UFOria

Challenge information

UFOria specializes in organizing your trip to space. Get some tickets while they last!

BACKEND SYSTEMS

Backend systems are running for you.

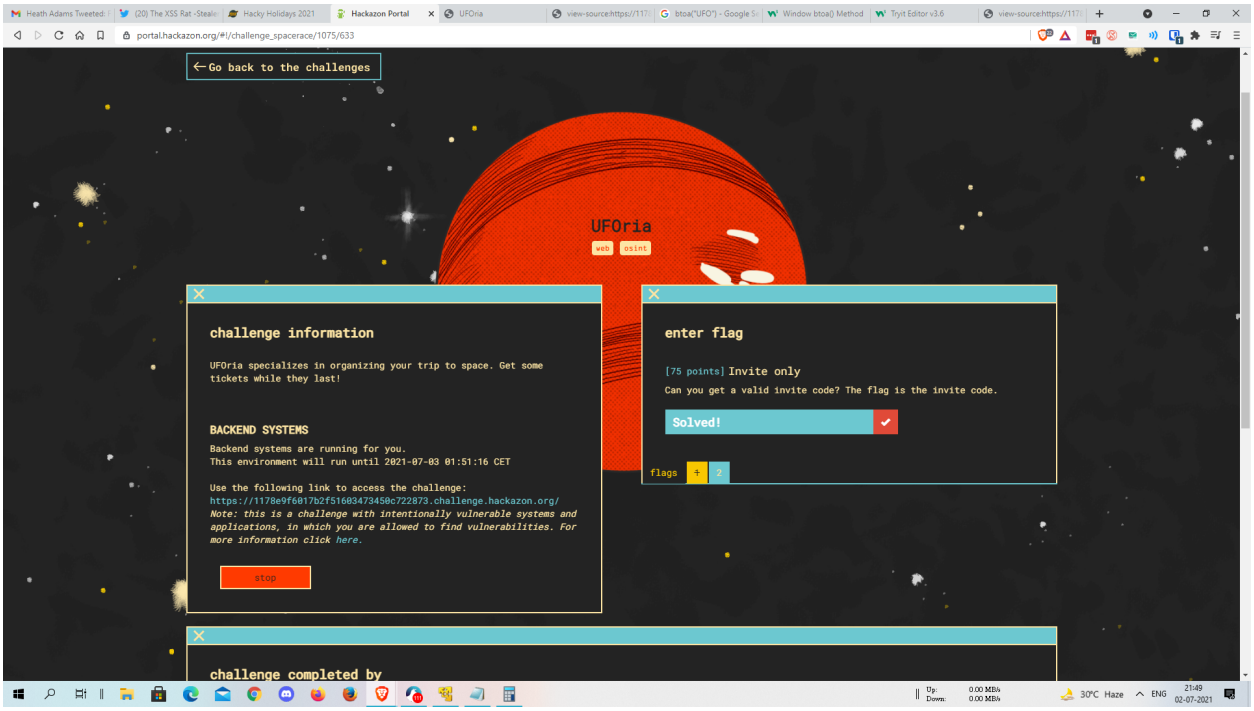
This environment will run until 2021-07-03 01:51:16 CET

Use the following link to access the challenge:https://1178e9f6017b2f51603473450c722873.challenge.hackazon.org/

Note: this is a challenge with intentionally vulnerable systems and applications, in which you are allowed to find vulnerabilities. For more information click here.

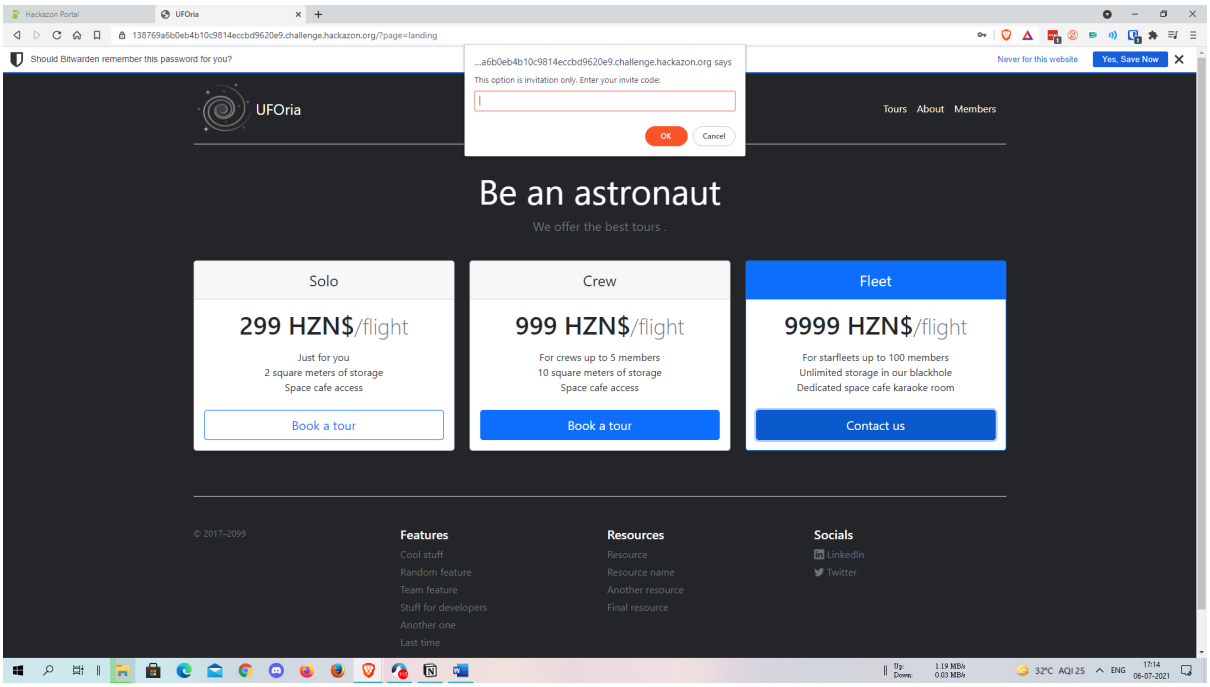
1> Invite only

Can you get a valid invite code? The flag is the invite code.

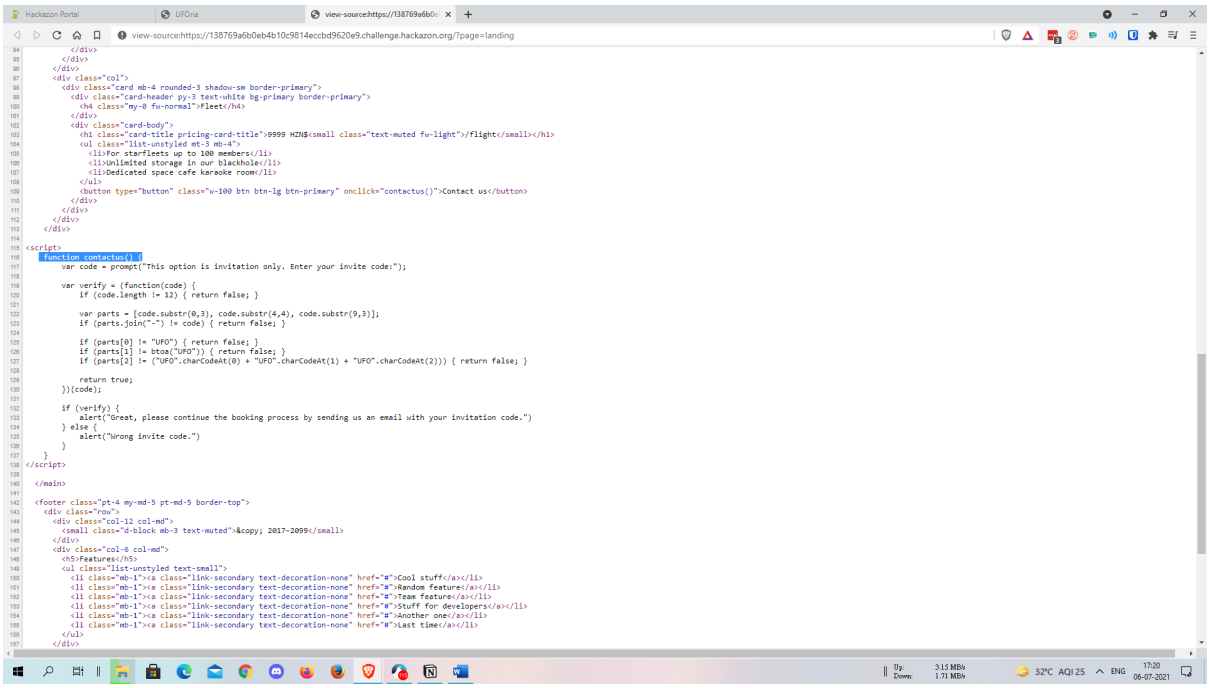


- The challenge says that we have to find a valid invite code to be used to get the tour on the tour's page we can see that they offer three tours (solo, crew, fleet) only Fleet tour has a contact us button when we clicked on it

prompts us to enter the invite code when I entered a random code see if it validates the code or not and found out that it validates the code so we can use this prompt to check if the code is valid or not.



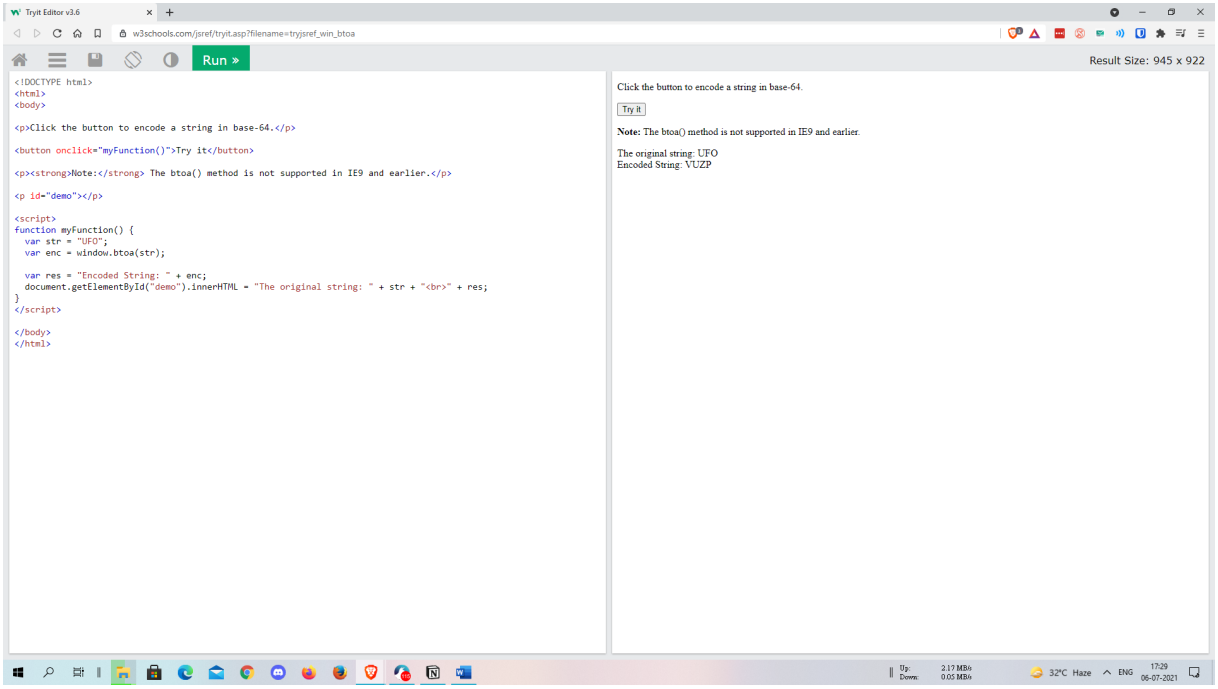
- Now I did some research to find out how the code is validating on viewing page source at the end of the page I found out the code that is being used to validate the invite code



```
function contactus() {
        var code = prompt("This option is invitation only. Enter your invite code:");

        var verify = (function(code) {
            if (code.length != 12) { return false; }

            var parts = [code.substr(0,3), code.substr(4,4), code.substr(9,3)];
            if (parts.join("-") != code) { return false; }

            if (parts[0] != "UFO") { return false; }
            if (parts[1] != btoa("UFO")) { return false; }
            if (parts[2] != ("UFO".charCodeAt(0) + "UFO".charCodeAt(1) + "UFO".charCodeAt(2))) { return false; }

            return true;
        })(code);

        if (verify) {
            alert("Great, please continue the booking process by sending us an email with your invitation code.")
        } else {
            alert("Wrong invite code.")
        }
    }
```

According to the code, I found out that verify function is used to verify the code and will accept the code if and only if the following conditions are met:-

- It will accept the invite code if and only if it of 12 characters in length
- It divides the code into three parts by using the substr function to make and joins these parts by using "-" to validate
- The first part of the code is just UFO
- Second part of the code is btoa("UFO"), bota a js function which encodes the given string to base64, so we have to use the base64 of UFO for the second part of the cod which is "VUZP"

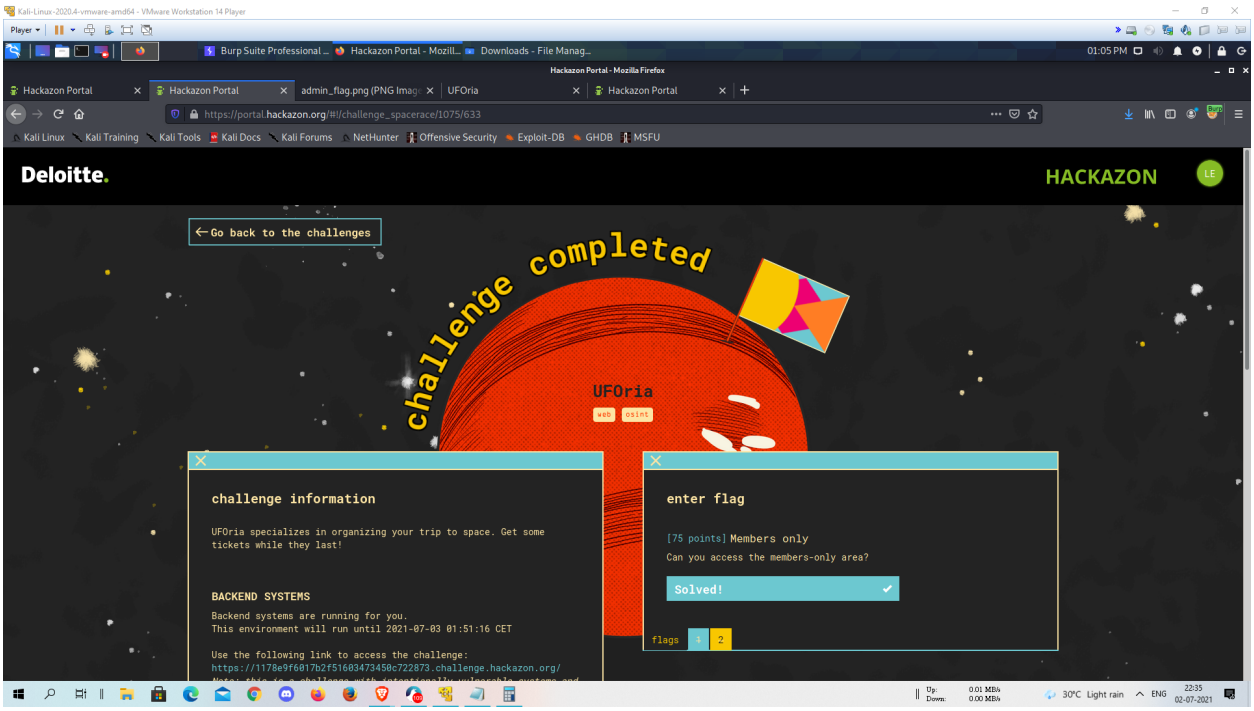


- The third part of the code use charCodeAt js function which returns the Unicode of the character at the specified index in a string. The third part of the code finds unicode for all the characters of UFO and add them up so after finding the unicode for them and adding them we get the sum as 234
- Now we have got all the three-part we have to join them using - and get the invite code which when entered on the prompt it prompts us " Great, please continue the booking process by sending us an email with your invitation code".

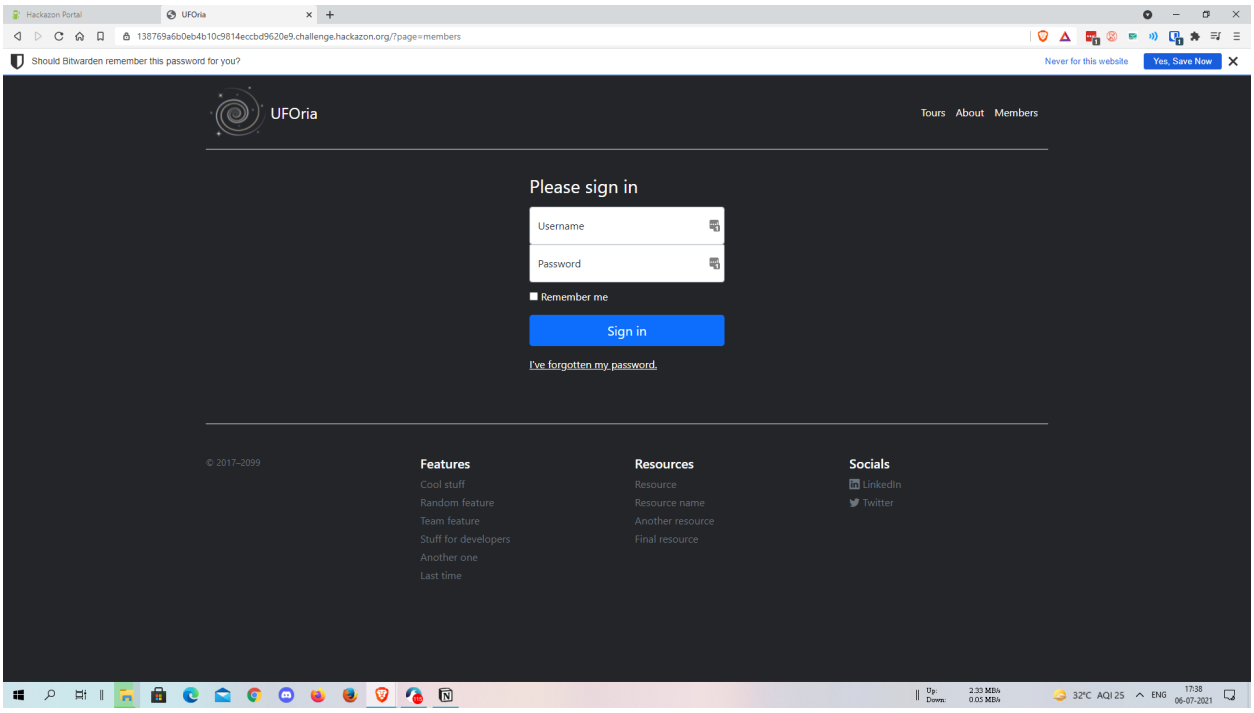
- Flag1 :- UFO-VUZP-234The second challenge tells us to access the members only area, to access it we have to have an account whose username and password we can use to access the area.

2> Members only

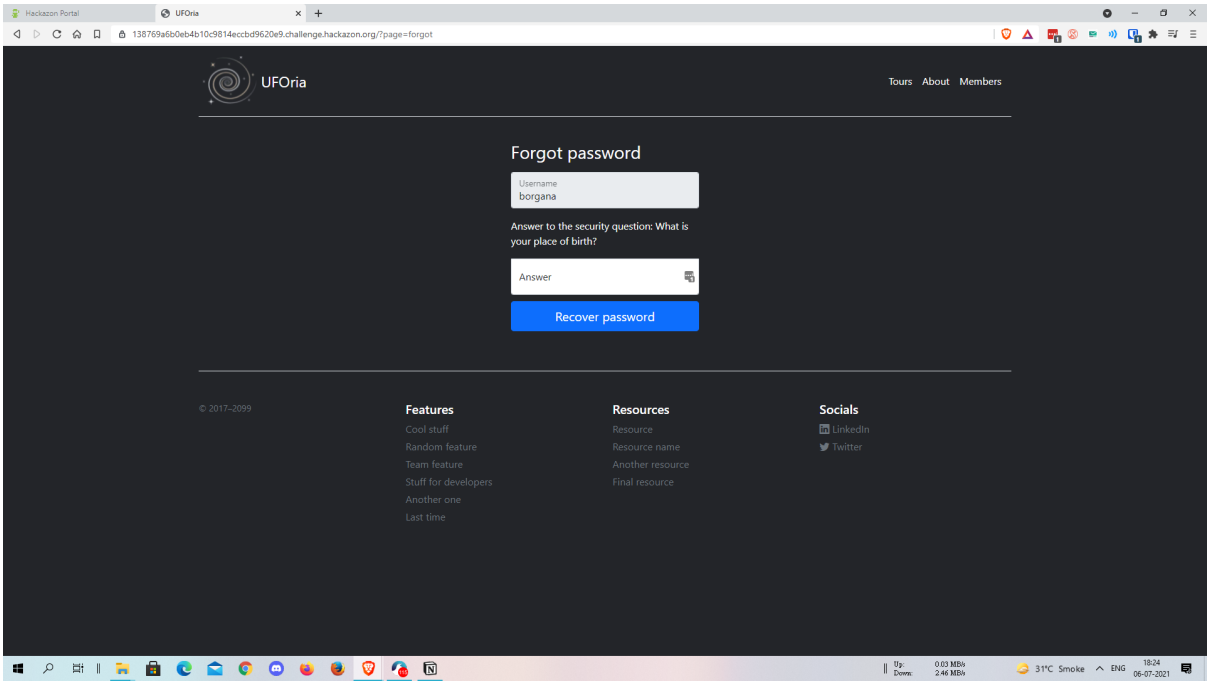
Can you access the members-only area?



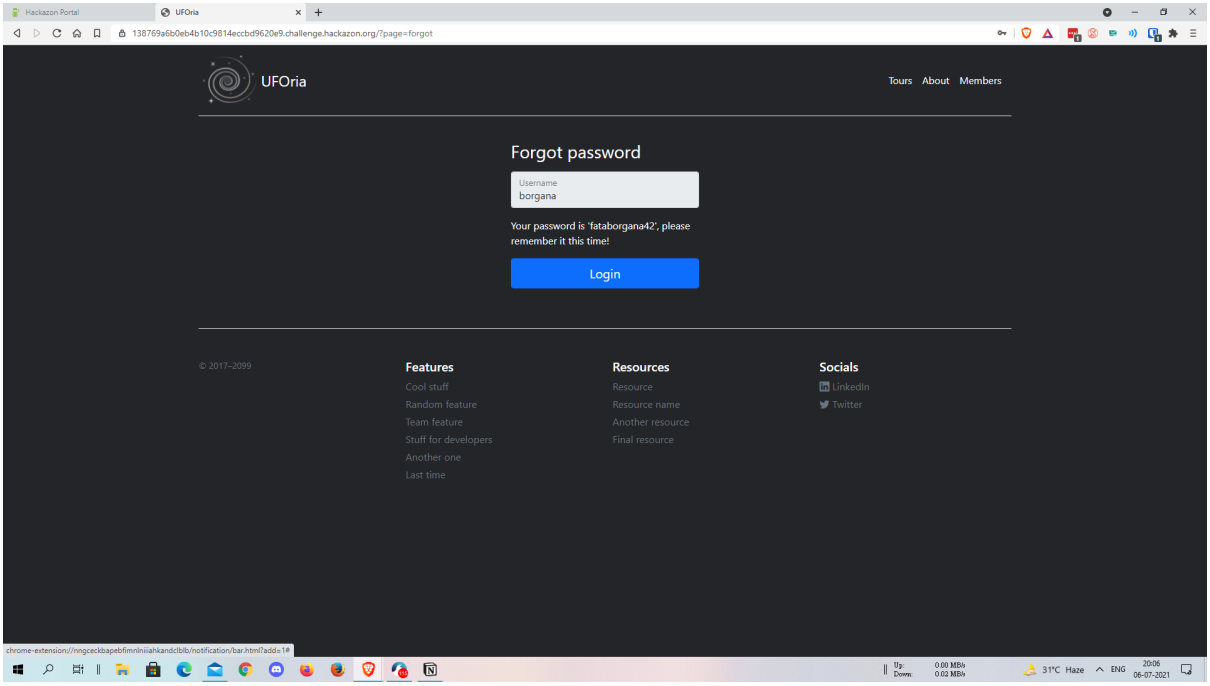
- The second challenge tells us to access the members only area, to access it we have to have an account whose username and password we can use to access the area.

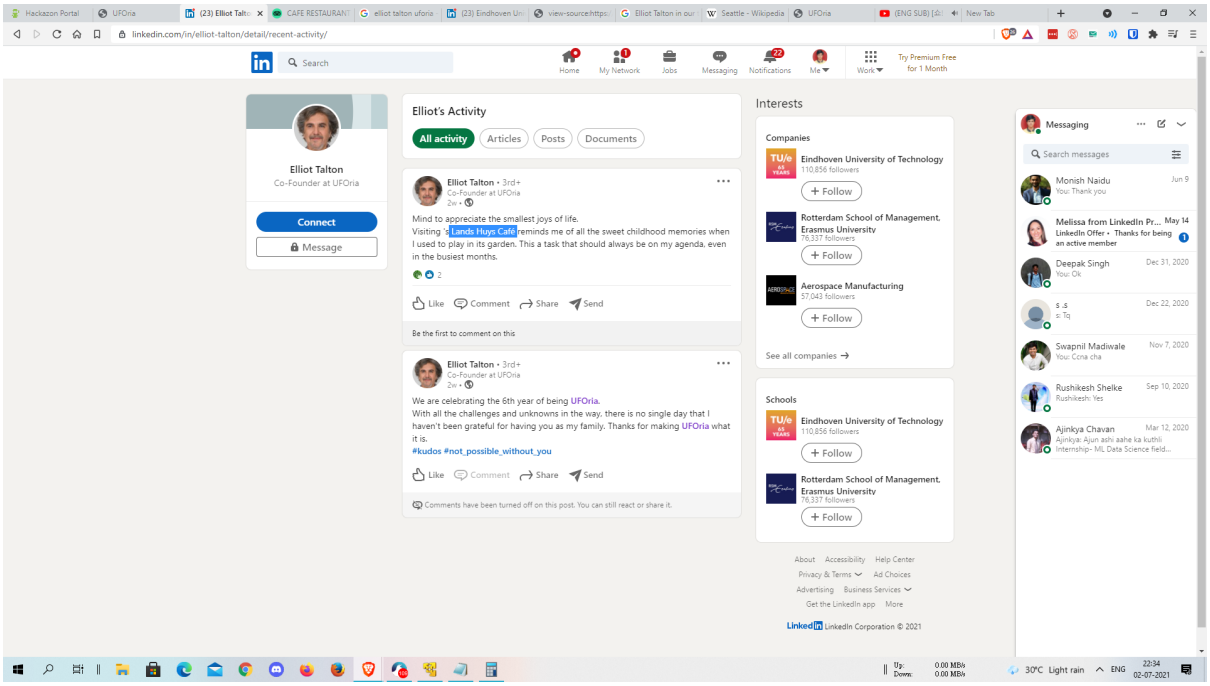


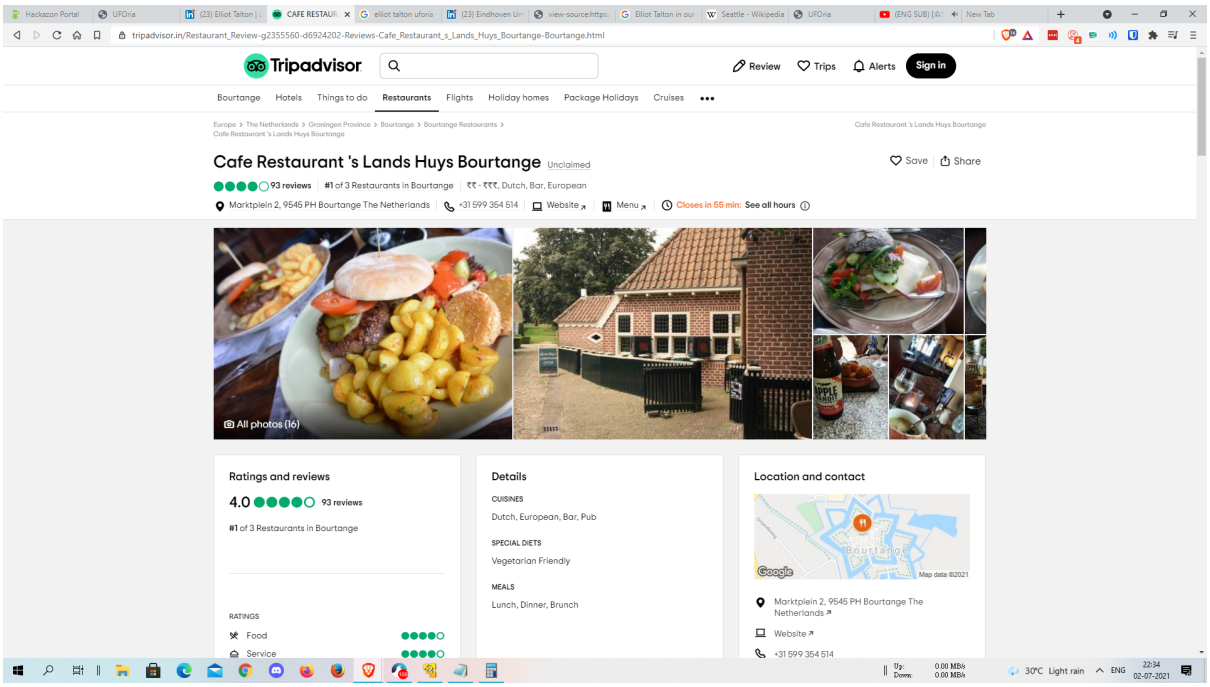
- My first thought was to fuzz the endpoint to find out the register or signup portal which I can use to register my account, but I was unable to find any such endpoint. So I concluded that we are unable to register on the site, so we have to find a valid username and password for some existing members.
- On some research on the, I found out that the about page has Information about the CEO of UFOria Ben organa (aka borgana), so tired borgana as the username for the login page since I didn't know the password for it so I tried forgot password using the same username and found out that it was valid as the page prompted me to enter birthplace as a security question for the username.



- Now after reading the description about the CEO and fuzzing the social media link I found out that his friend "Elliot Talton"(Who is cofounder of the company) and he had a trip to his home town and when they had founded their company. so tried to search his friend's name on all the social media platforms and found Elliot Talton's profile on Linkedin where he had a post that he visited a cafe name laLands Huys Café so searched that cafe on the web and found out that it is located in Bourtange when entered this as birthplace it accepted this and gave me the password for the account, when I entered this password I was presented with the flag.







- Flag2 :- CTF{fataborgana42}