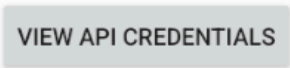


Lecture 8

9. Access Control Issues – Part 1

In this task, there is a button <View API Credentials> that, when pressed, shows the following:

9. Access Control Issues - Part 1	Vendor API Credentials
<p>Objective: You are able to access the API credentials when you click the button. Now, try to access the API credentials from outside the app.</p> <p>Hint: Components of an app can be accessed from other apps or users if they are not properly protected. Components such as activities, services, content providers are prone to this.</p>	<p>API Key: 123secretapikey123 API User name: diva API Password: p@ssword</p>



When we open the adb logcat and click on the button, we can find the activity name.

Command – logcat | grep -i “APICredActivity”

```
130|emudxa:/data/data/jakhar.aseem.diva/shared_prefs # logcat | grep -i "APICredActivity"
06-10 10:47:10.823 604 2209 I ActivityTaskManager: START u0 {act-jakhar.aseem.diva.action.VIEW_CREDS cmp=jakhar.aseem.diva/.APICredActivity} with LAUNCH_MULTIPLE from uid 10196 (BAL_ALLOW_VISIBLE_WINDOW)
result code=0
06-10 10:47:10.824 1103 1147 V WindowManagerShell: Transition requested: android.os.BinderProxy@9df57a0 TransitionRequestInfo { type = OPEN, triggerTask = TaskInfo{userId=0 taskId=31 displayId=0 isRunning=true baseIntent=Intent { act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] flg=0x10200000 cmp=jakhar.aseem.diva/.MainActivity } baseActivity=ComponentInfo{jakhar.aseem.diva/jakhar.aseem.diva.MainActivity} topActivity=ComponentInfo{jakhar.aseem.diva/jakhar.aseem.diva.MainActivity} numActivities=3 lastActiveTime=15806753 supportsMultiWindow=true resizeMode=4 isResizable=true minWidth=-1 minHeight=-1 defaultMinSize=220 token=ACT{android.window.WindowContainerToken$Stub$Proxy@68b3f59} topActivityType=1 pictureInPictureParams=null shouldDockBigOverlays=false launchIntoPipHostTaskId=-1 lastParentTaskIdBeforePip=-1 displayCutoutSafeInsets=null topActivityInfo=ActivityInfo{e6d471e jakhar.aseem.diva.APICredActivity} launchCookies=[android.os.BinderProxy@d20b82] positionInParent=Point(0, 0) parentTaskId=-1 isFocused=true isVisible=true isVisibleRequested=true isSleeping=false topActivityInSizeCompat=false topActivityEligibleForLetterboxEducation=false topActivityLetterboxed=false isFromDoubleTap=false topActivityLetterboxVerticalPosition=-1 topActivityLetterboxHorizontalPosition=-1 topActivityLetterboxWidth=-1 topActivityLetterboxHeight=-1 locusId=null displayAreaFeatureId=1 cameraCompatControlState=hidden, remoteTransition=null, displayChange=null }
06-10 10:47:10.830 604 2174 D CoreBackPreview Window/228f3a u0 jakhar.aseem.diva/jakhar.aseem.diva.APICredActivity: Setting back callback OnBackInvokedCallbackInfo{mcallback=android.window.OnBackInvokedCallback$Stub$Proxy@774e59, mPriority=0, mAnimationCallback=false}
06-10 10:47:10.976 604 629 I ActivityTaskManager: Displayed jakhar.aseem.diva/.APICredActivity for user 0: +162ms
06-10 10:47:10.976 1103 1147 V WindowManagerShell: onTransitionReady android.os.BinderProxy@9df57a0: {id=138 t=OPEN f=0x0 trk=0 r=[0@Point(0, 0)] c=[{null m=OPEN f=NONE leash=Surface(name=ActivityRecord{6169a07 u0 jakhar.aseem.diva/.APICredActivity})/@0xf669bfff sb=Rect(0, 0 - 0, 0) eb=Rect(0, 0 - 1080, 2220) eo=Point(0, 73) d=-1-x0 r=-1-x0:-1}, {null m=TO_BACK f=NONE leash=Surface(name=ActivityRecord{a37fc27 u0 jakhar.aseem.diva/.AccessControlActivity})/@0x8724dccc sb=Rect(0, 73 - 1080, 2082) eb=Rect(0, 0 - 1080, 2220) eo=Point(0, 73) d=0}}]
06-10 10:47:10.976 604 629 V WindowManager: Sent Transition #138 createdAt=06-10 10:47:10.811 via request=TransitionRequestInfo { type = OPEN, triggerTask = TaskInfo{userId=0 taskId=31 displayId=0 isRunning=true baseIntent=Intent { act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] flg=0x10200000 cmp=jakhar.aseem.diva/.MainActivity } baseActivity=ComponentInfo{jakhar.aseem.diva/jakhar.aseem.diva.MainActivity} topActivity=ComponentInfo{jakhar.aseem.diva/jakhar.aseem.diva.MainActivity} numActivities=3 lastActiveTime=15806753 supportsMultiWindow=true resizeMode=4 isResizable=true minWidth=-1 minHeight=-1 defaultMinSize=220 token=ACT{RemoteToken{7fcc19f Task{c74ceaf #31 type=standard A=10196:jakhar.aseem.diva}}} topActivityType=1 pictureInPictureParams=null shouldDockBigOverlays=false launchIntoPipHostTaskId=-1 lastParentTaskIdBeforePip=-1 displayCutoutSafeInsets=null topActivityInfo=ActivityInfo{2936f91 jakhar.aseem.diva.APICredActivity} launchCookies=[android.os.BinderProxy@09f26b5] positionInParent=Point(0, 0) parentTaskId=-1 isFocused=true isVisible=true isVisibleRequested=true isSleeping=false topActivityInSizeCompat=false topActivityEligibleForLetterboxEducation=false topActivityLetterboxed=false isFromDoubleTap=false topActivityLetterboxVerticalPosition=-1 topActivityLetterboxHorizontalPosition=-1 topActivityLetterboxWidth=-1 topActivityLetterboxHeight=-1 locusId=null displayAreaFeatureId=1 cameraCompatControlState=hidden, remoteTransition=null, displayChange=null }
06-10 10:47:10.976 604 629 V WindowManager: Info{id=138 t=OPEN f=0x0 trk=0 r=[0@Point(0, 0)] c=[{null m=OPEN f=NONE leash=Surface(name=ActivityRecord{6169a07 u0 jakhar.aseem.diva/.APICredActivity})/@0x869901b sb=Rect(0, 0 - 0, 0) eb=Rect(0, 0 - 1080, 2220) eo=Point(0, 73) d=-1-x0 r=-1-x0:-1}, {null m=TO_BACK f=NONE leash=Surface(name=ActivityRecord{a37fc27 u0 jakhar.aseem.diva/.AccessControlActivity})/@0x9b5b58 sb=Rect(0, 73 - 1080, 2082) eb=Rect(0, 0 - 1080, 2220) eo=Point(0, 73) d=0}}]
06-10 10:47:10.977 1103 1147 V WindowManagerShell: Transition doesn't have explicit remote, search filters for match for {id=138 t=OPEN f=0x0 trk=0 r=[0@Point(0, 0)] c=[{null m=OPEN f=NONE leash=Surface(name=ActivityRecord{6169a07 u0 jakhar.aseem.diva/.APICredActivity})/@0xf669bfff sb=Rect(0, 0 - 0, 0) eb=Rect(0, 0 - 1080, 2220) eo=Point(0, 73) d=-1-x0 r=-1-x0:-1}, {null m=TO_BACK f=NONE leash=Surface(name=ActivityRecord{a37fc27 u0 jakhar.aseem.diva/.AccessControlActivity})/@0x8724dccc sb=Rect(0, 73 - 1080, 2082) eb=Rect(0, 0 - 1080, 2220) eo=Point(0, 73) d=0}}]
06-10 10:47:10.977 1103 1147 V WindowManagerShell: start default transition animation, info = {id=138 t=OPEN f=0x0 trk=0 r=[0@Point(0, 0)] c=[{null m=OPEN f=NONE leash=Surface(name=ActivityRecord{6169a07 u0 jakhar.aseem.diva/.APICredActivity})/@0xf669bfff sb=Rect(0, 0 - 0, 0) eb=Rect(0, 0 - 1080, 2220) eo=Point(0, 73) d=-1-x0 r=-1-x0:-1}, {null m=TO_BACK f=NONE leash=Surface(name=ActivityRecord{a37fc27 u0 jakhar.aseem.diva/.AccessControlActivity})/@0x8724dccc sb=Rect(0, 73 - 1080, 2082) eb=Rect(0, 0 - 1080, 2220) eo=Point(0, 73) d=0}}]
```

So we run the following command:

adb shell am start -n jakhar.aseem.diva/.APICredActivity

and confirm that when we run the following command with the device on the screen with the button.

```
C:\Users\Giridharan\Desktop\Android Security\jdx\bin>adb shell am start -n jakhar.aseem.diva/.APICredsActivity
Starting: Intent { act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER] pkg=-n }
```

And it automatically shows the screen with the credentials without restrictions, like we had pressed the button.