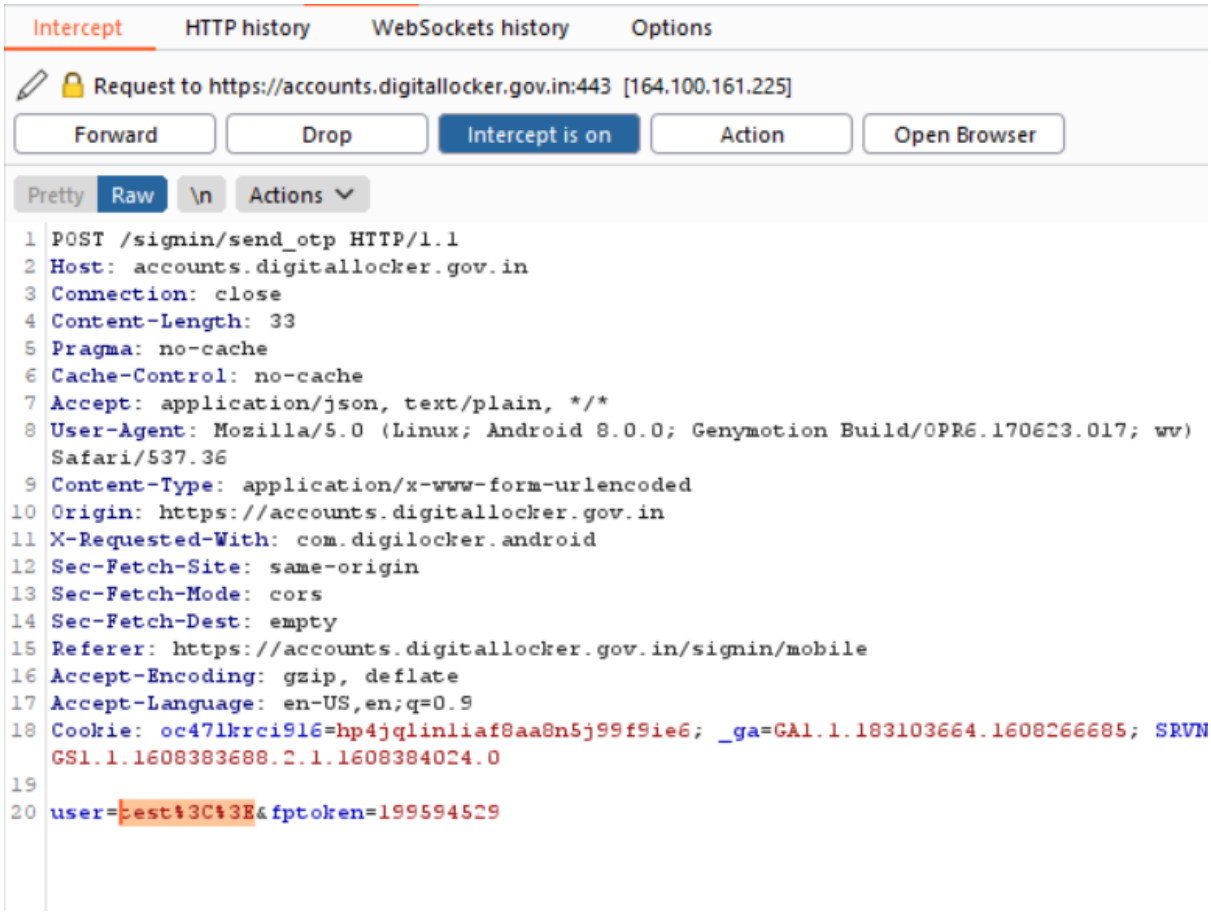
Title

Lack of Input Validation

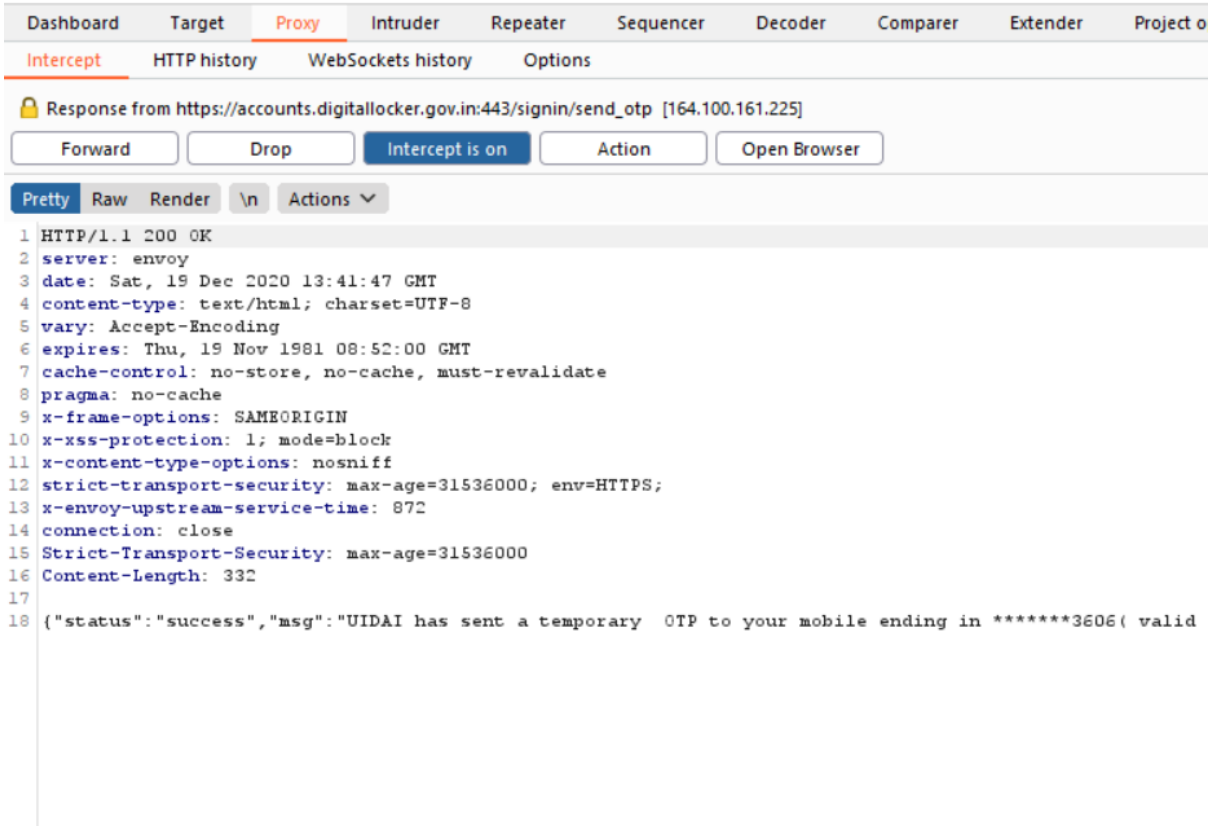
Description

This issue is present in login form of Digilocker App. In these whenever we input any symbols with any character then it will automatically send the OTP to random aadhar card number which can lead to get account details of that aadhar card holder and it shows some digit of aadhar card. Using that digit attacker can generate the aadhar card matches with that digit and can comprise that account.

Request



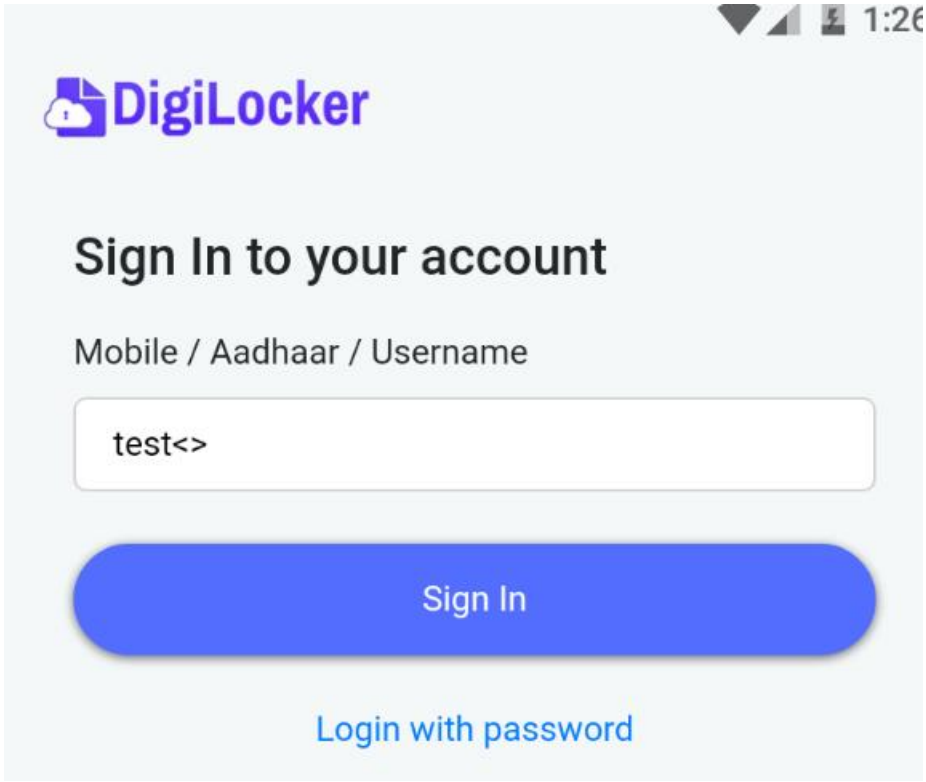
Response

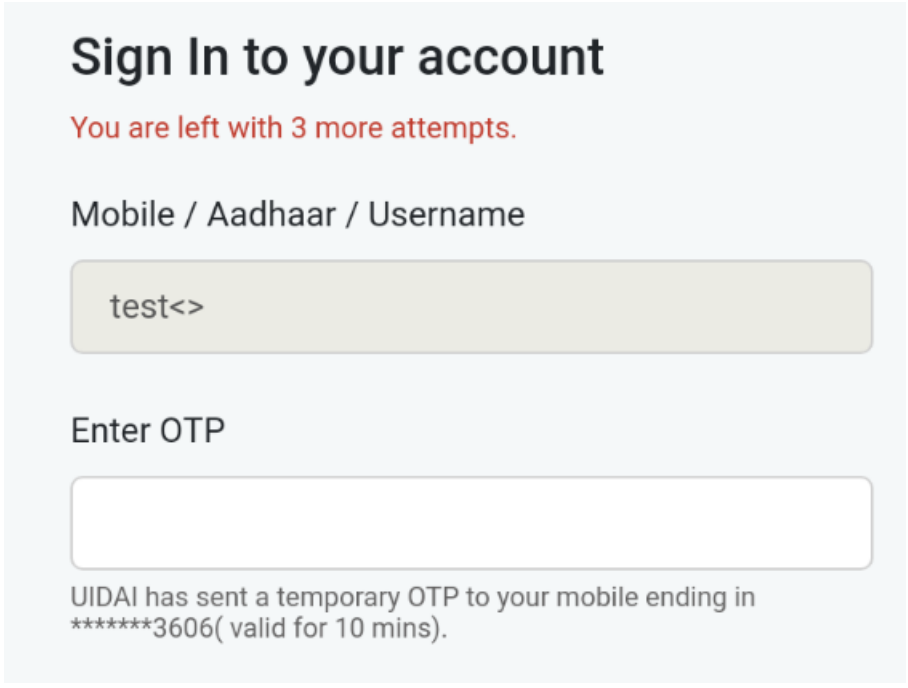


How to fix

1. Sanitize the input provided in form
2. Sometimes request can be intercept and change so, verify the input on server and both client side

Proof of concept


1:26
DigiLocker
Sign In to your account
Mobile / Aadhaar / Username
test<>
Sign In
Login with password


Sign In to your account
You are left with 3 more attempts.
Mobile / Aadhaar / Username
test<>
Enter OTP
UIDAI has sent a temporary OTP to your mobile ending in
*******3606(valid for 10 mins).