

# XSS

1. Buat akun dan register

## Register

Registration successful!

Username:

Username must be at least 10 characters long.

Password:

Password must be at least 10 characters long and include at least one digit, one special character, one uppercase letter, and one lowercase letter.

Register

Already have an account? [Login here.](#)

2. Login dengan menggunakan akun yang telah dibuat

## Login

Login successful!

Username:

Password:

Login

Don't have an account? [Sign up here.](#)

3. Masukkan data yang diminta dan update data

---

[Home](#) [Dashboard](#) [Logout](#) [Contact Support](#)

## Your Profile, <h1><script>alert(3)</script></h1>

Successfully updated

You need to finish setting up your profile before you can use all the features of this website.

Phone:

Credit Card:

Secret Question:

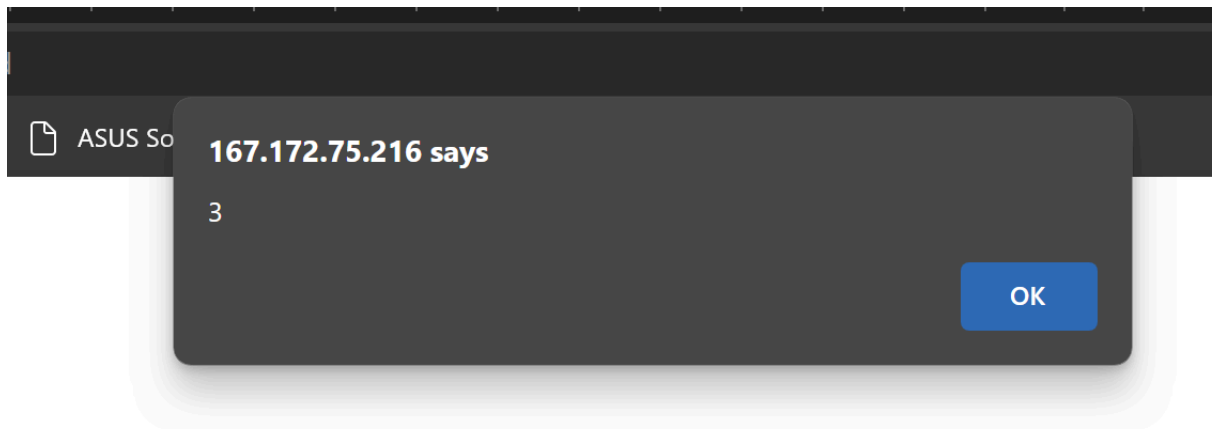
Secret Answer:

Current Password (for verification):

Update Profile

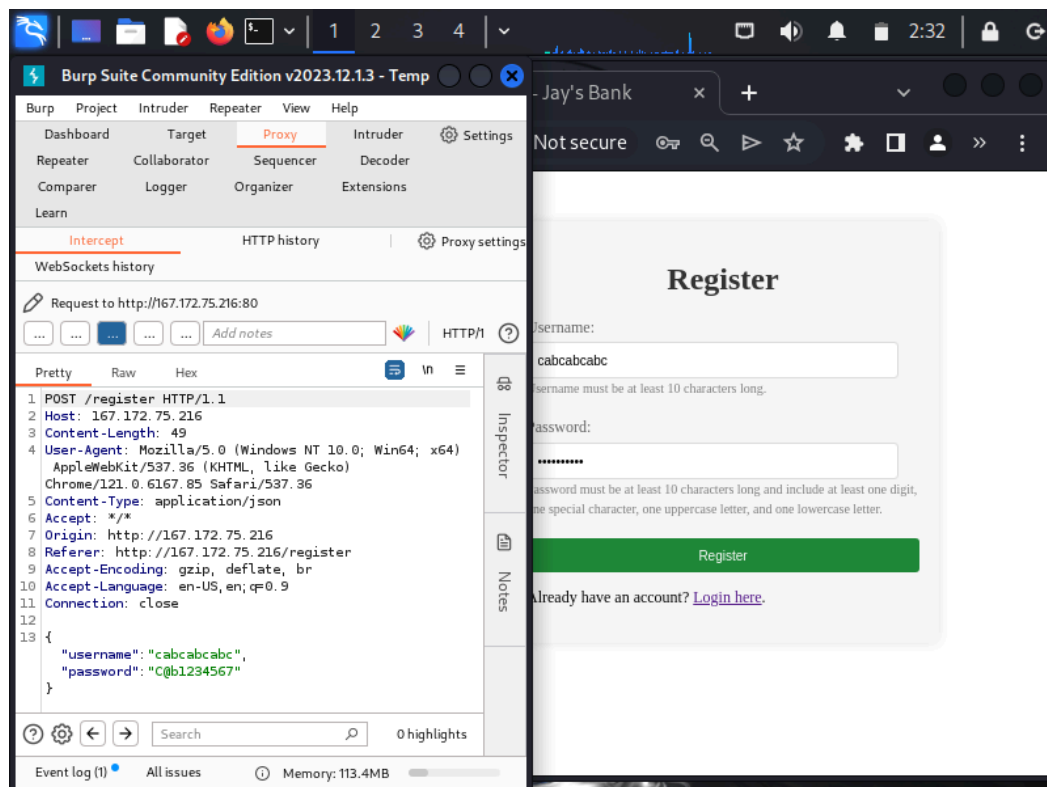
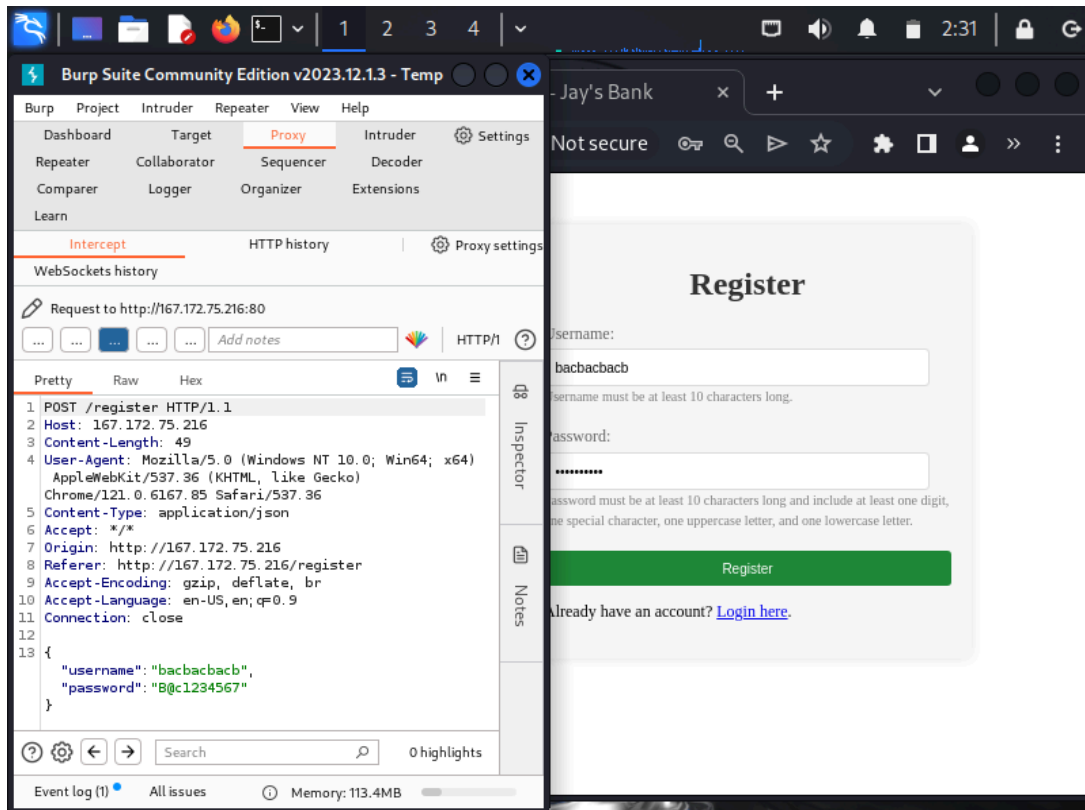
More Downloads

4. Logout dan login kembali maka akan muncul pop up berikut

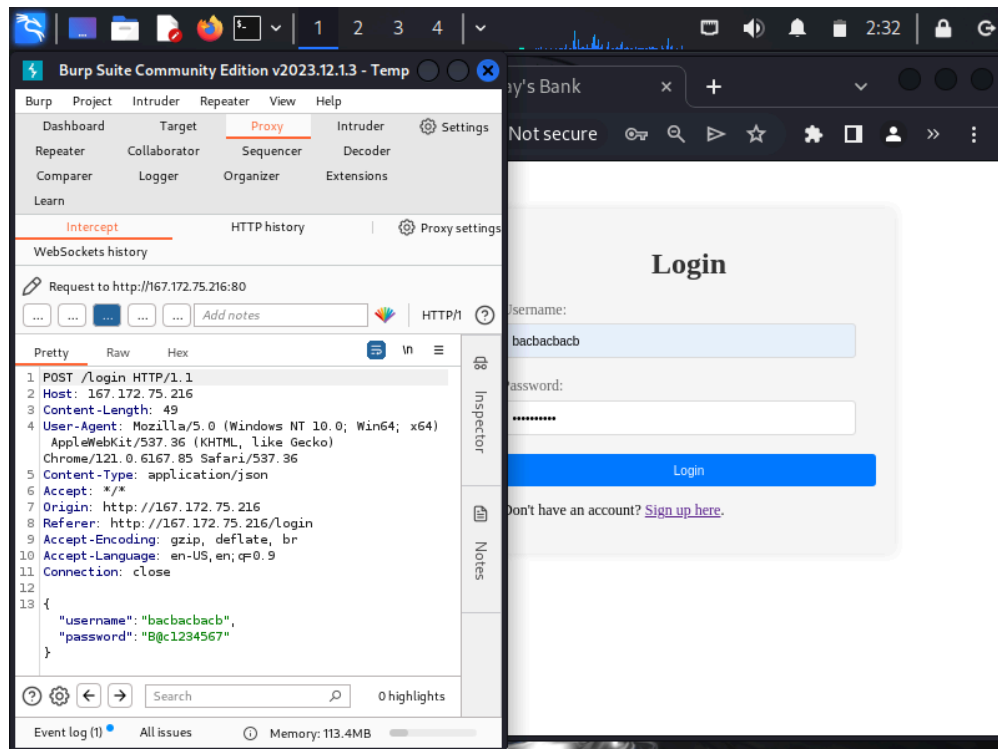


# BROKEN ACCESS CONTROL

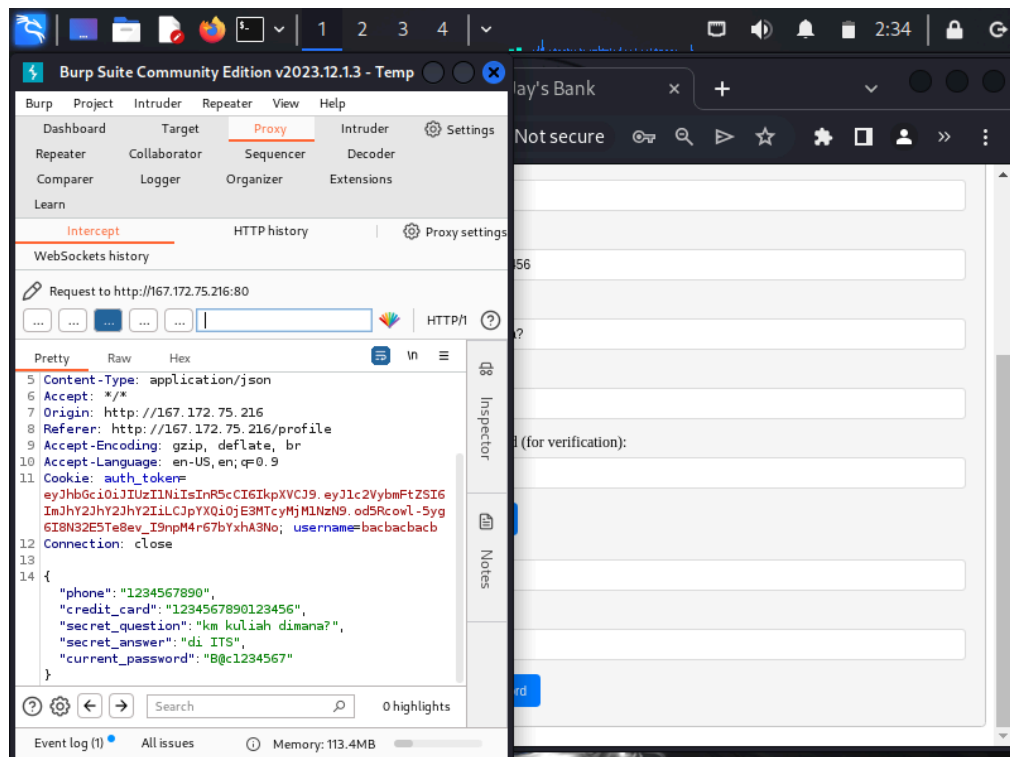
## 1. Register dengan menggunakan 2 akun

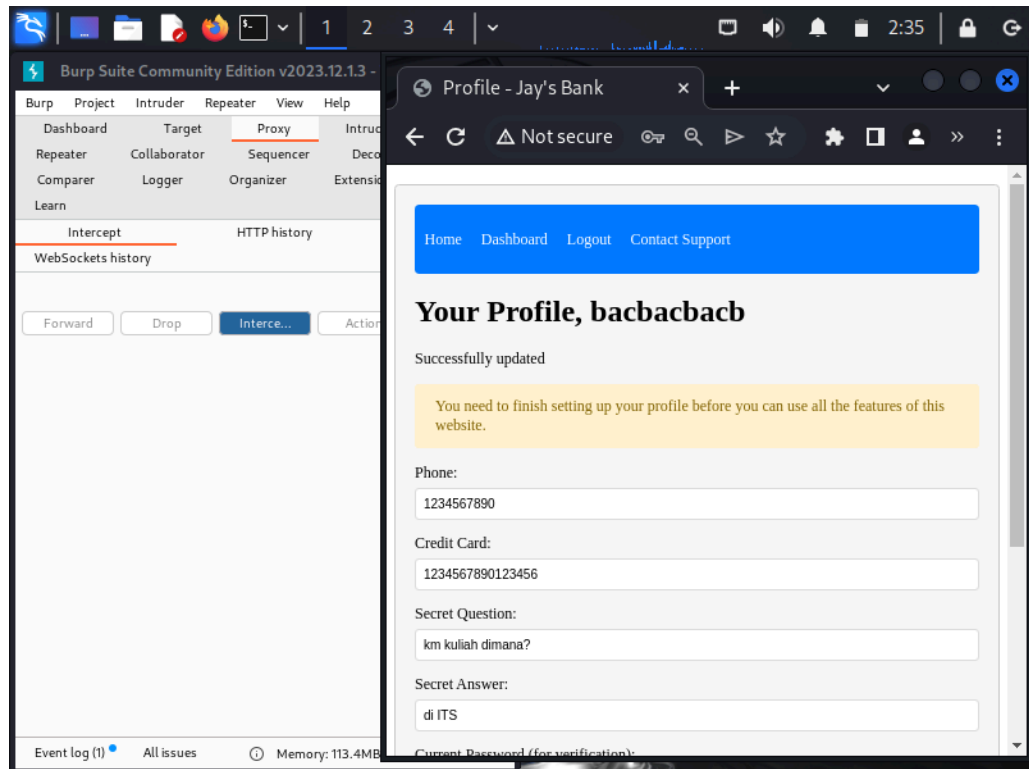


## 2. Login dengan akun pertama

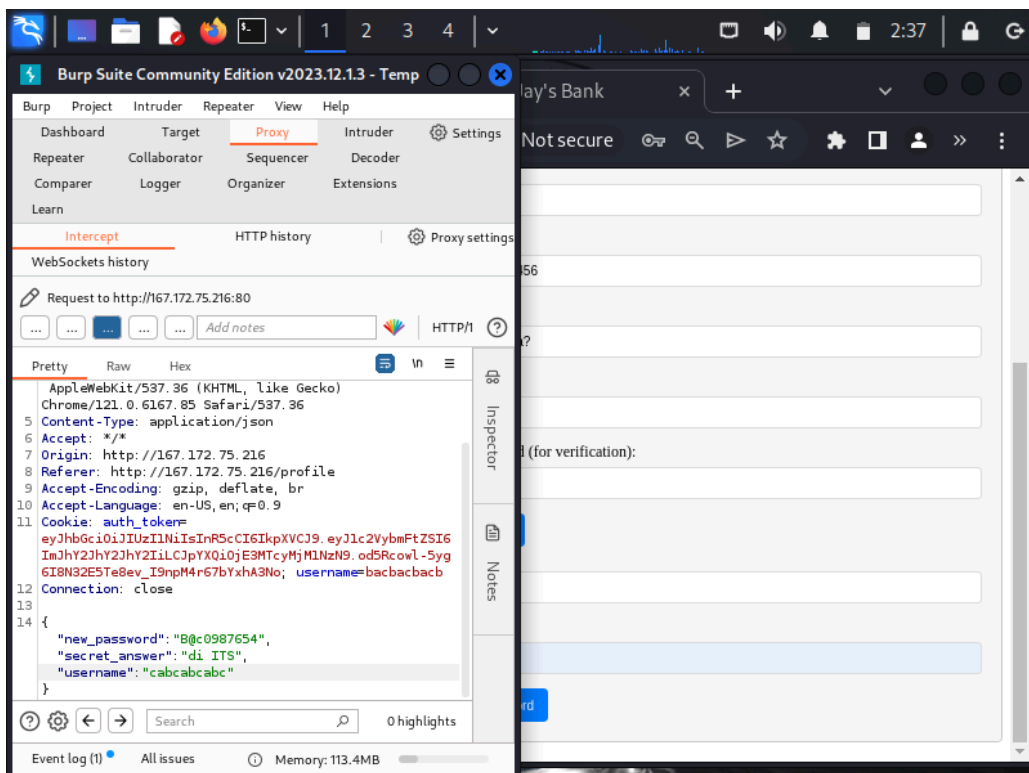


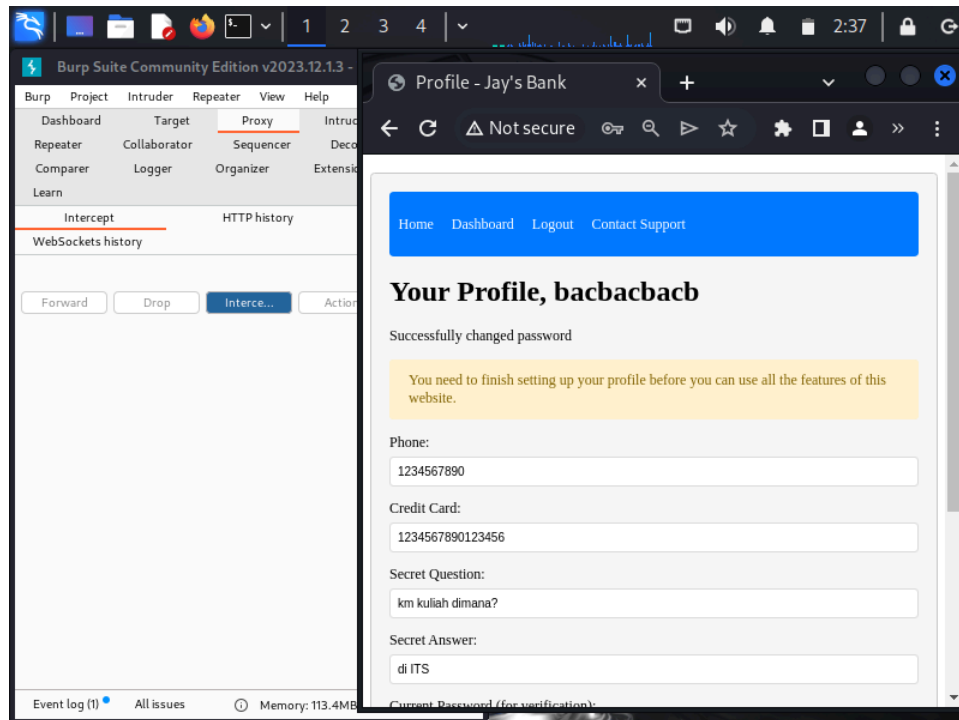
## 3. Masukkan data yang diminta dan update



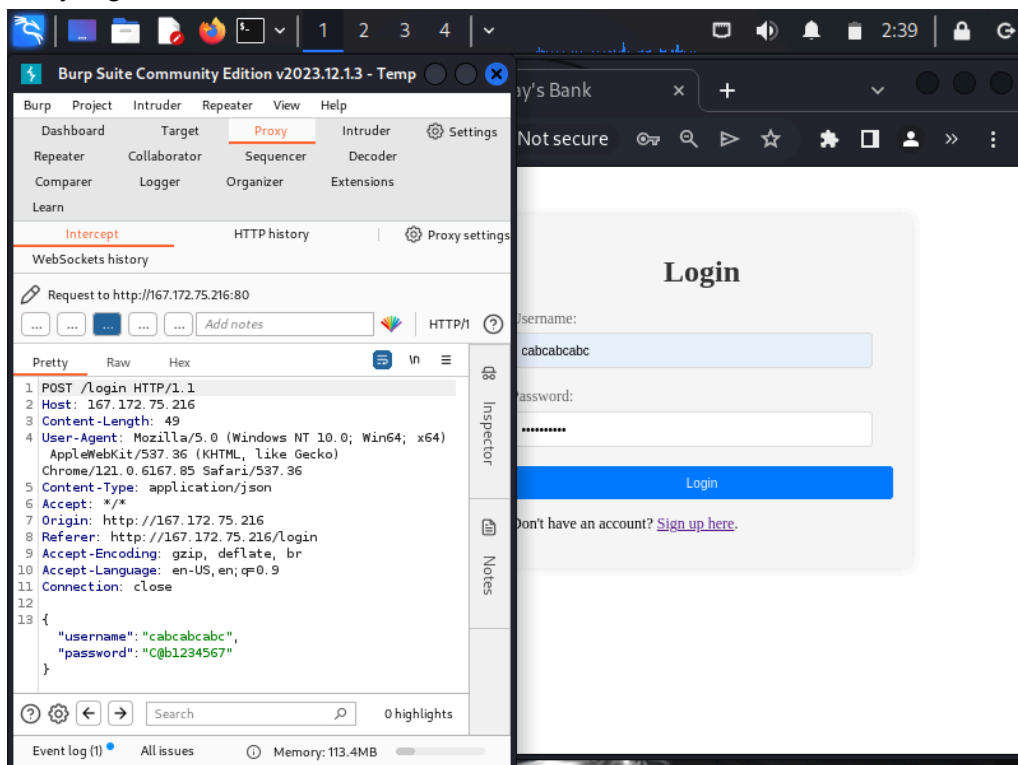


4. Ubah password dan pada panel kiri ubah username akun pertama menjadi username akun kedua

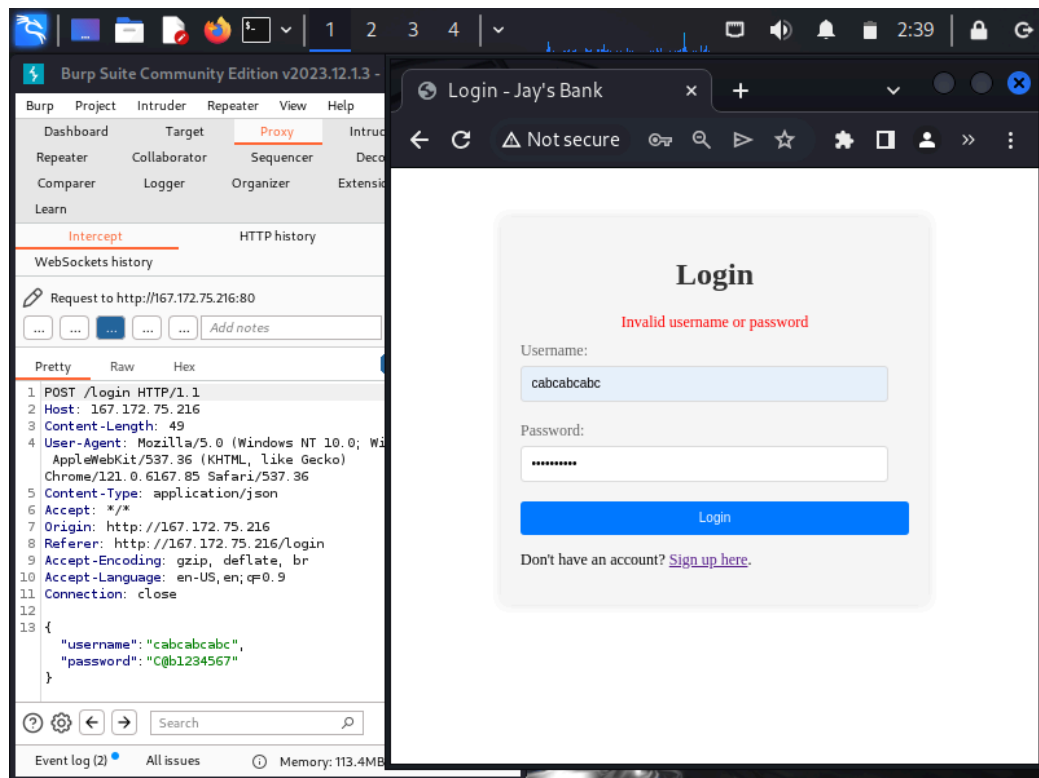




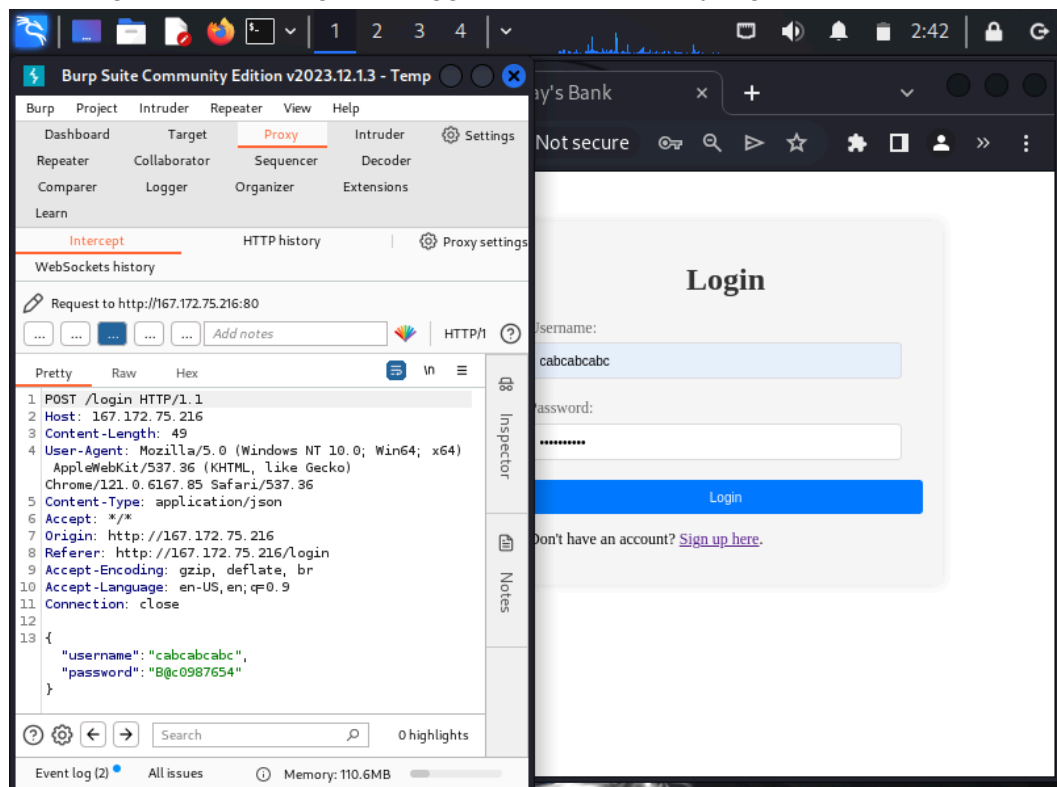
5. Logout, kemudian coba login ke akun kedua dengan password akun kedua yang asli

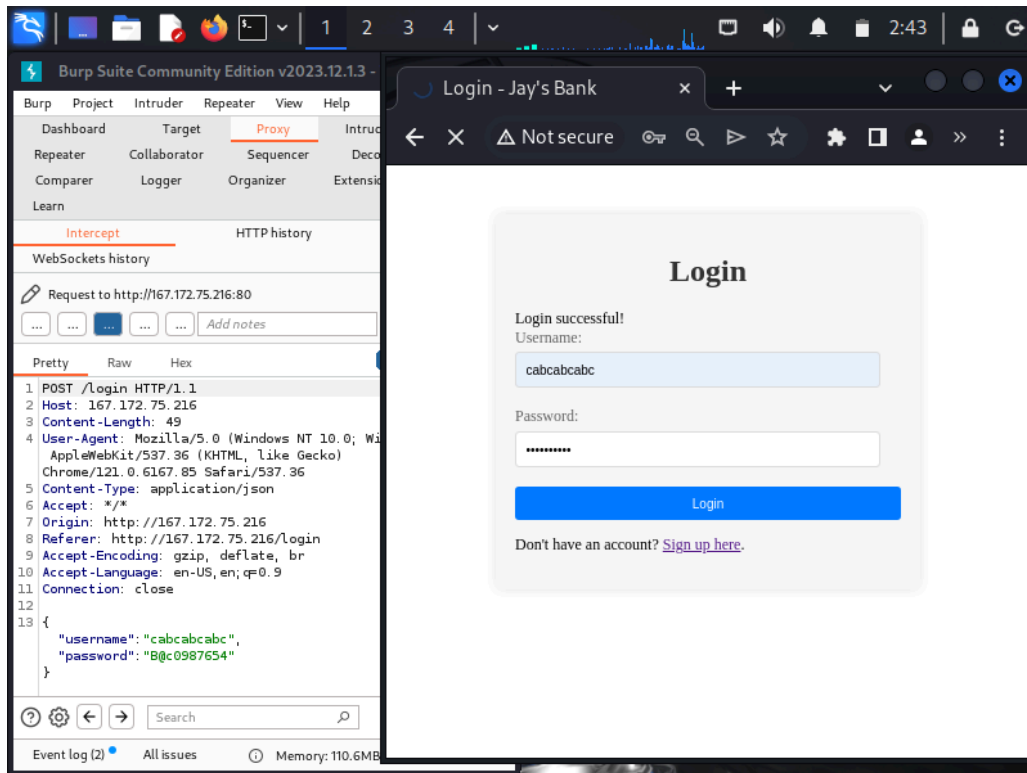


password asli menjadi invalid



## 6. Login kembali dengan menggunakan password yang diubah





login successful