PSP0201 Week 2 Writeup

Group Name: ikun no 1

Members

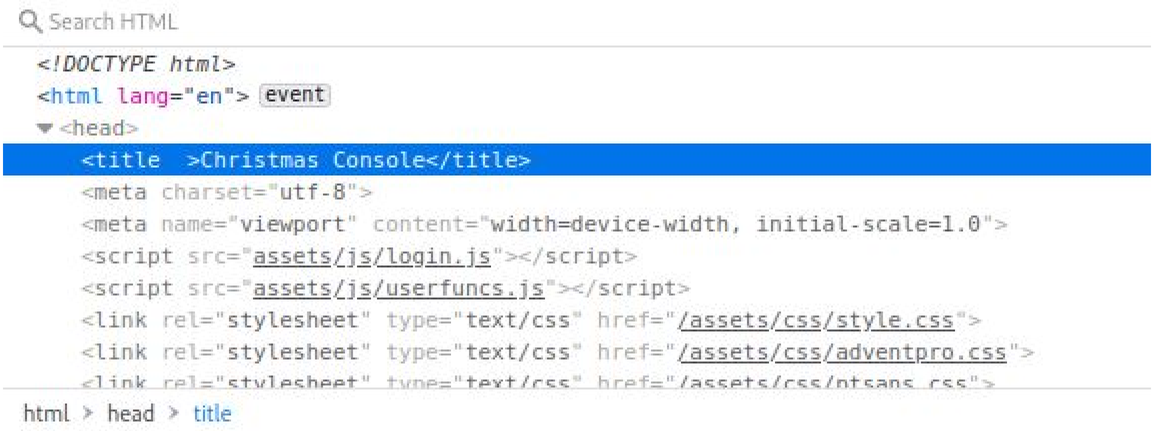
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

DAY 1: Web Exploitation   A Christmas Crisis

Tool used: kali Linux, Firefox

Solution/Walkthrough:

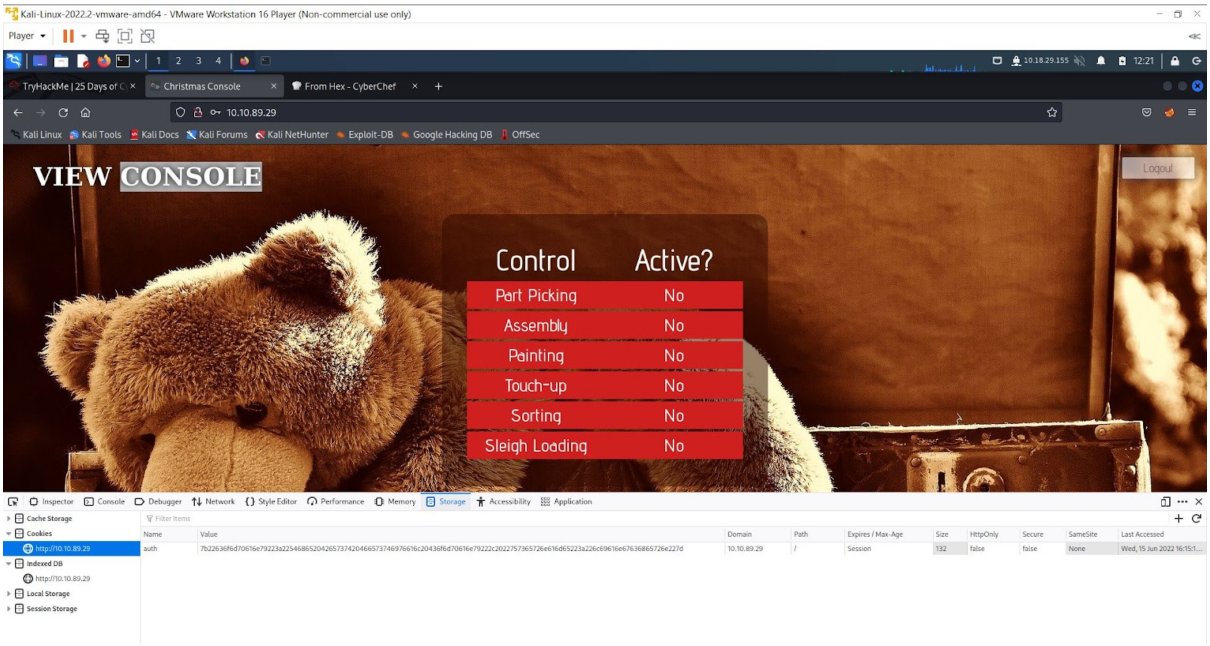
Q1



```
<!DOCTYPE html>
<html lang="en"> event
▾ <head>
    <title  >Christmas Console</title>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <script src="assets/js/login.js"></script>
    <script src="assets/js/userfuncs.js"></script>
    <link rel="stylesheet" type="text/css" href="/assets/css/style.css">
    <link rel="stylesheet" type="text/css" href="/assets/css/adventpro.css">
    <link rel="stylesheet" type="text/css" href="/assets/css/ntsans.css">
```

Register using own username and password. After that, inspect using developer tools, expand ‘head’ tags, text in between html title tag is the title of the website.

Q2

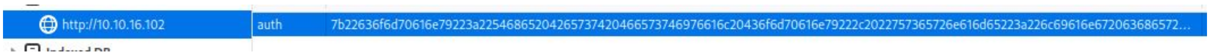


Control	Active?
Part Picking	No
Assembly	No
Painting	No
Touch-up	No
Sorting	No
Sleigh Loading	No

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
auth	7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a226c69616e67636865726e227d	10.10.89.29	/	Session	132	false	false	None	Wed, 15 Jun 2022 16:15:1...

Check the cookie name by opening the developer tools – storage – cookies. The name of the cookie is stated under the name row, which is auth.

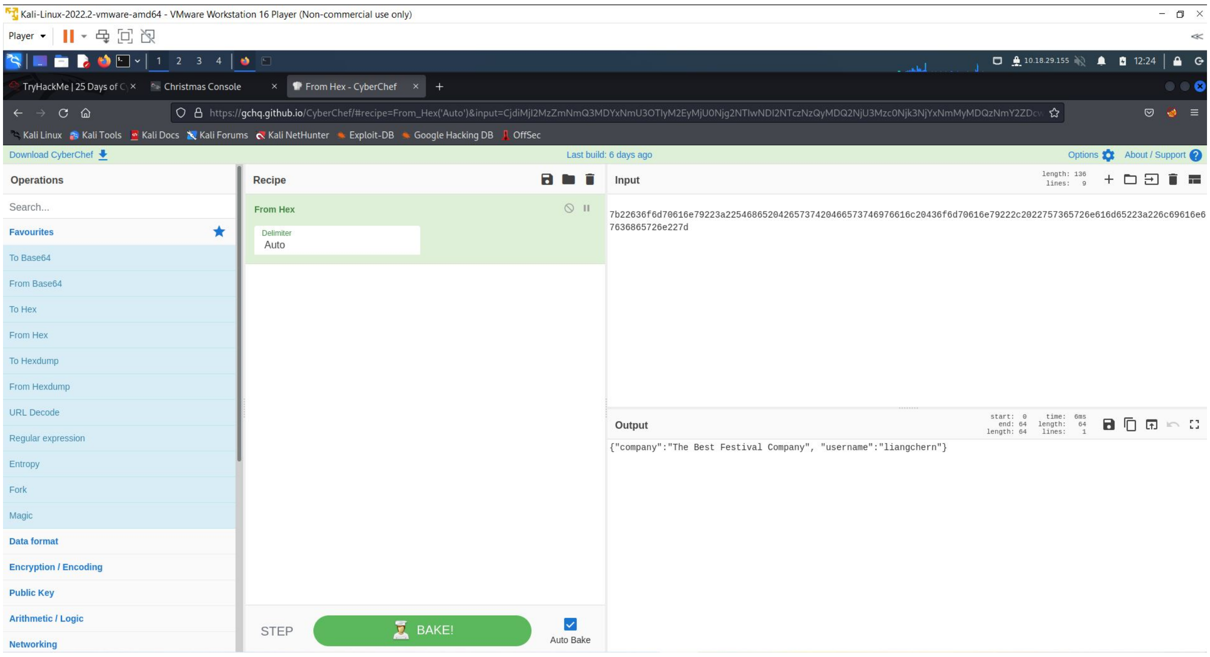
Q3



```
http://10.10.16.102    auth    7b22636f6d70616e79223a225468652042657374204665737469766616c20436f6d70616e79222c2022757365726e616d65223a226c69616e672063686572...
```

Obtain the value of the cookie. Observe and examine the orientation and pattern of the code obtained, thus can identify that it is hexadecimal.

Q4 & Q5 & Q6



https://gchq.github.io/CyberChef/#recipe=From_Hex('Auto')&input=CjdiMjI2MzZmNmQ3MDYxNmU3OTIyM2EyMjU0Njg2NTIwNDI2NTczNzQyMDQ2NjU3Mzc0Njk3NjYxNmMyMDQzNmY2ZDc

From Hex

Delimiter

Auto

```
7b22636f6d70616e79223a225468652042657374204665737469766616c20436f6d70616e79222c2022757365726e616d65223a226c69616e6
7636865726e227d
```

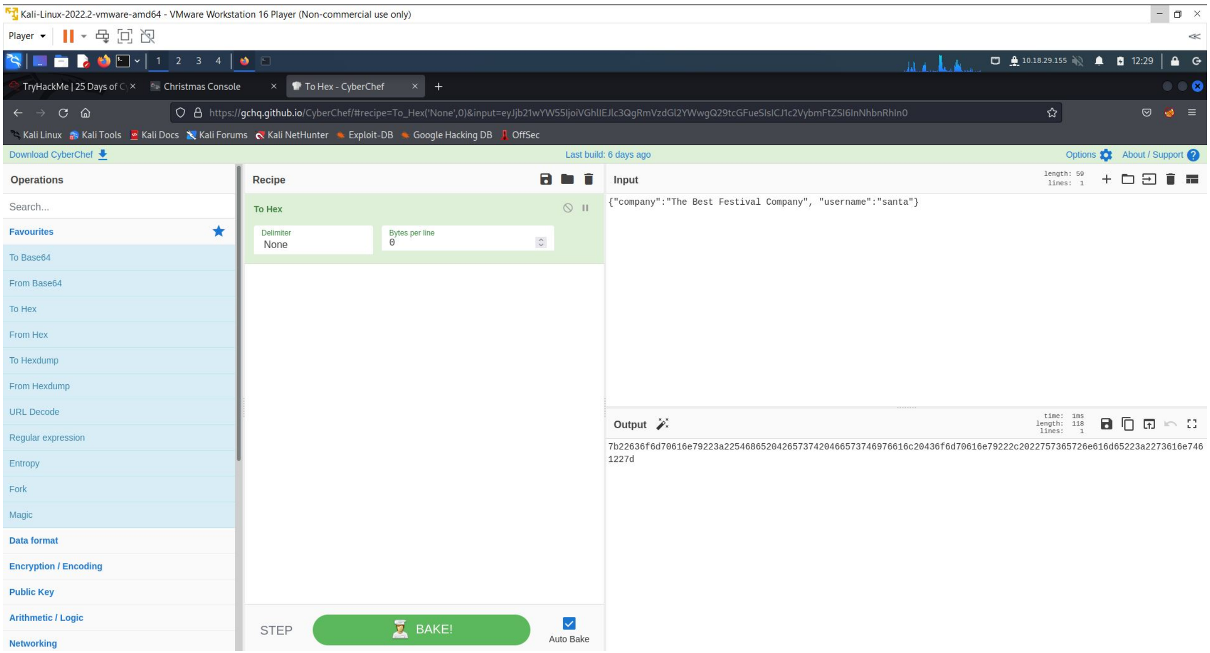
```
{"company":"The Best Festival Company", "username":"liangchern"}
```

Q4) Translate and convert the cookie value from hexadecimal to string using Cyberchef. Observe and examine the orientation and pattern of the string obtained, it is in {“key”:”value”} format, thus can identify that it is in JSON format.

Q5) The name of the company is “The Best Festival Company”, because it is the “value” beside company “key”.

Q6) Examine the whole converted, thus can identify the other field found is username.

Q7



Recipe: To Hex — Delimiter: None, Bytes per line: 0

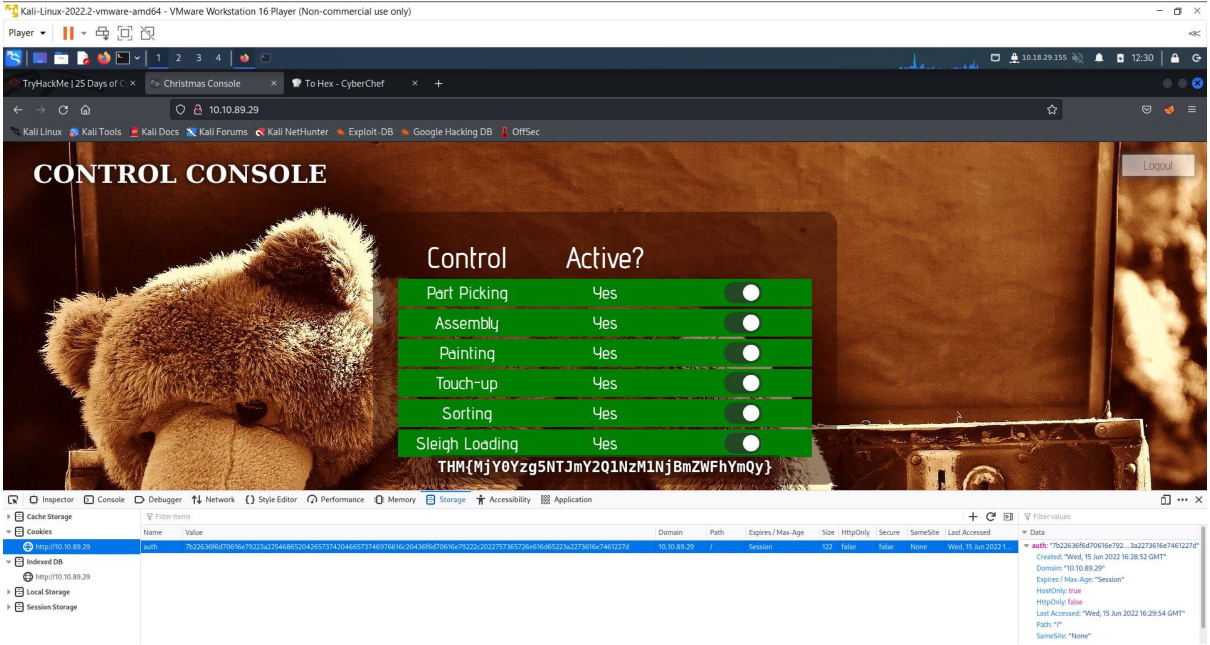
Input (length: 59, lines: 1):

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

Output (time: 1ms, length: 118, lines: 1):

```
7b22636f6d70616e79223a225468652042657374204665737469766616c20436f6d70616e79222c2022757365726e616d65223a2273616e746
1227d
```

Copy the string and change the username into “santa”, then convert the JSON statement back to hexadecimal. Change the delimiter into none, then copy the output obtained.



CONTROL CONSOLE

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

THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWFhYmQy}

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite
auth	7b22636f6d70616e79223a225468652042657374204665737469766616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d	10.10.89.29	/	Session	122	false	false	None

Back to the site. Paste the output obtained into the value row. Refresh the site. The access is granted, activate all and catch the flag.