NFSU National Forensic Sciences University
Knowledge | Wisdom | Fulfilment

An Institute of National Importance
(Ministry of Home Affairs, Government of India)

Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor & Associate Dean
School of Cyber Security and Digital Forensics
National Forensic Sciences University with status of Institution of National Importance

digvijay.rathod@gfsu.edu.in

Authentication

Based Access

Control Issues Part - II

Authentication Based Access Control Issues

- ✓ a.In this case the attacker authenticate him or herself and somehow get the access to protected resources or sensitive information that this issues comes under the authentication based access control issues.
- ✓ In this challenge is same as before but this case we have to access the protected resources which contain the twitter API credential but only difference is that you can access Twitter API credential after entering the PIN number,

Authentication Based Access Control Issues

- ✓ which means that you are authenticated and then only you can access the sensitive information with the option register now or already registered.
- ✓ c.Now our job is to abuse this mechanism and by pass the authenticate check.
- ✓ d.DIVA: Access Control Issues Part – 2. In this case to view the view twitter API Credentials either by register now or by already registered.

Authentication Based Access Control Issues

- ✓ e.If you click on register now then it as for register with http://payatu.com to get you pin and then login with the PIN.
- ✓ f.In the second scenario Already Register then we are able to see the Twitter API credential.
- ✓ g.Now we can invoke the activity which shows twitter API credential directly,

Authentication Based Access Control Issues

- ✓ h.santoku@santoku:Desktop/jadx/bin/diva:#
- ✓ i.santoku@santoku:Desktop/jadx/bin/: # vim AdndroidManifest.xml
- ✓ j.you can finds all the activity with their respective permission in the manifest file.

Authentication Based Access Control Issues

- ✓ k.Find the activity entry android name=”jakhar.aseem.diva.AccessControl2Activity”, this activity which contain button label with ViewAPICredentials and when we click on it as we observed it will open one more activity which is registered as android name=”jakhar.aseem.diva.APICreds2Activity” in the manifest.xml file. This activity contain sensitive information related to API.

Authentication Based Access Control Issues

- ✓ l.Now AccessControl1Activity invokes the APICredsActivity activity using <intent-filter> activity
- ✓ <action android name=”jakhar.aseem.diva.action.VIEW_CREDS2” which contain API sensitive data.
- ✓ m.Now copy the above filter intent and opens using activity manger directly

Authentication Based Access Control Issues

- Every android has activity manger and we will use same.
- santoku@santoku:/$ adb shell
- root@santoku:/am // and you can see all the help / information related to activity mangar.
- root@santoku:$: am start –a jakhar.aseem.diva.action.VIEW_CREDS2 // intent filter

Authentication Based Access Control Issues

- ✓ hit enter and see in the Genymotion that the said activity has not opened because the said activity which contain Twitter API information can be open after entering the PIN number only. So it is protected and we can not access the said activity directly through Android Manger with start option.

Authentication Based Access Control Issues

- ✓ s.Let wee the source code so we can get inside of it.
- ✓ t.santoku@santoku:Desktop/jadx/bin/: # cd diva
- ✓ u.santoku@santoku:Desktop/jadx/bin/diva:# cd jakhar/
- ✓ v.santoku@santoku:Desktop/jadx/bin/diva/jakhar/: #cd assem/
- ✓ w.santoku@santoku:Desktop/jadx/bin/diva/jakhar/assem/: #cd diva
- ✓ x.santoku@santoku:Desktop/jadx/bin/diva/jakhar/assem/diva: #ls

Authentication Based Access Control Issues

- ✓ z.santoku@santoku:Desktop/jadx/bin/diva/jakhar/asse m/diva:# vim AccessControl2Activity.java
- ✓ aa.he in the source code we finds function public void viewAPICredentials(View view)
- ✓ it has one variable chk_pin which is of Boolean type. So every thing is controlled by the chk_pin value that is true or false.

Authentication Based Access Control Issues

- ✓ ab.So we need to pass the value of chk_pin with android manager but it is not that much easy.
- ✓ ac.Now remember chk_pin is not actual string but string.xml file contain the reference of string and actual value of chk_pin is different.
- ✓ ad.Now open the source code of diva-android from https://github.com/payatu/diva-android, from which we can download the source code.

Authentication Based Access Control Issues

- ✓ ae.Click on app folder and src (source) main res (resources) values string.xml. itcontain all the string with the values.
- ✓ af.Now search for chk_pin and found the following entry
- ✓ ag.<stringname="chk_pin">check_pin</string>
- ✓ ah.santoku@santoku:$ adb shell

Authentication Based Access Control Issues

- ✓ ai.root@santoku: check the option. Check the option of <INTENT> to pass the parameter we need to use
- ✓ -e (for string value), -ez (<EXTRA_KEY><EXTRA_BOOLEAN_VALUE>) with –a. For other value check other options.
- ✓ aj.root@santoku:$: am start –a jakhar.aseem.diva.action.VIEW_CREDS2 –ez "check_pin" false

Authentication Based Access Control Issues

- ✓ ak.Now check in the Gynimotion and found that activity is stared and shown the sensitive information of Twitter API without authentication.

NFSU National Forensic Sciences University
Knowledge | Wisdom | Fulfilment

विद्यया अमृतं अश्नुते

An Institute of National Importance
(Ministry of Home Affairs, Government of India)

Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor & Associate Dean
School of Cyber Security and Digital Forensics
National Forensic Sciences University with status of Institution of National Importance

digvijay.rathod@gfsu.edu.in