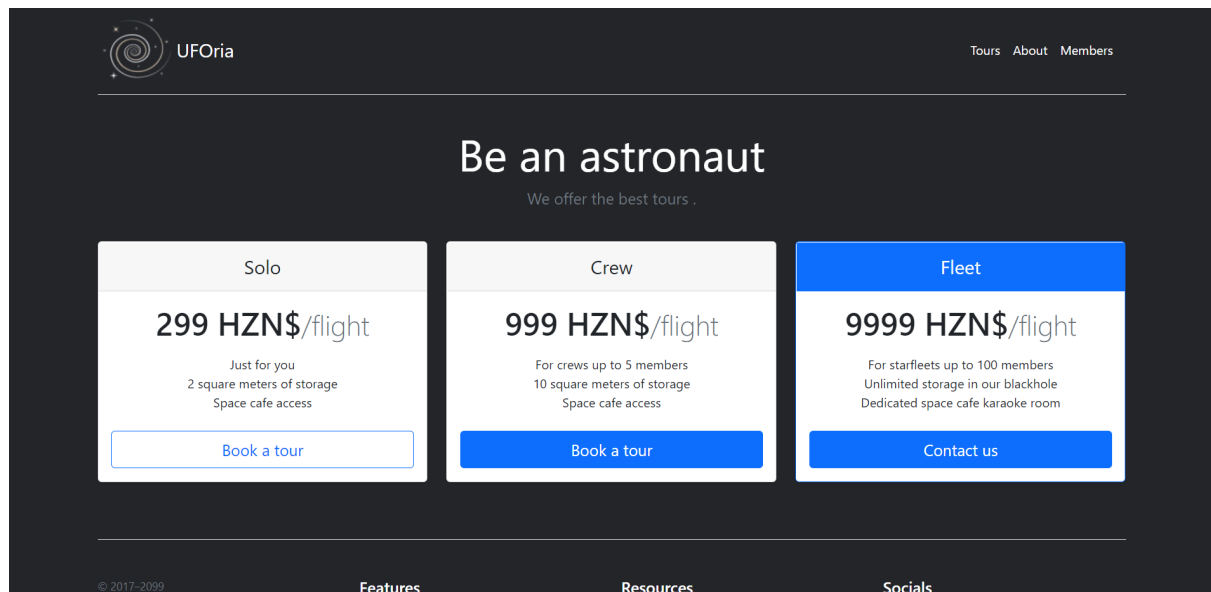# 🛸

UFOria

≡ Tags | osint | web
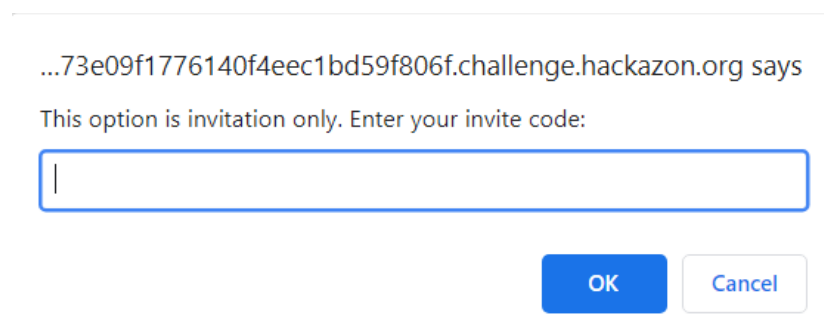
Part 1.

Invite only

[75 points]

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

Firing up the webpage, it looks like this.

I started to the click the "Book a tour" buttons, Nothing happens. Ok, lets click on the contact us button.

So I need to work out the code, this is meant to be an easy challenge after all. Lets see if it is in the source code....

Alas not. But there is this in the source code

```
<script>
    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.")
        }
    }
</script>
```

So the invite code is generated from this code. Lets take it apart.

if code.length does not (! =) equal 12. So we know that the code needs to be 12 characters long.

parts = code.substr... This breaks a string in to multiple parts.

0,3 4,4 and 9,3 The first number is starting location, assuming that the string has an index of 0 and the second is how far along to take it. So we have characters 0-3, 4 - 8, 9-12.

parts.join("-") this means that between each of the different "parts" there will be a - symbol

So at this point we know that the code will look like this

```
XXX-XXXX-XXX
```

if (parts[0] != "UFO") - So the first part is UFO

if (parts[1] != btoa("UFO")) - btoa.. I am not familar with that command. After a little research this appears to be the command to base64 encode the the letters UFO. Resulting in VUZP

if (parts[2] != ("UFO".charCodeAt(0) + "UFO".charCodeAt(1) + "UFO".charCodeAt(2))) - Again, after research in to charCodeAt, it is a function within JavaScript that converts characters into their ASCII decimal counterparts.

A table of the codes can be found at

JavaScript Character Table Generater
https://net-comber.com/charset.html

U charCodeAt = 119

F charCodeAt = 102

O charCodeAt = 111

Combine the total and you get 332

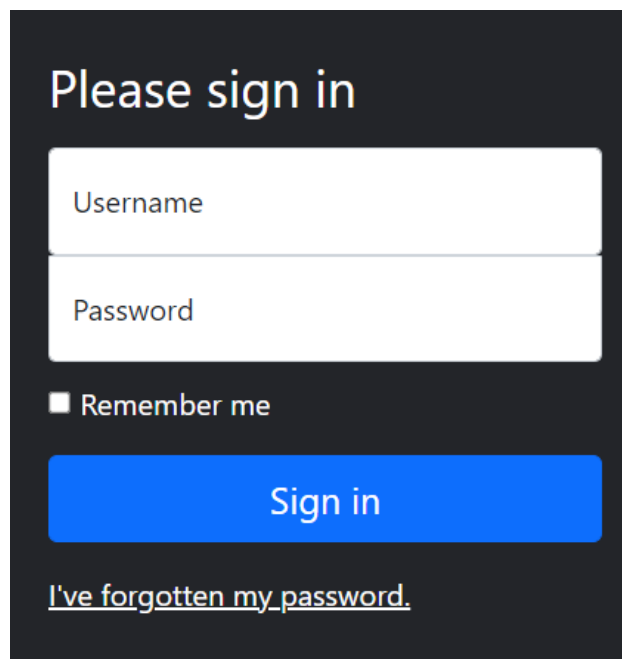So the final answer is UFO-VULP-332

Part 2.

Members only

[75 points]

Can you access the members-only area?

After I gained the access to the contact area, the rest of the site opened up.

So I went to the login page. Standard affair.

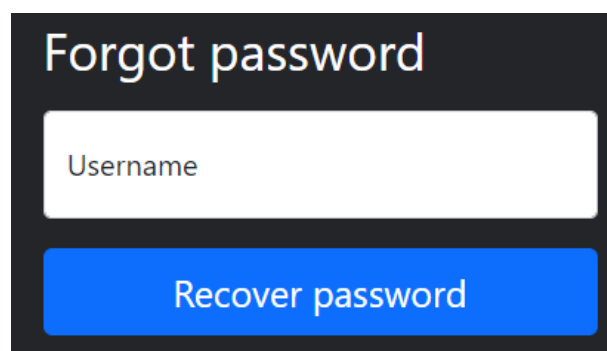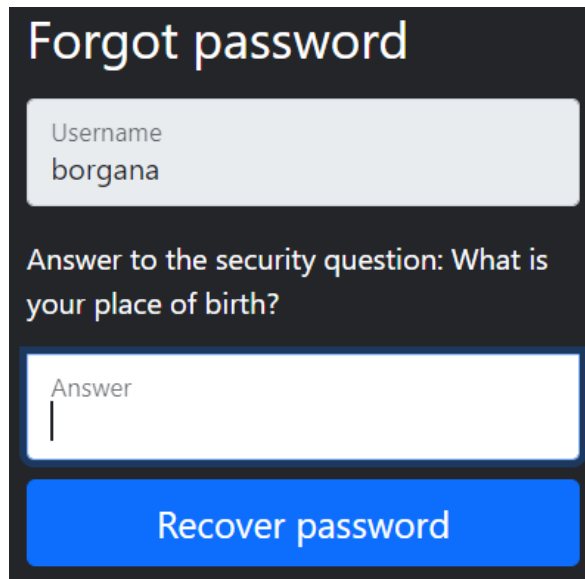But there is a forgotten password option.

Is there a username written on the site that I could use? On the About Us page there was a section titled Word from our CEO – Ben Organa (aka borgana), UFOria CEO.

Thank you Ben, now I have your username. Lets see if that works with the forgot password.
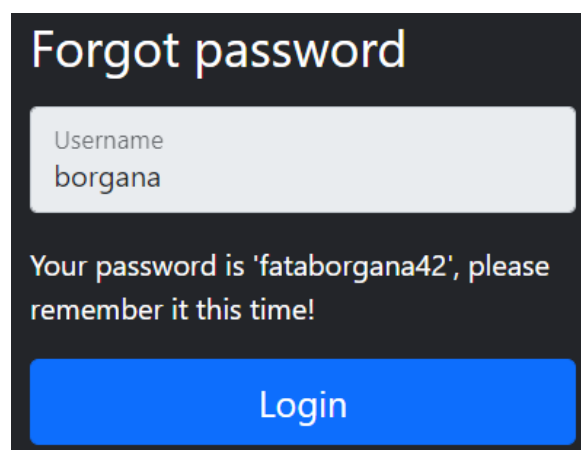
Success! Next job, where was Ben born? The site has links for both LinkedIn and Twitter. The Twitter link comes up with a message about it coming soon. The LinkedIn link goes to the page about UFOria with one member attached. But because this person is not in my network of friends I cant see anything on his profile. So a seemingly dead end. Back on the About Us page, it makes reference to Elliot Talton, a co-founder of site. A quick Google search of Elliot, LinkedIn and UFOria reveals the person that I couldnt link up with earlier. I appear to be on the right track.

I add Elliot to my network then start to look over his profile. His activity has an interesting post.

```
Mind to appreciate the smallest joys of life.
Visiting 's Lands Huys Café reminds me of all the sweet childhood memories
when I used to play in its garden. This a task that should always be on my
agenda, even in the busiest months.
```

Head over to Google Maps and bring up Lands Huys Café in the Netherlands. The Netherlands was plastered all over the UFOria linkedin page. Lands Huys is in a place called Bourtange. Seems like a reasonable guess for the password.

Login success! No member functionality implemented for now :) Have a flag instead: CTF{fataborgana42}

Excellent!