh Tracker - Mozilla Firefox' window in THM AttackBox. It displays the 'Santa Sleigh Tracker App' interface with a world map and the flag: THM{885ffab980e049847516f9d8fe99ad1a}

## Thought Process/Methodology:

The aim of this session is to look for the correct username and password to log in in Santa's Portal to gain access back to the system. In this case, we will use BurpSuite to perform a dictionary attack on a web login form to look for the information needed. Once BurpSuite is loaded, we can intercept the traffic by proxying it through BurpSuite. We can achieve this by using FoxyProxy on Firefox. After intercepting the traffic, BurpSuite now holds our request. This captured request will be shown in the Proxy tab. Send it to the intruder using the right click. On the intruder tab, we can now see our request. Select "cluster bomb" in the attack type. In the payloads we fill in the usernames and passwords as recommended in THM. Click the "start attack" button. We can sort by the "Length" or "Status" to identify a successful login. Enter the correct username and password to Santa's portal to obtain flag.

#### **Day 4: Web Exploitation - Santa's watching**

**Tools used:** Attackbox, mozilla firefox, terminal

**Solution/walkthrough:**

##### **Question 1:**

Open the IP addresses given in the firefox.

Then find the accurate parameter and command.

Common wfuzz dash c to get the colour output, dash z to select that we are going to use a file. Then we want the big.txt and we put the url which is '<https://shibes.xyz/api.php>' and breed for FUZZ at the end.

With all that in mind, we should be able to get a flag.

## Recommended Rooms:

[TryHackMe | ZTH: Web 2](#)

[TryHackMe | CC: Pen Testing](#)

**Answer the questions below**

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 (10.10.68.29) into the browser search bar.

No answer needed      Question Done

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)

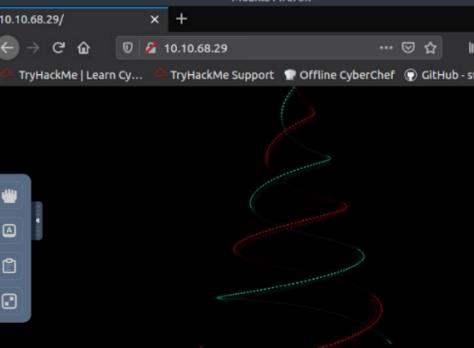
**Note:** For legal reasons, do *not* actually run this command as the site in question has not consented to being fuzzed!

wfuzz -c -z file.big.txt http://shibes.xyz/api.php?breed=FU;      Correct Answer      Hint

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

site-log.php      Correct Answer      Hint

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



**You h4v3 b33n d3f4c3d y0ur f0rums ar3 g0ne**

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!

Refresh Firefox...      52m 13s

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 (10.10.68.29) into the browser search bar.

No answer needed      Question Done

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!

wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FU;      Correct Answer      Hint

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

site-log.php      Correct Answer      Hint

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]      Correct Answer      Hint

Task 7 [Day 5] Web Exploitation Someone stole Santa's gift list! More

Task 8 [Day 6] Web Exploitation Be careful with what you wish on a Christmas night More

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!

Refresh Firefox... X

36m 36s

## Question 2:

We enter the IP addresses and navigate with the api directory and find the file site-log.php

The screenshot shows a split-screen view. On the left, a challenge page from [tryhackme.com/room/learncyberin25days](https://tryhackme.com/room/learncyberin25days) displays a task about wfuzzing a URL. On the right, a Mozilla Firefox window shows the file listing at <http://10.10.68.29/api/>, which includes a file named "site-log.php" last modified on 2020-11-22 at 06:38. The status bar at the bottom indicates "Apache/2.4.29 (Ubuntu) Server at 10.10.68.29 Port 80".

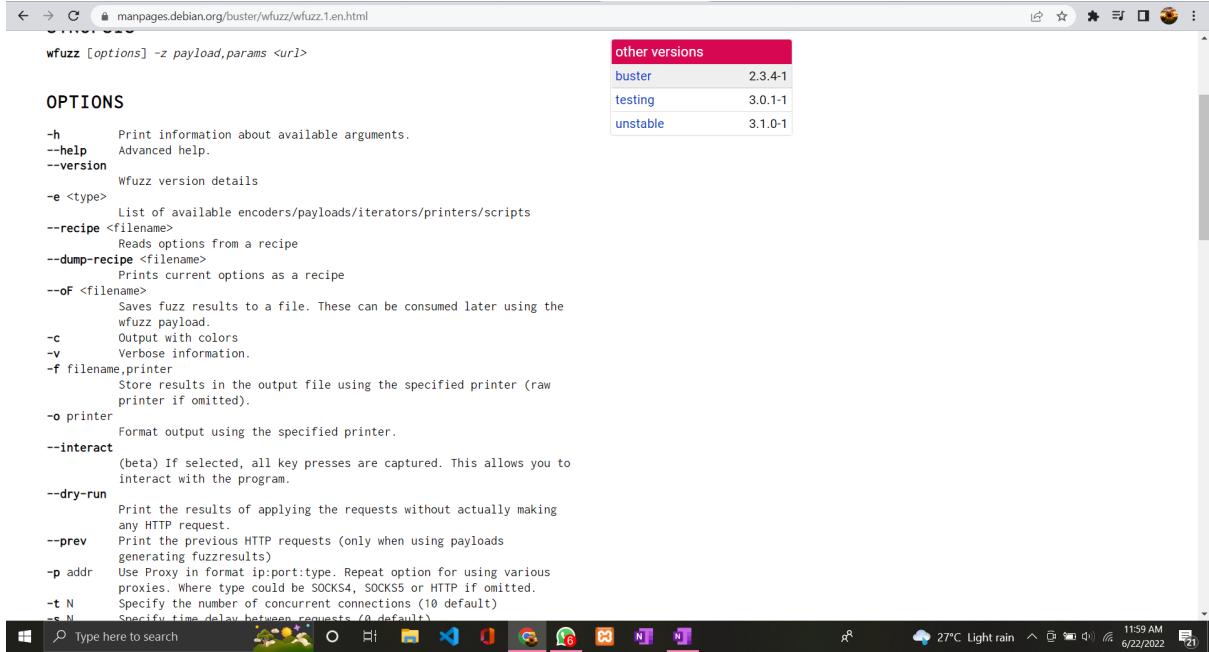
### Question 3:

Search the IP address, the file and the date of the file using the command  
date=YYYYMMDD.

The screenshot shows a split-screen view. On the left, a challenge page from [tryhackme.com/room/learncyberin25days](https://tryhackme.com/room/learncyberin25days) displays a task about wfuzzing a URL. On the right, a Mozilla Firefox window shows the file listing at <http://10.10.68.29/api/>, which includes a file named "site-log.php" last modified on 2020-11-20 at 14:00. The status bar at the bottom indicates "Apache/2.4.29 (Ubuntu) Server at 10.10.68.29 Port 80".

## Question 4:

-f parameter store results to printer and filenames.



The screenshot shows a web browser displaying the manpage for wfuzz. The page lists various command-line options, including the `-f` option which is described as "Store results in the output file using the specified printer (raw printer if omitted)". To the right of the main text, there is a table titled "other versions" showing the version history for wfuzz across different Debian releases: buster (2.3.4-1), testing (3.0.1-1), and unstable (3.1.0-1).

other versions
buster 2.3.4-1
testing 3.0.1-1
unstable 3.1.0-1

## Thought process and methodology:

We have to understand the parameter in the WFUZZ and handle it in the terminal. In the terminal, we use the gobuster directory to discover the valuable directories if they exist. We use `-u` to specify which url to enumerate, `-w` as path to the wordlist and lastly, `-x` to specify file extension. We also use the API directory to navigate the files in the Mozilla Firefox's search. To find the flag, we navigate with the api directory and use the file name which is site-log.php and the date command. The date of the file we can see beside the file on the screen is 2020-11-22. With the date format, YYYYMMDD. Then, we get the secret flag.

## **Day 5: Web Exploitation - Someone stole Santa's Gift List**

**Tools used:** Kali linux, Firefox, Burp Suite, FoxyProxy

**Solution/walkthrough:**

### **Question 1**

Open microsoft documentation on firefox to obtain default port number for SQL server running on TCP

The security team have worked hard on reviving Santa's personal portal. Hence, 'Santa's forum 2' went live.

After the attack, logs have revealed that someone has found Santa's panel on the website and logged into his account! After doing so, they were able to dump the whole gift list database, getting all the 2020 gifts in their hands. An attacker has threatened to publish a wishlist.txt file, containing all information, but happily, for us, he was caught by the CBI (Christmas Bureau of Investigation) before that. On **MACHINE\_IP:8009** you'll find the copy of the website and your goal is to replicate the attacker's actions by dumping the gift list!

Task created by **Swafox**

**What is SQL Injection?**

A SQL injection (SQLi) attack consists of the injection of a SQL query to the remote web application. A successful SQL injection exploit can read sensitive data from the database (usernames & passwords), modify database data (Add/Delete), execute administration operations on the database (such as shutdown the database), and in some cases execute commands on the operating system.

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

Configure a Server to Listen on a Specific TCP Port

SQL Server 2022 Preview

Filter by title

- Configure a Server to Listen on a Specific TCP Port
- Configure a Server to Listen on an Alternate Pipe
- Enable Encrypted Connections to the Database Engine
- Connect to SQL Server Through a Proxy Server
- Configure a Windows Firewall for Database Engine Access
- Hide an Instance of SQL Server Database Engine
- Configure the Database Engine to Listen on Multiple TCP Ports
- How to enable the TCP protocol with SQLPS
- Determine Whether the Database Engine Is Installed & Started

Download PDF

## Question 2

Bypassing through santa's login panel by inserting username and comment the rest of the query

Week 2 Tutorial Progress | PSP0201 T2130 - Tutorial V | Hactocrats week 2 report - | day 5 - Hacktocrats - Google | TryHackMe | 25 Days of Cybersecurity | TryHackMe Advent of Cybersecurity | +

[tryhackme.com/room/learnbyciberin25days](https://tryhackme.com/room/learnbyciberin25days)

Github Telegram WhatsApp MMLS Canvas Student Sci-Hub Y Z-Library CaMSyS Rumah Terbuka IU ... TryHackMe | Dash...

you've forgotten the command, you can tell SQLmap to try and bypass the WAF by using  
--tamper=space2comment

## Resources

Check out this cheat sheet: [swisskyrepo/PayloadsAllTheThings](#)

Payload list: [payloadbox/sql-injection-payload-list](#)

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

### Answer the questions below

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

/santapanel Correct Answer Hint

Visit Santa's secret login panel and bypass the login using SQLi

No answer needed Question Done

How many entries are there in the gift database?

22 Correct Answer

What did Paul ask for?

GitHub Ownership Correct Answer

What is the flag?

thmfox{All\_I\_Want\_for\_Christmas\_Is\_You} Correct Answer Hint

What is admin's password?

admin' or 1=1 --

Sequel - Mozilla Firefox

Applications Places Sun 19 Jun, 04:33 AttackBox IP:10.48.72 Sequel - Mozilla Firefox

Sequel

10.10.27.37:8000/santapanel

Greetings stranger...

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

Username: admin' or 1=1 --

Password: admin'

Login

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!

Refresh Firefox... 54m 31s

### Question 3

## Obtaining database used in Santa's TODO list

The screenshot shows a browser window with multiple tabs open, including "Week 2", "PSP020", "Hactf", "tryHackme.com/room/learncyberin25days", "TryHackMe", "GitHub", "Telegram", "WhatsApp", "MMLS", "Canvas Student", "Sci-Hub", "Z-Library", and "CaMSys". The main content area displays a challenge titled "Challenge" from "tryHackme.com/room/learncyberin25days". The challenge text reads:

Visit the vulnerable application in Firefox, find Santa's secret login panel and bypass the login. Use some of the commands and tools covered throughout today's task to answer Questions #3 to #6.

Santa reads some documentation that he wrote when setting up the application, it reads:

Santa's TODO: Look at alternative database systems that are better than [sqlite](#). Also, don't forget that you installed a Web Application Firewall (WAF) after last year's attack. In case you've forgotten the command, you can tell SQLMap to try and bypass the WAF by using `--tamper=space2comment`

## Resources

Check out this cheat sheet: [swisskyrepo/PayloadsAllTheThings](#)

Payload list: [payloadbox/sql-injection-payload-list](#)

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

*Answer the questions below*

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

[/santapanel](#) [Correct Answer](#) [Hint](#)

The right side of the image shows a Kali Linux desktop environment with a terminal window open. The terminal window title is "kali@kali: ~" and the command entered is "zsh: corrupt history file /home/kali/.zsh\_history". The desktop background features a blue gradient with a faint white swan logo.

## Question 4

Insert burp suite saved request into SQL commands and successfully obtained the wishlist from the database.

We can then use this request in SQLMap:

```
sqlmap -r filename
```

SQLMap will automatically translate the request and exploit the database for you.

### Challenge

Visit the vulnerable application in Firefox, find Santa's secret login panel and bypass the login. Use some of the commands and tools covered throughout today's task to answer Questions #3 to #6.

Santa reads some documentation that he wrote when setting up the application, it reads:

Santa's TODO: Look at alternative database systems that are better than sqlite. Also, don't forget that you installed a Web Application Firewall (WAF) after last year's attack. In case you've forgotten the command, you can tell SQLMap to try and bypass the WAF by using

```
--tamper=space2comment
```

### Resources

Check out this cheat sheet: [swisskyrepo/PayloadsAllTheThings](#)

Payload list: [payloadbox/sql-injection-payload-list](#)

The database has been updated while you were away!

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!

Refresh Firefox... X

37m 46s

Get number of entries, Paul's christmas gift and James' age.

Check out this cheat sheet: [swisskyrepo/PayloadsAllTheThings](#)

Payload list: [payloadbox/sql-injection-payload-list](#)

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

**Answer the questions below**

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

Answer format: \*\*\*\*\*

Visit Santa's secret login panel and bypass the login using SQLi

No answer needed

How many entries are there in the gift database?

Answer format: \*\*

What did Paul ask for?

Answer format: \*\*\*\*\*

What is the flag?

Answer format: \*\*\*\*\*  
\*\*\*\*\*

What is admin's password?

Answer format: \*\*\*\*\*

The database has been updated while you were away!

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!

Refresh Firefox... X

34m 59s

Question 5

Scroll down to see THM flag

Check out this cheat sheet: [swisskyrepo/PayloadsAllTheThings](#)

Payload list: [payloadbox/sql-injection-payload-list](#)

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

**Answer the questions below**

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

Answer format: /\*\*\*\*\*  
Submit Hint

Visit Santa's secret login panel and bypass the login using SQLi

No answer needed  
Completed

How many entries are there in the gift database?

22  
Submit

What did Paul ask for?

github ownership  
Submit

What is the flag?

Answer format: \*\*\*\*\*  
Submit Hint

What is admin's password?

Answer format: \*\*\*\*\*  
Submit

Thu 16 Jun, 05:28 AttackBox IP:10.10.14.240

Santa's admin panel - Mozilla Firefox

root@ip-10-10-14-240:~

[05:26:51] [INFO] fetching columns for table 'hidden\_table' in database 'SQLite\_masterdb'

[05:26:51] [INFO] fetching entries for table 'hidden\_table' in database 'SQLite\_masterdb'

Database: SQLite\_masterdb

Table: hidden\_table

[1 entry]

+-----+  
| flag |  
+-----+  
| thmFox{ALL\_I\_Want\_For\_Christmas\_Is\_You} |  
+-----+

[05:26:51] [INFO] table 'SQLite\_masterdb.hidden\_table' dumped to CSV file '/root/.sqlmap/output/10.10.10.15/dump/SQLite\_masterdb/hidden\_table.csv'

[05:26:51] [INFO] fetching columns for table 'users' in database 'SQLite\_masterdb'

[05:26:51] [INFO] fetching entries for table 'users' in database 'SQLite\_masterdb'

Database: SQLite\_masterdb

Table: users

[1 entry]

+-----+  
| username | password |  
+-----+  
| admin | EhCNSWzzFP6sc7gB |  
+-----+

[05:26:51] [INFO] table 'SQLite\_masterdb.users' dumped to CSV file '/root/.sqlmap/output/10.10.10.15/dump/SQLite\_masterdb/users.csv'

[05:26:51] [WARNING] HTTP error codes detected during run:  
400 (Bad Request) - 1 times

[05:26:51] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.10.10.15'

[\*] shutting down at 05:26:51

The database has been updated while you were away!

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!

Refresh Firefox... X

THM AttackBox

34m 10s

## Question 6

Scroll down further to see admin's password

Check out this cheat sheet: [swisskyrepo/PayloadsAllTheThings](#)

Payload list: [payloadbox/sql-injection-payload-list](#)

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

**Answer the questions below**

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

Answer format: /\*\*\*\*\*  
Submit Hint

Visit Santa's secret login panel and bypass the login using SQLi

No answer needed  
Completed

How many entries are there in the gift database?

22  
Submit

What did Paul ask for?

github ownership  
Submit

What is the flag?

thmFox{All\_I\_Want\_for\_Christmas\_Is\_You}  
Submit Hint

What is admin's password?

Answer format: \*\*\*\*\*  
Submit

Thu 16 Jun, 05:29 AttackBox IP:10.10.14.240

Santa's admin panel - Mozilla Firefox

root@ip-10-10-14-240:~

[05:26:51] [INFO] table 'SQLite\_masterdb.hidden\_table' dumped to CSV file '/root/.sqlmap/output/10.10.10.15/dump/SQLite\_masterdb/hidden\_table.csv'

[05:26:51] [INFO] fetching columns for table 'users' in database 'SQLite\_masterdb'

[05:26:51] [INFO] fetching entries for table 'users' in database 'SQLite\_masterdb'

Database: SQLite\_masterdb

Table: users

[1 entry]

+-----+  
| username | password |  
+-----+  
| admin | EhCNSWzzFP6sc7gB |  
+-----+

[05:26:51] [INFO] table 'SQLite\_masterdb.users' dumped to CSV file '/root/.sqlmap/output/10.10.10.15/dump/SQLite\_masterdb/users.csv'

[05:26:51] [WARNING] HTTP error codes detected during run:  
400 (Bad Request) - 1 times

[05:26:51] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.10.10.15'

[\*] shutting down at 05:26:51

The database has been updated while you were away!

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!

Refresh Firefox... X

THM AttackBox

33m 17s

## Thought process/methodology:

We browsed to the copy of the website and managed to access santa's secret login panel using try and error method. We tried inserting a few names after the ip address and found out that the name for santa's secret login panel is santapanel. After that, we used BurpSuite to intercept request from the webpage and save the request to our local machine. We then use sqlmap in the terminal to get the data in the gift list database. Sql commands that we used includes “--tamper=space2comment” to bypass the firewall, “--dump-all” to show the entire database and “--dbms” to specify the type of database that is running. We successfully obtain the gift list, THM flag and admin's password.