OTP BYPASS

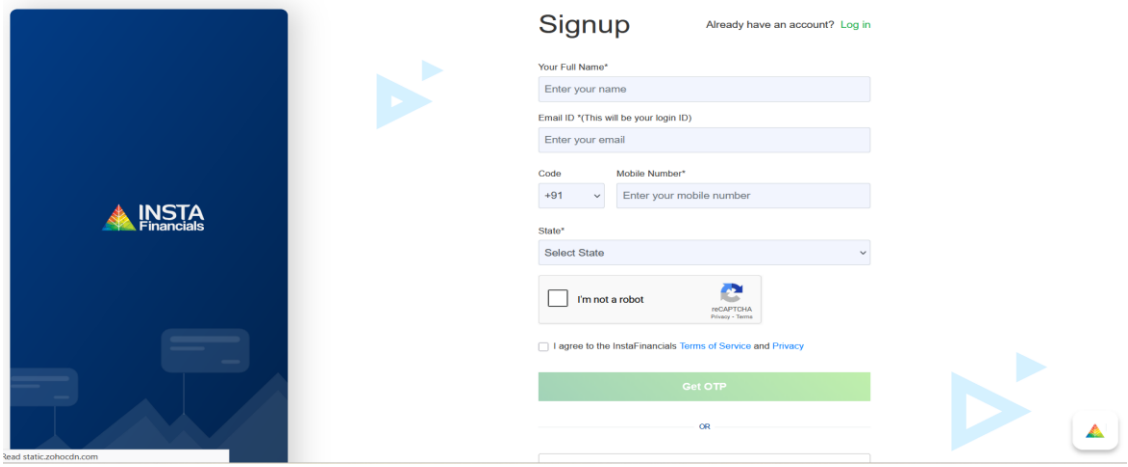
1. Website: - Insta Financial

This project focuses on identifying and preventing OTP bypass vulnerabilities in financial web applications through controlled and authorized testing environments.

Steps 1 Open https://www.instafinancials.com/Signup

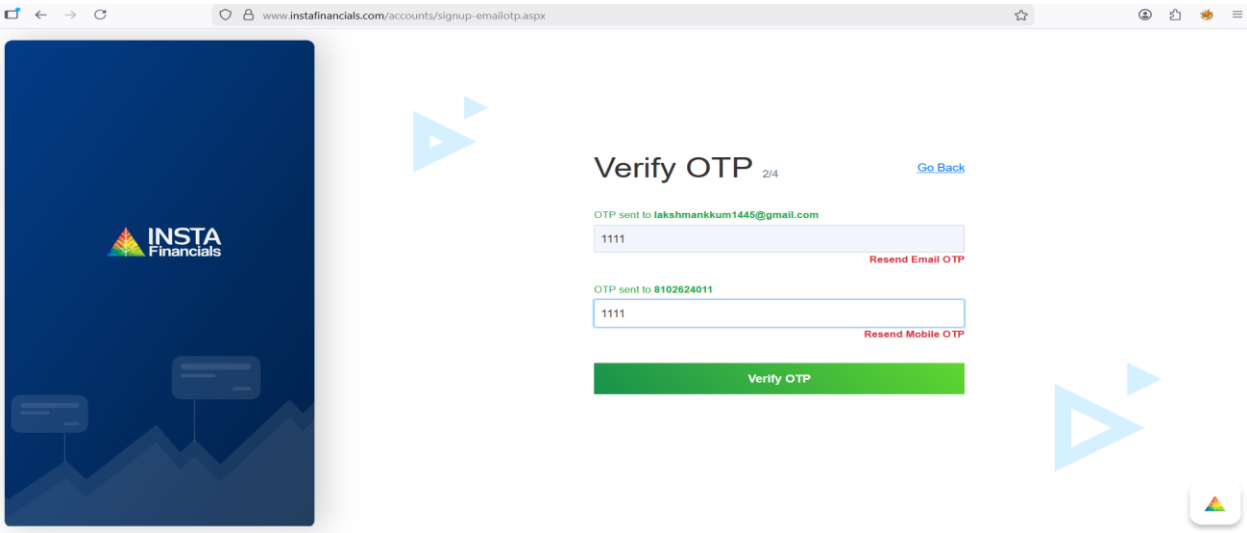
Step 2 Fill out the details on the website like (Name, Email, phone no. etc.)

Step 3 clicks the login button and enters the credential



Step 4 After filling in all the details when we give the request to the server to get OTP it shown the interface and we enter the OTP by our choice e.g. (1111)

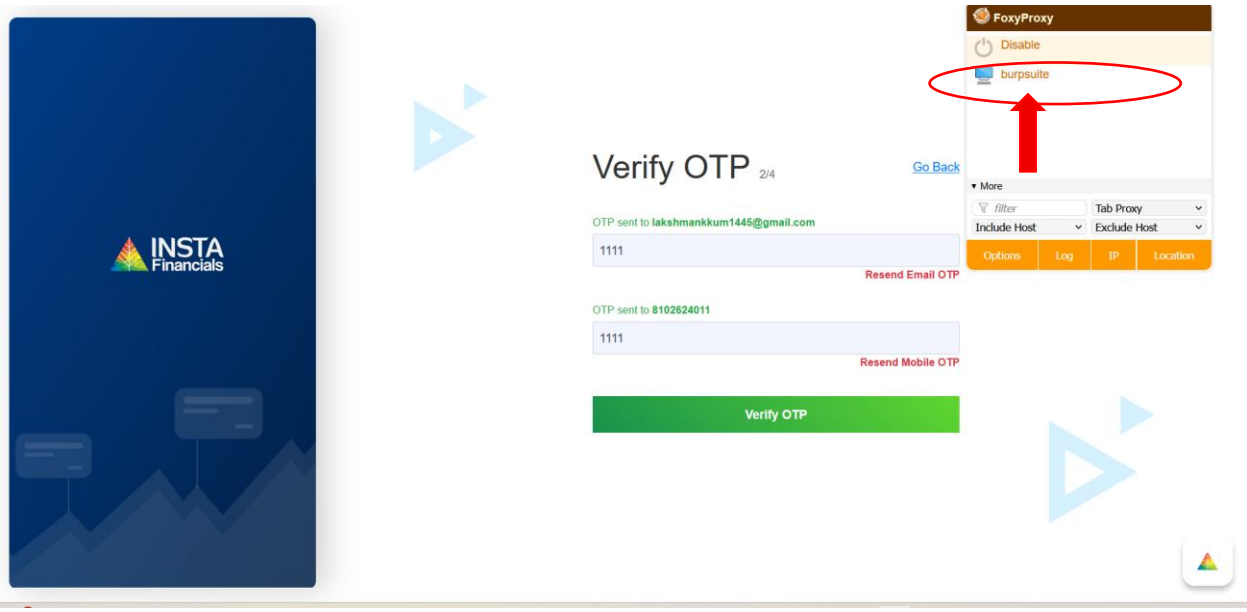
Reported BY: Lakshman Kumar Das



Step 5 Then we open Burp suite to make changes that make our OTP verify both email and number.

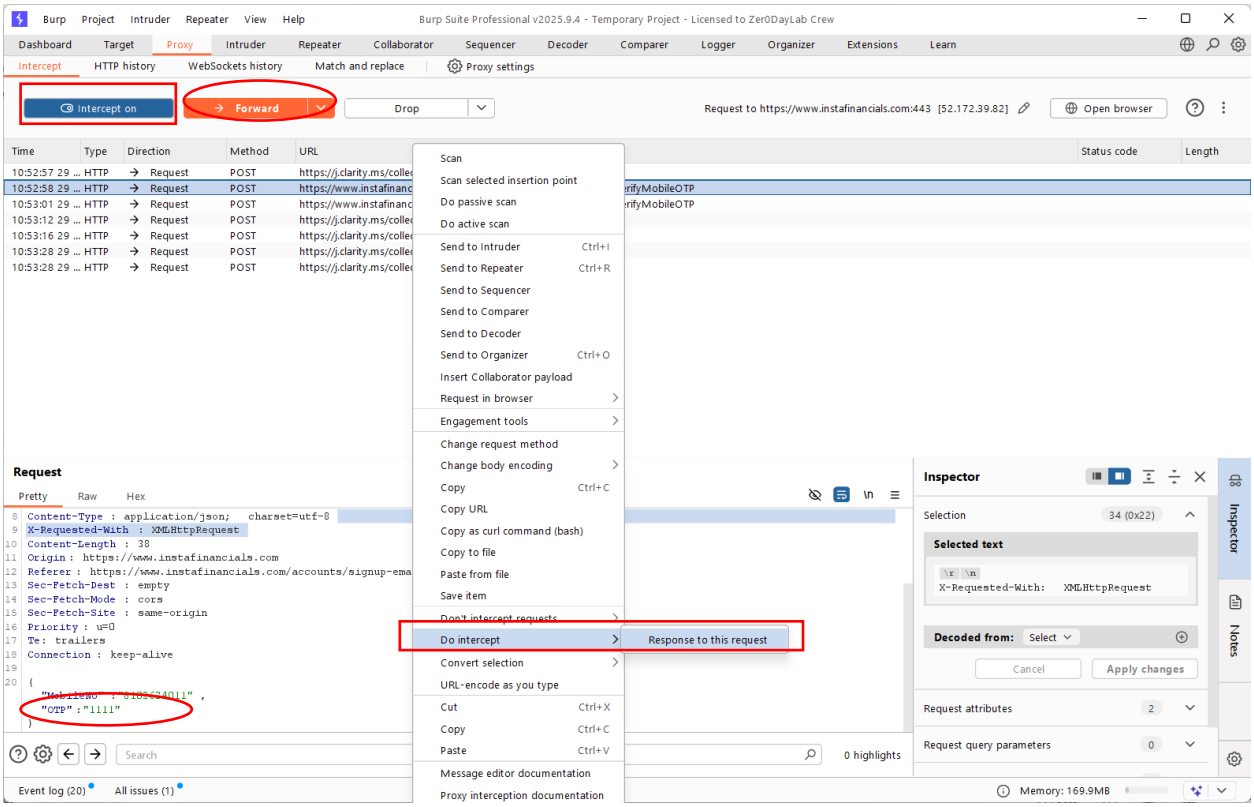
Step 6 Firstly we do the process with OTP verified

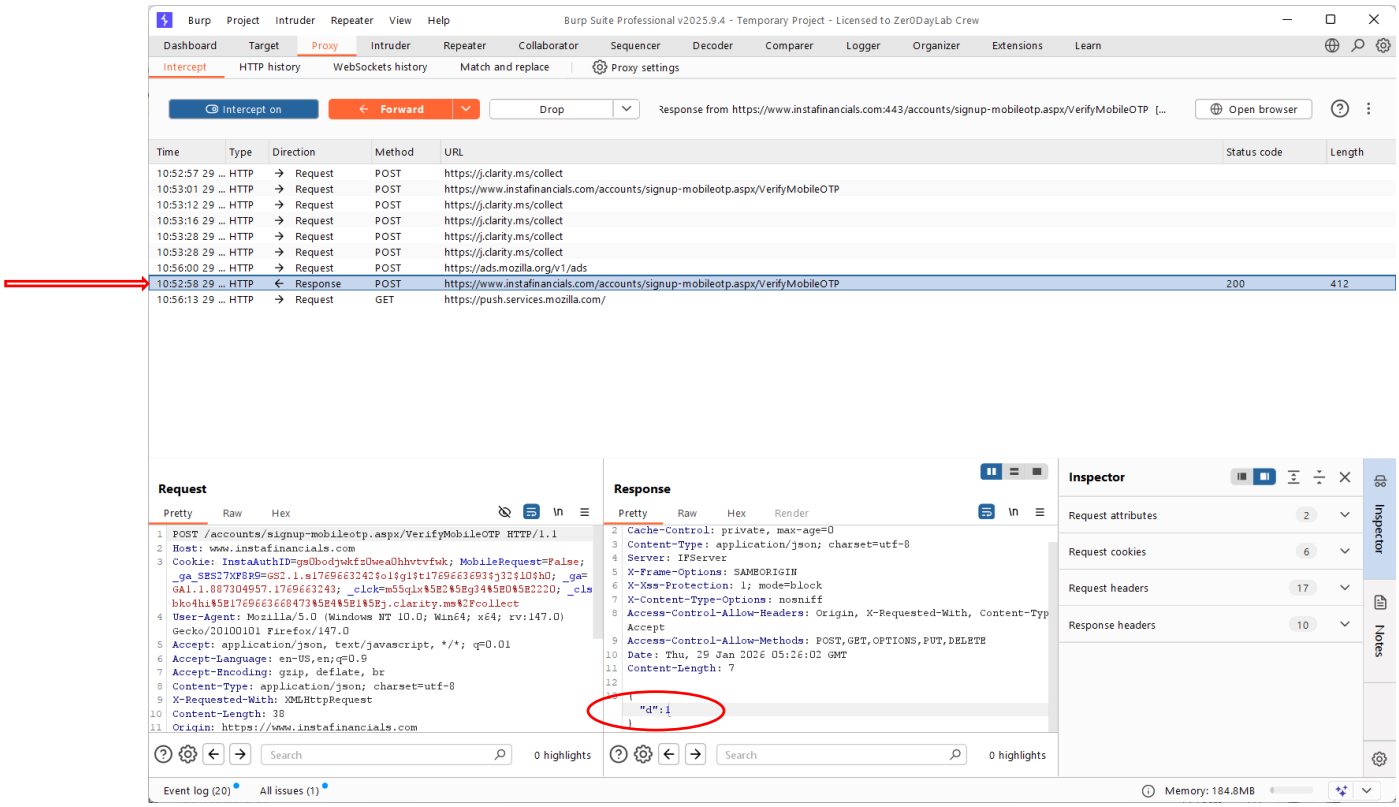
- After opening **Burp suite** go to the option proxy and then on the **Intercept** and Do the task on the web
- On the web we use the extensions like (Foxy Proxy)



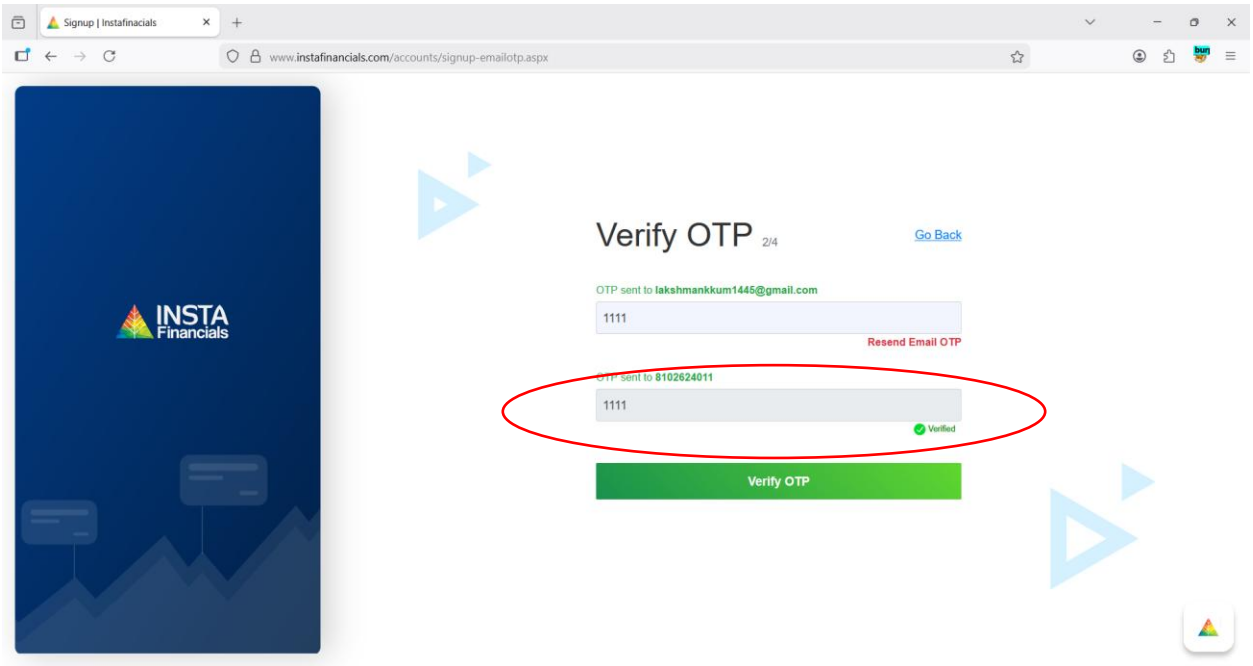
Step 7 After on the **Foxy Proxy** to the **Burp suite** all the requests are sent to the **Burp suite** Fig 2.1.1.4

- After this we must find the OTP verify
- Then do intercept and send response to the request and forward it
- Then we get the response
- After getting response we must change the value **(d=2 --> d=1)**

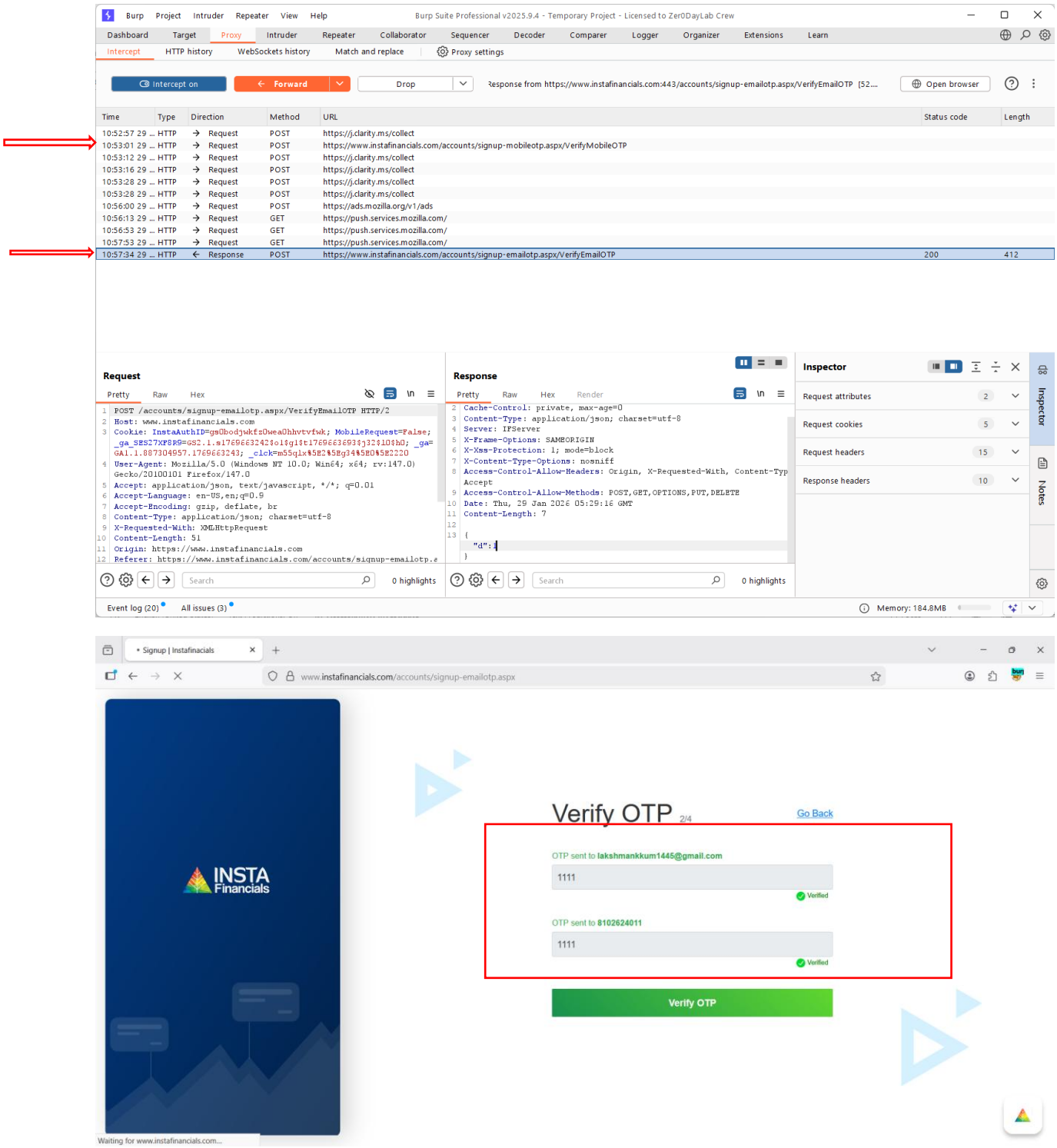




Step 8 After changing the values and **forward** it. We are getting that our OTP are bypass and verified



Reported BY: Lakshman Kumar Das



CONCLUSION

In this web application there is a venerability that by OTP bypass anyone can login the user account by doing the OTP bypass that leads to the damaging the CIA.

Reported BY: Lakshman Kumar Das