Mobile Application Security Audit of Neva android app

Test APK

release.apk

Interim Report

08th June 2020

AAA Technologies P. Ltd

278-280, F Wing, Solaris-1,
Saki Vihar Road, Opp. L & T Gate No. 6,
Powai, Andheri (East),
Mumbai 400 072, INDIA
Tel: + 91 22 28573815 / 16
Fax: + 91 22 40152501
info@aaatechnologies.co.in
www.aaatechnologies.co.in

Mobile Application Security Test Report For Neva Android App

S.No.	Severity	Vulnerability Description	Level-1	Compliance Status
1.	High	Insecure Authorization.	Open	Not Complied
2.	High	Debug mode is enabled in the app.	Open	Complied
3.	High	Allow backup is enabled in the app.	Open	Complied
4.	High	External Storage is allowed in the app.	Open	Not Complied
5.	High	OTP Flooding attack is possible in the app.	Open	Complied
6.	High	OTP brute force is possible in the app.	Open	Complied
7.	High	User password is travel in the clear text in the app.	Open	Complied
8.	High	Brute force attack is possible in the app.	Open	Complied
9.	Medium	Old version of ASP.NET is used in the app.	Open	-
10.	Medium	OTP is not getting validated in the app.	Open	Complied
11.	Low	Web Server Information Disclosure.	Open	Complied
12.	Low	Max. Length for input fields is not defined called in the application.	Open	Complied
13.	Low	Input fields are not getting cleared after invalid login attempts.	Open	Not Complied
14.	Low	Change password module is not implemented.	Open	Not Complied

15.	**Medium**	Password is not getting validated.	**-**	**Complied**
16.	**Medium**	Sensitive information disclosure is possible in the app.	**-**	**Complied**
17.	**Low**	Forgot password is not implemented in the app.	**-**	**Complied**
18.	**Informational**	Functionality Issues.	**-**	**Not Complied**

S.No.	**Severity**	**Vulnerability Description**	**Level-1**	**Compliance Status**
1.	**High**	Dangerous permissions are used in the app.	-	**NEW**
2.	**High**	Aadhar number shows in the response.	**-**	**NEW**
3.	**Medium**	Java hash code is used in the app.	**-**	**NEW**
4.	**Medium**	Base64 encoding is used in the app.	**-**	**NEW**
5.	**Low**	PrintStackTrace method is used in the app.	**-**	**NEW**
6.	**Low**	Weak algorithm is used in the app.	**-**	**NEW**

High

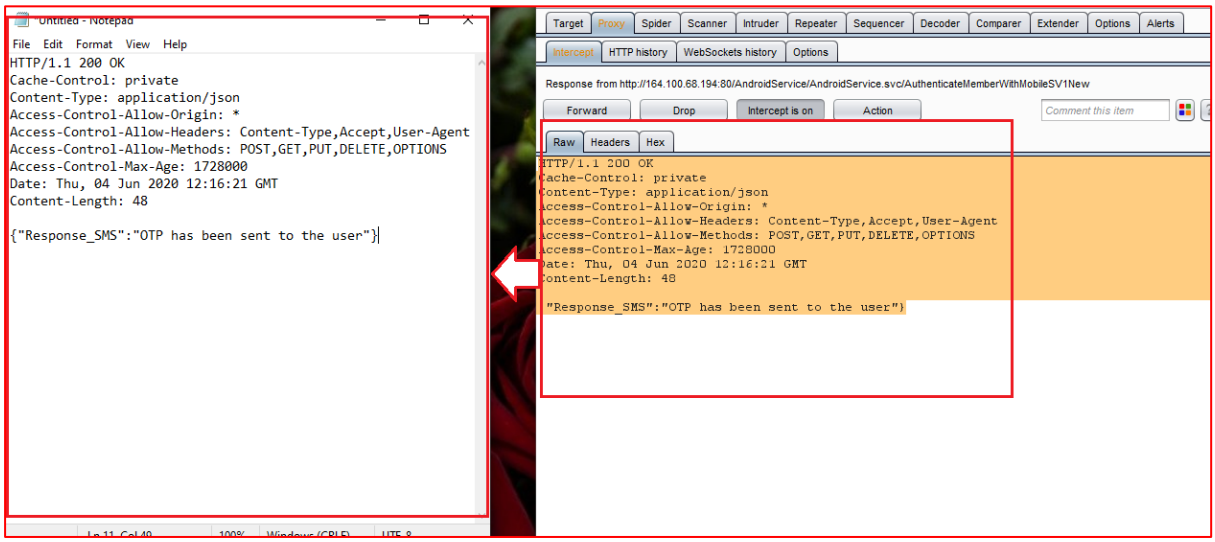
1. Insecure Authentication.

1) Vulnerability Title: Insecure Authentication mechanism (Response Replay) is possible in the app.	
Risk	**High**
Abstract	It was observed that Authentication bypass is possible in the application.
Ease of Exploitation	Medium
Impact	Insecure Authentication mechanism is used in the application. Attacker can bypass the authentication to gain access to the application
Recommendations	Proper Authentication mechanism must be implemented to avoid authentication bypass.
Snapshot	

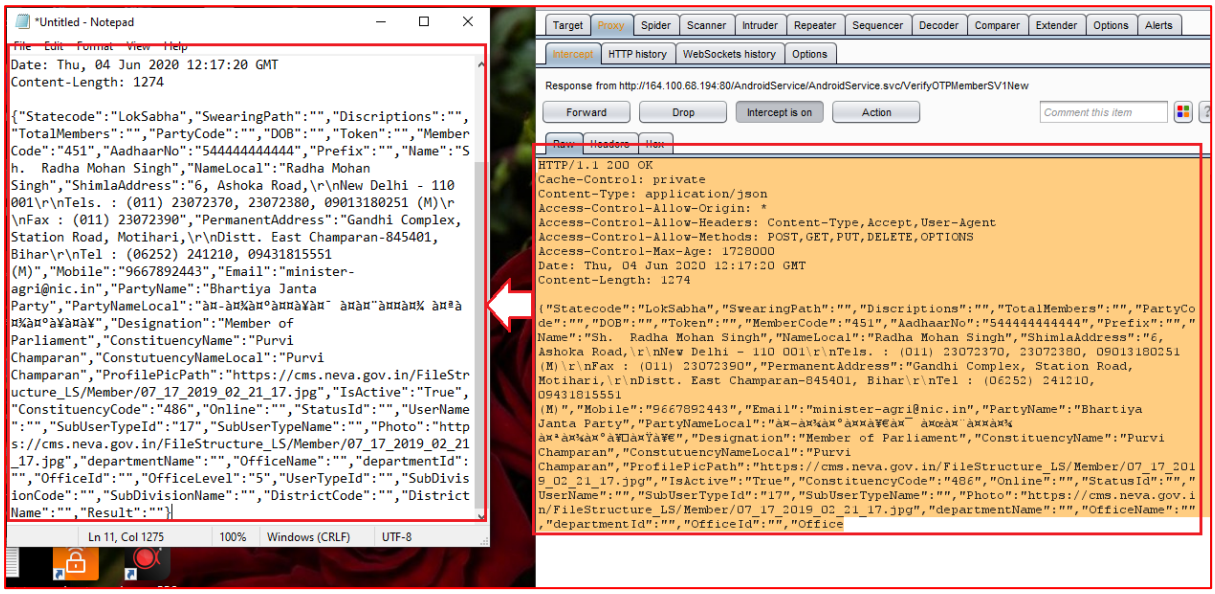
How Test was performed:

Step#1: Open release.apk and login with valid credentials (U: 9667892443, P: neva42) and intercept the request as shown below:

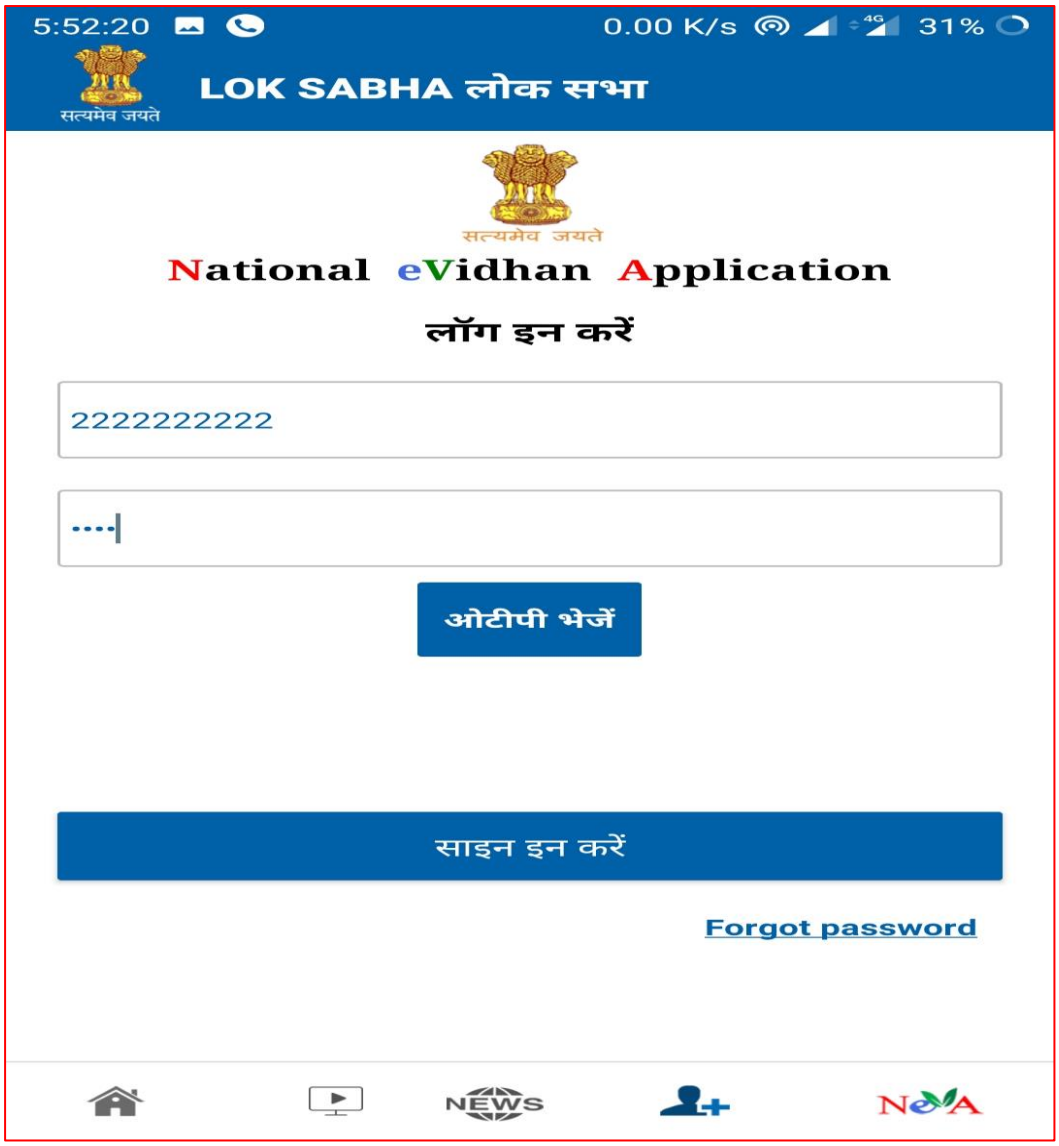
Step#2: Copy valid response into the notepad and forward the request as shown below:



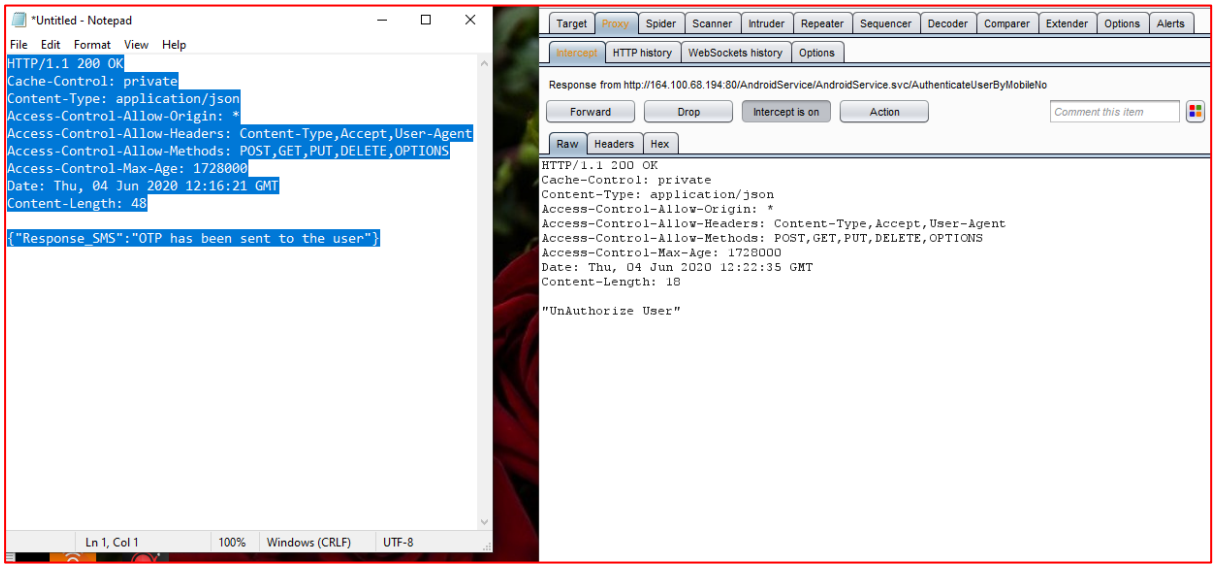
Step#3: Now enter the valid OTP and intercept the request then copy the valid response into the notepad and forward the request as shown below:

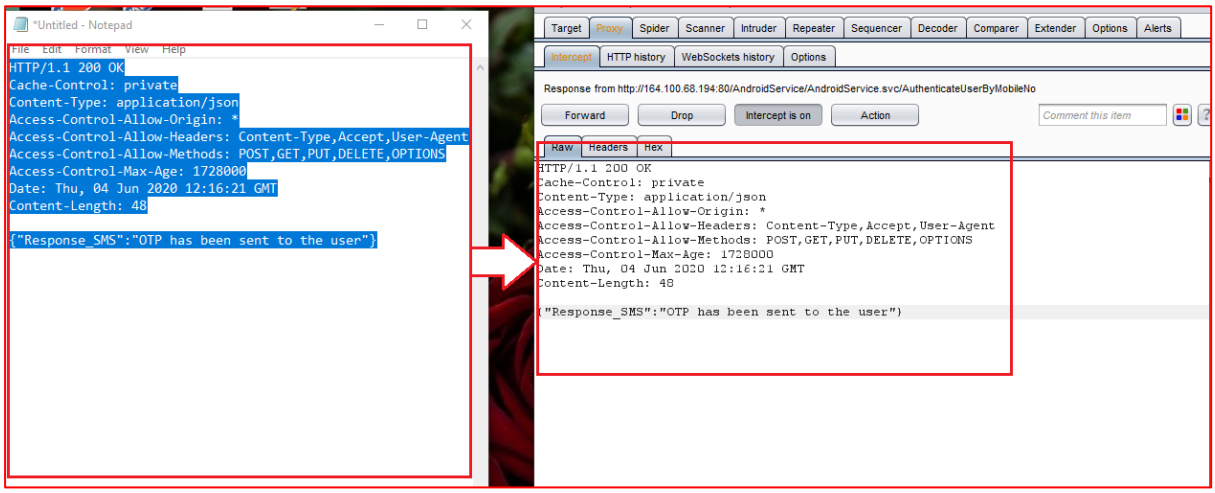


Step#4: Now logout from the app and again login with invalid credentials, intercept the request as shown below:

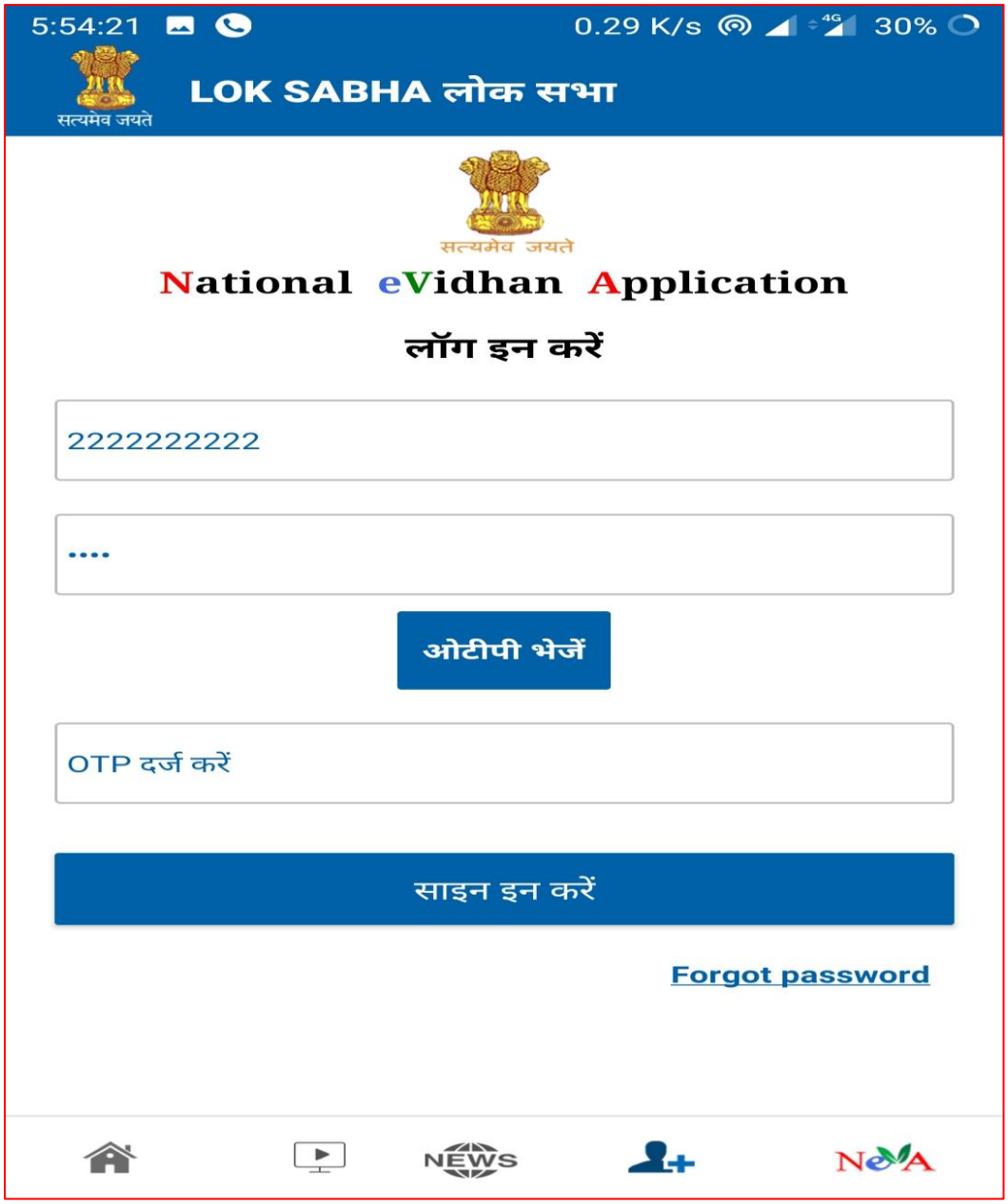


Step#5: Now replace invalid response with copied valid response and forward the request as shown below:

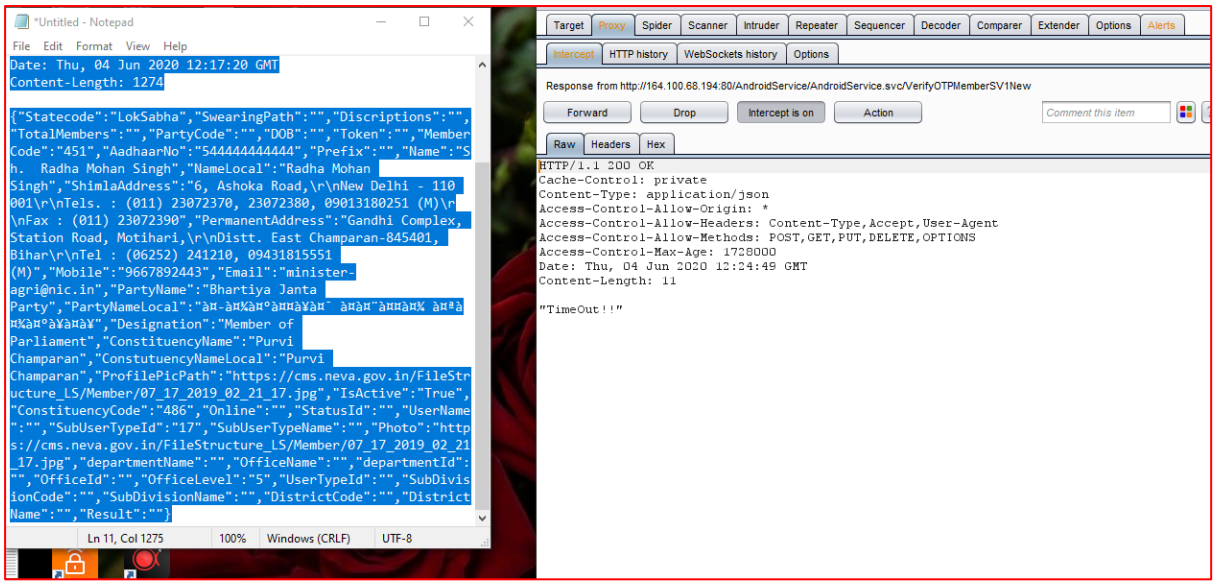


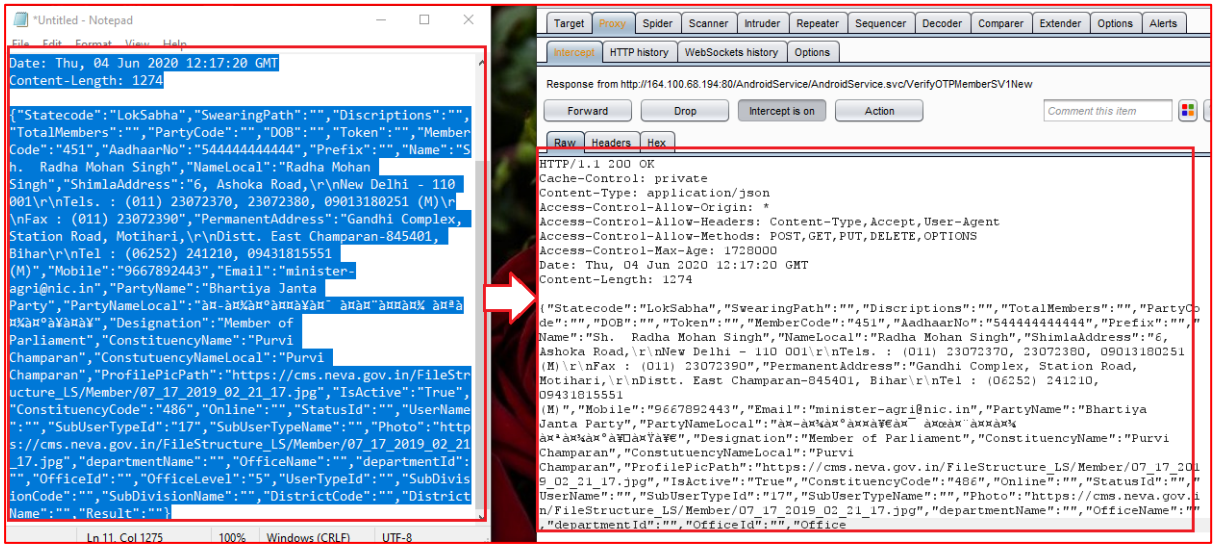


Step#6: It is been observed that the other is successfully bypass the login:

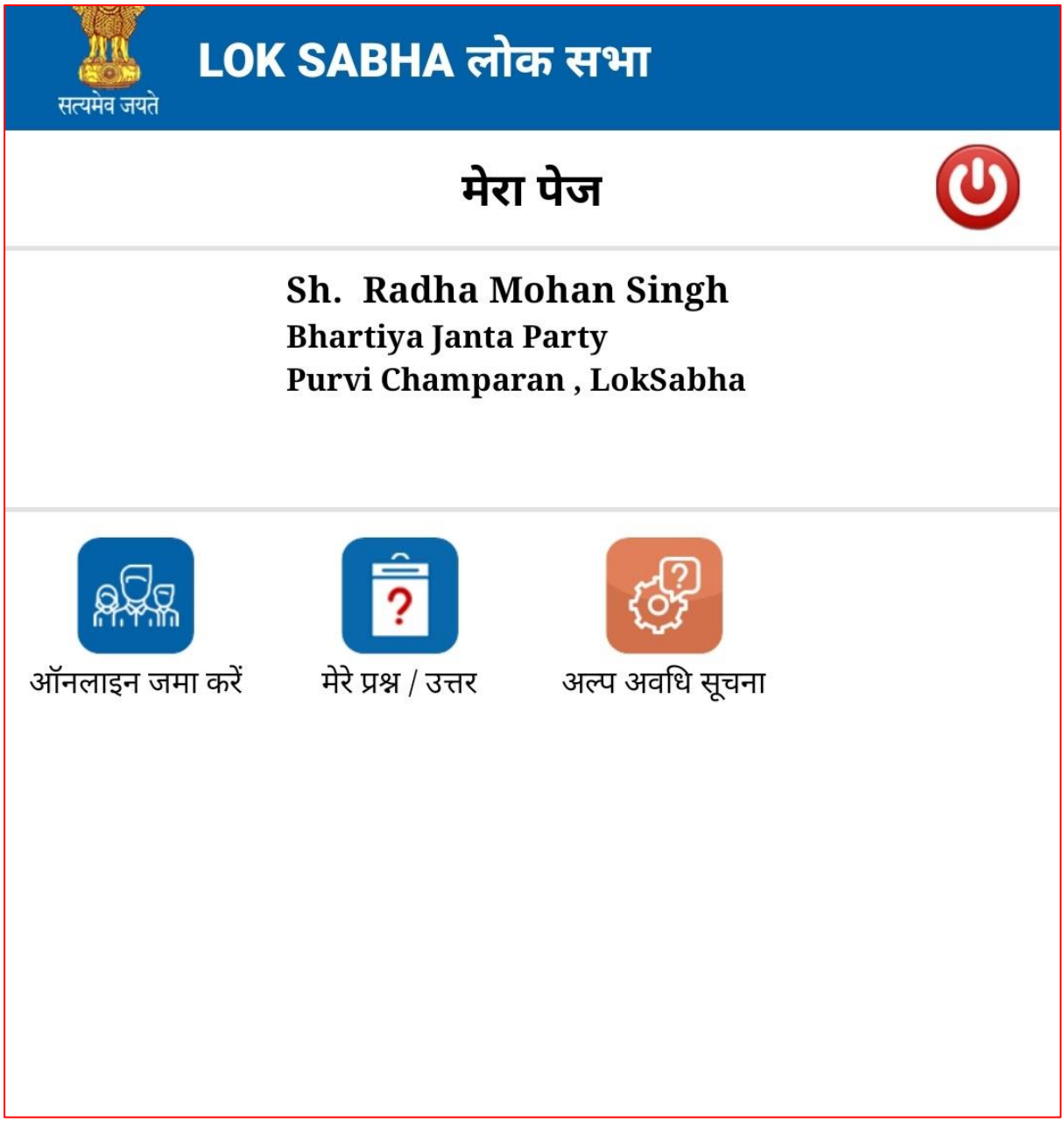


Step#7: Now enter invalid OTP and intercept the request and then replace the response with copied valid response and forward the request as shown below:

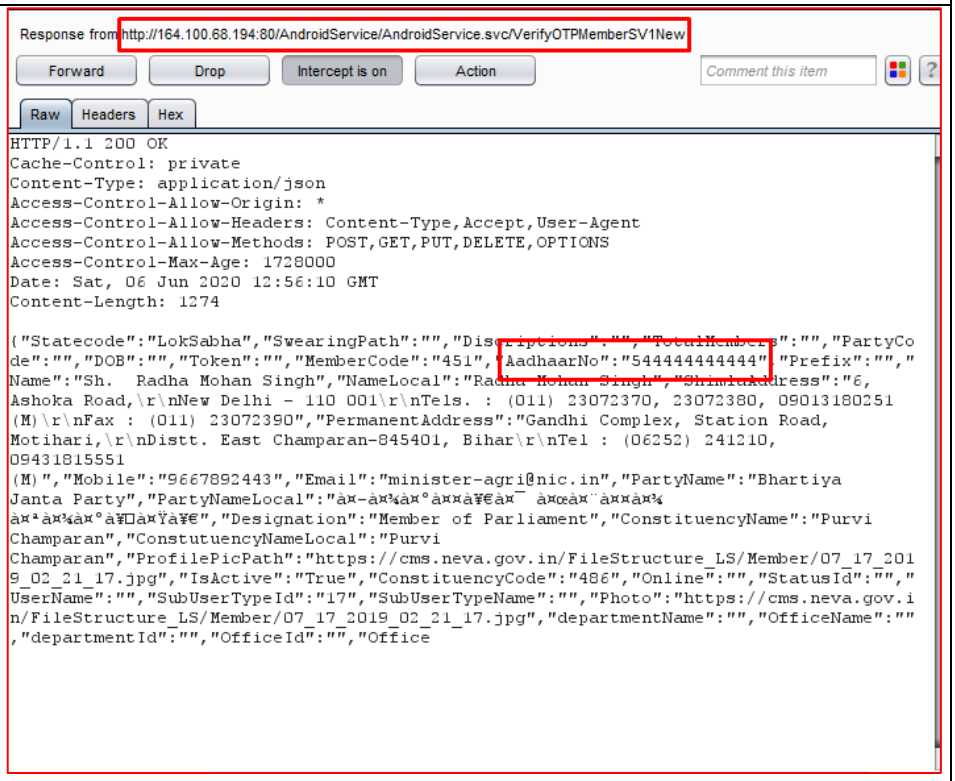




Step#8: It is been observed that the other is successfully login in the app without valid credentials and able to access authenticated links:



2. Aadhar number shows in the response

2) Vulnerability Title: Aadhar number shows in the response	
Risk	**High**
Abstract	It was observed that Aadhar number (sensitive information) is shows in the application.
Ease of Exploitation	Easy
Impact	An attacker may be able to Sniff the Aadhar No.
Recommendations	It is recommended that the sensitive information should not show in the response.
Snapshot	

Response from http://164.100.68.194:80/AndroidService/AndroidService.svc/VerifyOTPMemberSV1New

Forward | Drop | Intercept is on | Action | Comment this item

Raw | Headers | Hex


```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/json
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Content-Type,Accept,User-Agent
Access-Control-Allow-Methods: POST,GET,PUT,DELETE,OPTIONS
Access-Control-Max-Age: 1728000
Date: Sat, 06 Jun 2020 12:56:10 GMT
Content-Length: 1274

{"Statecode":"LokSabha","SwearingPath":"","Discriptions":"","TotalMembers":"","PartyCo
de":"","DOB":"","Token":"","MemberCode":"451","AadhaarNo":"544444444444","Prefix":"","
Name":"Sh.  Radha Mohan Singh","NameLocal":"Radha Mohan Singh","ShimlaAddress":"6,
Ashoka Road,\r\nNew Delhi - 110 001\r\nTels. : (011) 23072370, 23072380, 09013180251
(M)\r\nFax : (011) 23072390","PermanentAddress":"Gandhi Complex, Station Road,
Motihari,\r\nDistt. East Champaran-845401, Bihar\r\nTel : (06252) 241210,
09431815551
(M)","Mobile":"9667892443","Email":"minister-agri@nic.in","PartyName":"Bhartiya
Janta Party","PartyNameLocal":"à¤-à¤¾à¤°à¤¤à¥€à¤¯ à¤œà¤¨à¤¤à¤¾
à¤ª à¤¾à¤°à¥à¤Ÿà¥€","Designation":"Member of Parliament","ConstituencyName":"Purvi
Champaran","ConstutuencyNameLocal":"Purvi
Champaran","ProfilePicPath":"https://cms.neva.gov.in/FileStructure_LS/Member/07_17_201
9_02_21_17.jpg","IsActive":"True","ConstituencyCode":"486","Online":"","StatusId":"","
UserName":"","SubUserTypeId":"17","SubUserTypeName":"","Photo":"https://cms.neva.gov.i
n/FileStructure_LS/Member/07_17_2019_02_21_17.jpg","departmentName":"","OfficeName":""
,"departmentId":"","OfficeId":"","Office
```

3. Dangerous permissions are allowed in the Android Application

3) Vulnerability Title: Dangerous permissions are allowed in the Android Application	
Risk	**High**
Abstract	It was observed that Dangerous permissions are allowed in the Android Application.
Ease of Exploitation	Easy
Impact	It is allow an app to view network status, create network socket, prevent phone from sleeping, display system level alerts.
Recommendations	It is recommended to restrict app permissions.
Snapshot	

```
D:\AAA\Applications\Neva ...
<?xml version="1.0" encoding="UTF-8"?>
- <manifest platformBuildVersionName="10" platformBuildVersionCode="29" package="evmember.sbl.nationalevidhan" android:compileSdkVersionCodename="10"
  android:compileSdkVersion="29" xmlns:android="http://schemas.android.com/apk/res/android">
    <uses-permission android:name="android.permission.ACCESS_DOWNLOAD_MANAGER"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.CALL_PHONE"/>
    <uses-permission android:name="android.permission.WAKE_LOCK"/>
    <uses-permission android:name="android.permission.ACCESS_DOWNLOAD_MANAGER"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="com.android.launcher.permission.INSTALL_SHORTCUT"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
    <supports-screens android:xlargeScreens="true" android:smallScreens="true" android:resizeable="true" android:normalScreens="true" android:largeScreens="true"
        android:anyDensity="true"/>
  - <application android:name="evmember.sbl.nationalevidhan.application.MyNevaApplication" android:usesCleartextTraffic="true" android:supportsRtl="true"
    android:roundIcon="@drawable/app_launcher" android:requestLegacyExternalStorage="true" android:largeHeap="true" android:label="@string/app_name"
    android:icon="@drawable/app_launcher" android:hardwareAccelerated="true" android:fullBackupContent="false" android:debuggable="false" android:configChanges="locale"
    android:appComponentFactory="androidx.core.app.CoreComponentFactory" android:allowBackup="false">
      <uses-library android:name="org.apache.http.legacy" android:required="false"/>
    - <activity android:name="evmember.sbl.nationalevidhan.SplashActivity" android:theme="@style/Theme.NoTitle" android:screenOrientation="portrait"
      android:noHistory="true">
        - <intent-filter>
            <action android:name="android.intent.action.MAIN"/>
            <category android:name="android.intent.category.LAUNCHER"/>
          </intent-filter>
      </activity>
      <activity android:name="evmember.sbl.nationalevidhan.TodayBirthdayActivity" android:configChanges="orientation" android:theme="@style/AppTheme"
          android:screenOrientation="portrait"/>
      <activity android:name="evmember.sbl.nationalevidhan.views.ChangePasswordActivity" android:configChanges="orientation" android:theme="@style/AppTheme"
          android:screenOrientation="portrait"/>
      <activity android:name="evmember.sbl.nationalevidhan.DebateTypeSearchActivity" android:configChanges="orientation" android:theme="@style/AppTheme"
          android:screenOrientation="portrait" android:windowSoftInputMode="adjustResize|stateHidden"/>
      <activity android:name="evmember.sbl.nationalevidhan.DebateGuidedSearchActivity" android:configChanges="orientation" android:theme="@style/AppTheme"
          android:screenOrientation="portrait" android:windowSoftInputMode="adjustResize|stateHidden"/>
      <activity android:name="evmember.sbl.nationalevidhan.BussinessGovermentBillActivity" android:configChanges="orientation" android:theme="@style/AppTheme"
```

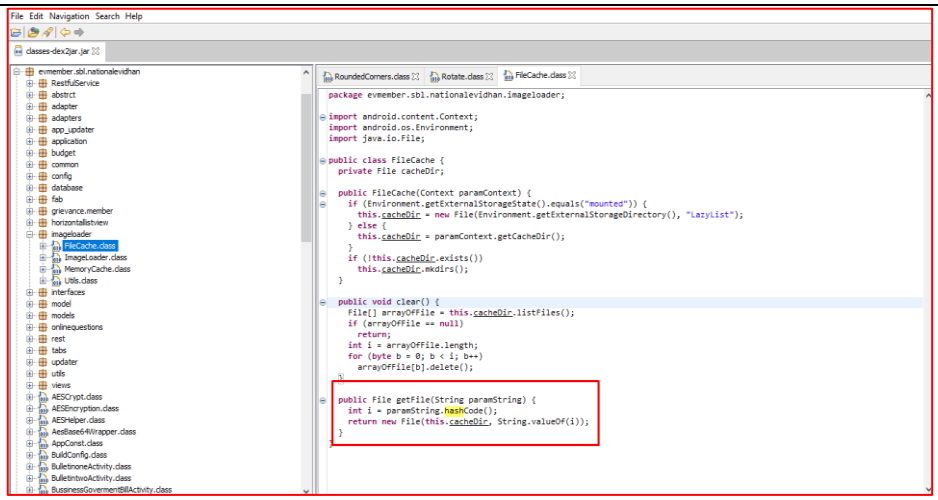
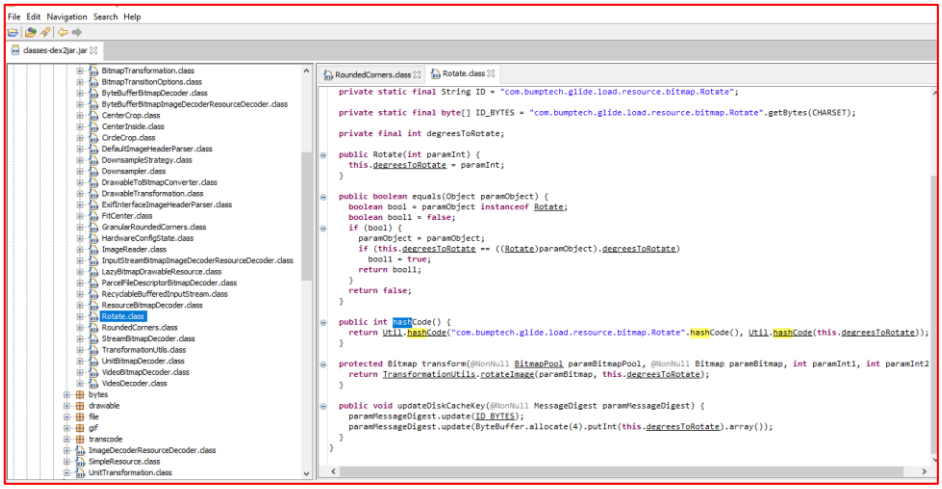
4. External Storage is assigned for data storage.

4) Vulnerability Title: External Storage is assigned for data storage.	
Risk	**High**
Abstract	External Storage is assigned for data storage.
Ease of Exploitation	Medium
Impact	App can read/write to External Storage. Any App can read data written to External Storage
Recommendations	Files created on external storage, such as SD cards, are globally readable and writable. Because external storage can be removed by the user and also modified by any application, don't store sensitive information using external storage. You should perform input validation when handling data from external storage as you would have done with data from any un-trusted source. You should not store executable or class files on external storage prior to dynamic loading. If your app does retrieve executable files from external storage, the files should be signed and cryptographically verified prior to dynamic loading
Snapshot	

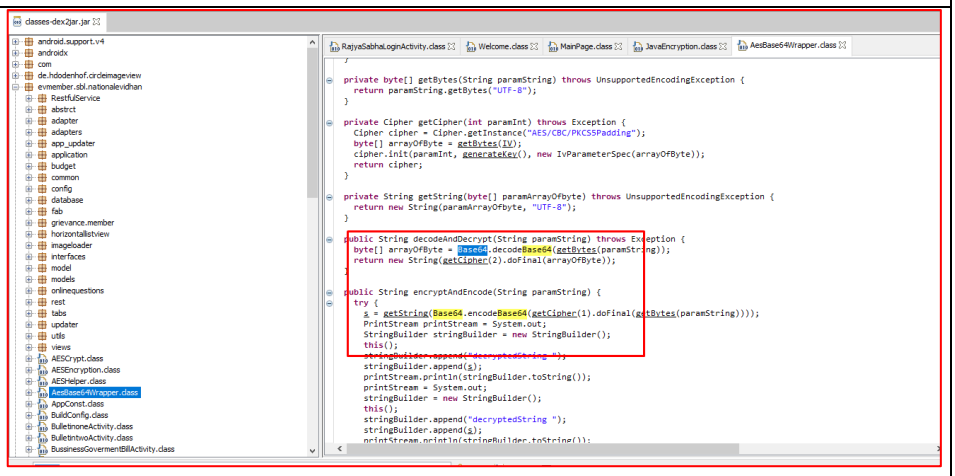

```
<?xml version="1.0" encoding="UTF-8"?>
- <manifest platformBuildVersionName="10" platformBuildVersionCode="29" package="evmember.sbl.nationalevidhan" android:compileSdkVersionCodename="10"
  android:compileSdkVersion="29" xmlns:android="http://schemas.android.com/apk/res/android">
      <uses-permission android:name="android.permission.ACCESS_DOWNLOAD_MANAGER"/>
      <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
      <uses-permission android:name="android.permission.INTERNET"/>
      <uses-permission android:name="android.permission.CALL_PHONE"/>
      <uses-permission android:name="android.permission.WAKE_LOCK"/>
      <uses-permission android:name="android.permission.ACCESS_DOWNLOAD_MANAGER"/>
      <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
      <uses-permission android:name="android.permission.INTERNET"/>
      <uses-permission android:name="com.android.launcher.permission.INSTALL_SHORTCUT"/>
      <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
      <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
      <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
      <supports-screens android:xlargeScreens="true" android:smallScreens="true" android:resizeable="true" android:normalScreens="true" android:largeScreens="true"
          android:anyDensity="true"/>
    - <application android:name="evmember.sbl.nationalevidhan.application.MyNevaApplication" android:usesCleartextTraffic="true" android:supportsRtl="true"
      android:roundIcon="@drawable/app_launcher" android:requestLegacyExternalStorage="true" android:largeHeap="true" android:label="@string/app_name"
      android:icon="@drawable/app_launcher" android:hardwareAccelerated="true" android:fullBackupContent="false" android:debuggable="false" android:configChanges="locale"
      android:appComponentFactory="androidx.core.app.CoreComponentFactory" android:allowBackup="false">
          <uses-library android:name="org.apache.http.legacy" android:required="false"/>
        - <activity android:name="evmember.sbl.nationalevidhan.SplashActivity" android:theme="@style/Theme.NoTitle" android:screenOrientation="portrait"
          android:noHistory="true">
            - <intent-filter>
                  <action android:name="android.intent.action.MAIN"/>
                  <category android:name="android.intent.category.LAUNCHER"/>
              </intent-filter>
          </activity>
          <activity android:name="evmember.sbl.nationalevidhan.TodayBirthdayActivity" android:configChanges="orientation" android:theme="@style/AppTheme"
              android:screenOrientation="portrait"/>
          <activity android:name="evmember.sbl.nationalevidhan.views.ChangePasswordActivity" android:configChanges="orientation" android:theme="@style/AppTheme"
              android:screenOrientation="portrait"/>
          <activity android:name="evmember.sbl.nationalevidhan.DebateTypeSearchActivity" android:configChanges="orientation" android:theme="@style/AppTheme"
              android:screenOrientation="portrait" android:windowSoftInputMode="adjustResize|stateHidden"/>
          <activity android:name="evmember.sbl.nationalevidhan.DebateGuidedSearchActivity" android:configChanges="orientation" android:theme="@style/AppTheme"
              android:screenOrientation="portrait" android:windowSoftInputMode="adjustResize|stateHidden"/>
```

Medium

5. Java Hash code is used in the application

1) Vulnerability Title: Java hash code is used in the application	
Risk	**Medium**
Abstract	It was observed that the App uses Java Hash Code.
Ease of Exploitation	Easy
Impact	It's a weak hash function and should never be used in Secure Crypto Implementation
Recommendations	Need to serialize the object to a byte stream (which you need to do anyway if you're going to send it over the network). If you're using a serialization that always maps the same values to the same sequence of bytes, you can just hash that byte stream. A cryptographic hash such as MD5 or SHA-1 would be ok for many cases, but might be a bit heavyweight if you're dealing with a really high throughput service.
Snapshot	 

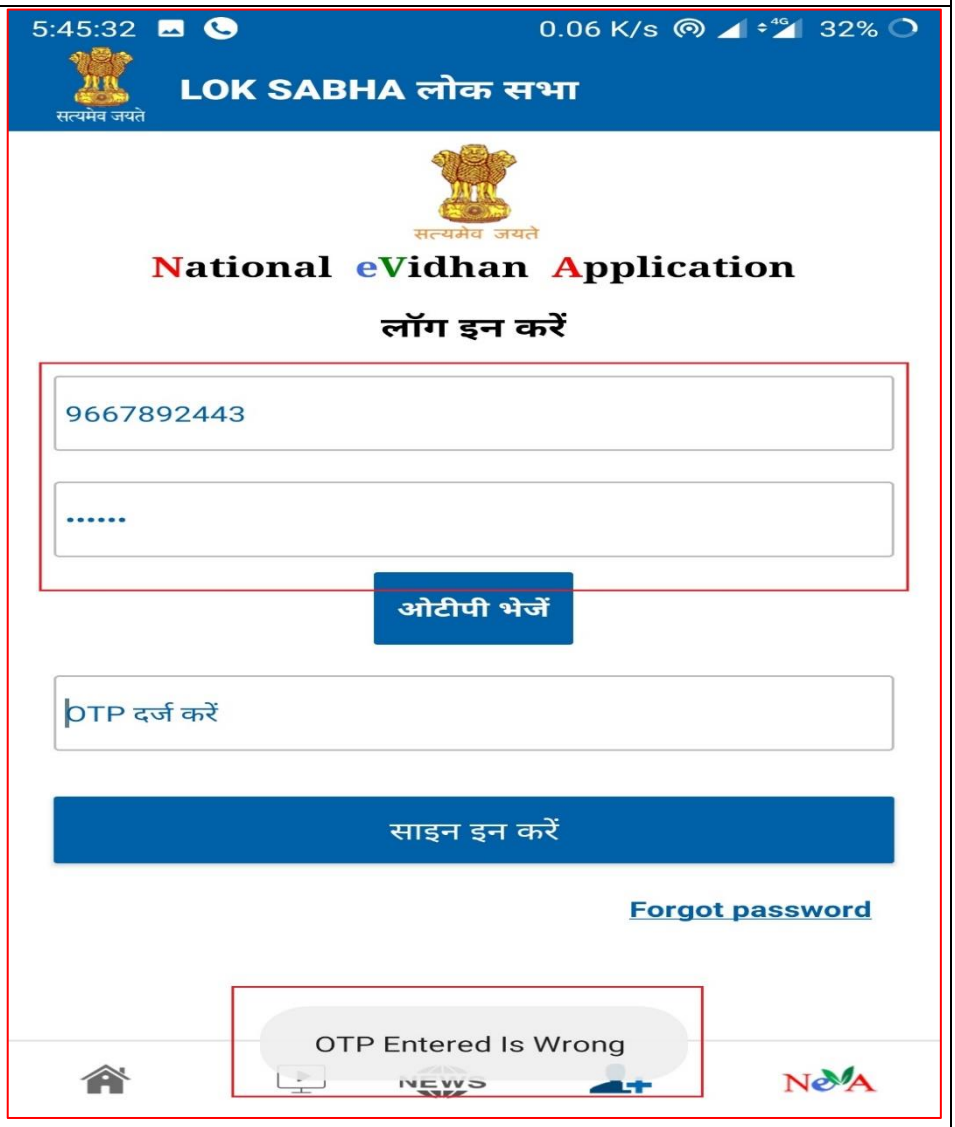
6. Base64 encoding is used in the application

2) Vulnerability Title: Base64 encoding is used in the application	
Risk	**Medium**
Abstract	It was observed that the App uses base64 encoding.
Ease of Exploitation	Easy
Impact	Base64 Encoded values can be decode easily.
Recommendations	It is recommended to use strong encryption along with salt value instead of Base64 encryption.
Snapshot	

```
private byte[] getBytes(String paramString) throws UnsupportedEncodingException {
  return paramString.getBytes("UTF-8");
}

private Cipher getCipher(int paramInt) throws Exception {
  Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
  byte[] arrayOfByte = getBytes(IV);
  cipher.init(paramInt, generateKey(), new IvParameterSpec(arrayOfByte));
  return cipher;
}

private String getString(byte[] paramArrayOfbyte) throws UnsupportedEncodingException {
  return new String(paramArrayOfbyte, "UTF-8");
}

public String decodeAndDecrypt(String paramString) throws Exception {
  byte[] arrayOfByte = Base64.decodeBase64(getBytes(paramString));
  return new String(getCipher(2).doFinal(arrayOfByte));
}

public String encryptAndEncode(String paramString) {
  try {
    s = getString(Base64.encodeBase64(getCipher(1).doFinal(getBytes(paramString))));
    PrintStream printStream = System.out;
    StringBuilder stringBuilder = new StringBuilder();
    this();
    stringBuilder.append("decryptedString ");
    stringBuilder.append(s);
    printStream.println(stringBuilder.toString());
    printStream = System.out;
    stringBuilder = new StringBuilder();
    this();
    stringBuilder.append("decryptedString ");
    stringBuilder.append(s);
    printStream.println(stringBuilder.toString());
```

Low

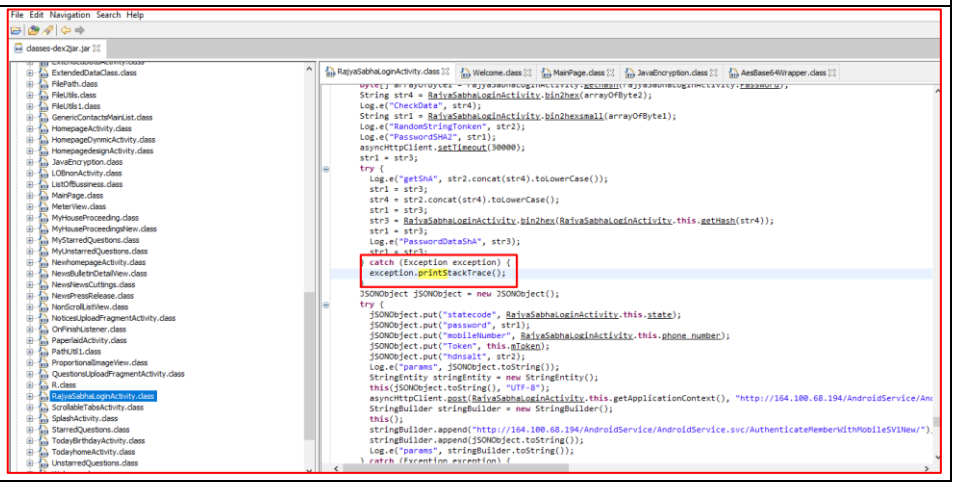
7. Input field is not getting cleared after invalid login attempts

1) Vulnerability Title: Input field is not getting cleared after invalid login attempts	
Risk	**Low**
Abstract	It was observed that form fields values are not getting cleared after an invalid attempt.
Ease of Exploitation	Easy
Impact	Attacker may misuse the details or user enumeration.
Recommendations	All login form field values must get clear on page refresh or reload.
Snapshot	

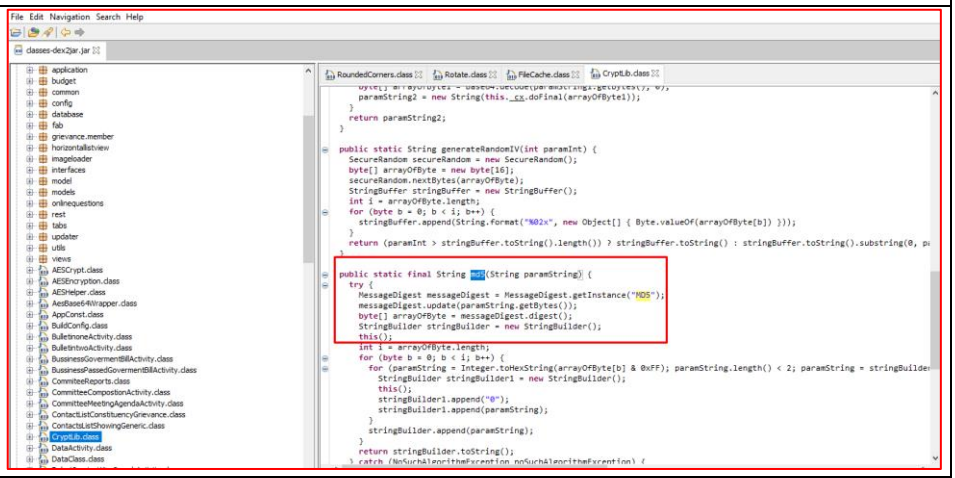
8. Change Password module is not implemented in the application

2) Vulnerability Title: Change Password module is not implemented in the application	
Risk	**Low**
Abstract	It was observed that change password module is missing in the app.
Ease of Exploitation	Easy
Impact	Change password allows administrators to customize the password change experience for the users from the begging to the end.
Recommendations	Change password module should be implemented in the application.
Snapshot	-

9. PrintStackTrace method is used in the application

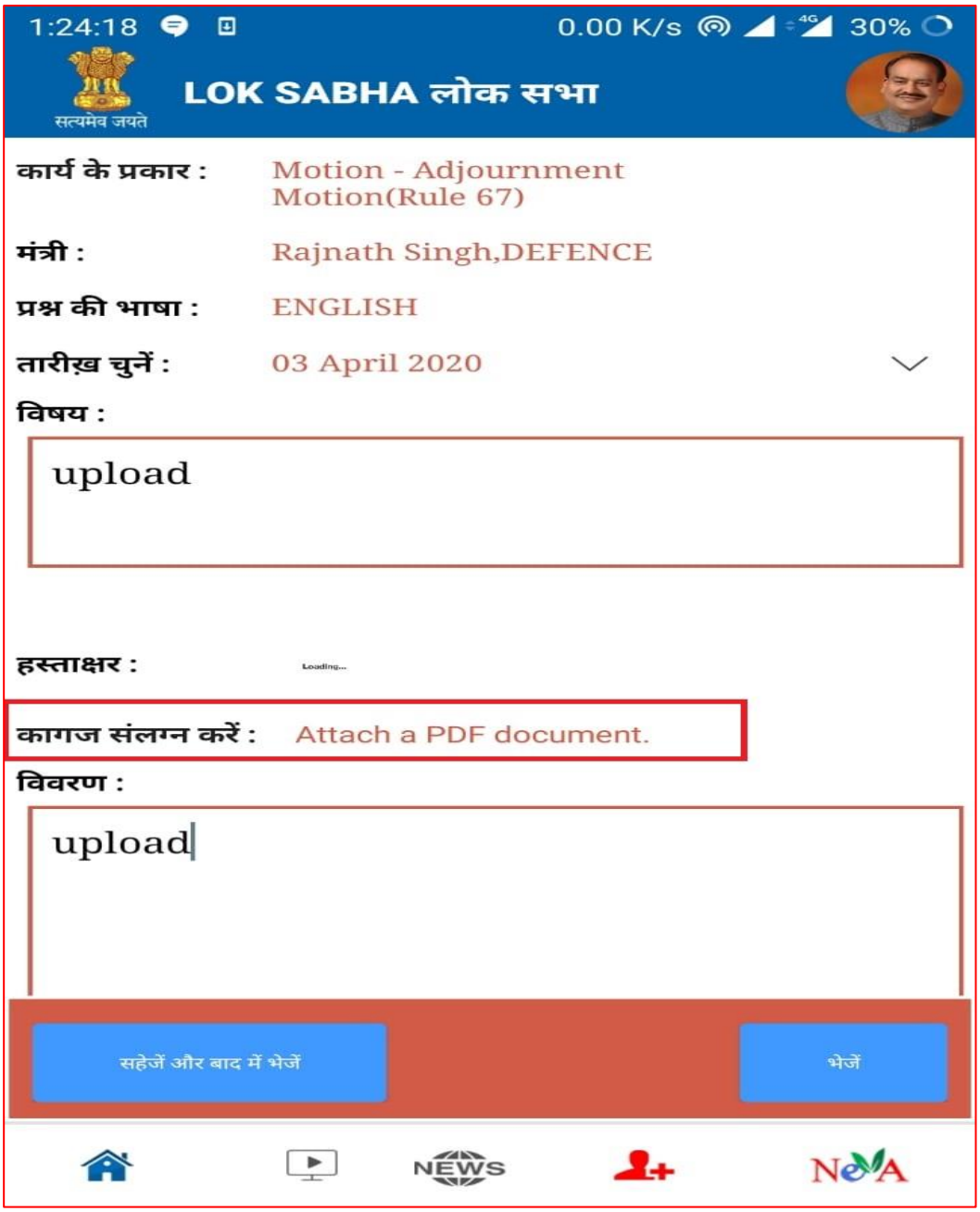
3) Vulnerability Title: PrintStackTrace method is used in the application	
Risk	**Low**
Abstract	It was observed that PrintStackTrace method is used in the app.
Ease of Exploitation	Easy
Impact	printStackTrace function is used for exception handling that may lead to data leakage.
Recommendations	The use of printStackTrace() exception method can reveal information about the application which may help an adversary in exploiting the application. The printStackTrace() method displays detailed information such as stack traces, database dumps, exception and application details. An adversary may gain sensitive information of application and can exploit the weakness. It is recommended not to use printStackTrace() method in production environment. Store such error messages on server side in error log file and display customized messages to the user
Snapshot	

10. Weak Hashing algorithm is used in the application

4) Vulnerability Title: Weak algorithm is used in the application	
Risk	**Low**
Abstract	It was observed that weak algorithm MD5 is used in the app.
Ease of Exploitation	Easy
Impact	Weak hashing algorithms [e.g. MD2, MD4, MD5, SHA-0 or SHA-1] can be vulnerable to hash collisions, so they should not be used when reliable data hashing is required
Recommendations	It is recommended to use strong hashing algorithm
Snapshot	

11. Functionality Issues

1. We are not able to upload file in Notice link.



2. Home page – Committee- Composition, meetings, reports links are not working, as dropdown is not showing any data.