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

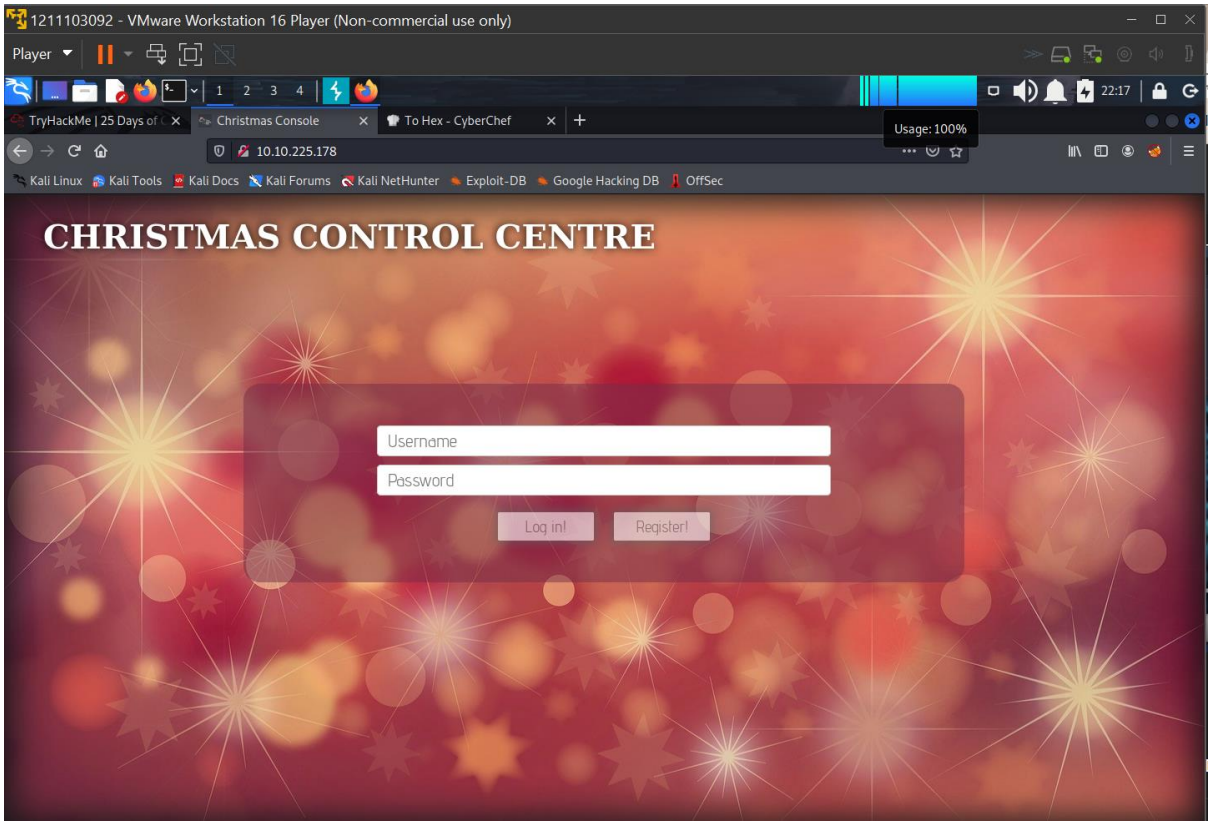
Day 1: Web Exploitation – A Christmas Crisis

Tools used: Kali Linux, Firefox

Solution/walkthrough:

Question 1

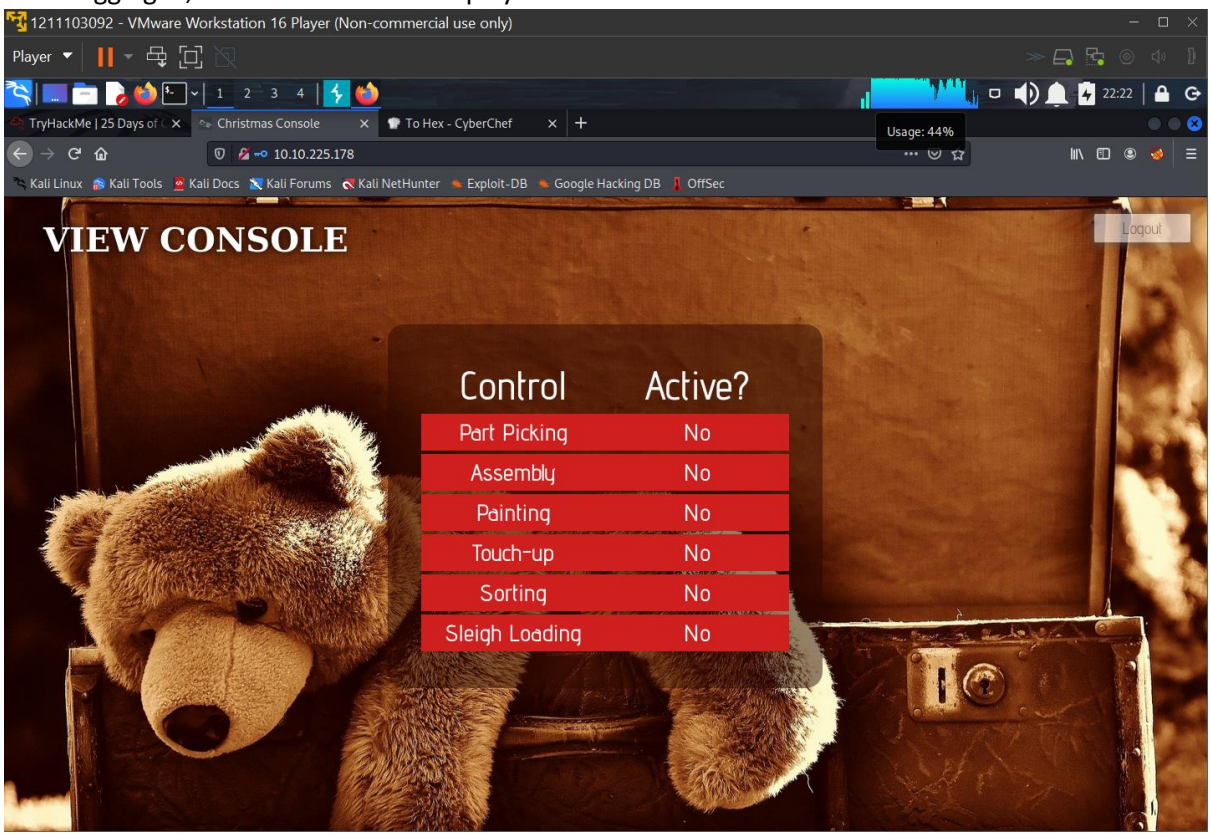
Upon entering the IP address provided from the machine, we were brought to the 'Christmas Control Centre' page where we register and log in to the Christmas Control Centre by entering a random username password. As of now, we still have no access to the control console.



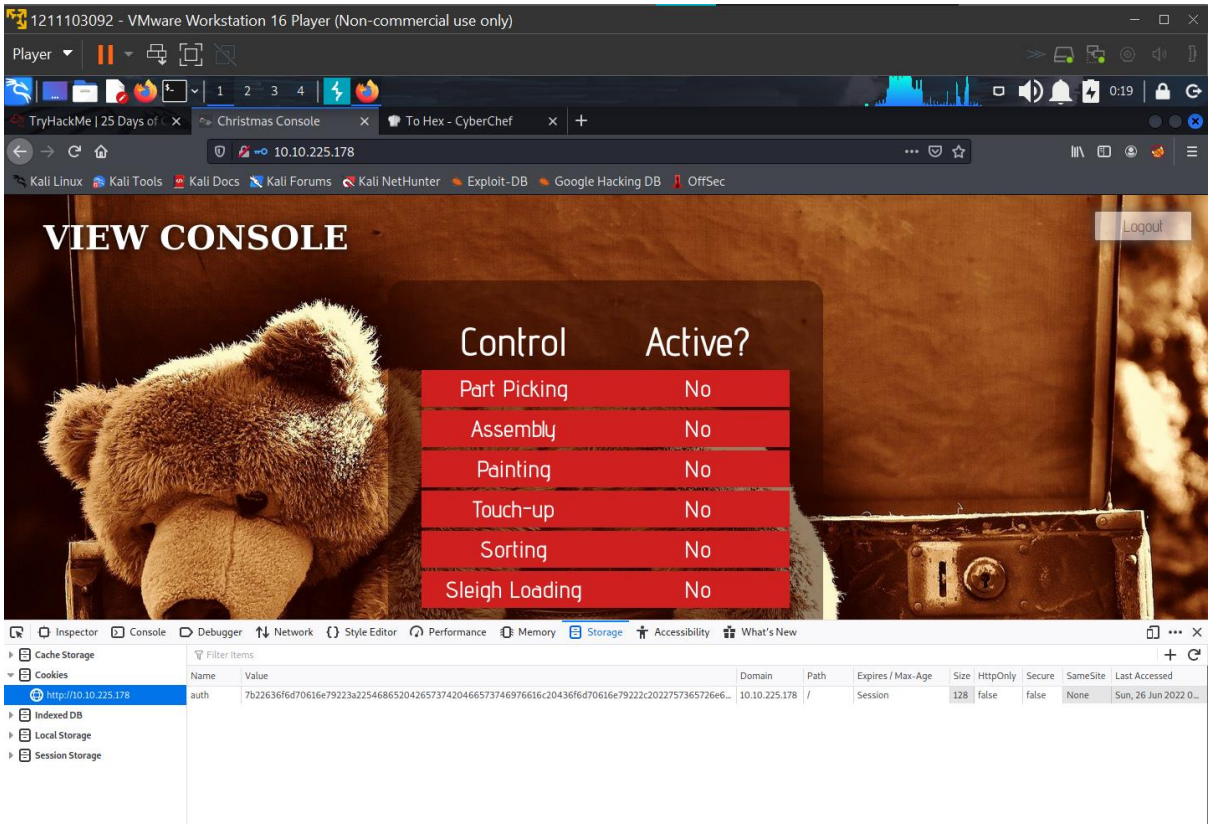
The title of the website is Christmas Console Centre as shown in the picture above.

Question 2

After logging in, the view console is displayed.



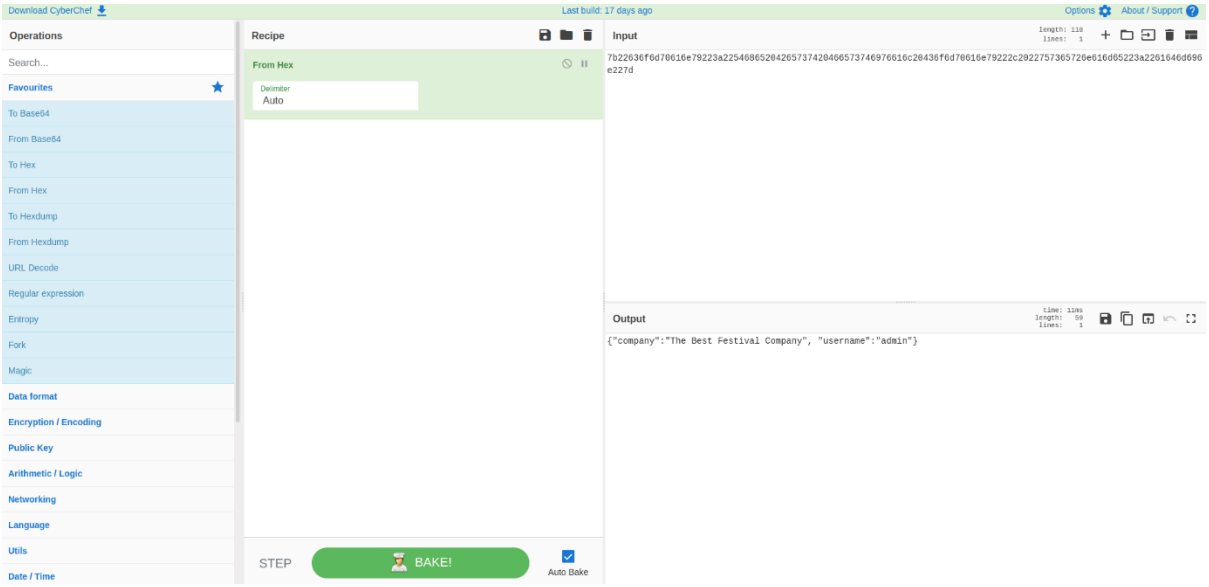
Inspect the browser and navigate to storage to check the cookies.



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.



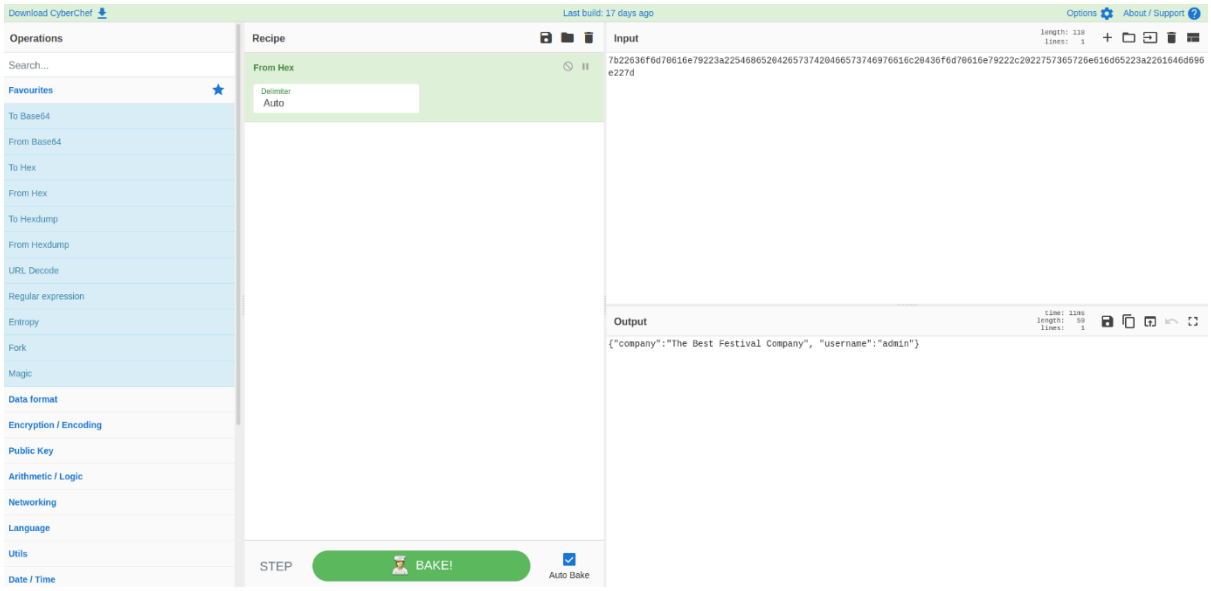
We learn that the format of the value this cookie encoded is hexadecimal.

Question 4

The format that the data is stored in is JSON.

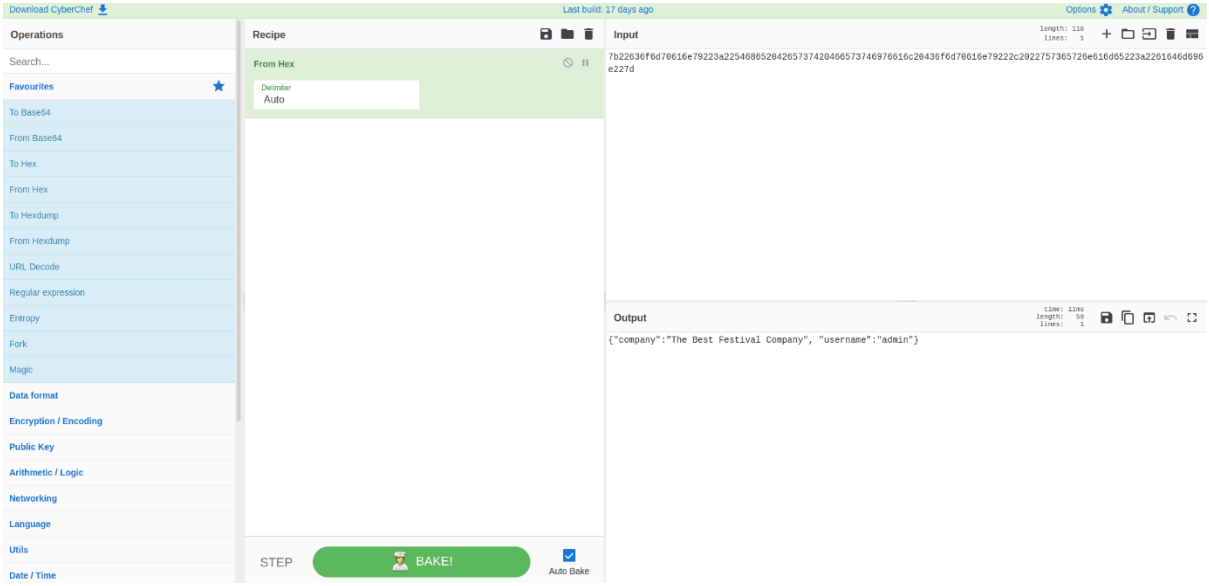
Question 5

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’.



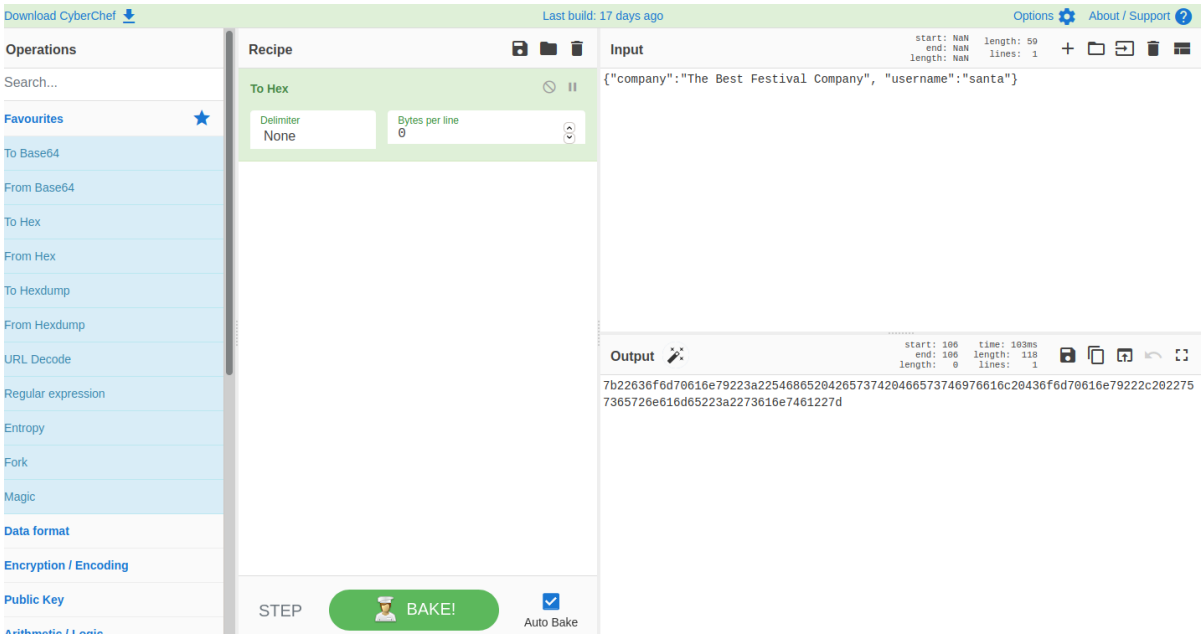
Question 6

The other field found in the cookie is fullname.



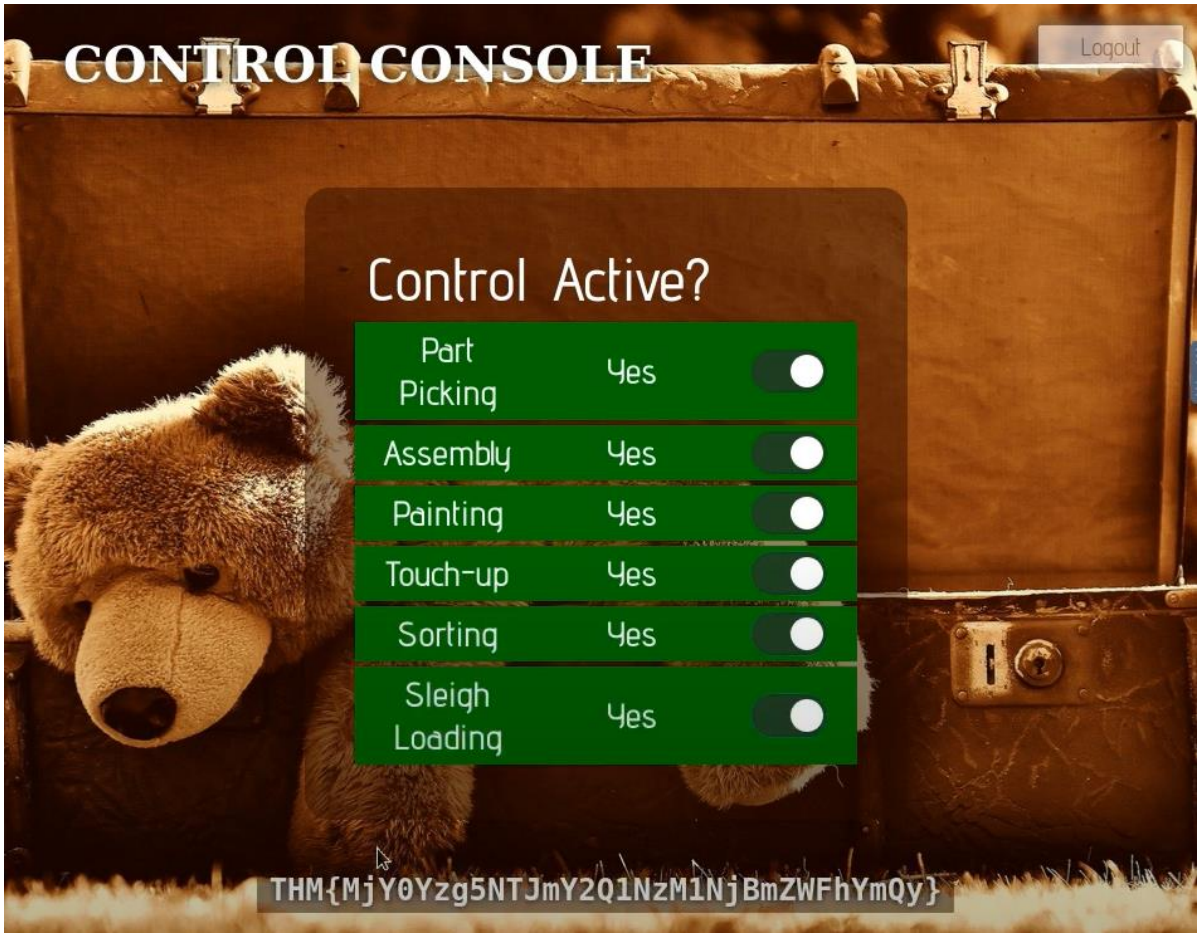
Question 7

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



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{MjY0Yzg5NTTmY2Q1NzM1NjBmZWFhYmQy}.



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 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.