OTP Bypass on Register account via Response manipulation

1. First Method

1. Register account with mobile number and request for OTP.

2. Enter incorrect OTP and capture the request in Burpsuite.

3. Do intercept response to this request and forward the request.

4. response will be

{"verificationStatus”: false,"mobile":9072346577","profileId":"84673832"}

5. Change this response to

{"verificationStatus”: true,"mobile":9072346577","profileId":"84673832"}

6. And forward the response.

7. You will be logged in to the account.

Impact: Account Takeover

2. Second Method.

1. Go to login and wait for OTP pop up.

2. Enter incorrect OTP and capture the request in Burp suite.

3. Do intercept response to this request and forward the request.

4. response will be error

5. Change this response to success

6. And forward the response.

7. You will be logged in to the account.

Impact: Account Takeover

3. Third Method:

1.Register 2 accounts with any 2 mobile number (first enter right otp)

2.Intercept your request

3.click on action -> Do intercept -> intercept response to this request.

4.check what the message will display like status:1

5.Follow the same procedure with other account but this time enter wrong otp

6.Intercept response to the request

7.See the message like you get status:0

8.Change status to 1 i.e, status:1 and forward the request if you logged in means you just done authentication bypass.

Bypassing OTP in registration forms by repeating the form

submission multiple times using repeater

Steps:

No Rate Limit

Steps: -

1. Create an account with a non-existing phone number

2. Intercept the Request in Burp Suite

3. Send the request to the repeater and forward

4. Go to Repeater tab and change the non-existent phone number to your phone number

5. If you got an OTP to your phone, try using that OTP to register that non-existent number

1) Create an Account

2) When Application Ask you For the OTP (One-time password), Enter wrong OTP and Capture this Request in Burp.

3) Send This Request into Repeater and repeat it by setting up payload on otp Value.

4) if there is no Rate Limit then wait for 200 Status Code (Sometimes 302)

5)if you get 200 ok or 302 Found Status Code that means you've bypass OTP