

PSP0201

Week 2

Writeup

Group Name: Undecided

Members

ID	Name	Role
1211101390	Aslamia Najwa Binti Ahmad Khadri	Leader
1211100431	Mohammad Omar Torofder	Member
1211103388	Vishnu Karmegam	Member
1211103092	Farryn Aisha binti Muhd Firdaus	Member

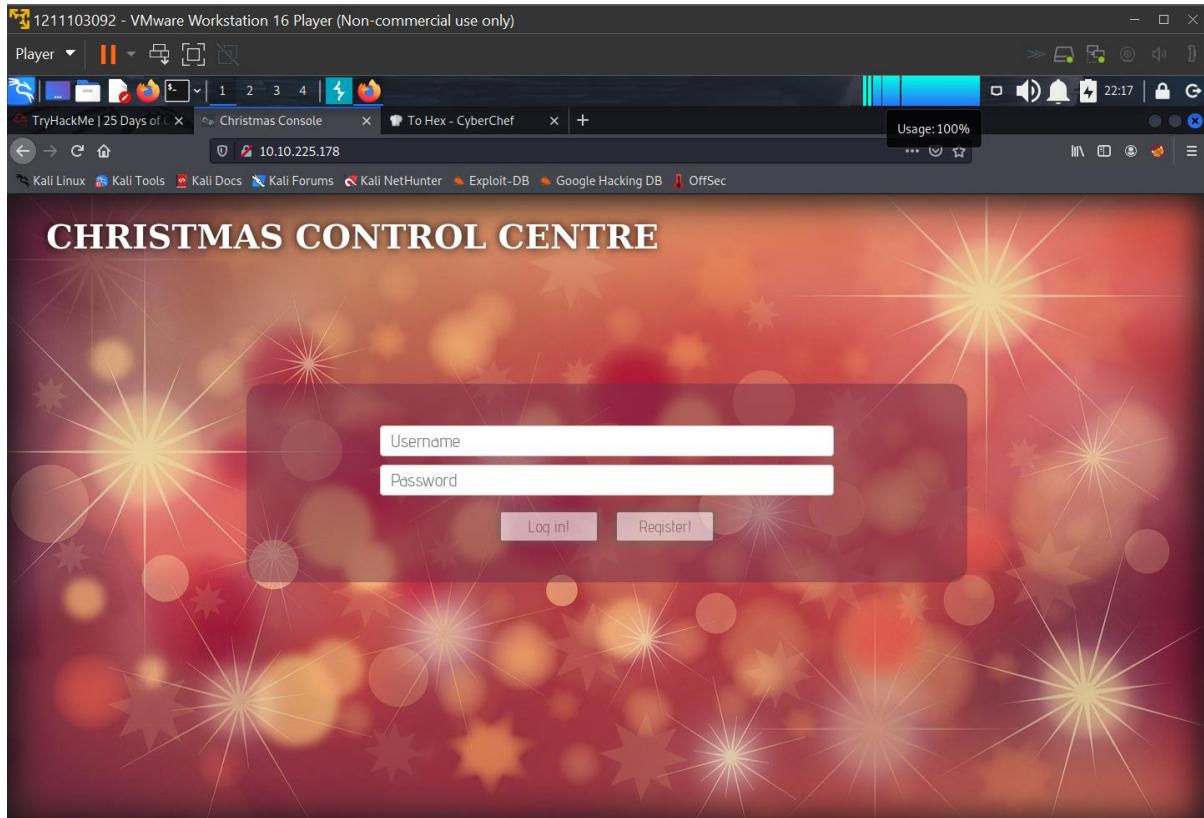
Day 1: Web Exploitation – A Christmas Crisis

Tools used: Kali Linux, Firefox

Solution/walkthrough:

Question 1

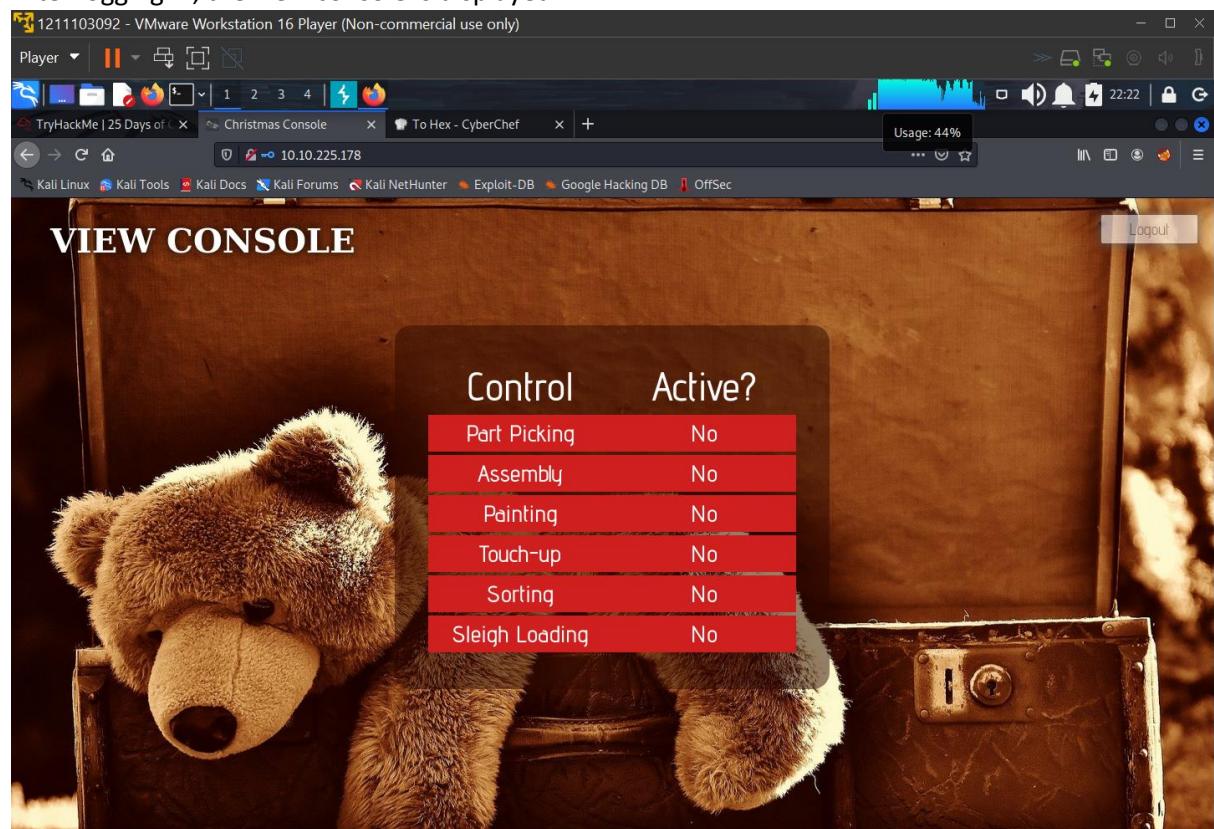
Upon entering the IP address provided from the machine, we were brought to the ‘Christmas Control Centre’ page where we register and log in to the Christmas Control Centre by entering a random username password. As of now, we still have no access to the control console.



The title of the website is Christmas Console Centre as shown in the picture above.

Question 2

After logging in, the view console is displayed.



Inspect the browser and navigate to storage to check the cookies.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
auth	7b22636f6d7061e79223a22546865204265737420466573746976616c0436f6d7061e7922c2022757365726e...	10.10.225.178	/	Session	128	false	false	None	Sun, 26 Jun 2022 0...

The name of the cookie used for authentication is auth as shown above.

Question 3

We took the cookie value and converted it to string using Cyberchef.

The screenshot shows the CyberChef interface. On the left, there's a sidebar with various operations like 'To Base64', 'From Hex', etc. The main area has two sections: 'Input' and 'Output'. In the 'Input' section, there's a large text area containing a long hex string: 7b22636f6d70e16e79223a22546865204265737420466573746976616c26430f6d70010e79222c2922757365726e916d65223a2201046d690e227d. Below this, under 'Delimiter' is set to 'Auto'. In the 'Output' section, the resulting JSON object is shown: {"company": "The Best Festival Company", "username": "admin"}. The CyberChef interface includes a 'BAKE!' button at the bottom.

We learn that the format of the value this cookie encoded is hexadecimal.

Question 4

The format that the data is stored in is JSON.

Question 5

The cookie value is converted to string using Cyberchef. From the string, we obtain the value for the company field which is 'The Best Festival Company'.

The screenshot shows the CyberChef interface with the following details:

- Operations:** Favourites (selected), To Base64, From Base64, To Hex, From Hex, To Hexdump, From Hexdump, URL Decode, Regular expression, Entropy, Fork, Magic.
- Recipe:** From Hex
- Input:** A long hex string: 7b22036f6d70616e79223a22546865284265737420466573746976616c28436fd70616e79222c2922757365726e616d65223a2261646d696e227d
- Output:** A JSON object: {"company": "The Best Festival Company", "username": "admin"}
- Options:** Last build: 17 days ago, Options, About / Support.
- Buttons:** STEP, BAKE!, Auto Bake.

Question 6

The other field found in the cookie is fullname.

The screenshot shows the CyberChef interface with the following details:

- Operations:** Favourites (selected), To Base64, From Base64, To Hex, From Hex, To Hexdump, From Hexdump, URL Decode, Regular expression, Entropy, Fork, Magic.
- Recipe:** From Hex
- Input:** A long hex string: 7b22036f6d70616e79223a22546865284265737420466573746976616c28436fd70616e79222c2922757365726e616d65223a2261646d696e227d
- Output:** A JSON object: {"company": "The Best Festival Company", "username": "admin"}
- Options:** Last build: 17 days ago, Options, About / Support.
- Buttons:** STEP, BAKE!, Auto Bake.

Question 7

With the value of cookie we obtained earlier from the inspection of website, we change the username to santa and we change it back into hexadecimal form. The new value is the value of Santa's cookie

The screenshot shows the CyberChef interface with a 'To Hex' recipe selected. The input is a JSON object: {"company": "The Best Festival Company", "username": "santa"}.

The output is the hex representation of the JSON object:

```
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d
```

Question 8

We log out from the previous page, click right on the mouse, and click on inspect. Under the storage section, in the cookie, we add a new filter item, set auth as the name and insert the value of the santa's cookie. Then, we reload the page. The control console can now be accessed. We switched on all the control and received our flag. The flag that is given when the line is fully active is THM{MjY0Yzg5NTTmY2Q1NzM1NjBmZWFlhYmQy}.



Thought Process/Methodology:

After accessing the target engine, we found the title of the website which is Christmas Console. On that page, we register our account and log in. After logging in, we access the inspection tool and navigate to the storage where the cookie is stored. By looking at the value of the cookie, we inferred that it stored in hexadecimal value and proceeded to convert it to text using Cyberchef. After converting the value, we found a JSON statement with a username and company element. Using Cyberchef, we changed the username to 'santa', the administrator account, and converted the statement back to hexadecimal using Cyberchef. We went back to website home page and replace the cookie value with the new changed value. Then, we reload the page. We were led to the administrator page where we gain access to the control console. We proceed to enable each control, which in turn showed the flag.