Diva Mobil Uygulamasına Güvenlik Testleri Dersleri

Bu makalede Diva (Damn Insecure and Vulnerable Application) adlı kasıtlı zafiyet içeren bir mobil uygulamaya güvenlik testleri uygulanacaktır.

Gereksinimler

Santoku Mobile Security and Forensic Linux VM Samsung Galaxy S4 VM DIVA Vulnerable Mobile Application // Attacker Desktop VM // Victim Mobile VM // Victim Mobile App

Santoku adlı mobil güvenlik ve adli analiz araçlarının bulunduğu sanal makinadan hedef bir mobil cihazdaki zafiyete sahip mobil uygulamaya güvenlik testleri uygulanacaktır.

Öncelikle saldırıları düzenleyeceğimiz Santoku sanal makinasını başlatalım.





Santoku VM'de kullanacağımız araçlar şu şekildedir:

Santoku VM'de Kullanılacak Araçlar

// Reverse Engineering Tools// Reverse Engineering Tools// Dynamic Analysis Tool// Android Utilities

Ardından genymotion sanallaştırma aracı ile hedef bir mobil sanal sistem oluşturalım. Bunun için hedef mobil sanal sistem olarak Samsung Galaxy S4 belirleyelim.

Ubuntu 18.4 LTS Terminal:

> genymotion

					Genymotion				e e 😣
Geny	motion Help								
GEI	NYMOTION 00								۵
Fil Q	ters Search	Ø	Availab	le templates			Dentil		141
	Form factor Android API	> >	D	Custom Phone	4.1 - API 16	768 x 1280	320 - XHDPI	Genymotion	:
퍜	Density	>		Custom Tablet	4.1 - API 16	1536 x 2048	320 - XHDPI	Genymotion	:
4	Size	> >	0	Google Galaxy Nexus	4.1 - API 16	720 x 1280	320 - XHDPI	Genymotion	:
			0	Google Nexus 4	4.1 - API 16	768 x 1280	320 - XHDPI	Genymotion	1
			U	Google Nexus 7	4.1 - API 16	800 x 1280	213 - TVDPI	Genymotion	:
				Google Nexus S	4.1 - API 16	480 x 800	240 - HDPI	Genymotion	:
			0	HTC One X	4.1 - API 16	720 x 1280	320 - XHDPI	Genymotion	:
			0	HTC One XL	4.1 - API 16	720 x 1280	320 - XHDPI	Genymotion	:
			0	LG Optimus L3 II	4.1 - API 16	240 x 320	120 - LDPI	Genymotion	:
			6	Motorola Droid Razr	4.1 - API 16	540 x 960	240 - HDPI	Genvmotion	:

(Genymotion Sanallaştırma Aracı Başlar)

				Genymotion				008
Genymotion Help								
GENYMOTION			_					٠
Filters Q Search		0	HTC One XL	4.2 - API 17	720 x 1280	320 - XHDPI	Genymotion	:
Form factor	>	0	Motorola Moto X	4.2 - API 17	720 x 1280	320 - XHDPI	Genymotion	1
Android API	>	0	Samsung Galaxy Note 2	4.2 - API 17	720 x 1280	320 - XHDPI	Genymotion	:
크는 Density	>	0	Samsung Galaxy S3	4.2 - API 17	720 x 1280	320 - XHDPI	Genymotion	1
Source	>		Samsung Galaxy S4	4.2 - API 17	1080 x 1920	480 - XXHDPI	Genymotion	:
		0	Sony Xperia Tablet Z	4.2 - API 17	1920 x 1200	320 - XHDPI	Install	
/		0	Sony Xperia Z	4.2 - API 17	1080 x 1920	- XXH OPI	Details	Ctrl+I
		0	Custom Phone	4.3 - API 18	7 ox 1280	320 - XHDPI	Genymotion	1
		E	Custom Tablet	4.3 - API 18	1536 x 2048	320 - XHDPI	Genymotion	1
		0	Google Galaxy Nexus	4.3 - API 18	720 x 1280	320 - XHDPI	Genymotion	1
		E	Google Nexus 10	4.3 - API 18	2560 x 1600	320 - XHDPI	Genymotion	:
		0	Google Nexus 4	4.3 - API 18	768 x 1280	320 - XHDPI	Genymotion	1

(Samsung Galaxy S4 Mobil Sanal Sistemini Oluştur Denir)

		Genymotion			008
Genymotion Help					
GENYMOTION 00	Install virtual device		×		۰
Filters Q Search	Name Samsung Galaxy S4			motion	:
Form factor	Display			motion	:
I Android API	Predefined	1080 x 1920 - 480 - XXHDPI	•	motion	:
Density	O Custom		rmotion	:	
Source	Start in full-screen mode			rmotion	:
	System			rmotion	:
	Android version	4.	2 🕶	rmotion	:
	Processor(s)		1	motion	:
	Memory size		2048	motion	:
	Android system options			motion	:
				motion	:
		CANCEL	INSTALL	motion	:

(Samsung Galaxy S4 Mobil Sanal Sistemi İsmi Düzenlenir)

	Genym	otion			008
Genymotion Help					
GENYMOTION ⁰⁰	Install virtual device		×		,
Filters	O Custom			motion	:
Q Search	Start in full-screen mode			motion	:
Form factor	System			motion	
표 코는 Density	Android version		4.2 🔻	motion	
다. Size	Processor(s)				
Source	Memory size		2048	motion	:
	Android system options			motion	:
	Show Android navigation bar			motion	:
	Use virtual keyboard for text input			motion	:
	Network mode		1	motion	:
	O NAT (default)			motion	:
\rightarrow	🖲 Bridge 🥝	wlp2s0	V/	motion	:
		CANCEL	L INSTALL	/motion	:

(Samsung Galaxy S4 Mobil Sanal Sistemi Network Ayarı Düzenlenir)

				Genymotion					000
enymotion Help									
GENYMOTION									1
Filters	Ø	My inst	alled devices						2
Q Search		Туре	Device A	Android API	Size	Density	Source	Status	
Form factor	> >	0	MobSF_VM_0.3	4.1 - API 16	1080 x 1920	420	Genymotion	Off	:
Density	>	0	Samsung Galaxy S4	4.2 - API 17	1080 x 1920	480 - XXHDPI	Genymotion	Off	:
tī, size ● source	7	Availab	le templates						141
Source		Туре	Device	Android API	Size	Density	Source		
		0	Custom Phone	4.1 - API 16	768 x 1280	320 - XHDPI	Genymotion		:
			Custom Tablet	4.1 - API 16	1536 x 2048	320 - XHDPI	Genymotion		÷
		0	Google Galaxy Nexus	4.1 - API 16	720 x 1280	320 - XHDPI	Genymotion		:
		0	Google Nexus 4	4.1 - API 16	768 x 1280	320 - XHDPI	Genymotion		:
		0	Google Nexus 7	4.1 - API 16	800 x 1280	213 - TVDPI	Genymotion		:
		0	Google Nexus S	4.1 - API 16	480 x 800	240 - HDPI	Genymotion		:
			UTC D AC LTC		700-1000		e		

(Genmotion Cihazlarım Sekmesine Samsung Galaxy S4 Mobil Sanal Sistemi Yerleşir)

				Genymotion					••
enymotion Help									
GENYMOTION 00									(
Filters Q Search	Ø	My inst	alled devices						
Form factor	>	Type	MobSF_VM_0.3	4.1 - API 16	1080 x 1920	420	Genymotion	Off	J
Density	>	0	Samsung Galaxy S4	4.2 - API 17	1080 × 1920	480 - XXHDPI	Genymotion	Off	1
Source	> >	Availab	le templates			7	Start Edit		
		Туре	Custom Phone	Android API A	Size 768 x 128	320 - XHDPI	Delete Duplicate		
			Custom Tablet	4.1 - API 16	1536 x 2048	320 - XHDPI	Factory reset		
		0	Google Galaxy Nexus	4.1-116	720 x 1280	320 - XHDPI	Generate logs	-	Ctrl+K
			Google Nexus 4 Google Nexus 7	4.1 - API 16	768 x 1280 800 x 1280	320 - XHDPI 213 - TVDPI	Genymotion		:
		0	Google Nexus S	4.1 - API 16	480 x 800	240 - HDPI	Genymotion		:
					700	000 1000	C		

(Samsung Galaxy S4 Mobil Sanal Sistemi Başlatılır)



(Samsung Galaxy S4 Mobil Sistemi Başlar)

Şimdi saldırgan makina ve hedef makina hazır olduğuna göre hedef makinaya zafiyete sahip DIVA adlı mobil uygulamayı yükleyelim.

Ubuntu 18.04 LTS Terminal:

(

not: Ubuntu 18.04 LTS ana makinaya adb tool'u kurulumu için bkz. Yaz Tatili 2014 / Android Mobil Belgeler / Adb Kurulumu.txt

)

```
> adb devices
```

> adb install "/home/hefese/Desktop/diva-beta.apk"

Çıktı:



Görüldüğü üzere adb tool'u ile Diva adlı vulnerable apk dosyası yüklenir ve uygulama sanal mobil sisteme yerleşir.





Şimdi testlere geçelim.

Başlangıç: Android Uygulamalarda Tersine Mühendislik ile Okunabilir Java Kaynak Kodları Elde Etme (Dex2Jar, JD-GUI, ApkTool)

Başlangıç olarak santoku saldırgan sistemimizden hedef mobil sistemdeki Diva adlı zafiyete sahip mobil uygulamanın tersine mühendislik ile okunabilir kaynak kodlarını (.java kaynak kodlarını ve sonra .smali assembly kaynak kodlarını) elde edelim. Çünkü bu kaynak kodlar uygulanacak güvenlik testlerinde üzerlerinden geçilerek tespit / teyit / ... gibi işlemlerde yardımcı olacaktır.

[-] Uyarı:

Santoku sanal makinası genymotion mobil sanal makinasını göremediğinden / erişemediğinden Santoku makinasında yüklü adb aracıyla genymotion mobil sanal makinasındaki .apk çekilememektedir. Bu nedenle önce ana makinadan genymotion mobil sanal makinasındaki apk dosyası çekilecektir ve sonra Santoku sanal makinasına ana makinadaki apk dosyası scp ile kopyalanacaktır.

Ana makinadan hedef mobil sistemdeki zafiyete sahip Diva isimli uygulamayı çekebilmek için dosya yolunu tespit edelim.

Ubuntu 18.04 LTS Terminal:

> adb shell root@android:/# cd /data/app/ root@android:/data/app# ls | grep "diva" Çıktı:

jakhar.aseem.diva-1.apk root@android:/data/app# exit

Hedef sanal mobil sistemdeki zafiyete sahip Diva isimli uygulamanın dosya yolu tespiti (/data/app/jakhar.aseem.diva-1.apk) sonrası ana makinadan adb pull komutu ile Diva apk uygulamasını çekelim.

Ubuntu 18.04 LTS Terminal:

> adb pull "/data/app/jakhar.aseem.diva-1.apk" "/home/hefese/Desktop/jakhar.aseem.diva-1.apk"

Çıktı:



Sonra ana makinadaki Diva apk dosyasını santoku sanal makinasına scp ile kopyalayalım.

Santoku Terminal:

(Not: scp için santoku sanal sisteminde ssh server kurulu olmalıdır)

> sudo su
> apt-get install openssh-server

Şifre : santoku
ssh server kurulur

Ubuntu 18.04 LTS Terminal:

> scp "/home/hefese/Desktop/jakhar.aseem.diva-1.apk"
santoku@192.168.0.15:"/home/santoku/Desktop/jakhar.aseem.diva-1.apk"

Çıktı:



Böylece Santoku sistemi hedef mobil sistemdeki apk dosyasını alır.



Şimdi Santoku sanal sistemindeki tersine mühendislik araçları ile Diva isimli mobil uygulama apk dosyasından okunabilir kaynak kodlar elde edelim.

i) Dex2Jar ve JD-GUI

Mobil uygulama dosyasındaki (.apk'daki) binary kodlardan okunabilir .java kaynak kodları elde etmek için dex2jar dönüştürme aracı kullanılabilir. JD-GUI aracı ile de okunabilir .java kaynak kodları görüntülenebilir.

Bilgi:

Android sistemlerde mobil uygulama dosyaları (.java dosyaları) derlendiklerinde .dex (dalvik executable) çalıştırılabilir formatında olurlar. Bu .dex (dalvik executable) çalıştırılabilir formatındaki dosyalar tek bir dosya halinde sıkıştırıldıklarından .apk halinde olurlar. Dex2Jar ile mobil uygulama dosyasını (dex dosyalarını) okunabilir .java kaynak kodları haline dönüştürelim.

Santoku Terminal:

> dex2jar /home/santoku/Desktop/jakhar.aseem.diva-1.apk

Çıktı:



Dönüşen .java okunabilir kaynak kodlarını görüntüleyelim.

Santoku Terminal:

> jd-gui

Çıktı:

	(u (Mobil Gereçler VM) [Running] - Oracle VM	VirtualBox 🛛 🖨 🖨 🕻
File Machine Vie	w Input Devices Help	
<u>Ó</u>	Java Decompiler	- + ×
File Edit Navigate	2 Search Help	
🕒 Open File	Ctrl+O	
🛛 Close	Ctrl+W	
🛓 Save Source	Ctrl+S	
Save All Sources	Ctrl+Alt+S	
Recent Files	•	
🕞 Exit	Alt+X	

	Open File			- +
'				,
Places	Name		Size	Modified
Search	📔 jakhar.aseem.diva-1_dex2jar.j	ar	2,0 MB	17:32
Recently Used				
santoku				
Desktop				
File System				
Documents				
a Music				
Music Pictures				
9 Music 9 Pictures 9 Videos				
a Music 9 Pictures 9 Videos 9 Downloads				
a Music ∋ Pictures ∋ Videos ∋ Downloads ⊕ =		All f	iles	





ii) ApkTool

Mobil uygulama dosyasındaki (.apk'daki) binary kodlardan okunabilir .smali assembly kodları elde etmek için ve okunabilir AndroidManifest.xml dosyasını elde etmek için apktool aracı kullanılabilir.

[\] Bilgi: Smali Assembly Kodları Nedir

Smali ve Baksmali birer assembly / disassembly araçlarıdır. Android sistemlerdeki Dalvik Virtual Machine tarafından üretilen çalıştırılabilir android uygulama dosyalarını (.dex dosyalarını) assembly formatına çevirmeye veya geri dex formatına çevirmeye yarar. Bu araçlar dex formattaki tüm işlevleri (annotation'ları, debug bilgileri, satır bilgileri,...) destekler niteliktedir.

Örneğin; android java dosyasındaki;

int x = 42

ifadesi derlendiğinde ve çalıştırılabilir dex formatına dönüştüğünde şu binary koda (daha öz olarka hex koda) dönüşür:

13 00 2A 00

Eğer bu binary kodu baksmali aracı ile disassembly yaparsak,

const/16 v0, 42

okunabilir assembly kodu elde edilir. Yani dex binary kodundan baksmali aracı ile bir smali okunabilir assembly kodu elde edilir. Assembly koda smali assembly denmesinin nedeni smali aracı teknojisiyle dex binary kodlardan assembly kodların elde edilebiliyor olmasındandır veya elde edilen assembly kodlardan dex binary koda dönüşümün yapılabiliyor olmasındandır.

Şimdi apktool aracı ile okunabilir smali assembly kodlarını ve AndroidManifest.xml dosyasını elde edelim.

[!] Uyarı:

Santoku sanal sisteminde yüklü apktool aracı eski teknoloji içeren Diva adlı mobil uygulama dosyasından smali assembly dosyalarını ve manifest dosyasını çıkaramamıştır. Hata olarak major/minor versiyon uyuşmazlığı hatası vermiştir. Bu nedenle yararlanılan makalede apktool'unun eski sürümü 2.0.3 üzerinden gidilerek Diva uygulama dosyası üzerinde test yapıldığından internetten apktool'unun 2.0.3 eski sürümü indirilmiştir,

https://bitbucket.org/iBotPeaches/apktool/downloads/

ve java -jar ile apktool 2.0.3 sürümü diva mobil uygulama dosyası üzerinde başarılı bir şekilde çalıştırılabilmiştir.

Not: apktool aracının yeni sürümlerinde parametre syntax'ı değişmiştir.

Santoku Linux Terminal:

> cd Downloads
> chmod a+x apktool_2.0.3.jar
> java -jar apktool_2.0.3.jar d "/home/santoku/Desktop/jakhar.aseem.diva-1.apk"
-o ManifestVeAssemblyDosyalar/ // (*) d : decode

Çıktı:





apktool aracının mobil uygulama dosyasından (.apk'dan) dönüştürdüğü smali assembly dosyaları çıktı klasöründeki smali/ dizini altında yer alır.



apktool aracının mobil uygulama dosyasından (.apk'dan) dönüştürdüğü ve elde ettiği AndroidManifest.xml dosyası çıktı klasöründeki kök dizinde yer alır.



		Santo	ku (M	obil (Gereçler V	VM) [Ru	nning] -	Oracle	• VM Vir	tualBo	< C		0
File	Mach	ine Vie	ew In	nput	Devices	Help							
					Android	Manife	st.xml	3			-	+	×
File	Edit	Search	Optio	ons	Help								
xm<br <mar <us <us <us <us <us <us <us <us <us <us< td=""><td>l versio nifest xr es-pern es-pern es-pern activity <intent <activity activity activity activity activity activity activity activity activity activity activity activity activity activity activity activity activity activity activity</activity </intent </td><th>n="1.0" (mIns:and nission a nission a on android -filter> on android android android android android android android android android android android android android android android android android android android android android</th><th>encod Iroid= Iroid= Indroi Indroi Indroi Idcialld Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel</th><th>ing="" "http id:nan id:nan owBa ="@sl ="@sl ="@sl ="@sl ="@sl ="@sl ="@sl ="@sl ="@sl ="@sl</th><th>utf-8" star i//schema ne="andr ne="andr ckup="tru tring/app android.ii ="android. tring/d1" tring/d2" tring/d2" tring/d3" tring/d5" tring/d6" tring/d6" tring/d6" tring/d9" tring/apic</th><td>ndalone: as.andro pid.pern pid.pern pid.pern pid.pern me" andro andro andro d.intent.acd d.intent.acd d.intent.acd android android android android android android android android android android android</td><td>"no"?> id.com/ nission.l nission.l nission.l id:debu android: tion.MAI categor :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name"</td><td>apk/res WRITE_E READ_E NTERNI Iggable :name= IN"/> y.LAUN jakhar.a jakhar.a jakhar.a jakhar.a jakhar.a jakhar.a jakhar.a</td><td>s/androii EXTERNA XTERNA ET"/> ="true" a "jakhar.a CHER"/> aseem.di aseem.di aseem.di aseem.di aseem.di aseem.di aseem.di aseem.di aseem.di aseem.di aseem.di</td><td>d" packa L_STOR IL_STOR indroid: iseem.d iva.LogA iva.lnsec iva.lnsec iva.lnsec iva.lnsec iva.lnsec iva.sQLI iva.Acce seem.di</td><th>age="jak AGE"/> AGE"/> icon="@ iva.Main Activity" IcodeAc cureDat cureDat cureDat tureDat tureDat tureDat tureDat cureDat cureDat cureDat</th><td>khar. pmip nAct ctivit aSto aSto aSto nAct ion Cred!</td><td>a bi bi bi bi bi bi bi bi bi bi bi bi bi</td></us<></us </us </us </us </us </us </us </us </us </mar 	l versio nifest xr es-pern es-pern es-pern activity <intent <activity activity activity activity activity activity activity activity activity activity activity activity activity activity activity activity activity activity activity</activity </intent 	n="1.0" (mIns:and nission a nission a on android -filter> on android android android android android android android android android android android android android android android android android android android android android	encod Iroid= Iroid= Indroi Indroi Indroi Idcialld Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel: Iabel	ing="" "http id:nan id:nan owBa ="@sl ="@sl ="@sl ="@sl ="@sl ="@sl ="@sl ="@sl ="@sl ="@sl	utf-8" star i//schema ne="andr ne="andr ckup="tru tring/app android.ii ="android. tring/d1" tring/d2" tring/d2" tring/d3" tring/d5" tring/d6" tring/d6" tring/d6" tring/d9" tring/apic	ndalone: as.andro pid.pern pid.pern pid.pern pid.pern me" andro andro andro d.intent.acd d.intent.acd d.intent.acd android android android android android android android android android android android	"no"?> id.com/ nission.l nission.l nission.l id:debu android: tion.MAI categor :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name=" :name"	apk/res WRITE_E READ_E NTERNI Iggable :name= IN"/> y.LAUN jakhar.a jakhar.a jakhar.a jakhar.a jakhar.a jakhar.a jakhar.a	s/androii EXTERNA XTERNA ET"/> ="true" a "jakhar.a CHER"/> aseem.di aseem.di aseem.di aseem.di aseem.di aseem.di aseem.di aseem.di aseem.di aseem.di aseem.di	d" packa L_STOR IL_STOR indroid: iseem.d iva.LogA iva.lnsec iva.lnsec iva.lnsec iva.lnsec iva.lnsec iva.sQLI iva.Acce seem.di	age="jak AGE"/> AGE"/> icon="@ iva.Main Activity" IcodeAc cureDat cureDat cureDat tureDat tureDat tureDat tureDat cureDat cureDat cureDat	khar. pmip nAct ctivit aSto aSto aSto nAct ion Cred!	a bi bi bi bi bi bi bi bi bi bi bi bi bi
	Lances		<u>r</u> 7			N	<u></u> 		()) TR	🖻 💼	1 1	0:26	Ċ

Şimdi zafiyetler içeren Diva mobil uygulamasındaki zafiyetleri test edelim ve sömürme adımlarını görelim.

Kaynaklar

http://www.payatu.com/damn-insecure-and-vulnerable-app/

https://resources.infosecinstitute.com/cracking-damn-insecure-and-vulnerable-apps-diva-part-1/ #gref

https://resources.infosecinstitute.com/android-penetration-tools-walkthrough-series-drozer/#gref https://gurelahmet.com/mobil-android-s%C4%B1zma-testine-giri%C5%9F/

https://stackoverflow.com/questions/7750448/what-are-dex-files-in-android

https://stackoverflow.com/questions/30054156/apktools-apk-studio-could-not-decode-arsc-file https://bitbucket.org/iBotPeaches/apktool/downloads/

https://stackoverflow.com/questions/4191762/how-to-view-androidmanifest-xml-from-apk-file https://stackoverflow.com/questions/30054156/apktools-apk-studio-could-not-decode-arsc-file https://tools.kali.org/reverse-engineering/smali https://stackoverflow.com/guestions/20927450/what is smali code android

https://stackoverflow.com/questions/30837450/what-is-smali-code-android

Paketleme İçin Gözden Geçirilecekler / Mobil Hk / İnternetten Edinilmiş Belgeler / Adb Tool Nedir ve Kullanımı.docs#Uygulama 1