# Lab Name: - OTP Bypass using Response Manipulation in BurpSuite

The goal is to exploit the website by bypassing the security mechanism.

Whenever we create a new account, we have to enter our number and Email for verification.

And we get OTP on the number or email. But we can bypass this security mechanism using Response manipulator using burpsuite.

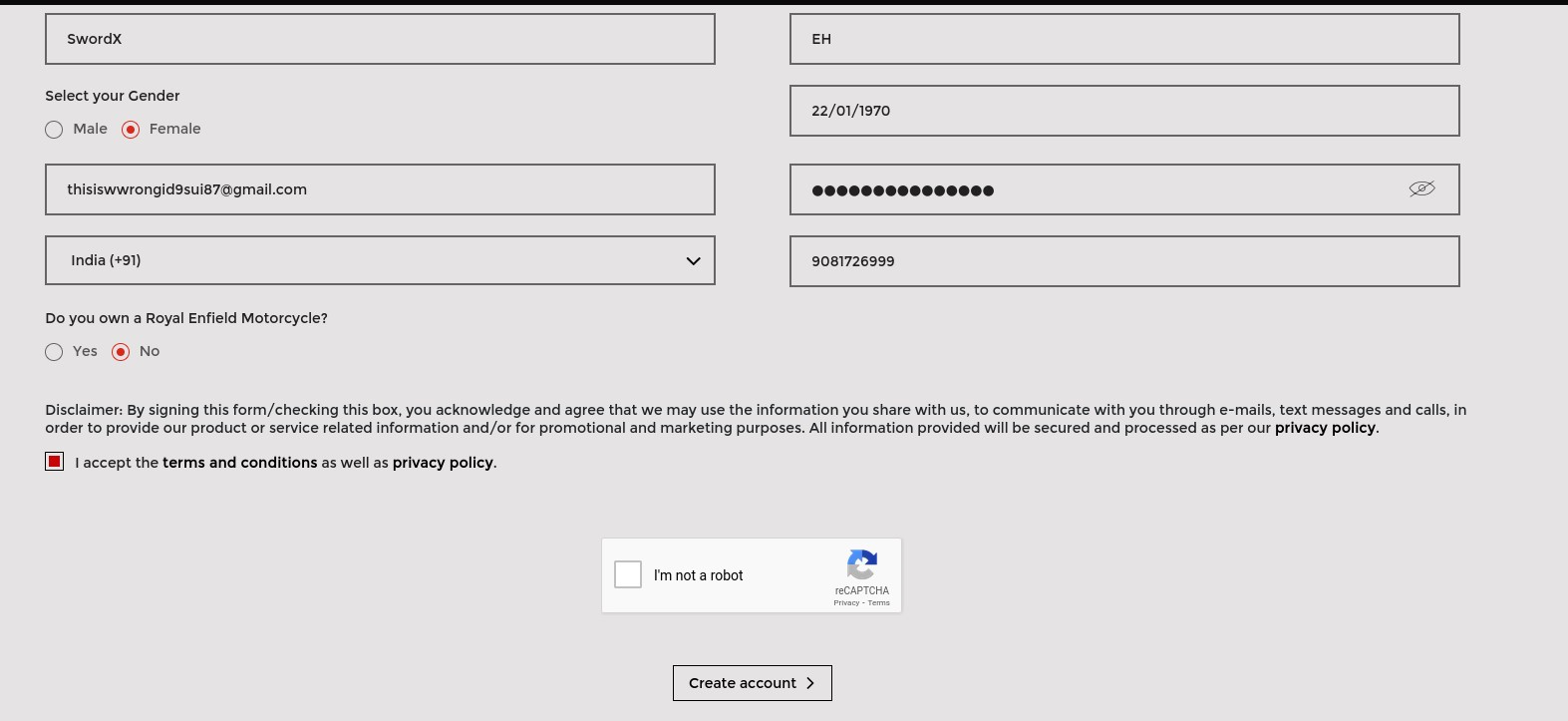
To solve the lab, we will use Burpsuite

Make sure the interceptor and the BURP proxy is on.

My target is <https://www.royalenfield.com/sg/en/home/>

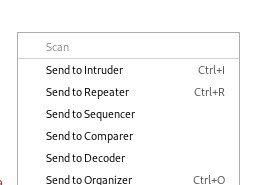
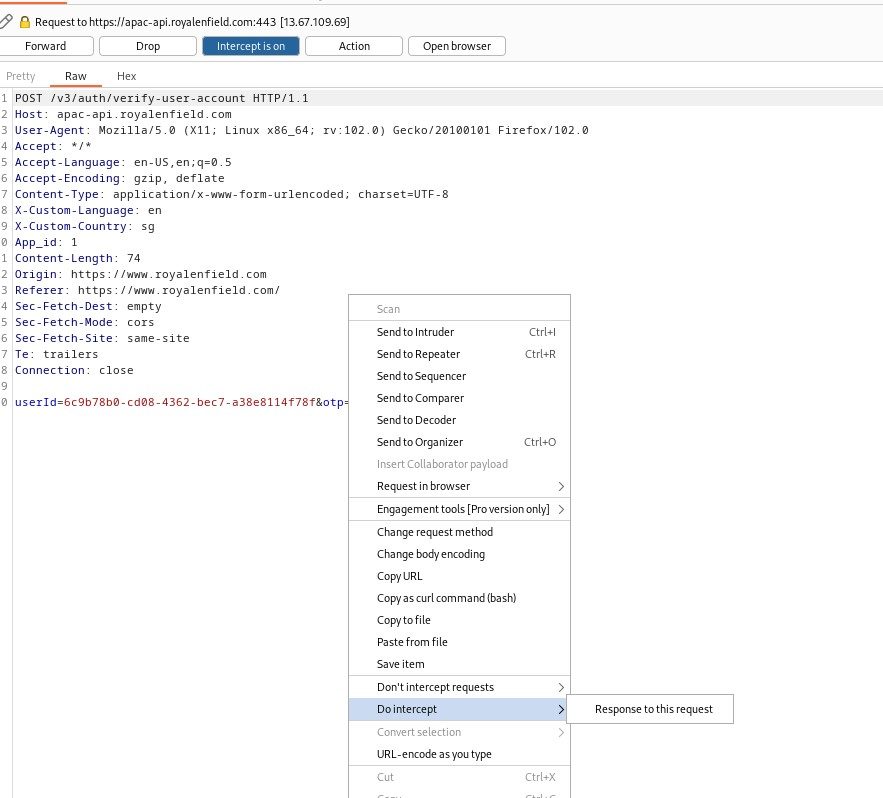
First we have to create a new account on the website.

I have create the account and for security purpose I have used a fake Email ID and fake number.



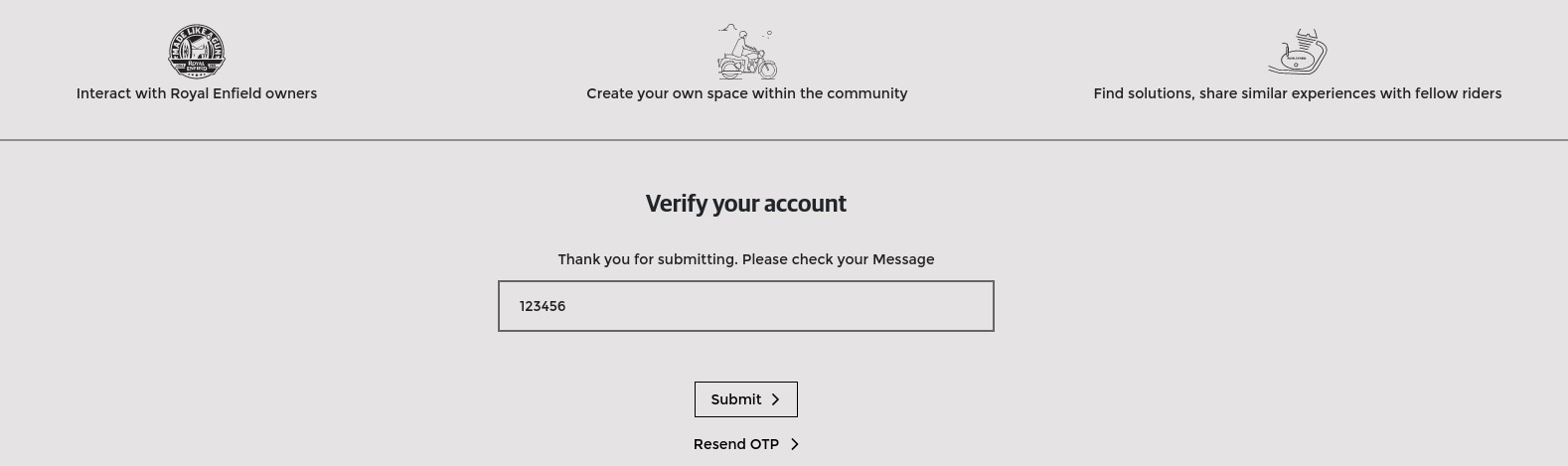
I will click on create account.

In Burpsuite I’ll get on this page because my intercept is on. I’ll click on do intercept and then response to this request.



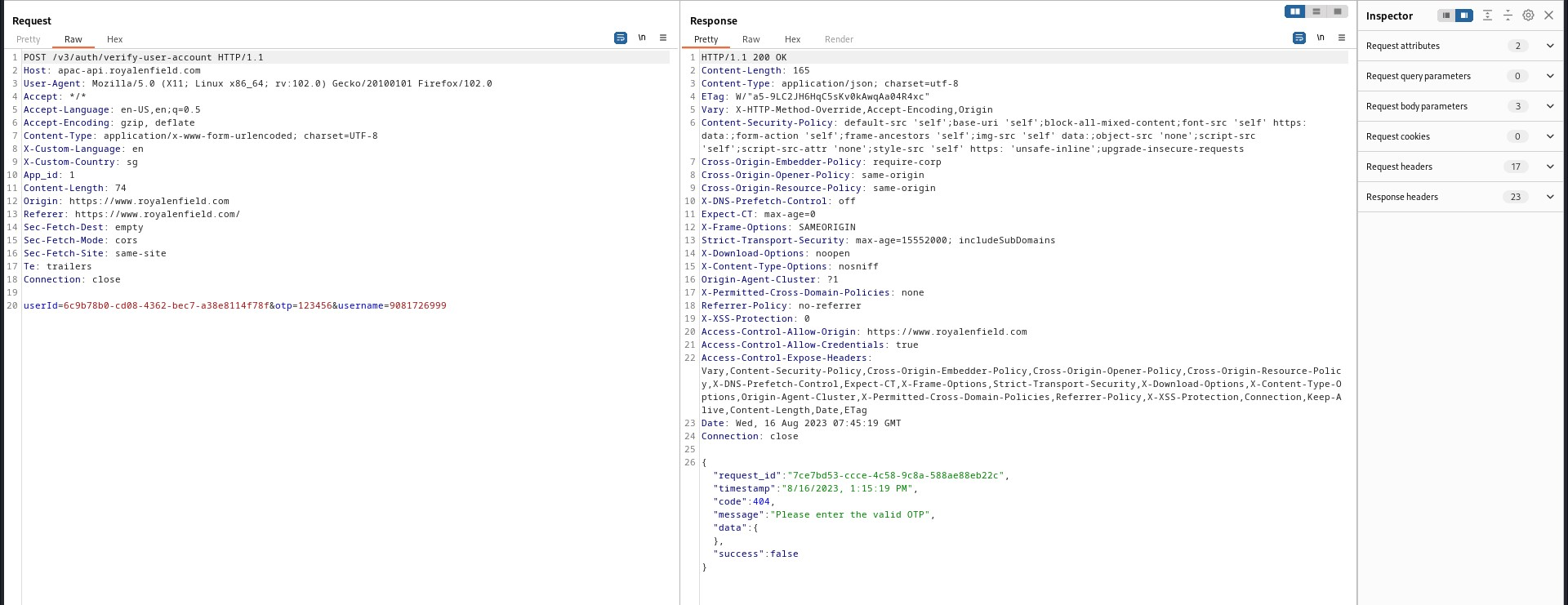
And then click on Forward till it no longer intercept the request.

I will put 123456 and click on submit.



Now the interceptor will intercept the request.

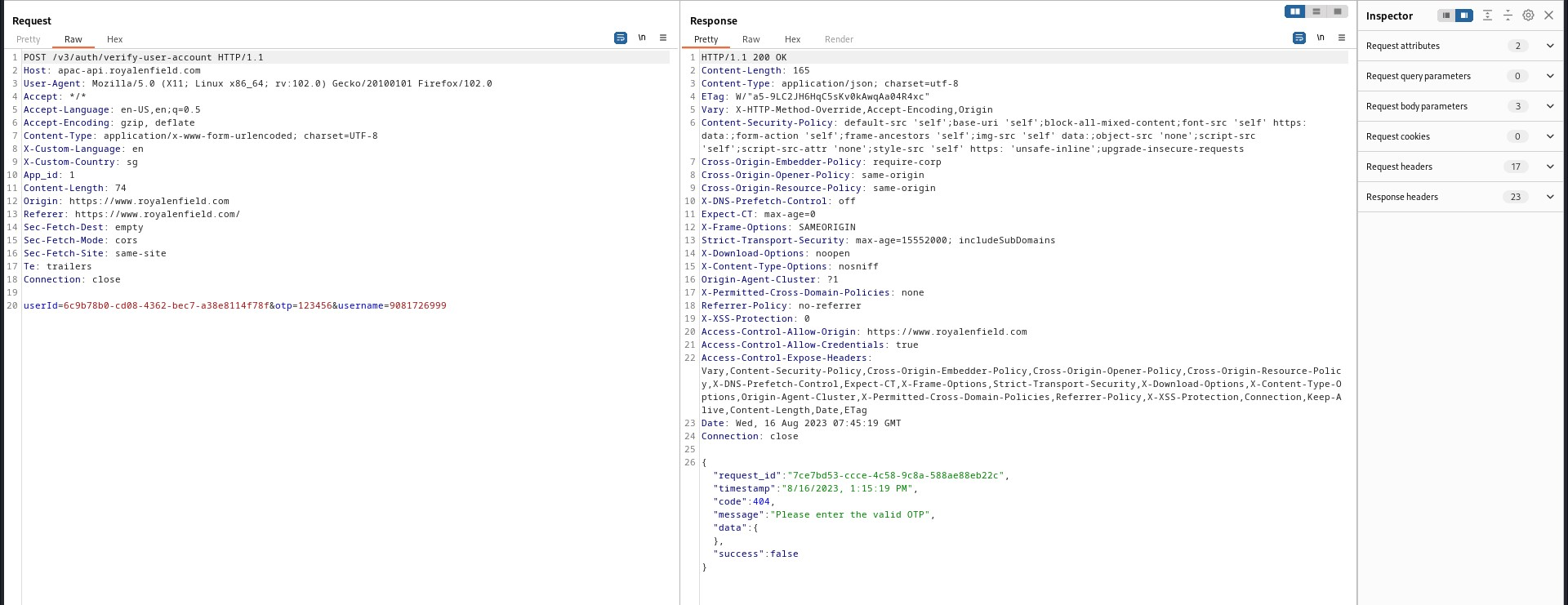
I’ll forward the request till I get on the page with OTP present.



I’ll click on do intercept and then response to this request.

And I’ll send this request to repeater.

Repeater will send a copy my request and get the response.

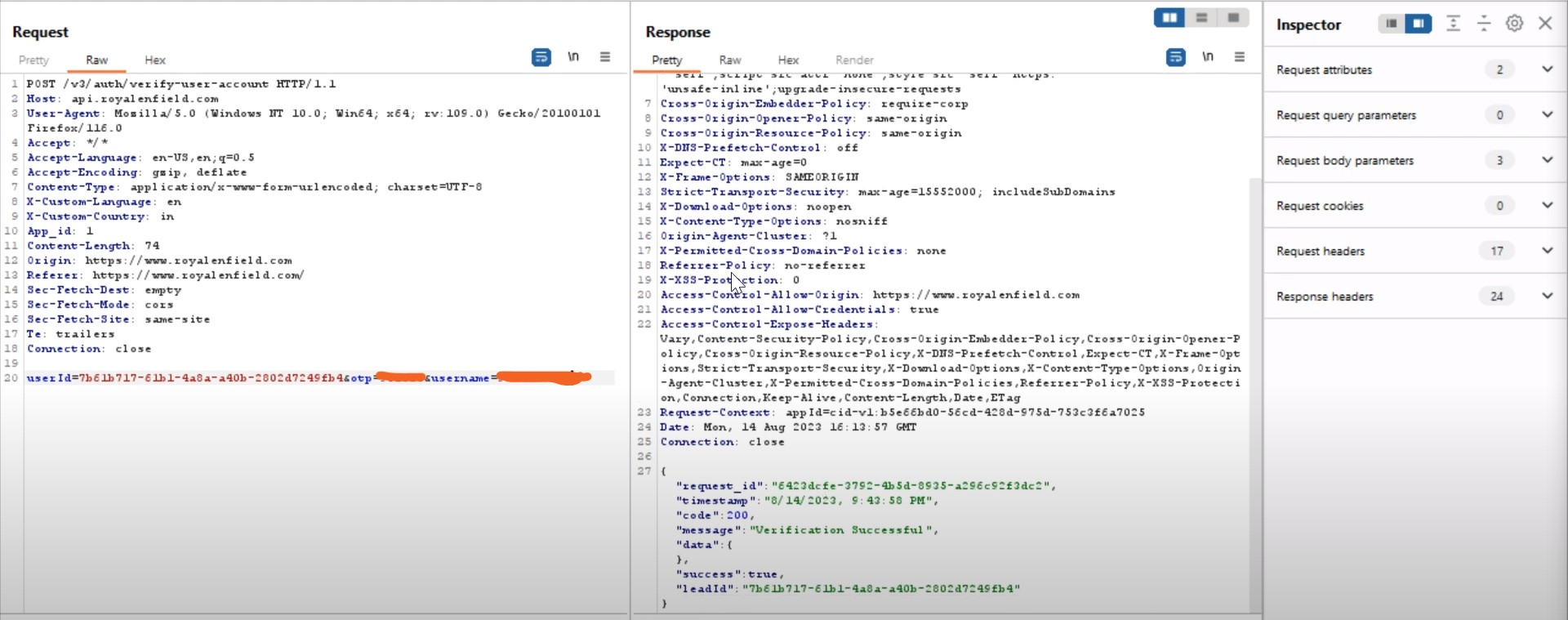


Now we will get a response like this.

**This is a response for the wrong OTP.**

**Now I’ll repeat the same process and I’ll enter my real mobile number and with real OTP.**

**And I got this response for the right OTP.**



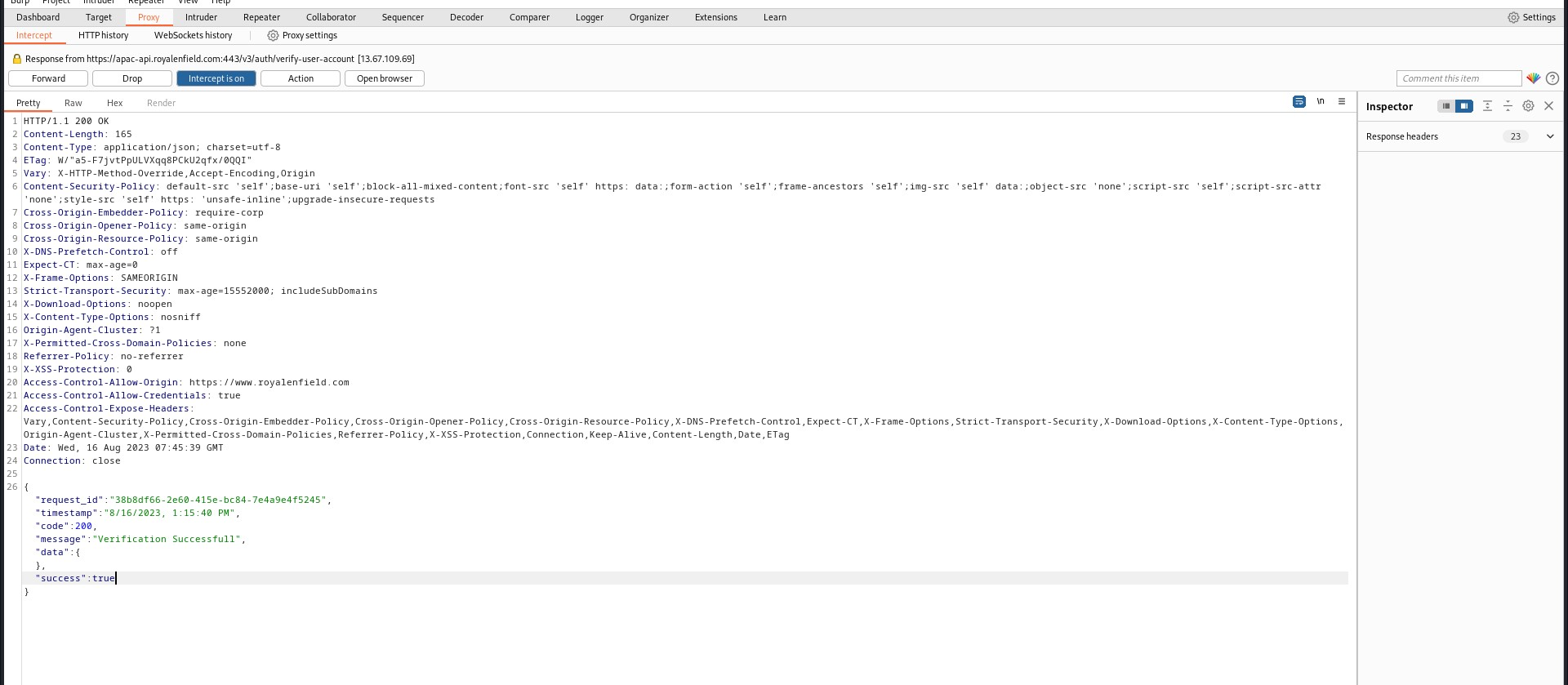
**Now we will go back to our wrong OTP proxy.**

And we will forward the request. Till will get to the page where we got the message to enter right OTP.



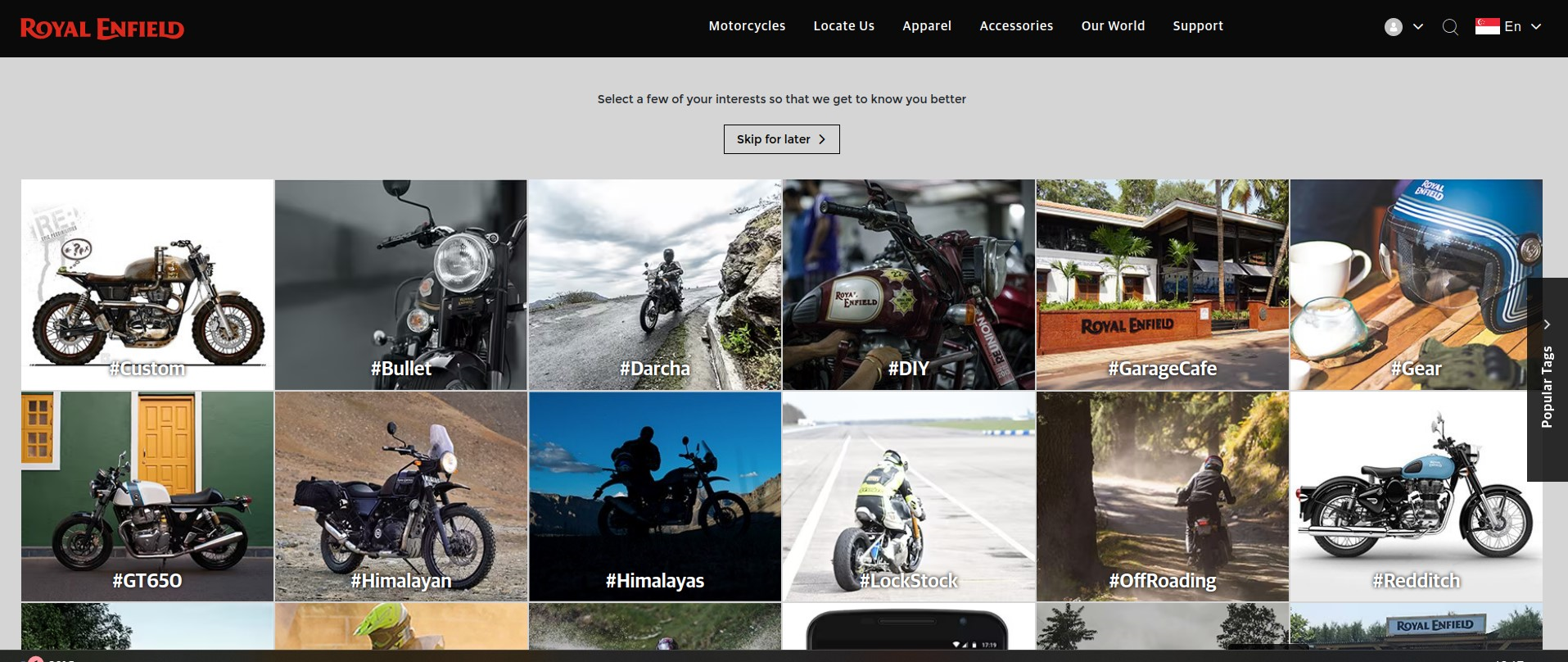
And now we will change the output of this wrong OTP to the output of the right OTP.

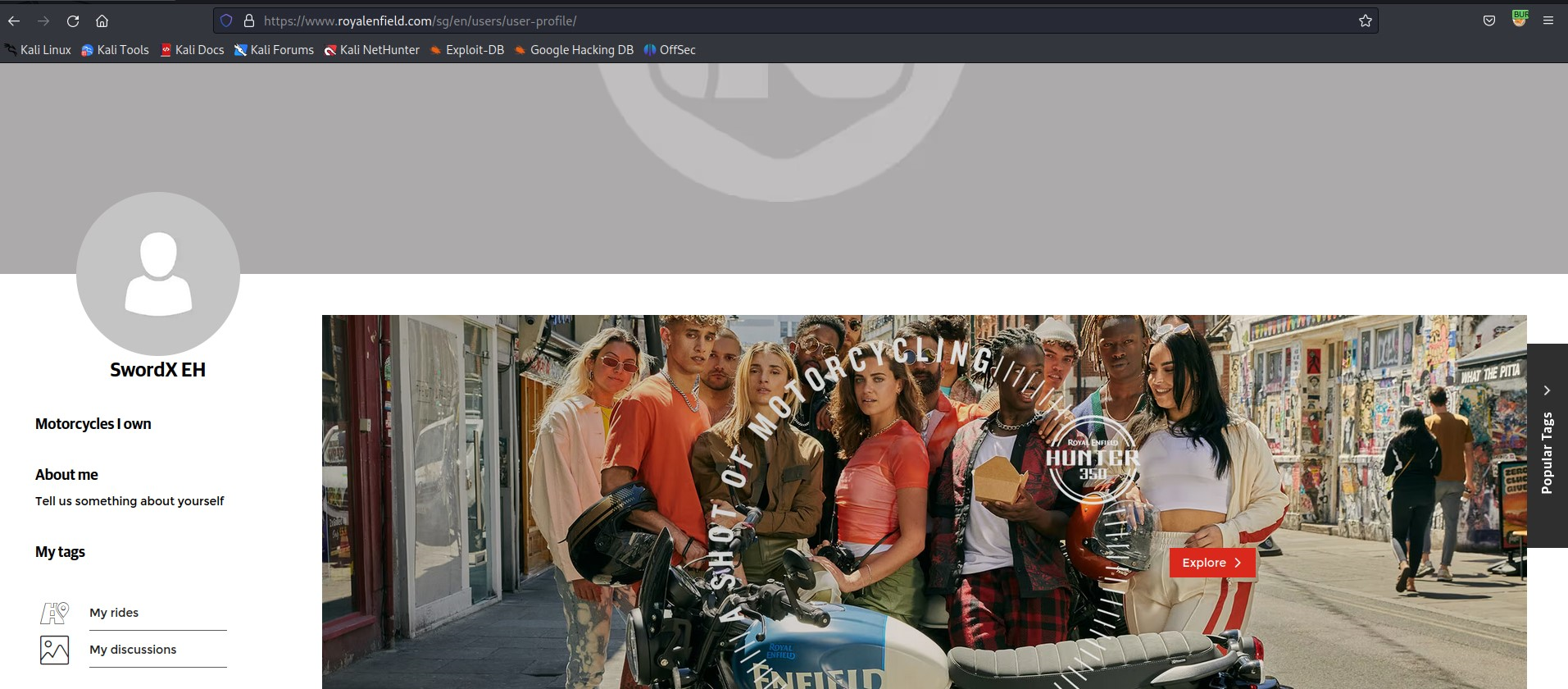
I have change code, Message and success.



And now I’ll forward the proxy. And I’ll keep on forwarding till it no longer intercept i.e., request is complete.

Now if we go back to the website using our browser. It will be logged in.





As we saw I have used wrong number and wrong OTP and still get to logged in.

We just have to change the response of wrong OTP similar to right OTP.

**The lab is solved.**