# Lab Name: - OTP Cracking using Brute Force Attack in BurpSuite

The goal is to exploit the website by cracking 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 crack this security mechanism using Brute Force Attack using burpsuite.

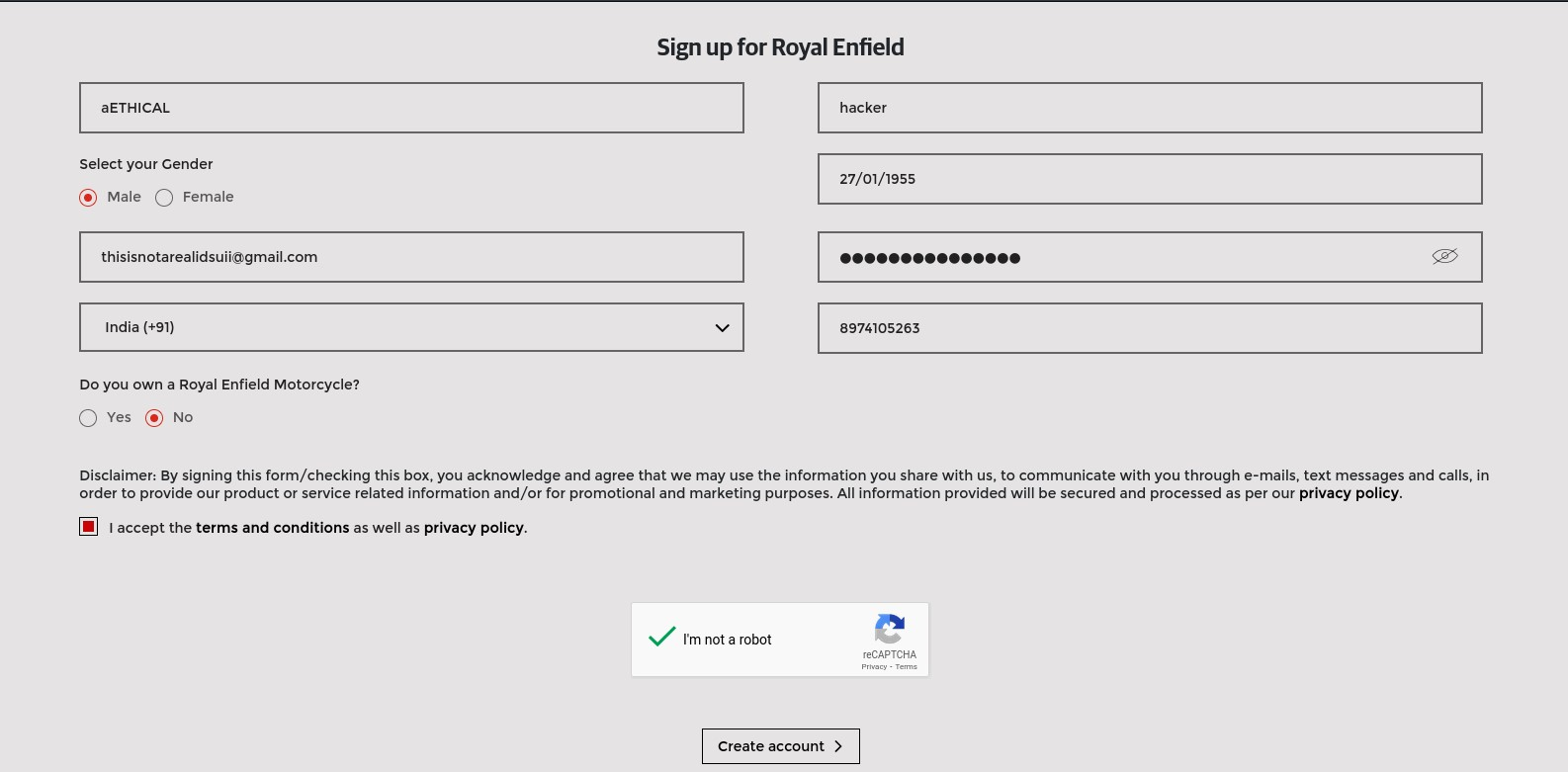
To solve the lab, we will use Burpsuite

Make sure the interceptor and the BURP proxy is on.

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

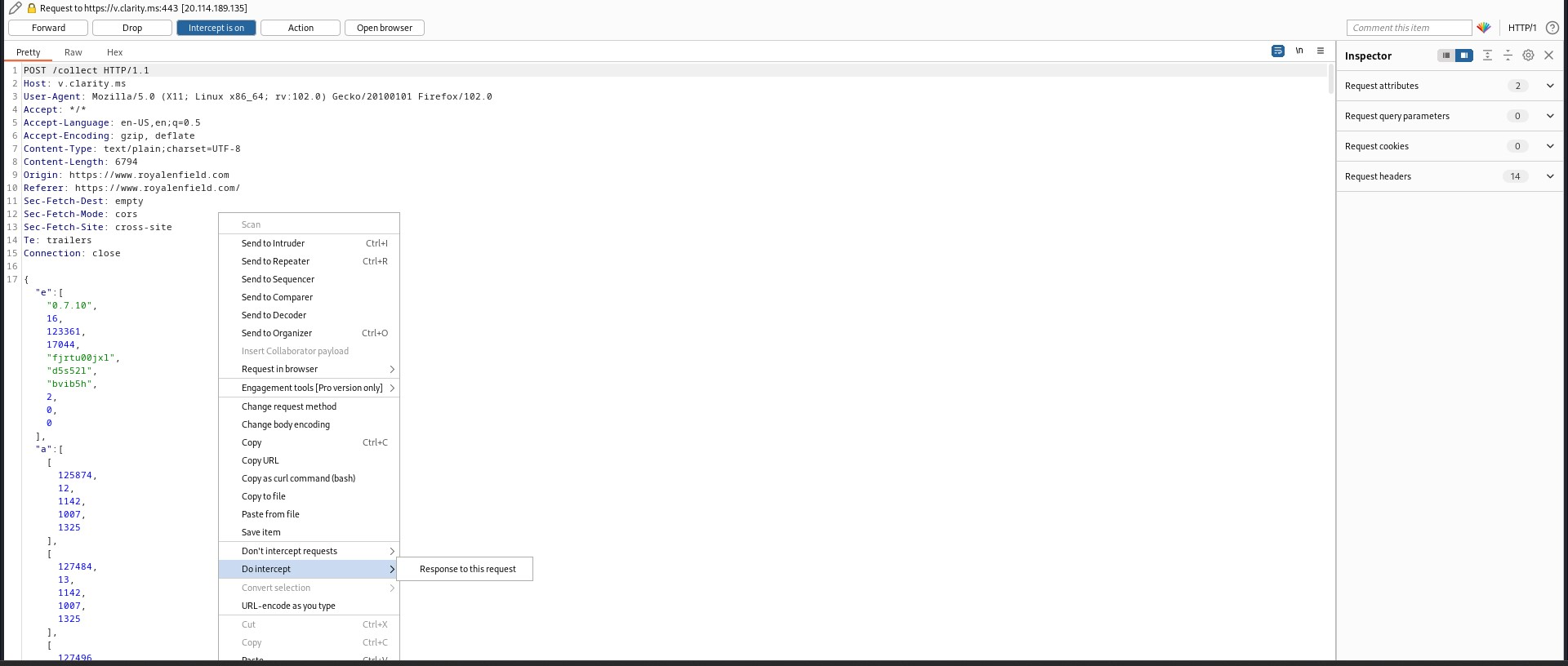
First we have to create a new account on the website.

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



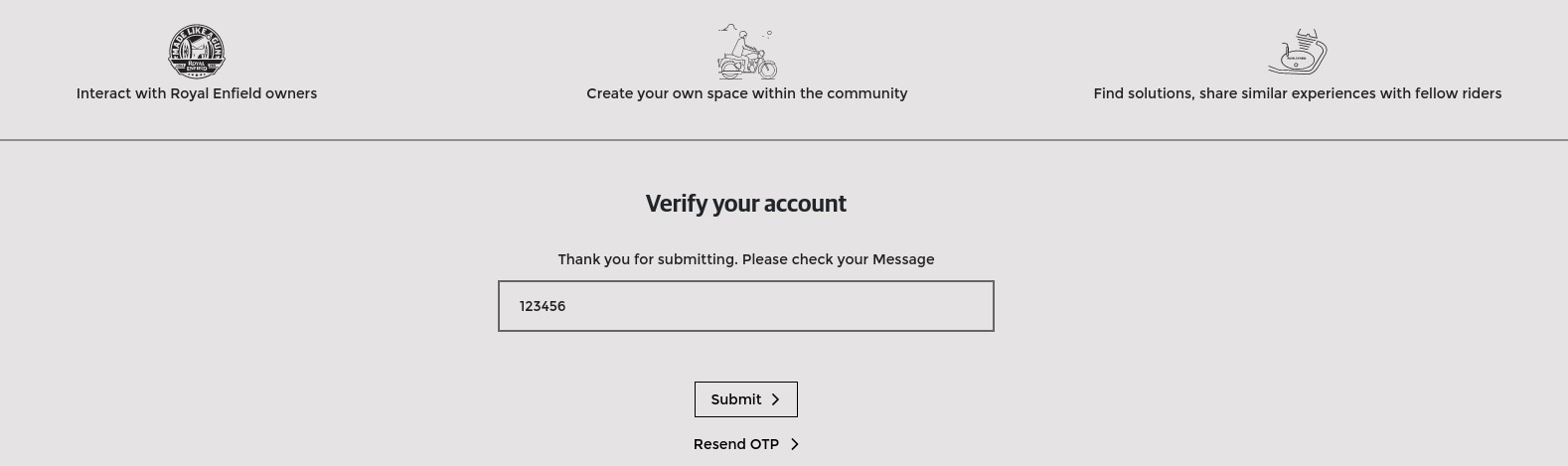
I will click on create account.

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.



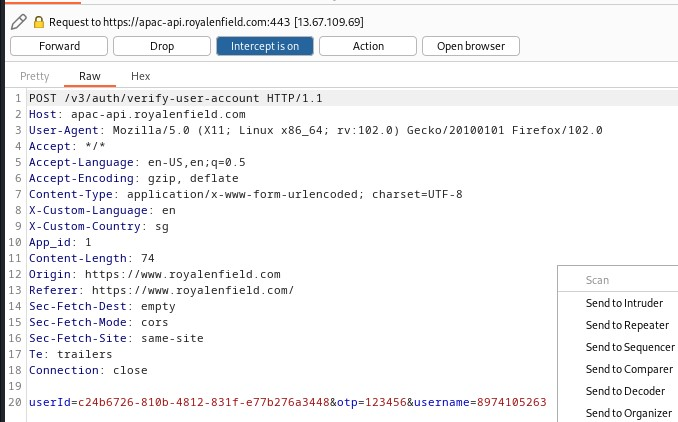
And then click on Forward till it no longer intercept the request.

I will put 123456 and click on submit.



Now the interceptor will intercept the request.

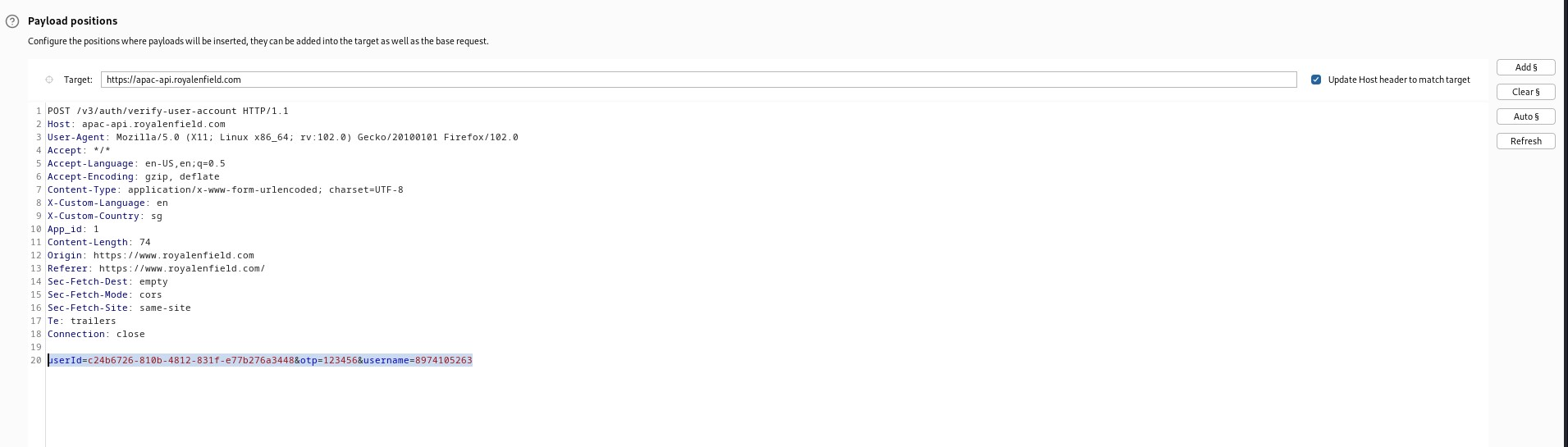
I’ll forward the request till I get on the page with OTP present.



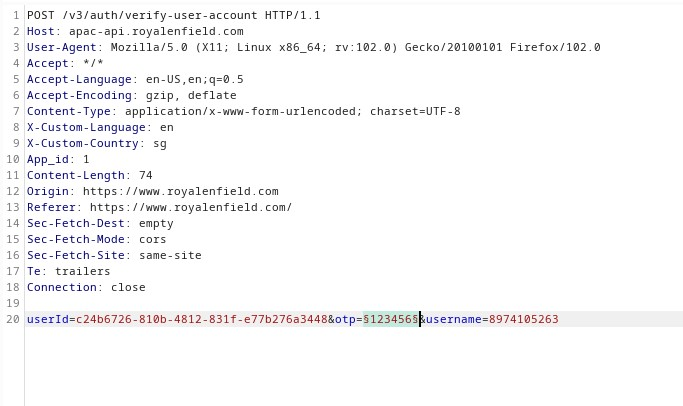
I’ll click on do intercept and then response to this request.

And I’ll send this request to Intruder.

Intruder enables you to insert payloads into defined positions in an HTTP request, then send each version of the request to the target server.



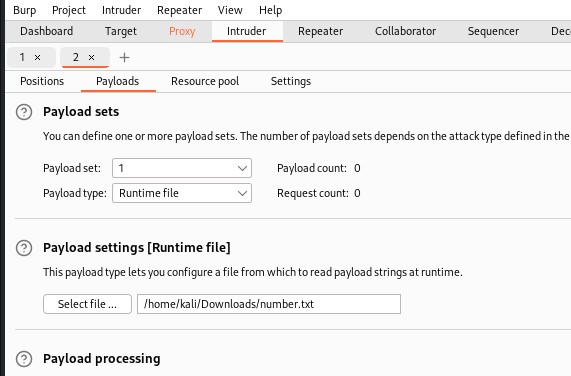
Then I’ll add a payload position on the 6-digit OTP.



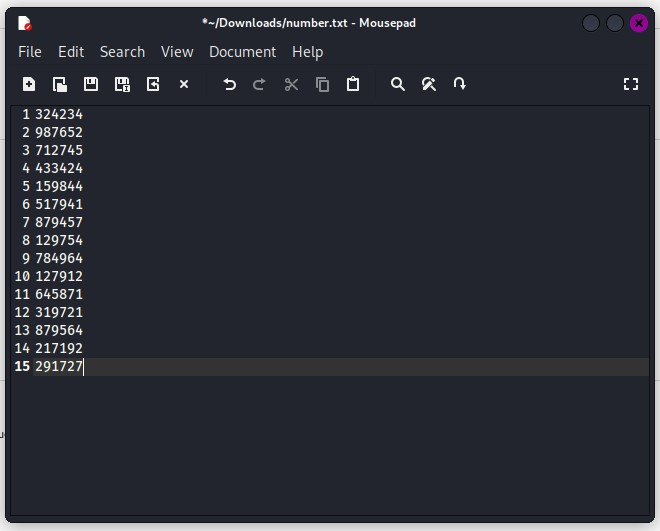
Now, we have to insert a payload.

I’ll use Sniper Attack. Sniper attack places each payload into each payload position in turn. It uses a single payload set.

In payload type I’ll use Runtime file.



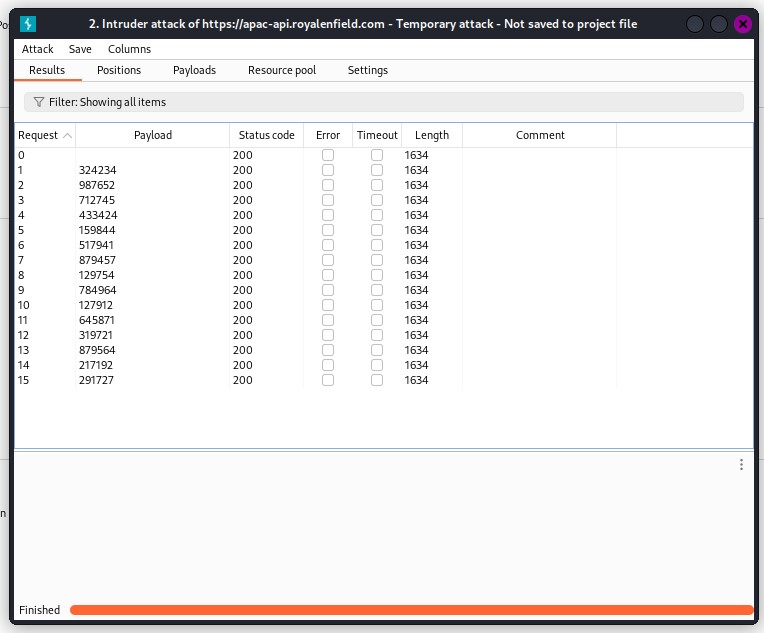
I have created a file named number.txt



The OTP is of 6 digits. So, this file should have every number starting from 111111 to 999999.

But I have entered only 15 random number.

Then we will start the Attack.



Here, we see all the numbers have status code as 200. So they are not our OTP.

The real OTP will have Status Code as 500 and the length of the real OTP will be different from the rest.

So whichever number have Status code as 500 and length different from other is our OTP.

This method works when we have OTP expiration time more than 15 minutes. Brute Force attack takes time and in between the attack OTP should not get expire.

**Find the different number and the lab will be solved.**