

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

(MINISTRY OF HOME AFFAIRS, GOVERNMENT OF INDIA)
AN INSTITUTE OF NATIONAL IMPORTANCE

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

Access Control Issues

Activity

- ✓ a. Access control issues arise when application does not authenticate user.
- ✓ b. Authorization check is missing
- ✓ c. Attacker with insufficient privilege can see the protected resource.
- ✓ This may be the case when attacker tries to access any sensitive information without authentication or if he / she authenticated but not authorized.

Activity

- ✓ d. It means that if developer does not manage authentication or authorization to access any resource this vulnerability may exist and can results in loss of sensitive information disclosure.

Diva: Access Control Issues : Part - I

- ✓ f.Challenges is available with options view API credential, means when you click on this button it opens one activity though which you can access / see API credential.
- ✓ g.Our job is to access this API credential directly through the activity without clicking on that button.
- ✓ h.Just open the DIVA and check what happen when you click on Access Control Issues – Part. As you can finds that after clicking the button it opens one activity which shows API key, Username and Password.

Diva: Access Control Issues : Part - I

- ✓ i. Now challenges is to show same sensitive information that is API key, Username and Password without clicking the button or without opening the DIVA application also.
- ✓ j. Let's open the source code and understand it.

Divya: Access Control Issues : Part - I

- ✓ k.Decompile the APK file with jadx
- ✓ l.santoku@santoku:-\$ cd desktop
- ✓ m.santoku@santoku:Desktop:# cd jadx/
- ✓ n.santoku@santoku:Desktop/ jadx/: #cd bin
- ✓ o.santoku@santoku:Desktop/jadx/bin/:#cd diva/
- ✓ p.santoku@santoku:Desktop/jadx/bin/diva:#ls
- ✓ ind android, AndroidManifest.xml, jakhar, and res files and directories

Diva: Access Control Issues : Part - I

- ✓ `santoku@santoku:Desktop/jadx/bin/:` # `vim`
`AdndroidManifest.xml`
- ✓ you can find all the activity with their respective permission in the manifest file.
- ✓ Find the activity entry android
`name="jakhar.aseem.diva.AccessControl1Activity"`,
this activity which contains button label with
`ViewAPICredentials` and when we click on it as we
observed it will open one more activity which is
registered as android

Diva: Access Control Issues : Part - I

- ✓ t.name="jakhar.aseem.diva.APICredsActivity" in the manifest.xml file. This activity contain sensitive information related to API.
- ✓ u.Now AccessControl1Activity invokes the APICredsActivity activity using <intent-filter> activity <action android:name="jakhar.aseem.diva.action.VIEW_CREDS" which contain API sensitive data.

Diva: Access Control Issues : Part - I

- ✓ v.Now copy the above filter intent and opens using activity manger directly
- ✓ w.Every android has activity manger and we will use same.
- ✓ x.santoku@santoku:/\$ adb shell
- ✓ y.root@santoku:/am // and you can see all the help / information related to activity mangar.

Diva: Access Control Issues : Part - I

- ✓ `z.root@santoku:$: am start -a jakhar.aseem.diva.action.VIEW_CREDS // intent filter`
- ✓ `aa.hit` enter and see in the Genymotion that the said activity has opened without clicking the button and it shows same sensitive information.

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