Ders 9 - Access Control Issues - Part 1

Dersin Hedefi

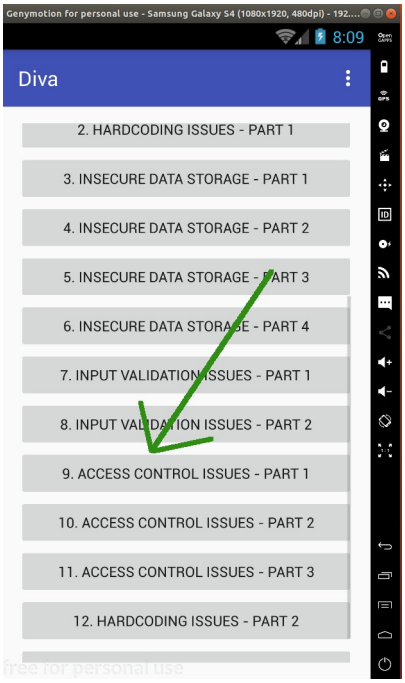
Diva uygulamasındaki “Access Control Issues - Part 1” seçeneğine tıklayın. Uygulama sayfasında senaryo gereği oturumunuz açıkken API Creds seçeneği ile üçüncü taraf api hesap bilgileriniz görüntülenecektir. Bu sayfayı uygulama oturumunuz açık değilken görüntülemeye çalışın.

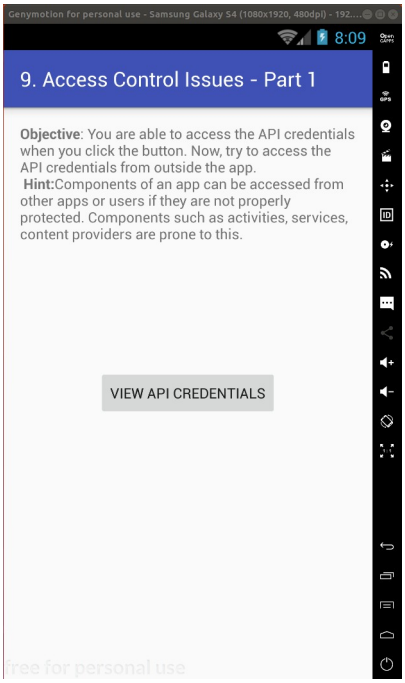
Dersin Açıklaması

Access Control Issues, yani erişim kontrol problemleri uygulama sayfalarından yetkili kişilerin erişebildikleri sayfalara yetkisiz kişilerin erişiminin de yanlışlıkla açık bırakılmasına denir.

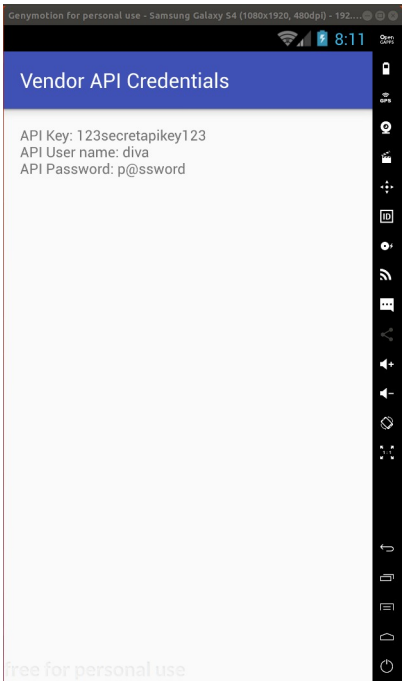
Dersin Çözümü

Ders sayfasına bir göz atalım.

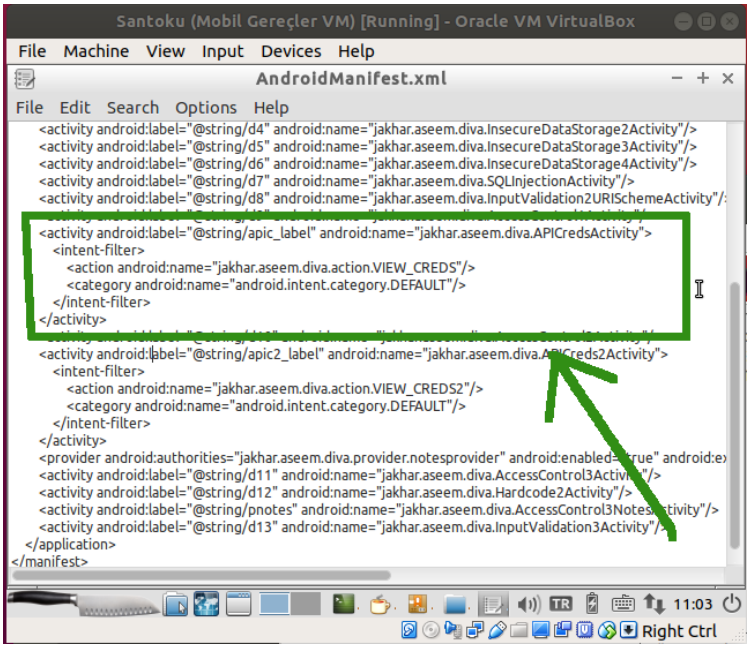




Uygulama sayfasında senaryo gereği uygulamada oturumumuz açıkken view api credentias ile üçüncü taraf bir api'a olan hesap bilgilerimiz ekrana verilmektedir.



Bizden istenen şey uygulamada oturumumuz açık değilken bu sayfayı çağırabilmemiz ve görüntüleyebilmemizdir. Bu işlem için öncelikle bu sayfanın dışarıdan başka uygulamalarca çağırılabilir olup olmadığına bakmamız gerekir. Bunu AndroidManifest.xml dosyasından öğrenebiliriz. Hatırlarsanız makale serisinin en başında apktool aracıyla AndroidManifest.xml dosyasını elde etmiştik:



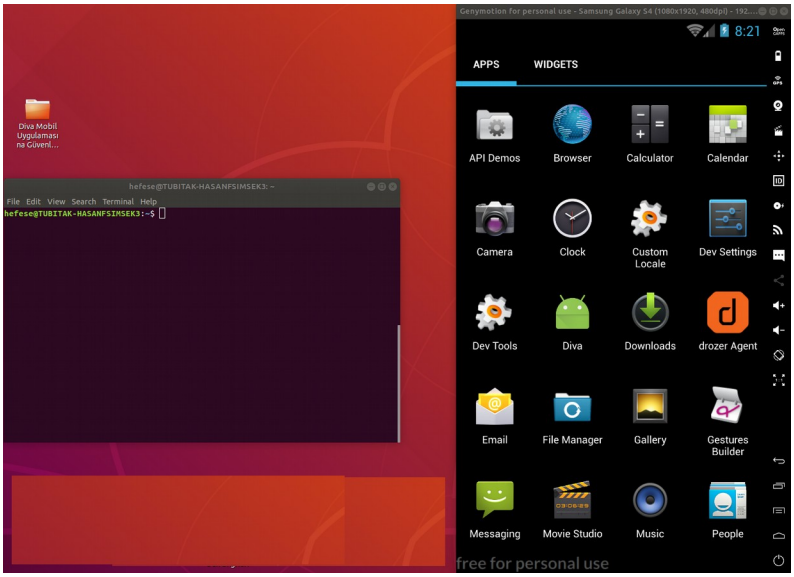
Görüldüğü üzere AndroidManifest.xml dosyasında üçüncü taraf api hesap bilgilerini görütüleyen sayfa <intent-filter> ile tanımlanmış. Bu durum uygulama sayfasının cihazdaki başka uygulamalarca çağırılabileceğini gösterir. Bu nedenle şimdi bilgisayardan mobil cihaza adb aracı ile bağlanalım ve üçüncü taraf api hesap bilgilerini gösteren sayfayı dışardan çağıralım.

Ubuntu 18.04 LTS Terminal:

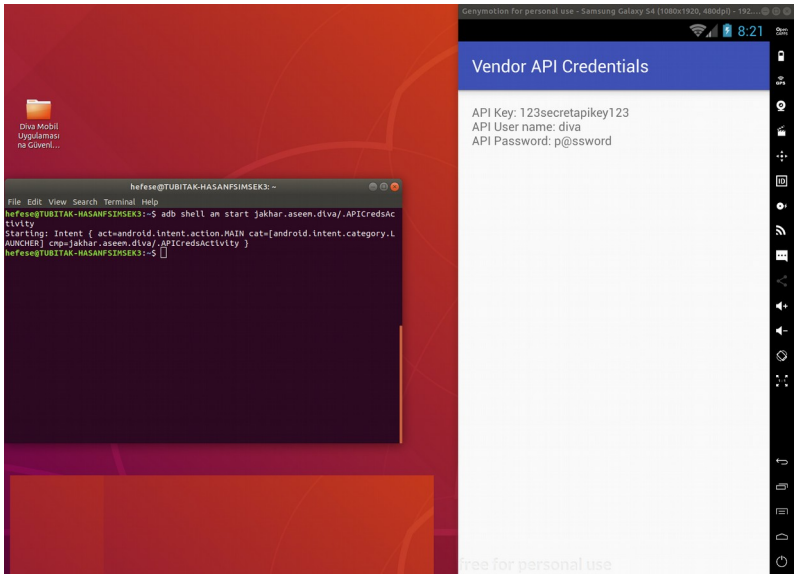
> adb shell am start jakhar.aseem.diva/.APICredsActivity

Not: am komutu (a)ctivity (m)anager'dır. start parametresi ile belirtilen activity'yi (sayfayı) çağırır.

Çıktı:



(Önce)



(Sonra)

Bir kötü niyetli kimse eline geçen mobil cihaz üzerinde örneğin normalde yetkili kişinin görüntüleyebileceği bir uygulama sayfasını bu şekilde çağırarak mobil cihaz kullanıcısının uygulamadaki hesap bilgilerini elde edebilir.

Sonuç

Başka uygulamalarca uygulama sayfasının çağırılması <intent-filter> tanımlaması nedeniyle olmaktadır. Kritik uygulama sayfalarında bu tanımlama kullanılmamalıdır. Aksi takdirde bu derste olduğu gibi dışardan kritik uygulama sayfası oturum vs. açmadan çağırılabilir.