

PSP0201

Week 2

Writeup

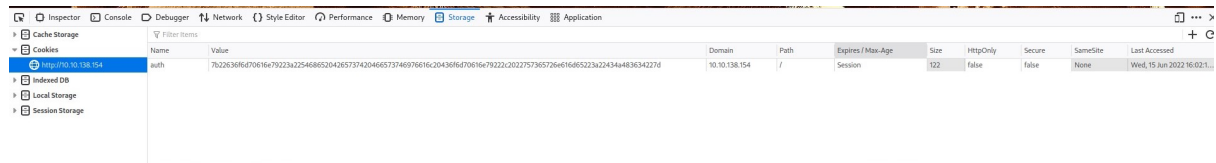
Group Name: ikun no 1

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

From developer tools we can then click into storage → cookies to look for the details of the cookies. The name of the cookie is stated under the name row which is 'auth'.

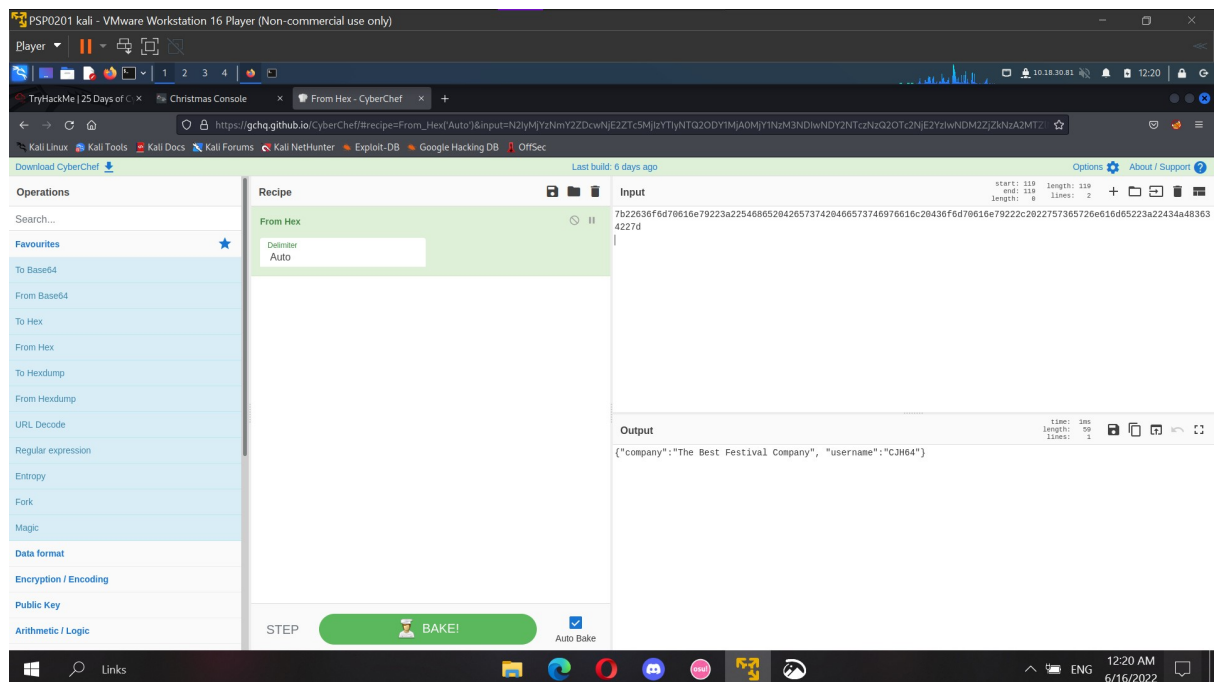
Q3



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
auth	7b22636fd70616e79223a22546865204285737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a22434a483634227d	10.10.138.154	/	Session	122	false	false	None	Wed, 15 Jun 2022 16:02:1...

Obtain the value of the cookie. Observe and examine the orientation and pattern of the code obtained. The value we can get is in hexadecimal format.

Q4 & Q5 & Q6



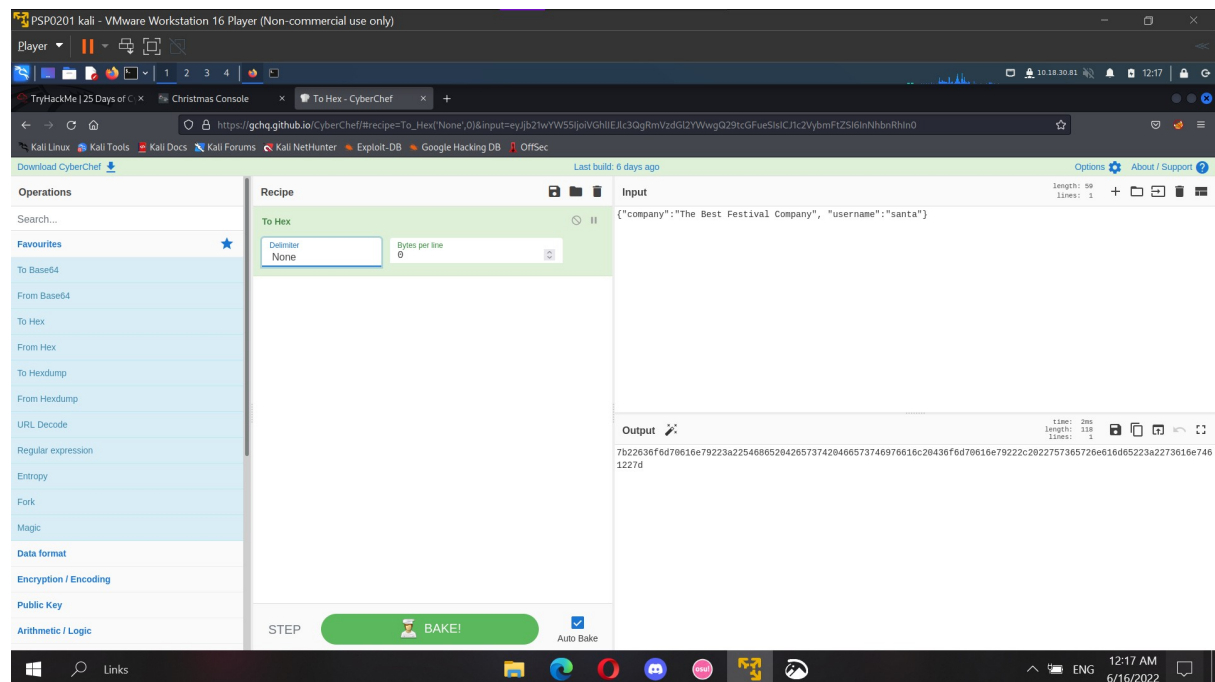
The screenshot shows the CyberChef web application interface. On the left is a sidebar with various operations like 'To Base64', 'From Base64', 'To Hex', 'From Hex', 'To Hexdump', 'From Hexdump', 'URL Decode', 'Regular expression', 'Entropy', 'Fork', 'Magic', 'Data format', 'Encryption / Encoding', 'Public Key', and 'Arithmetic / Logic'. The main area displays a 'Recipe' with a single step 'From Hex' and a 'Delimiter' set to 'Auto'. The 'Input' field contains a long hexadecimal string: 7b22636fd70616e79223a22546865204285737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a22434a483634227d. The 'Output' field shows the result of the conversion: {"company":"The Best Festival Company", "username":"CJH64"}. At the bottom, there is a 'BAKE!' button and an 'Auto Bake' checkbox.

Q4) Type the cookie into Cyberchef and convert it into a string from hexadecimal. The pattern of the string is in {"key":"value"} format, thus we can identify that it is a JSON.

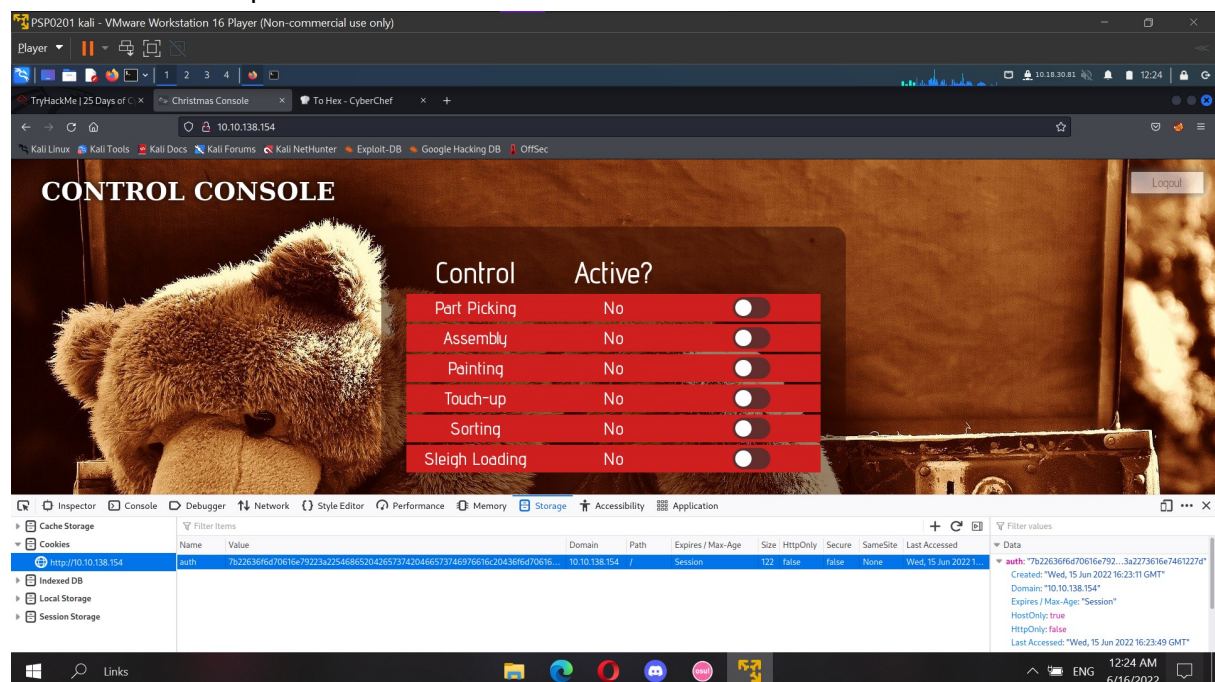
Q5) The name of the company is "The Best Festival Company" and can be found beside the "key" which is the "company".

Q6) Username is stated in the other field of the string.

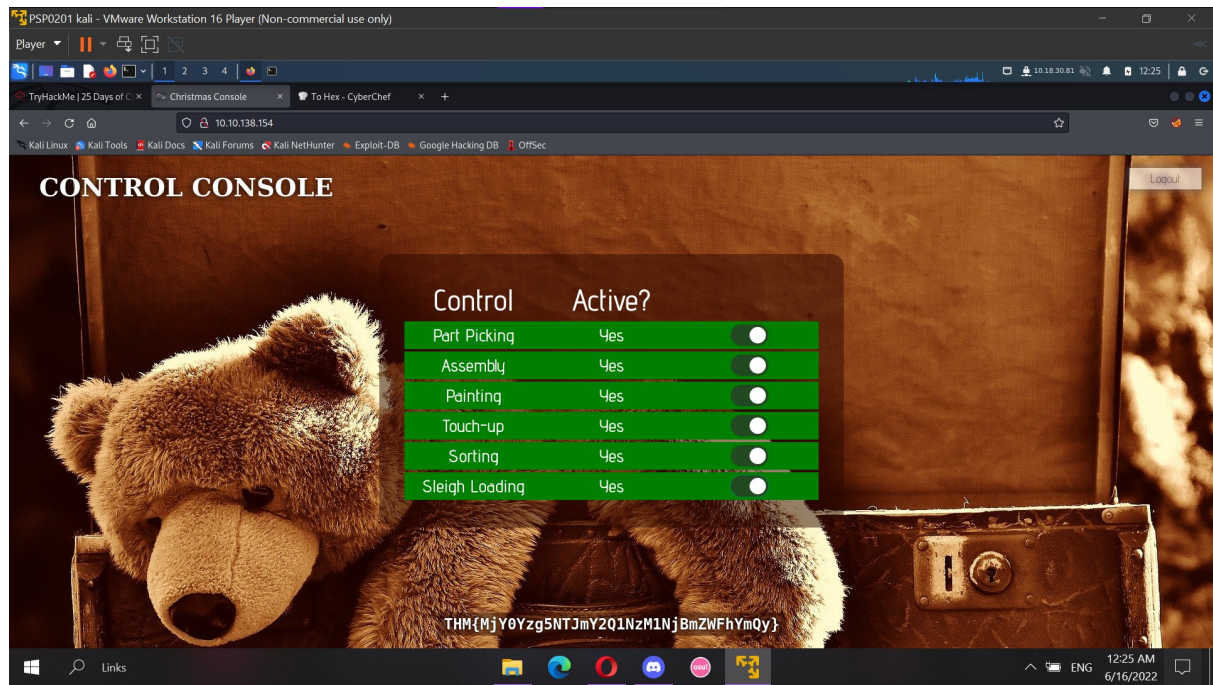
Q7



Copy the string and change the username info to “santa”. Convert the JSON data back to hexadecimal. Change the delimiter from space to none. The value of the new cookie can be obtained at the output.



Change the value of cookie from the output we get from cyberchef and refresh the page again.



After refreshing the site, tick all the controls and the flag can be caught.