Try Hack Me : Advent of Cyber day 1 | A Christmas Crisis

This room covers cookies, How they are created and how to exploit them. It also shines a light on the background processes that make up the internet. Such as DNS and HTTP

"The Best Festival Company's brand new OpenVPN server has been hacked. This is a crisis!

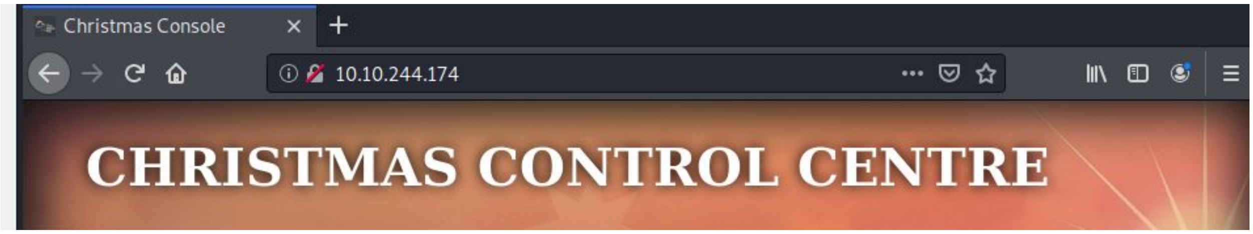
The attacker has damaged various aspects of the company infrastructure -- including using the Christmas Control Centre to shut off the assembly line!

It's only 24 days until Christmas, and that line has to be operational or there won't be any presents! You have to hack your way back into Santa's account (blast that hacker changing the password!) and getting the assembly line up and running again, or Christmas will be ruined!"

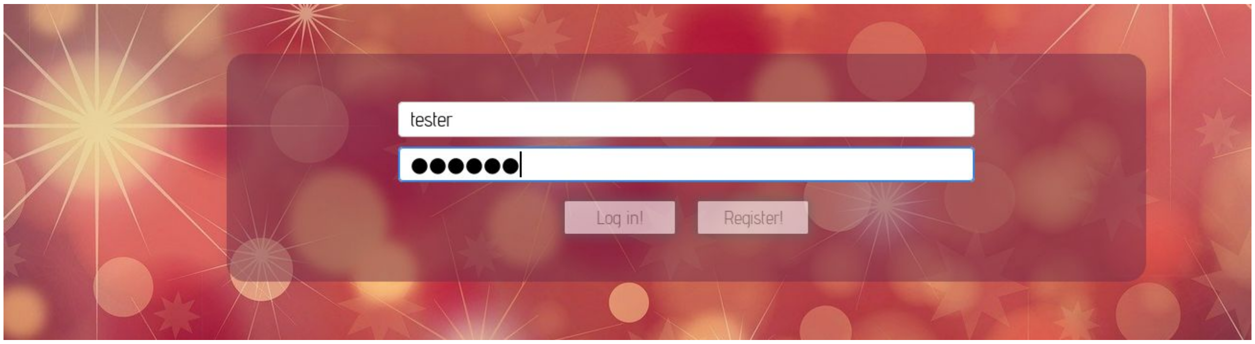
-Elf McSkidy

What is the name of the cookie used for authentication?

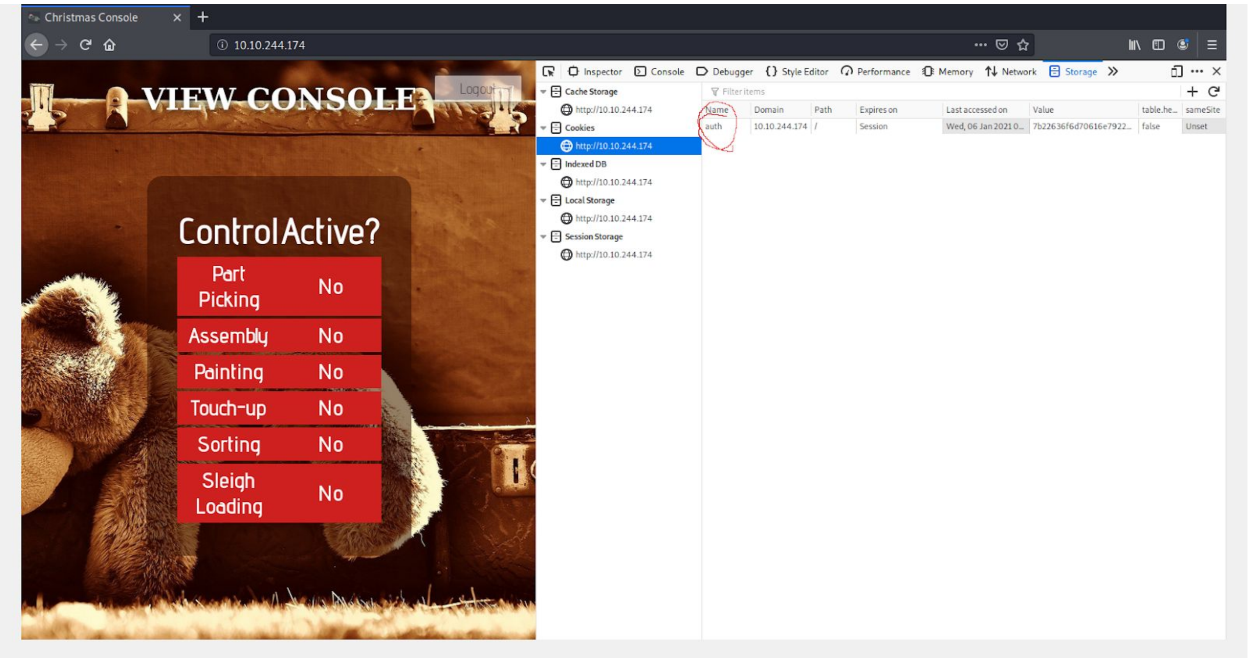
To begin I browse to the ip of the website.



Register on the site and log in



We are presented with a control console for Santas workshop. The challenge wants to know what the name of the cookie used for authentication. To found out lets go to our browser's developer console. In firefox this can be found by clicking the F12 key, then clicking on storage, then cookies. Below you can see that the name of the cookie is auth.



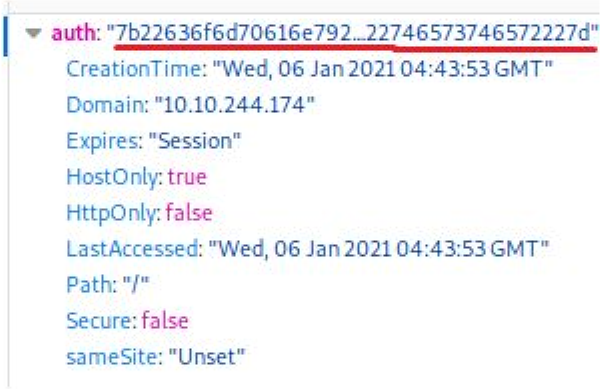
Control Active?

Part Picking	No
Assembly	No
Painting	No
Touch-up	No
Sorting	No
Sleigh Loading	No

Name	Domain	Path	Expires on	Last accessed on	Value	table.he...	sameSite
auth	10.10.244.174	/	Session	Wed, 06 Jan 2021 0...	7b22636f6d70616e7922...	false	Unset

In what format is the value of this cookie encoded?

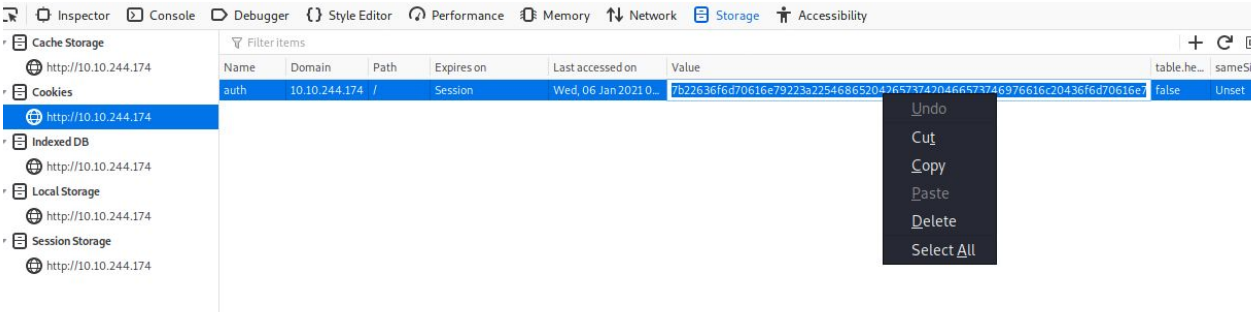
Looking at the cookie we see a string of letters and numbers. From experience I know that this type of data is called Hexadecimal or Hex. Hexadecimal is base 16 number system used to make raw binary data easier to read for humans. The easiest way to tell you are dealing with Hexadecimal is that your will have the numbers 0-9 accompanied by the letters a-f. Either in long strings (like the example below) or in pairs like this (CE 00 36 00 EF).



```
auth: "7b22636f6d70616e792...22746573746572227d"
    CreationTime: "Wed, 06 Jan 2021 04:43:53 GMT"
    Domain: "10.10.244.174"
    Expires: "Session"
    HostOnly: true
    HttpOnly: false
    LastAccessed: "Wed, 06 Jan 2021 04:43:53 GMT"
    Path: "/"
    Secure: false
    sameSite: "Unset"
```

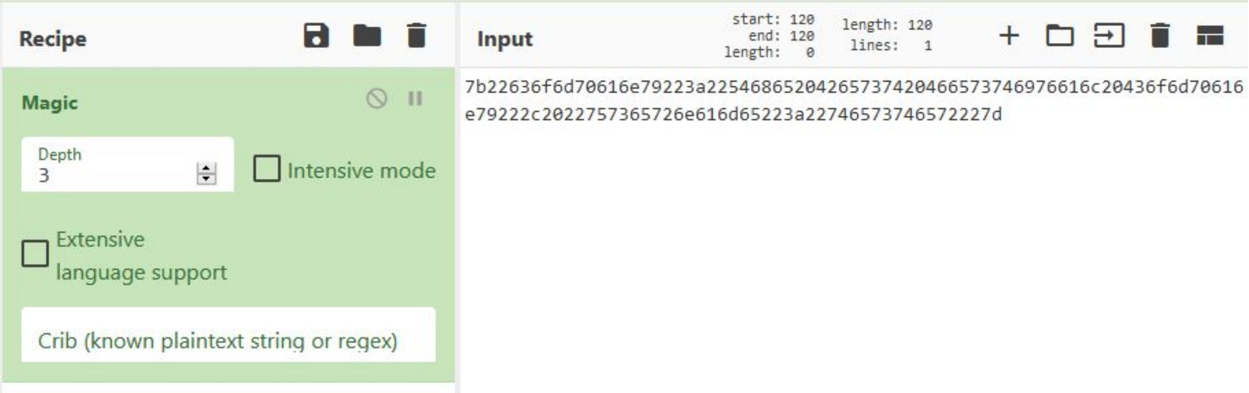
Having decoded the cookie, what format is the data stored in?

First we have to copy the hexadecimal from the cookie.



Name	Domain	Path	Expires on	Last accessed on	Value	table.he...	sameSi
auth	10.10.244.174	/	Session	Wed, 06 Jan 2021 0...	7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e7	false	Unset

Then we head over to CyberChef and paste it in, select magic and let it do it’s thing.



Depth 3

□ Intensive mode

□ Extensive language support

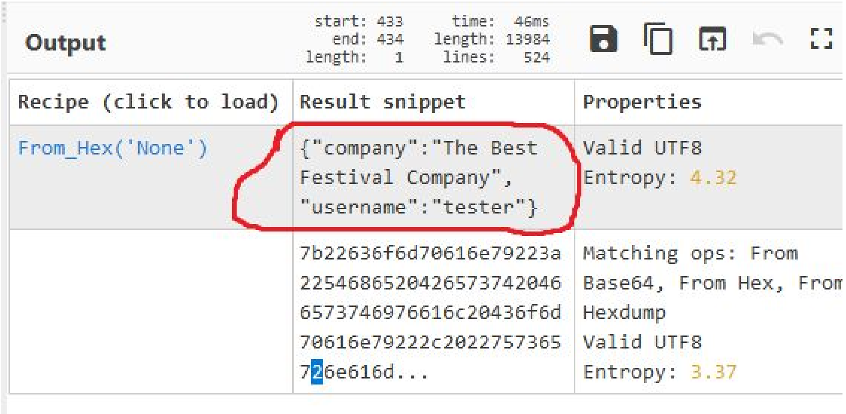
Crib (known plaintext string or regex)

```
start: 120    length: 120
  end: 120     lines:   1
length:   0
```

```
7b22636f6d70616e79223a225468652042657374204665737469766616c20436f6d70616
e79222c2022757365726e616d65223a2274657374657222 7d
```

CyberChef will spit out something that we can understand. Looking at this data I know this is a JSON format. This can take some experience to know. If you need hints on what type of data you are working with. You can look in the debugger and get some hints based on the file types you see. Most website use Javascript and we can see that this website is no different.

This data works together with the code that runs on the website to remember if you logged in. Without this file you would have to log in each time you wanted to use a page. If you look closely you can see that the username is saved inside the cookie.



```
 start: 433     time:   46ms
   end: 434   length: 13984
length:   1    lines:    524
```

Recipe (click to load)	Result snippet	Properties
From_Hex('None')	{"company":"The Best Festival Company", "username":"tester"}	Valid UTF8 Entropy: 4.32
	7b22636f6d70616e79223a2254686520426573742046 6573746976616c20436f6d70616e79222c2022757365 726e616d...	Matching ops: From Base64, From Hex, From Hexdump Valid UTF8 Entropy: 3.37

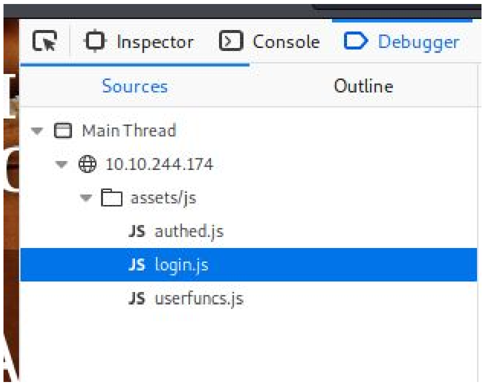
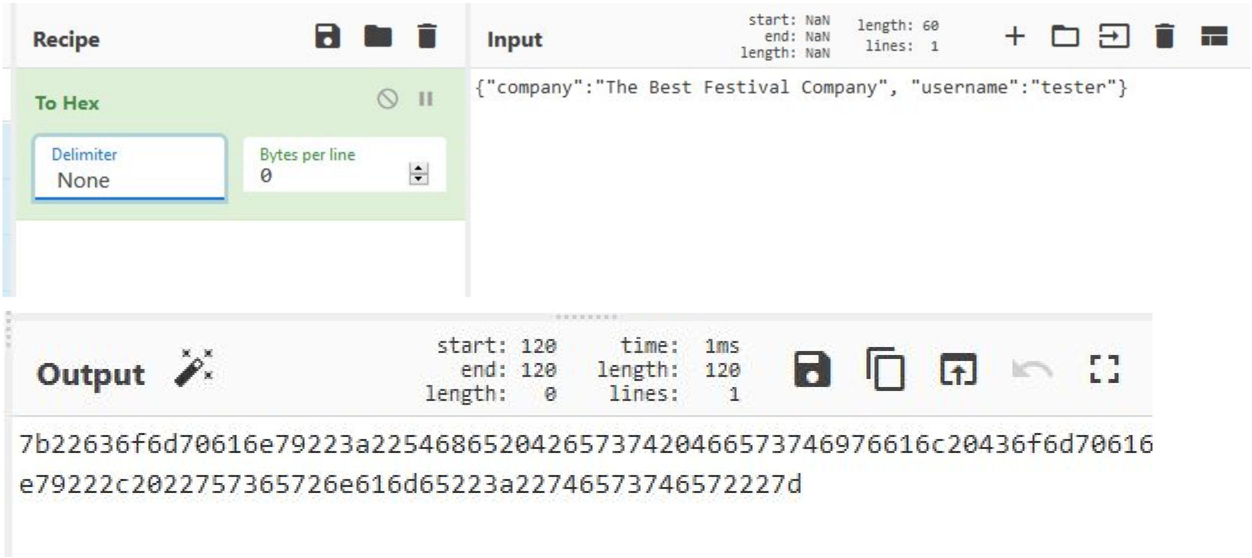


Figure out how to bypass the authentication. What is the value of Santa's cookie?

This is where things get a little cheeky! Take a good look at the hex below



Recipe

To Hex

Delimiter: None

Bytes per line: 0

Input

start: NaN
end: NaN
length: NaN

length: 60
lines: 1

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

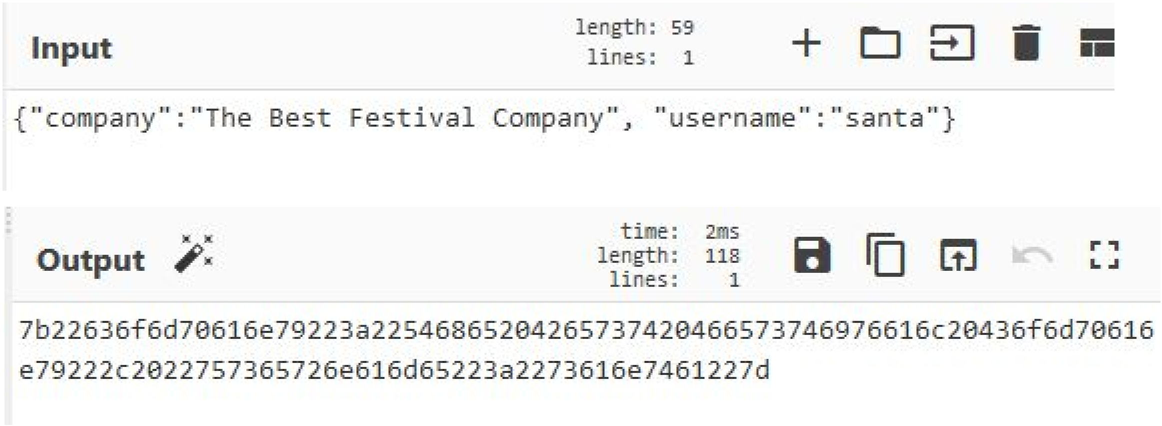
Output

start: 120
end: 120
length: 0

time: 1ms
length: 120
lines: 1

```
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616
e79222c2022757365726e616d65223a22746573746572227d
```

See how the Hex changes when we change the username. This new hex value is the answer to this question.



Input

length: 59
lines: 1

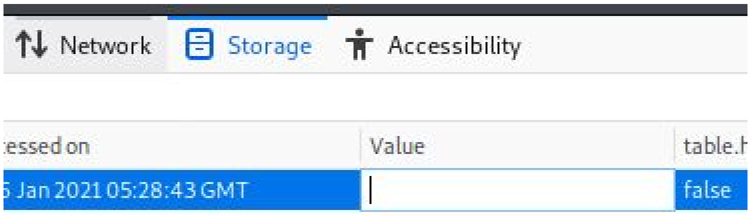
```
{"company":"The Best Festival Company", "username":"santa"}
```

Output

time: 2ms
length: 118
lines: 1

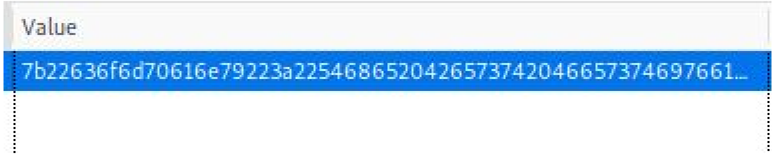
```
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616
e79222c2022757365726e616d65223a2273616e7461227d
```

Delete the value for the cookie then paste the new hex you created



essed on	Value	table.h
5 Jan 2021 05:28:43 GMT		false

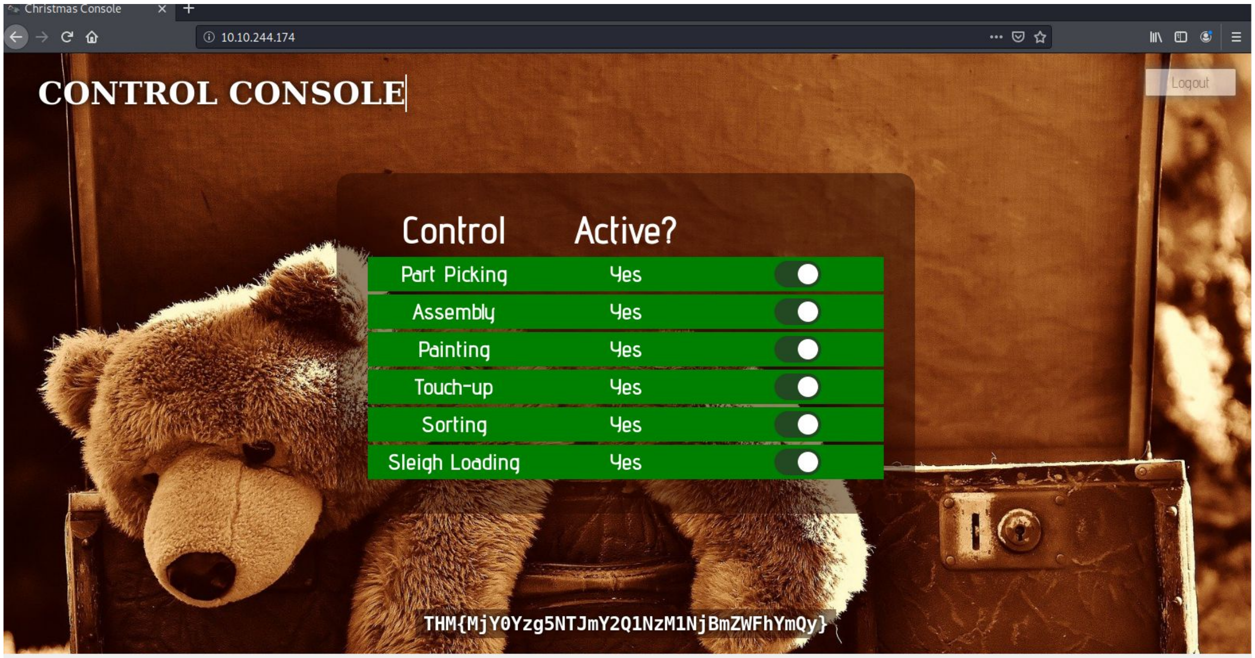
.



Value
7b22636f6d70616e79223a2254686520426573742046657374697661…

Now that you are the santa user, you can re-activate the assembly line! What is the flag you're given when the line is fully active?

Refresh your page and now you are in Santas account. Be sure to turn everything the hacker turned off. You'll be rewarded with a Flag



CONTROL CONSOLE

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

THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWFhYmQy}