UMassCTF 2024 Holesome Birthday Party Writeup

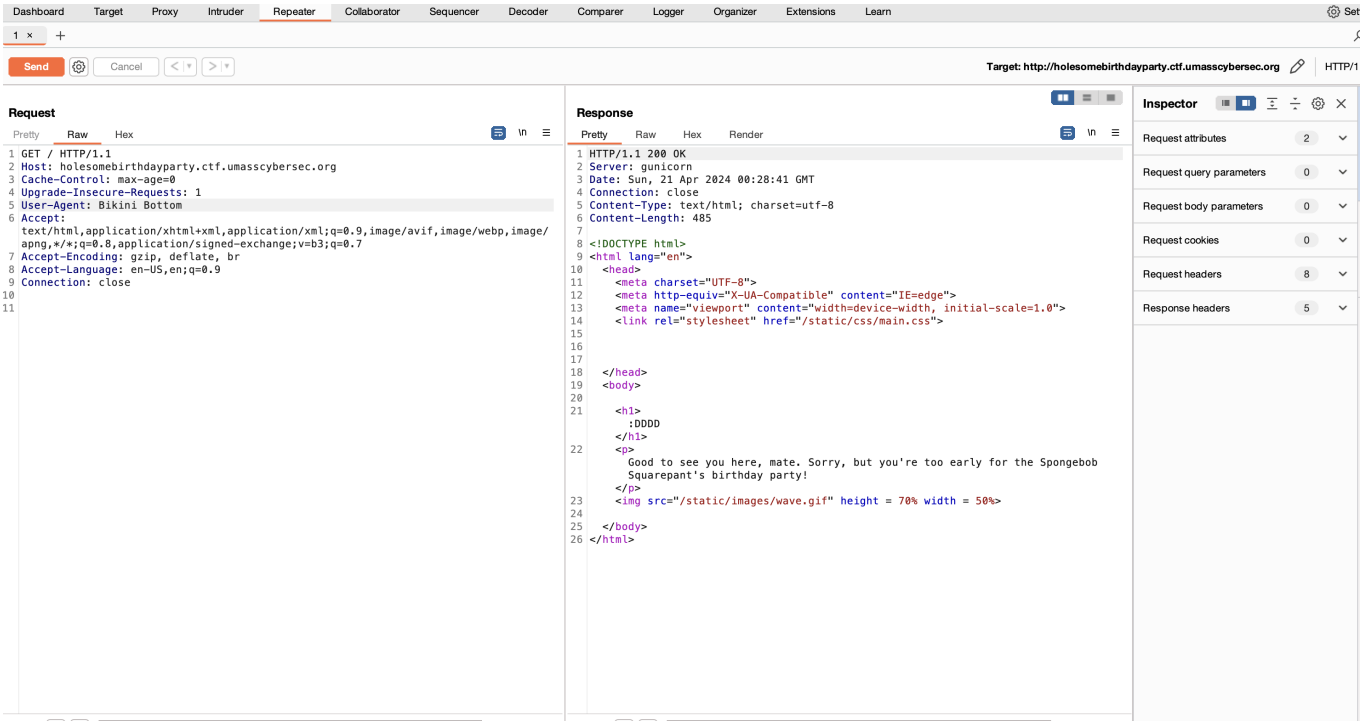
Challenge Description: You just got invited to Spongebob's birthday! But he's decided to test your friendship with a series of challenges before granting you with the ticket of entrance. Can you prove that you're truly his friend and earn your entrance to this holesome birthday party?

Approach

In order to solve this challenge, you can use either `curl` to add in the headers or the recommended tool is `Burp Suite`. This challenge consists of 5 stages.

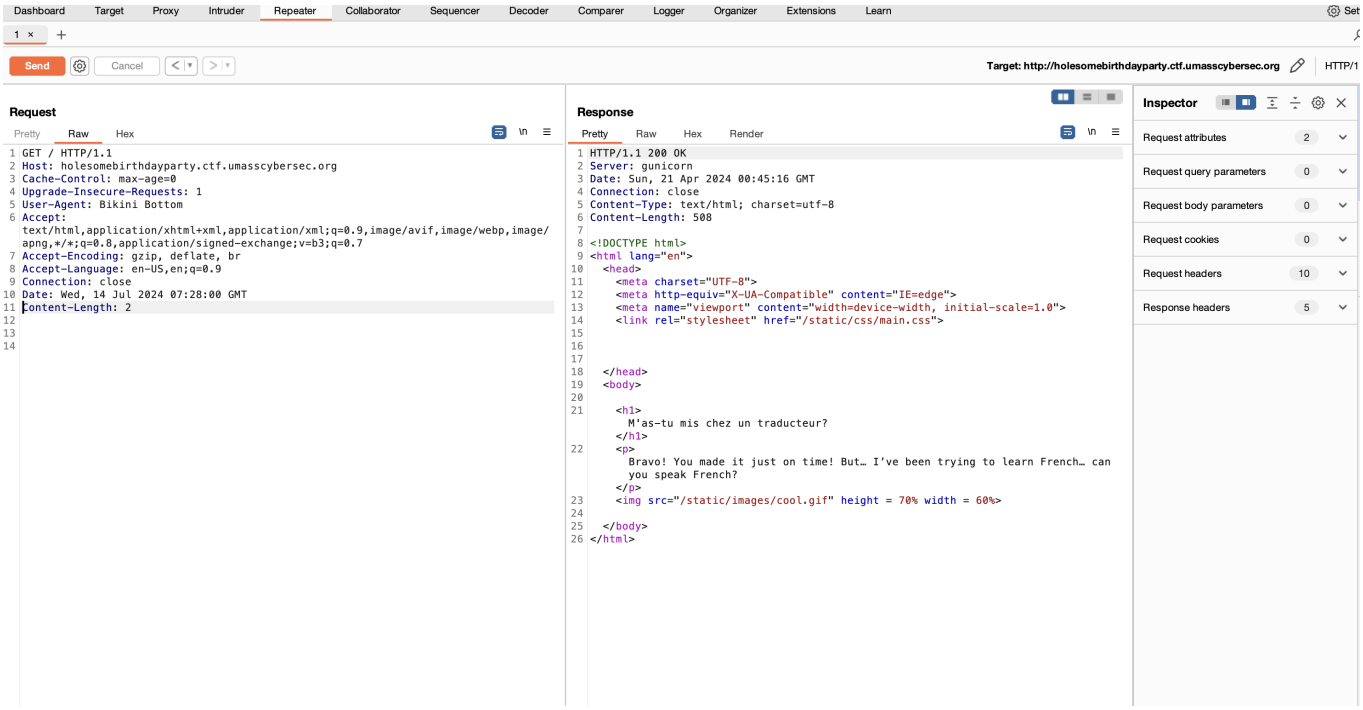
Stage 1

When we first open up the website, we get the message saying that Spongebob wants us to prove that our browser is from "Bikini Bottom". We can intercept the request and send it to the repeater on Burp Suite. Change the user-agent to "Bikini Bottom" returns us the next stage.



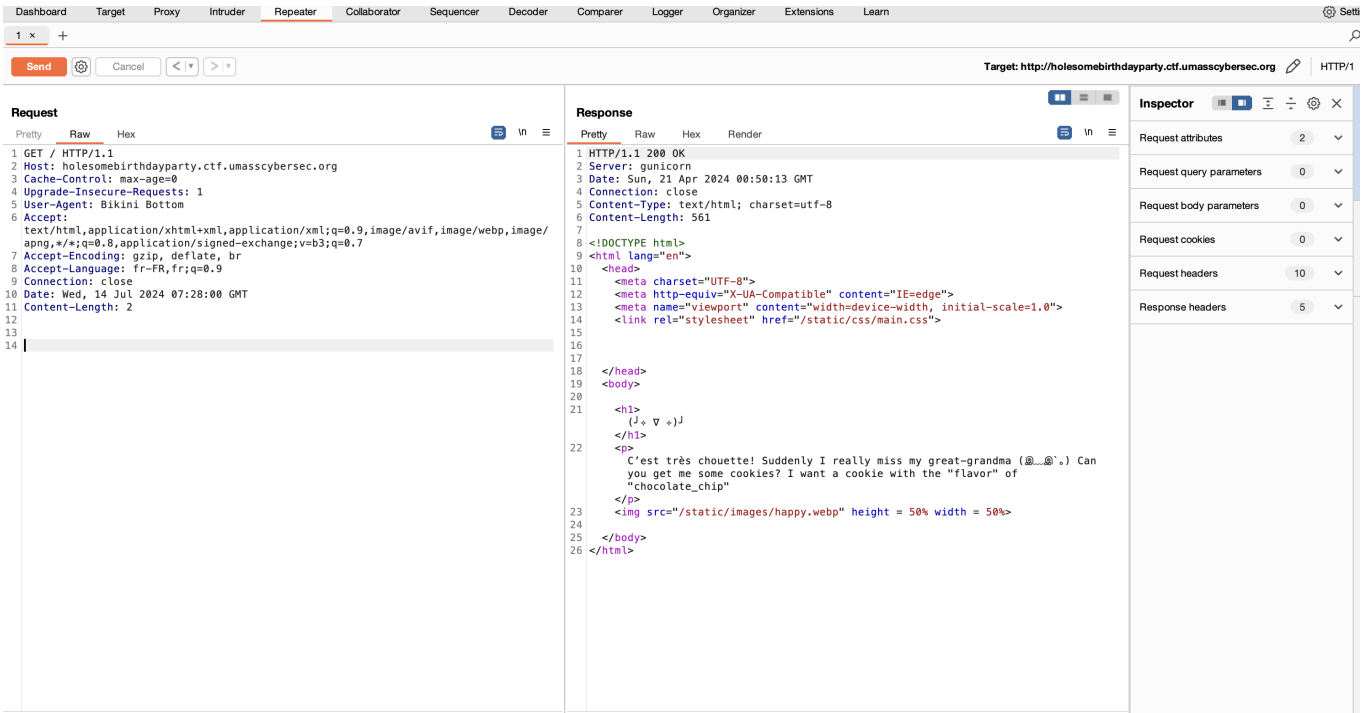
Stage 2

From the message on the web page, we can infer that it wants a `Date` header. Make sure the header is in the correct format `"<day-name>, <day> <month> <year> <hour>:<minute>:<second> GMT"` and change the day month year to `Jul 14 2024`. The day and time does not matter here.



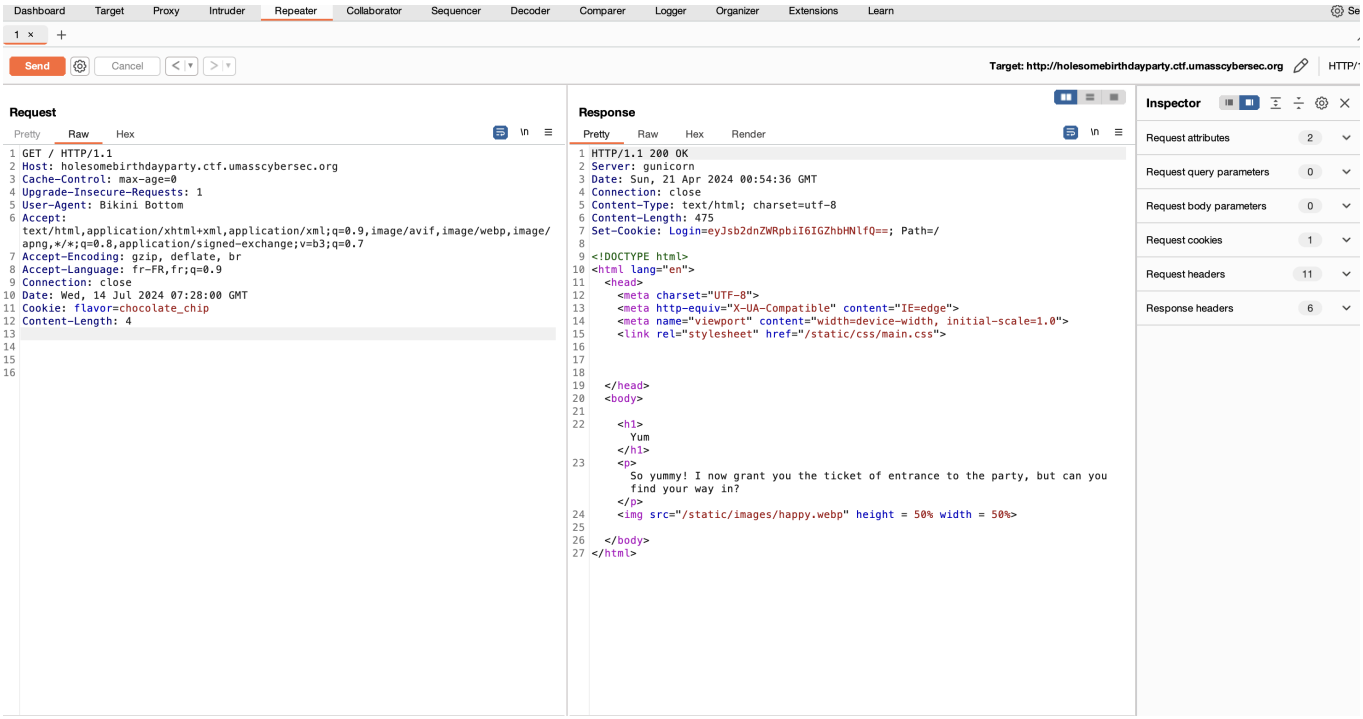
Stage 3

As we advance to the next stage, Spongebob asks if we can speak French. There is an `Accept-Language` header and we want to change it to French. Note that both `fr` and `fr-FR` are acceptable.



Stage 4

The next stage is asking for a cookie with the "flavor" of "chocolate_chip". We need to add a cookie header pair `flavor=chocolate_chip`.



Last Stage

As we proceed to the last stage, we see on the response page intercepted by Burp Suite that there is a cookie pair set by the server. The cookie name is "Login" and the value is base64 encoded. We can highlight the string on Burp Suite and see that it's decoded as `{"loggedin": false}`. Change "false" to "true" and encode it as a base64 string. You can base64 encode this on Burp Suite repeater or use an online encoder. The challenge is now completed.