



Android Uygulama Güvenliğine Saldırgan Yaklaşım

Offensive Approach to Mobile Application Security

Ahmet GÜREL www.gurelahmet.com









- Blogger
- Canyoupwnme Ekip Üyesi
- Güvenlik Danışmanı / Sızma Testi Uzmanı







Eğitim Başlıkları

- Android Dünyasına Giriş
- Android Güvenlik Modeli
- Android Uygulamaları
- APK ve Paket İçeriği
- Android Tersine Mühendislik İşlemleri
- OWASP Mobil Top 10 Zafiyetleri
- Test Ortamının Kurulumu
- Android Uygulama Dosyaları
- Android Uygulama İzinleri
- SSL Pinning ve Bypass Yöntemleri
- Mobil Sızma Testi Araçları
- Mobil Sızma Testi Uygulamaları

Android Dünyasına Giriş

- Open Handset Alliance liderliğinde Google firması tarafından akıllı telefon ve tablet bilgisayarlar gibi mobil cihazlar için geliştirilmiş Linux tabanlı işletim sistemi.
- Android cihazlarda uygulamaların çalışabilmesi için .apk uzantılı dosyalar ile uygulamalar yüklenir ve cihazlara dağıtabilir.
- Günümüzde Native ve Hybrid uygulamalardan söz edilmekte.
- Native uygulama dediğimiz C++ veya Java dilini temel alan Android ile yazılan uygulamalar Native fakat HTML, CSS, JavaScript tabanlı kodu yazıp birçok platforma çıktı veren frameworkler ile geliştirildiğinde Hybrid uygulama olarak geçmektedir.

Neden Android ?

- Açık kaynak kodlu
- Linux tabanlı
- Kullanım yaygınlığı telefonlar, tabletler, arabalar...
- Gelişmiş ve ücretsiz yazılım geliştirme ortamı sunması
- Açık uygulama marketi

Android Kullanım Alanları

- Cep telefonları, tabletler, akıllı saatler vs....
- Arabalar, akıllı ev sistemleri
- Mobil bankacılık
- Internet of Things (IoT)

Android Güvenlik Modeli

- Linux güvenlik modeli baz alınmıştır (UID/GUID).
- Uygulama bazlı izinler kullanılmaktadır.
- Uygulama izinleri, AndroidManifest.xml dosyasında tanımlanmaktadır.
- Uygulama kurulumu için uygulamanın sertifika ile imzalanmış olması gerekmektedir.
- Her bir uygulama farklı bir DVM(Dalvik Virtual Machine) içerisinde çalışmaktadır.
- Sistem güvenliği açısından kullanıcı kilit rol oynamaktadır.
- Rootlanmamış bir cihaz için root erişimi mümkün değildir. "su" uygulaması sistemde bulunmaz.

Android Güvenlik Modeli





Android Uygulamaları

- Java + Android SDK ile geliştirilir.
- Android Dalvik VM ile çalıştırılır.
- JAVA -> .class -> .dex



Android Uygulamaları



$\mathbf{APK} = \mathbf{JAR} = \mathbf{ZIP}$

JAVA Archive

Android Application Package

APK

- Android Application Package File (APK) dosyası zip dosya formatına sahip .apk uzantılı dosyalardır.
- APK dosyasının uzantısı .zip olarak değiştirildikten sonra WinZip, WinRAR gibi arşiv programları ile dosya içeriği görüntülenebilir.







- İşlemci mimarisine göre compile edilmiş native kütüphaneler (Native ELF dosyaları)
- JAR Dosyaları (kütüphaneler)



- anim: Compile edilmiş
 animasyon dosyaları
- drawable: Resim dosyaları
- layout: UI/view tanımlamaları
- values: Diziler, renkler, style'lar, string'ler dimensions
- xml: Compile edilmiş XML dosyaları
- raw: <u>Compile edilmemiş</u> raw dosyalar

Compile işlemi AAPT (Android Asset Packaging Tool) tarafından yapılır



- Çoğu zaman raw dosyalar bulunur.
- Resimler, fontlar, ses dosyaları
- Bazı malware'ler bu dizinde cihaza kurrmak üzere APK dosyaları saklarlar





- DEX: Dalvik Executable
- Android'in EXE'si
- Dalvik VM üzerinde çalışır
- DEX: Dalvik VM için compile edilmiş class dosyaları



- Compile edilmiş resource'lar
 - R.java
 - string.xml
 - ids.xml
 - layouts.xml

Kaynak Kod Dönüşümü - Decompile



Decompile Dex -> JAR -> JAVA

Java Decompiler > JD-GUI > JAD > Jadx > Procyon > ...











JAVA

Kaynak Kod Dönüşümü - Decompile

 Dex2jar aracı ile class dosyasına dönüştürülmüş olan Android uygulaması, JD-GUI aracı ile kaynak koduna (decompile) geri çevirilebilir.

 Decompile işleminin yetersiz olduğu durumlarda incelenecek uygulamayı Disassembling işleminden geçirmek gerekebilir.

Android Tersine Mühendislik Dex2Jar

Adından da anlaşılacağı üzere dex dosyalarını jar dosyalarına çevirmektedir.

Resimde görüldüğü üzere apk dosyamızı jar haline getirdik.

Android Tersine Mühendislik Dex2Jar

C:\Mobil Pentest\dex2jar-0.0.9.15>dex2jar.bat insecurebank.apk this cmd is deprecated, use the d2j-dex2jar if possible dex2jar version: translator-0.0.9.15 dex2jar insecurebank.apk -> insecurebank_dex2jar.jar Done.

C:\Mobil Pentest\dex2jar-0.0.9.15>

Android Tersine Mühendislik

JD-GUI

JAR haline getirdiğimiz dosyamızı görüntülemek için kullanacağız.

🙀 javaw.exe (Admin)				- 🔒 📑	= _ [×
File Edit Navigation Search Help						^
😑 🥭 🦧 🖕 🔿						
👼 insecurebank_dex2jar.jar 🔀						
android.support annotation v4 v7 android.insecurebankv2 android.insecureb						

Kaynak Kod Dönüşümü - Decompile

- Decompile edilmiş JAR kodu tekrar compile edilerek çalıştırılabilir hale getirilemez.
- Decompile edilen kod yaklaşık koddur. %100 geri dönüşüm gerçekleştirilemez.
- Dex2jar çıktısından elde edilen JAR kodu çalıştırılamaz.
- Dalvik Bytecode, JAR koduna dönüştürülerek kolay okunabilir ve anlaşılabilir hale gelir.

Disassembling



Disassemble Dex -> .smali









.smali .smali .smali

Dex Disassembler > Baksmali > Dedexer > apktool

Android Tersine Mühendislik APKTool

APKTool apk dosyalarını decompile ederek smali kodlarına dönüştürür.

Kullanımı oldukça basit aşağıdaki resimde görüldüğü üzere b parametresi ile decompile etmekte.

Android Tersine Mühendislik APKTool

Komut İstemi Microsoft Windows [Version 10.0.14393] (c) 2016 Microsoft Corporation. Tüm hakları saklıdır. :\Users\Ahmet GUREL>cd C:\ C:\>cd "Mobil Pentest\APKTool" :\Mobil Pentest\APKTool>apktool.bat b insecurebank.apk Exception in thread "main" brut.androlib.AndrolibException: brut.directory.PathNotExist: apktool.yml at brut.androlib.Androlib.readMetaFile(Androlib.java:143) at brut.androlib.Androlib.build(Androlib.java:160) at brut.androlib.Androlib.build(Androlib.java:155) at brut.apktool.Main.cmdBuild(Main.java:182) at brut.apktool.Main.main(Main.java:67) Caused by: brut.directory.PathNotExist: apktool.yml at brut.directory.AbstractDirectory.getFileInput(AbstractDirectory.java:103) at brut.androlib.Androlib.readMetaFile(Androlib.java:139) ... 4 more

C:\Mobil Pentest\APKTool>

Disassembling

Disassemble DEX -> .smali

DEX dosyası okunabilir Dalvik Bytecode'a dönüştürülüyor.

.smali uzantılı Dalvik bytecode modifiye edilebilir.

Modifiye edilen Dalvik bytecode tekrar imzalanır, paketlenir ve cihazda çalıştırılabilir.

Baksmali aracı ile disassemble işlemi yapılabilir.

Alınabilecek Önlemler / Anti Reversing

Kod Karmaşıklaştırma - Obfuscation



Progaurd



Dexgaurd





Java obfuscators

Alınabilecek Önlemler / Anti Reversing

Kod Karmaşıklaştırma - Obfuscation

- Kullanılmayan sınıflar, metodlar temizlenir.
- Bytecode optimize edilir.
- Kullanılmayan instructionlar temizlenir.
- Geriye kalan sınıflar, metodlar, alanlar ve değişkenler anlamsız kısa isimlerle adlandırılır.
- ProGuard, DexGuard ile obfuscation önlemi alınabilir.
- ALLATORI ile analistleri çıldırtacak obfuscation önlemleri alınabilir.

Alınabilecek Önlemler / Anti Reversing

Kod Karmaşıklaştırma - Obfuscation


Alınabilecek Önlemler / Anti Reversing

Kod Karmaşıklaştırma - Obfuscation

public class MyVehicleClass{

private Motor private Tekerlek private int myMotor; myTekerler; vitesSayisi;

public int suratHesapla(int sure){

....

}

}

return sonSurat;

public class A{ private B a; private C b; private int C; public int a(int a){ . . . return c;

Deobfuscation - Simplify

\varTheta 🔿 🎯 JEB		2 0 0	JEB – smali_simple.dex
🗎 🛃 🖉 🖸	🖤 🖣 🕨 😰 🙀 📉 C. 📉	🖴 💾 🧨 🛞 🧲 🕇	V 4 D O X N C X
evb	Assembly Decompiled Java 🖾 Strings Constants Notes	gdk	Assembly Decompiled Java 🕅 Strings Constants Notes
f	smiring = nuerder (nuerna) (//)	gtx	
fao	smv.hnn = 2;	n	smv.hnn = 2;
fin	smv.hmv = new int[]{75, 163099954, 300, 176529550, 1202, 31458303, 48	1e nom	<pre>smv.hmv = new int[]{75, 163099954, 300, 176529550, 1202, 31458303,</pre>
a	(10909, 11231, 30/842, 07/60, 1231553, 9627);	1	76969, 11231, 307842, 67760, 1231553, 9627};
adk	smv.itw = kut.ger(kut.hmv());	3	smv.olz = "000000001";
gan	<pre>smv.dsr = kut.ger(kut.olz());</pre>	jmi	Smv.jtw = "00000010";
BTX P	<pre>smv.eos = kut.qer(kut.jtw());</pre>	jpw	Smv. asr = 00000100;
n	<pre>smv.bst = kut.qer(kut.dsr());</pre>	jun	smv.bst = "000010000";
nam	<pre>smv.vav = kut.qer(kut.eos());</pre>	k	smv.vav = "000100000";
1	<pre>smv.dvf = kut.qer(kut.bst());</pre>	ksz	smv.duf = "001000000";
j	Smv.xrn = 2131298007;	kut	smv.xrh = 2131298007;
jmi	Smv. wun = 2131298000;	1	smv.djc = 2131298008;
јрw	smv. qqo = 2131298010;	lkh	smv.wun = 2131298009;
jun	smv.yln = 2131298011;		Smv.gqo = 2131298010;
k	<pre>smv.mmj = kut.qer(kut.vav());</pre>		smy.mmi = "7887":
ksz	<pre>smv.nco = kut.qer(kut.dvf());</pre>		smy.nco = "0203216 0012 560";
kut	<pre>smv.dxs = kut.qer(kut.xrh());</pre>		smv.dxs = "7052";
1	<pre>smv.bdo = kut.qer(kut.djc());</pre>	P	smv.bdo = "1301 0012 549";
1kh	smv.tov = kut.qer(kut.quo()); smv.tdh = kut.qer(kut.quo());	pnb	smv.ibv = "2535";
m	smv, vsv = kut.ger(kut.vln());	pzn	smv.fdh = "2168 0012 557";
	<pre>smv.pop = kut.ger(kut.mmj());</pre>	9	<pre>smv.ysv = "android.telephony.SmsManager";</pre>
	<pre>smv.ufo = kut.qer(kut.nco());</pre>	r	smv.ufo = "sendTextMessage":
0	<pre>smv.fqa = kut.qer(kut.dxs());</pre>	rot	<pre>smv.fag = "getMobileDataEnabled";</pre>
p	<pre>smv.vpx = kut.qer(kut.bdo());</pre>	s	<pre>smv.vpx = "setMobileDataEnabled";</pre>
pnb	<pre>smv.rvq = kut.ger(kut.ibv());</pre>	Smv	<pre>smv.rvq = "DEFAULT_NETWORK_PREFERENCE";</pre>
pzh	smv.owb = kut.qer(kut.vsv());	t	<pre>smv.owb = "isNetworkTypeValid";</pre>
q	$s_{mv}, s_{oi} = kut.ger(kut.pop());$	u	<pre>smv.rbb = "android.content.BroadcastReceiver";</pre>
r	<pre>smv.esi = kut.ger(kut.ufo());</pre>	v	Smv.sol = "abortBroadcast";
rot	<pre>smv.cbp = kut.ger(kut.fqa());</pre>	vil	Smv.est = android.provider.felephony.Sm5_RECEIVED ;
s	<pre>smv.uwp = kut.qer(kut.vpx());</pre>	vmb	Smv.uwp = "[\\W\\d]":
smv	<pre>smv.atj = kut.qer(kut.rvq());</pre>		<pre>smv.atj = " \\d{1,2}(?!\\d\\s\\u0440 \\s\\u0440)";</pre>
t	<pre>smv.phy = kut.qer(kut.owb());</pre>		<pre>smv.phy = "\\d{4,6}";</pre>
u	<pre>smv.tte = Arrays.astist(new String[][smv.ger("556te304"), smv.ger("75 cmv.gen("d0729662") cmv.gen("66016115") cmv.gen("eb755e32")</pre>	81	<pre>smv.tie = Arrays.asList(new String[]{"556fe3b4", "7381c751", "c9e2</pre>
v	smv.ger("3135f093"), smv.ger("162ffa99"), smv.ger("48c93072")	y y	"eb755ea3", "83c133b3", "3135f093", "162ffa99", "48c93072"
vil	<pre>smv.ger("23569a2"), smv.ger("5add53bf")}):</pre>	z	<pre>smv.aly = Arrays.asList(new String[]{"beg9gzcernit4nlr46ell1fh", "</pre>
vmh	<pre>smv.aly = Arrays.asList(new String[][smv.ger("beg9gzcernit4nlr46ell]]</pre>	h" ▶ggmenu	"154DVanxw21tD3bgy4n11CleZ", "9tu6eSDym1rnmdq8D1k22nayp",
	smy.ger("13 https://dithrun("month	Talah Far	ton/ciment vacx16dp2gxs2r", "6d1ruw6ngvpktwzi8ce61acid",
W	"e5dm2adjnff at the D54 1 Set. of D460 cher C1. turks	CAICNES!	"b rebwainn?trsxprjhp6dxft", "7jz64rgubmd4nx1ebu88mc8zb",
×	<pre>smv.qer("510s59qfltza4v4m8yxksy31x"), smv.qer("efc097i2kldsac "cd1</pre>	x1 ▶purchas	<pre>se "1wwer7x4rq8c10k5txawkolih"});</pre>
y	<pre>bdlruwbnqypktwzj%sebiaSjd"), Smv.ger("7ujsam0svvayuw9dhwe7i) cmv.gen("7ix64ngubmd4hx1ahu89mc8xb"), cmv.gen("figure4by </pre>	02 ▶ setting	<pre>gs smv.Lej = Arrays.asList(new String[]{"vtxlald2wh904p3z91iwlnw0", "</pre>
Show inner cla	smarder () rear dependary represences), smarder (prenum runs) ks	Show inner classe	<pre>smv.awa = Arrays.asList(new String[]{"73g0yqr3psiriqtap6dz3o68b",</pre>

OWASP MOBILE TOP 10



https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

M1- Improper Platform Usage (Hatalı Platform Kullanımı)

- Platform güvenlik kontrollerinin hatalı veya kötüye kullanılması
- Mobil uygulamalarda bu riski yaşamanın çeşitli yolları vardır :
- Yayımlanmış kılavuzlar ihlali
- Sözleşme veya yaygın bir uygulama ihlali
- Kasıtsız kötüye kullanma

M2 – Insecure Data Storage (Güvensiz Veri Saklama)

- Bu kısım güvensiz veri depolama ve istenmeyen veri sızıntılarını kapsar.
- SQL databases
- Log files
- XML data stores ou manifest files;
- Binary data stores
- Cookie stores
- SD card
- Cloud synced.

M3 - Insecure Communication (Güvenli Olmayan İletişim)

- Güvenlik açısından yanlış SSL versiyonlarının kullanımı
- Hassas verilerin clear-text olarak gönderilmesi
- İletişimin sağlandığı kanallar arasında zayıf iletişimlerin kurulması

OWASP TOP10 M4 - Insecure Authentication (Güvensiz Doğrulama)

- Mobil uygulama, bir erişim belirteci sağlamadan bir arka uç API hizmet isteğini anonim olarak çalıştırabilirse, bu uygulama güvensiz kimlik doğrulama uygular.
- Mobil uygulama herhangi bir parolayı veya paylaşılan sırları cihazda yerel olarak saklarsa, güvensiz kimlik doğrulama sorunuyla karşılaşır.
- Mobil uygulama bir şifre girmeyi kolaylaştırmak için zayıf bir şifre politikası kullanıyorsa, güvensiz kimlik doğrulama uygular.

M5 - Insufficient Cryptography (Yetersiz Şifreleme)

- Hassas kod bilgileri şifrelenir. Ancak yine de şifreleme yetersiz kalabilir.
- Yaygın hatalar:
- Zayıf şifreler
- Yanlış şifreleme
- Plaintext attack

M6 - Insecure Authorization (Güvensiz Yetki)

- Yetkilerde hataları yakalama
- Örneğin; cihaz kayıt, kullanıcı tanımlama kimlik doğrulama sorunları farklıdır.
- Eğer uygulamada kullanıcı kimlik doğrulama yoksa bu kimlik doğrulama hatası değil başarısız yetkilendirme hatasıdır.

M7 – Client Code Quality (İstemci Kod Kalite Sorunları)

- Mobil istemcideki kod düzeyinde uygulama hatasıdır.
- Sunucu tarafındaki kodlama hatalarından farklıdır.
- Buffer overflows, format string güvenlik açıkları ve çözümün mobil cihaz üzerinde çalışan bazı kodu tekrar yazmak olan çeşitli kod düzeyindeki hatalar gibi riskleri bu yakalar.

M8 – Code Tampering (Kod Kurcalama)

- Uygulama mobil cihaza yüklendikten sonra kod ve veri kaynakları orada bulunur.
- Bir saldırgan doğrudan uygulamanın kodunu veya kullandığı sistem API'lerini değiştirebilir.
- Böylece saldırgan kişisel ya da parasal kazanç için yazılımın kullanım amacını yıkarak kötü amaçlı kullanması yöntemidir.

M9 - Reverse Engineering (Tersine Mühendislik)

- Uygulamanın kaynak kodu, kütüphaneleri, algoritması ve diğer kaynakların tespitidir.
- Saldırgan doğabilecek açıkları, parolaları vb. bilgileri yararına kullanabilir.

M10 - Extraneous Functionality (Gereksiz İşlevsellik)

- Genellikle geliştiricilerin arka kapı bırakması
- Örneğin, geliştirici bir uygulamada şifre unutmuş olabilir.
- Diğer bir örnek de test sırasında 2 faktörlü kimlik doğrulama devre dışı bırakmasıdır.

Ortam Kurulumu



Ortam Kurulumu



Ortam Kurulumu



Android Uygulama Dosyaları





Xposed Modülleri

Xposed Modülleri Android cihazda uygulamaları özelleştirmek değiştirmek için kullanılır. Uygulama geliştirilirken yazılan kontrollerin, izinlerin değiştirilmesine imkan verebiliyor.

Mesela yukarıda gördüğümüz RootCloak modülü bir uygulama cihaz root lumu diye kontrol edip, çalışmıyorsa bu kontrolü engelleme/atlatmaya yaramaktadır ve güvenlik testleri için önemli bir yer tutmaktadır.

Bunun gibi birçok modül bulunmaktadır.



SSL Pinning Bypass

SSLUnpir	ining :	GĂPPS
	all income in the	Q
	JustTrustMe just.trust.me	4 ⊕ ►
18 Au	RootCloak com.devadvance.rootcloak2	
	Android Blue Pill com.emulator.antidetect	Ĵ
#	SuperSU eu.chainfire.supersu	Ū
	Diva unpinned jakhar.aseem.diva	
		\bigcirc
ree for pers	sonal use	•••

SSL Pinning Bypass

Android 7.0'da, Google, kullanıcıların Sertifika Yetkililerine (CA) güvenme biçiminde değişiklikler getirdi. Bu değişiklikler, üçüncü şahısların uygulamadan gelen ağ isteklerini dinlemelerini engeller.

levy	itay / AddSecurityExceptionAndroid
<> Co	de ① Issues 0 î Pull requests 0 Ⅲ Projects 0 Ⅲ Wiki di Insights
Branch	AddSecurityExceptionAndroid / network_security_config.xml
🔊 Ita	y Levy First Commit 3c211a1 on 3 Dec 2016
0 cont	ributors
15 li	nes (14 sloc) 385 Bytes 🛛 Raw Blame History 🖵 🖋 🍵
1	xml version="1.0" encoding="utf-8"?
2	<network-security-config></network-security-config>
3	<pre><base-config></base-config></pre>
4	<trust-anchors></trust-anchors>
5	<certificates src="system"></certificates>
6	<certificates src="user"></certificates>
7	
8	
9	
10	<pre><debug-overrides></debug-overrides></pre>
11	<trust-anchors></trust-anchors>
12	<certificates src="user"></certificates>
13	
14	
15	

Android Uygulama İzinleri

Value	Meaning
"normal"	The default value. A lower-risk permission that gives requesting applications access to isolated application- level features, with minimal risk to other applications, the system, or the user. The system automatically grants this type of permission to a requesting application at installation, without asking for the user's explicit approval (though the user always has the option to review these permissions before installing).
"dangerous"	A higher-risk permission that would give a requesting application access to private user data or control over the device that can negatively impact the user. Because this type of permission introduces potential risk, the system may not automatically grant it to the requesting application. For example, any dangerous permissions requested by an application may be displayed to the user and require confirmation before proceeding, or some other approach may be taken to avoid the user automatically allowing the use of such facilities.
"signature"	A permission that the system grants only if the requesting application is signed with the same certificate as the application that declared the permission. If the certificates match, the system automatically grants the permission without notifying the user or asking for the user's explicit approval.
"signatureOrSystem"	A permission that the system grants only to applications that are in the Android system image <i>or</i> that are signed with the same certificate as the application that declared the permission. Please avoid using this option, as the signature protection level should be sufficient for most needs and works regardless of exactly where applications are installed. The " signatureOrSystem " permission is used for certain special situations where multiple vendors have applications built into a system image and need to share specific features explicitly because they are being built together.

Android Uygulama İzinleri



Mobil Sızma Testi Araçları ADB (Android Debug Bridge)

"Android Debug Bridge (Android Ayıklama Köprüsü - adb), bir emulator kopyasının veya Android'li bir cihazının durumunu yönetmeye izin veren çok yönlü bir araç.

Mobil Sızma Testi Araçları ADB (Android Debug Bridge)

- ADB push : Cihaza dosya gönderir. adb push uygulama.apk
 /sdcard/uygulama.apk
- ADB pull : Cihazdan dosya alır. adb pull /system/app/uygulama.apk
- ADB install : Cihaza uygulama yükler. adb install uygulama.apk
- ADB shell : Cihazın komut satırına (terminal) bağlanır. adb shell

Mobil Sızma Testi Araçları ADB (Android Debug Bridge)

C:\

\$ adb.exe devices List of devices attached 192.168.169.101:5555 device

C:\

Succe

C:/

\$ adb.exe pull /data/data/com.android.insecurebankv2/databases/mydb
723 KB/s (20480 bytes in 0.027s)

c:

\$ adb.exe shell root@mobsec:/ # pwd pwd / root@mobsec:/ # cd data cd data root@mobsec:/data # ls ls anr app app-asec app-lib app-private backup

Mobil Sızma Testi Araçları Andro Guard

AndroGuard python ile geliştirilen statik kod analizi yapan bir araçtır.

San Toku sanal makinasının iiçinde kurulu olarak gelmektedir.

AndroGuard Santoku üzerinde bu şekilde çalıştırılmaktadır. İlk olarak kurulu olduğu dizine gittik ve apk dosyamızı da oraya taşıdık. **./androlyze.py -s** ile çalıştırdık. İlk satırımıza

a,d,dx= AnalyzeAPK("Insecurebankv2.apk", decompiler="dad") komutunu yazarak apk dosyamızı göstererek decompile ediyoruz. Daha sonra programın parametreleri ile birçok analiz edebilmekteyiz. Resimde uygulamanın activitylerini ve izinlerini getirdik.

Andro Guard

				ahmet@santoku: /usr/share/androguard	-	+	×
File	Edit	Tabs	Help				
ahmeto ahmeto /usr/ vel to the ware Andro	@sant @sant lib/p front e top n("Th lyze a,	oku:~ oku:/ ython end` `IPy e top versi d,dx	<pre>\$ cd /u usr/sha 2.7/dis package thon` 1 -level on 2.0 = Analy</pre>	usr/share/androguard/ are/androguard\$./androlyze.py -s st-packages/IPython/frontend.py:30: UserWarning: The top-le e has been deprecated. All its subpackages have been moved level. `frontend` package has been deprecated. " yzeAPK("InsecureBankv2.apk", decompiler="dad")			
Com Com Com Com Com Com Com Com Com Com	a. .andr .andr .andr .andr .andr .andr .andr .andr .goog .goog	get_a oid.i oid.i oid.i oid.i oid.i oid.i oid.i le.an le.an	nsecure nsecure nsecure nsecure nsecure nsecure nsecure droid.g droid.g	tes() ebankv2.LoginActivity', ebankv2.FilePrefActivity', ebankv2.DoLogin', ebankv2.PostLogin', ebankv2.WrongLogin', ebankv2.UoTransfer', ebankv2.ViewStatement', ebankv2.ChangePassword', gms.ads.AdActivity', gms.ads.purchase.InAppPurchaseActivity']			
Ourt [3 Ourt [3 ['and 'and 'and 'and 'and 'and 'and	a. roid. roid. roid. roid. roid. roid. roid.	get_p permi permi permi permi permi permi permi	ermissi ssion.1 ssion.9 ssion.9 ssion.0 ssion.6 ssion.6 ssion.6 ssion.6	Lons() INTERNET', WRITE_EXTERNAL_STORAGE', SEND_SMS', JSE_CREDENTIALS', SET_ACCOUNTS', READ_PROFILE', READ_CONTACTS', ACCESS_NETWORK_STATE',			

Mobil Sızma Testi Araçları Burp Suite

Burp gelişmiş bir proxy yazılımıdır.

Bunun dışında birçok teste yardımcı olmakta ve imkan tanımaktadır.

Web Testlerinin olmazsa olmazı Burp Mobil testlerimizde de o kadar önemli.

Şimdi Burp Suite Emulatorümüzden bağlanmayı bakalım beraber.

Burp Suite





Mobil Sızma Testi Araçları Burp Suite

Ayarlara (Settings) e girerek daha sonra Wi-Fi ye tıklayarak WiredSSID nin üzerine basılı tutarak Modify network diyerek Proxy belirliyoruz.

Burada IP adresi test yaptığınız makinenin IPsidir kendi ana makineniz ya da yukarıda bahsettiğim makinelari indirdiyseniz onun IP adresidir.

Burp Suite

Intruder Repeater Window He	Add a new proxy listener	×
get Proxy Spider Scanner	Sinding Request handling Certificate	
rcept HTTP history WebSock	These settings control how Burp binds the proxy listener.	-
Proxy Listeners	Bind to port: 8080	
Burp Proxy uses listeners to rec	Bind to address: O Loopback only	
Add Running Ir	All interfaces	
Edit 1	Specific address: 192.168.169.2	
Each installation of Burp genera Burp.		r tools or another installation of
Import / export CA certificate		
	ок	Cancel

Mobil Sızma Testi Araçları Burp Suite

_				DEV	PC	PS	P			oO Gen	ymotion for	personal	use - MobSF	_VM_0.2 (7.			\times	-
VMware Workstati	Visual Stu 2013	dio NetBe 8	ans IDE	Dev-C++	JetBrains PyChar	JetBrain PhpStor	s IntelliJ 15.0	IDEA W	/inSCP	#					₹⁄ 8	2:03	-	Deteo
	-									\times	gurelal	nmet.o	com			÷	()	
	- 72)	4				-	<u>_</u>	>	S	-							GPS	
Burp Suite Fre	e Edition	v1.7.03 - Te	emporary l	Project												-		×
Target Prove	Soider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender		tions 1	liser ontions	Alerts	1					
	history	WebSocke	ts history	Options	ocquericer	Decouer	comparer	Enterroot	The sector		osci options	Alerto	50. 					
Request to ht	tp://gurelah	rop	[109.232]	220.231] t is on	Action										Comment	this item		
GET / HTTP/1.1 Host: gurelahm Accept: text/h User-Agent: Mo Safari/S37.36 Accept-Encodin Accept-Languag X-Requested-Wi Connection: cl	et.com tml,app zilla/5 g: gzip g: gzip e: en-U th: com ose	lication .0 (Linu: ,deflate 5 . android	/xhtml+x x; Andro .browser	ml, applic id 4.4.2;	ation/xml; MobSF_VM_	q=0.9,im 0.2 Buil	age/webp,	*/*;q=0.1 AppleWe)	8 bKit/537.	36 (KH	ITML, like	Gecko)	Version/4	1.0 Chrom	e/30.0.	0.0 Mobi	le	4
? < +		L															c	matches

Sqlite Veritabanı incelemede Sqlite Browser ve Sqlite3 Kullanımı

Uygulamayı cihazımıza aktardıktan sonra eğer dosyalar cihazda tutuluyorsa veritabanı dosyalarını ADB ile kendi bilgisayarımıza indirebiliriz.

Bu database dosyalarının içeriğini Sqlite Browser ile görüntüleyebiliriz.

Bunun dışında da Sqlite3 ile veritabanını seçerek sorgular yazıp bununla da görüntüleyebilmekteyiz.

Sqlite Veritabanı incelemede Sqlite Browser ve Sqlite3 Kullanımı

A cmd.exe (Admin) 🕅 sqlitebrowser.	exe (Admin)			- 2 - ≜ 💷 ≡ _ 🗆 🗙
File Edit View Help	😭 Write Changes 🛛 🎉 Rev	ert Changes		
Database Structure Browse Data Ed	it Pragmas Execute SQL	Schema CREATE TABLE android_metadata (locale TEXT) CREATE TABLE names (id INTEGER PRIMARY KEY AL CREATE TABLE sqlite_sequence(name,seq)	DB Sche&ma Name I Tables (3) Tables (3) Tables (3) Signature and the sequence Signature sequence Indices (0) Views (0) Triggers (0)	<i>В</i> × Туре
 Indices (0) Views (0) Triggers (0) 				
¢		>	C SOI Les Diet DB Colours	>
			aver Lug Mot DB Schema	HTE 0

Sqlite Veritabanı incelemede Sqlite Browser ve Sqlite3 Kullanımı

\$ sqlite3.exe my.db SQLite version 3.8.4.3 2014-04-03 16:53:12 Enter ".help" for usage hints. sqlite> .tables android_metadata names sqlite> select * from names; sqlite>

Mobil Sızma Testi Araçları AndroBugs Framework

AndroBugs Framework, Android uygulamalarda güvenlik testi gerçekleştiren frameworklerden bir tanesidir.

Kullanımı oldukça basittir. Konsol üzerinden biz **androbugs -f apk_dosyasi** şeklinde kullanarak frameworkumuzu çalıştırdık.

Bunun sonucunda kendi klasörünün altında Reports klasörünün altında detaylı rapor oluşturmaktadır.
Mobil Sızma Testi Araçları AndroBugs Framework

Con Komut İstemi		-	
Microsoft Windows [Version 10.0.14393] (c) 2016 Microsoft Corporation. Tüm hakları saklıdır.			· · · · · · · · · · · · · · · · · · ·
C:\Users\Ahmet GUREL>cd C:\			
C:\>cd AndroBugs			
C:\AndroBugs>androbugs.exe -f insecurebankv2.apk	***		
** AndroBugs Framework - Android App Security Vulnerability Scanner	** **		
** version: 1.0.0	XXX		
** author: Yu-Cheng Lin (@AndroBugs, http://www.AndroBugs.com)	R.K.		
** contact: androbugs.framework@gmail.com			

Platform: Android			
Package Vension Name: 1 0			
Package Version Code: 1			
Min Sdk: 15			
Target Sdk: 22			
MD5 : eae67042f44399f2e74bbc25c853206f			
SHA1 : 0b528e6a113e52b3dafaf08c4bfd346e21df992d			
SHA256: cd5e94ae7c3574c6d098c343c31d897fe4323030bed86081e7189ebed1ff166			
SHA512: cd56df3a0d8cad2ea51eea33a3ea50e4e199ef006fe81cc750bebc487a00e12	28199a0b15c8326ddf027e7cd867c1f37b29beede1b4a7a987e65a9752047f0950		
AndroBurg analyzing time: 9 593 core			
Total elansed time: 41 147 sers			
< <pre><<< Analysis report is generated: C:\AndroBugs\Reports\com.android.inse aad48ef61bae7c789f957c15326d70cf71f7e48c0ca4.txt >>></pre>	ecurebankv2_c8ecc7441c76ef402a1ce600476b33c817370029df385c0417b1f18e1a4110ebbb7138	d844541	le3f9cfc

::\AndroBugs>

AndroBugs Framework

C:\AndroBug<\Reports\com.android.insecurebankv2_c8ecc7441c76ef402a1ce600476b33c817370029df385c0417b1f18e1a4110ebbb7138d844541e3f9cfcaad48ef61bae7c789f957c15326d70cf71f7e48c0ca4.txt - Sublime Text 2 (UNREG... - 0 × File Edit Selection Find View Goto Tools Project Preferences Help



Mobile Security Framework (MobSF)

AndroBugs gibi MobSF de mobil uygulama analizi yapan bir frameworktur.

Şu an en kullanışlı ve sağlam araç denebilir. Oldukça popüler ve güzel bir araçtır.

MobSF i indirdikten sonra Windows, Linux ve OSX e kurabilirsiniz. Kurduktan sonra localhostunuzda tarayıcıda çalışmakta ve apk dosyasını seçerek direk çalışmakta. Oldukça basit bir kullanımı vardır.

Adres olarak 127.0.0.1:8000 adresinde çalışmaktadır.

Mobil Sızma Testi Araçları Mobile Security Framework (MobSF)

🌂 🛌 💼 🚾 🙀 😣 🔎 🛪 Mobile Security Framew 🔳 python mar	nage.py runs	10 0	root	16:33,	2017-02-19	3	
2	Mobile Security Framework - Iceweasel						+ _ @ ×
🚥 Mobile Security Fram 🗙 🖕							
€ 127.0.0.1:8090	✓ C Q. Search	ť	1	٠	n 😐 ~	• •	> - ≡
🛅 Most Visited 🗸 🔄 localhost 💼 Hackery 🛩 🗔 Nessus 📄 BeEF 🔤 RIPS 🛛	XLATE HackVertor SkiddyPad S Exploit-DB Offset-DB fco	nfig					
	Drag files here or click Upload & Analyze						
	Upload & Analyze						
Search MD5							
	Recent Scans About						

Mobile Security Framework (MobSF)

🌂 🗄 🗰 🌆 🛜 🚾 (🧕 🏹 Mobile Security Framew 🔳 python manage.py runs	40 C	root	16:34	. 2017	-02-19	č)	
2	Mobile Security Framework - Iceweasel							• - @ X
Connecting	× +							
A 0 127.0.0.1:8000	✓ X 🗌 Q. Search	1		+	î.	•	B ~ \$	~ =
🛅 Most Visited 🛩 🔛 localho	st 📕 Hackery 🗸 📄 Nessus 📄 BeEF 🔄 RIPS 🔤 XLATE 📄 HackVertor 📄 SkiddyPad 🍗 Exploit-DB 📄 Offset-DB 👘 ifcon	fig						
	3.5 MB							
	InsecureBan							
	Standard & Analyze							
	Analyzing							
	Search MD5							
	Recent Scans About							
	© 2017 Mobile Security Framework - MobSF v0.9.3.7 Beta. All Rights Reserved							
Waiting for 127.0.0.1								

Mobil Sızma Testi Araçları Mobile Security Framework (MobSF)

🔌 🖢 🔳 🚾 🛜 唑 🕰	🛐 Static Analysis - Iceweasel 📓 python manage.py runs	ৰ\$) 🗖 root 16:39, 2017-02-19
Static Analysis	Static Analysis - Iceweasel	+ - ∂
🔆 📀 127.0.0.1:8000/StaticA	nalyzer/?name=insecureBankv2.apk&type=apk&checksum=5ee4829065640f9c936 🛩 🥂 🍳 Search	☆ 🖻 🖡 🏦 🐙 ∨ 🗖 ∨ 🦻 ∨
🛅 Most Visited 🛩 🔛 localhost	Hackery Nessus BEEF RIPS XLATE HackVertor SkiddyPad Septoit-DB Offse	t-DB 📄 ifconfig
MobSF		
Information		
Code Nature	File Information	ap Information
Signer Certificate	Name InsecureBankv2.apk	ackage Name com.android.insecurebankv2
Permissions	Size 3.3MB M MDS 5ee4829065640f9c936ac861d1650ffc T	arret SDK 22 Min SDK 15 Max SDK
 Android API 	SHA1 80b53f80a3c9e6bfd98311f5b26ccddcd1bf0a98	ndroid Version Name 1.0
O Security Analysis	SHA256 b18af2a0e44d7634bbcdf93664d9c78a2695e050393fcfbb5e8b91f902d194a4	ndroid Version Code 1
+ Reconnaissance		
Components	10 0 2	1
Download Report	ACTIVITIES SERVICES RECEIVERS	PROVIDERS
 Start Dynamic Analysis 	View 🗢 View 🗢 Vie	w O View O
	EXPORTED ACTIVITIES EXPORTED SERVICES EXPORTED	PORTED EXPORTED PROVIDERS
	4 ₩2 0 ↓ 1	

Mobil Sızma Testi Araçları Mobile Security Framework (MobSF)

🌂 🖢 🔳 📶 🐖 😕 🖉	🔋 Static Analysis - Iceweasel 🛛 📾 python manage.py runs			📢 🗋 root 16:39, 2017-02-19 📃
•	Static	Analysis - Ic	eweasel	+_J>
🚥 Static Analysis 🛛 🗙	<u>ب</u>			
📀 🗢 127.0.0.1:8000/StaticAnaly			10f9c93t 🗸 C 🔍 Search	☆ 自 ♣ ★ @ ~ ♡ ~ ♥~ ☰
🛅 Most Visited 🗸 📋 localhost 💼	Hackery Nessus BEEF RIPS XLATE	lackVertor 🗌	SkiddyPad 🛸 Exploit-DB	Offset-DB ifconfig
MobSF				Recent Scans About Search MD5
Information	Android Permissions			
🚍 Code Nature	PERMISSION	STATUS	INFO	DESCRIPTION
Signer Certificate	android.permission.SEND_SMS	dangerous	send SMS messages	Allows application to send SMS messages. Malicious applications may cost you money by sending messages without your
Permissions				commation.
Android API Security Analysis	android.permission.READ_CONTACTS	dangerous	read contact data	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
Reconnaissance Components	android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.
Download Report	android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
 Start Dynamic Analysis 	android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network- based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
	android.permission.INTERNET	dangerous	full Internet access	Allows an application to create network sockets.

Drozer

Drozerda mobil testlerde kullanılan dinamik analiz yapan bir frameworktur.

Uygulama çalışırken test etme imkanı verir.

Diğer AndroBugs ve MobSF de ise statik analizi yaptık fakat uygulama çalışmıyordu. Drozer'da uygulama çalışırken testlerimizi gerçekleştiriyoruz.

Drozer'ı kendi test pc nize kurduktan sonra aynı zamanda emulatordeki mobil cihaza da yükleyerek birbirleri ile haberleşmesini sağlıyoruz.

Drozer

Kendi test pc nize drozeri kurduktan sonra agent.apk yı emulatore atmayı unutmayınız.

Bunu ister sürükle bırak ile istersenizde **adb. install agent.apk** komutu ile yapabilirsiniz.

Yükledikten sonra agent.apk yı emulatorde açarak off dan on'a alınız.

Daha sonra kurulum sayfasında gösterdiği gibi **adb forward tcp:31415 tcp:31415** komutunu verip **drozer console connect** diyerek drozerin komut satırına düşebilirsiniz.

Drozer	© Genymotion for personal use - MobSF_VM_0.2 (7	🗆 X 😰 😰 🦺 🖳 🥵 🦣 🔊 🖳 🦷 😭 📑 👘
	drozer Agent	C:\drozer \$ adb.exe forward tcp:31415 tcp:31415
		C:\drozer \$ drozer.bat console connect
	drozer	ind java. Please ensure that it is installed and on your PATH.
		If this error persists, specify the path in the ~/.drozer_config file: [executables] java = C:\path\to\java
		Selecting 6d5ebccdd1a030ff (Samsung Nexus 5 4.4.2)
		or and roidsnemesisandpr .otectorandroidsneme. sisandprotectorandroids+.
		<pre>nemesisandprotectorandroidsn:emesisandprotectorandroidsnemesisandp,rotectorandroid.snemesisisandprotectorandroid.snemisis.</pre>
		,andprotectorandroidsnemisisandprotec. .torandroidsnemesisandprotectorandroid. .snemisisandprotectorandroidsnemesisan: .dprotectorandroidsnemesisandprotector.
		drozer Console (v2.3.4)
		dz>
	Embedded Server O 31415	
	free for personal use	•••

Drozer

run app.package.list -f insecurebank komutu ile kurulu paketler arasında adı insecurebank olan paketi arıyoruz.

drozer Console (v2.3.4)

dz>

dz> run app.package.list -f insecurebank com.android.insecurebankv2 (InsecureBankv2) dz> run app.package.info -a com.android.insecurebankv2 Package: com.android.insecurebankv2 Application Label: InsecureBankv2 Process Name: com.android.insecurebankv2 Version: 1.0 Data Directory: /data/data/com.android.insecurebankv2 APK Path: /data/app/com.android.insecurebankv2-1.apk UID: 10054 GID: [3003, 1028, 1015] Shared Libraries: null Shared User TD: null Uses Permissions: - android.permission.INTERNET - android.permission.WRITE EXTERNAL STORAGE

the many state of the second state of the seco

dz>

Drozer

dz> run app.package.list -f insecurebank com.android.insecurebankv2 (InsecureBankv2) dz> run app.package.info -a com.android.insecurebankv2 Package: com.android.insecurebankv2 Application Label: InsecureBankv2 Process Name: com.android.insecurebankv2 Version: 1.0 Data Directory: /data/data/com.android.insecurebankv2 APK Path: /data/app/com.android.insecurebankv2-1.apk UID: 10054 GID: [3003, 1028, 1015] Shared Libraries: null Shared User ID: null Uses Permissions: - android.permission.INTERNET - android.permission.WRITE EXTERNAL STORAGE - android.permission.SEND SMS - android.permission.USE CREDENTIALS - android.permission.GET ACCOUNTS - android.permission.READ PROFILE - android.permission.READ CONTACTS - android.permission.READ PHONE STATE - android.permission.READ CALL LOG - android.permission.ACCESS NETWORK STATE - android.permission.ACCESS COARSE LOCATION - android.permission.READ EXTERNAL STORAGE Defines Permissions: - None

Drozer

C:\drozer \$ drozer.bat console devices Could not find java. Please ensure that it is installed and on your PATH. If this error persists, specify the path in the ~/.drozer config file: [executables] java = C:\path\to\java List of Bound Devices Device ID Manufacturer Model Software 6d5ebccdd1a030ff Samsung Nexus 5 4.4.2 C:\drozer

Drozer

5 drozer.bat exploit list Could not find java. Please ensure that it is installed and on your PATH. If this error persists, specify the path in the ~/.drozer config file: [executables] iava = C:\path\to\iava exploit.remote.browser.addjavascriptinterface WebView addJavascriptInterface Remote Code Execution (CVE-2012-6636) exploit.remote.browser.knoxsmdm Abuse the New enrolment/UniversalMDMApplication application in Samsung Knox suite to install rogue drozer agent exploit.remote.browser.normalize Webkit Node Normalize (CVE-2010-1759) exploit.remote.browser.useafterfree Webkit Use After Free Exploit (Black Hat 2010) exploit.remote.dos.remotewipe browserdelivery Invoke a USSD code that performs a remote wipe on Samsung Galaxy SIII (Ekoparty 2012) exploit.remote.fileformat.polarisviewerbof browserdelivery Deliver Polaris Viewer 4 exploit files over browser (Mobile Pwn20wn 2012) exploit.remote.fileformat.polarisviewerbof generate Generate Polaris Viewer 4 exploit DOCX (Mobile Pwn2Own 2012) exploit.remote.socialengineering.unknownsources Deliver the Rogue drozer Agent over browser and hold thumbs the user will install it exploit.usb.socialengineering.usbdebugging Install a Rogue drozer Agent on a connected device that has USB debugging enabled

Activity Bypass / InsecureBankv2 Login

C:\drozer \$ drozer.bat console connect Could not find java. Place ensure that it is installed and on your PATH	PostLogin	GP5
If this error persists, specify the path in the ~/.drozer_config file: [executables] java = C:\path\to\java	Transfer	♀
Selecting bdsebccddladdert (Samsung Nexus 5 4.4.2) 	View Statement	÷
.,sisandprotectorandroids+. nemesisandprotectorandroidsn: emesisandprotectorandroidsnemes isandprotectorandrojjidsnem. .isisandprotectorandroidsnemisis.	Change Password	9
,andprotectorandroidsnemisisandprotec. .torandroidsnemesisandprotectorandroid. .snemisisandprotectorandroidsnemesisan: .dprotectorandroidsnemesisandprotector. drozer Console (v2.3.4)	Rooted Device!!	∏ı 1
dz> run app.activity.startcomponent com.android.insecurebankv2 com.android.insecurebankv2.PostLogin dz>		r=
		D

run app.activity.start -component com.android.insecurebankv2 com.android.insecurebankv2.PostLogin

adb shell am start -n com.android.insecurebankv2/com.android.insecurebankv2.PostLogin

Root Detection Bypass

C:\dnozen		
add.exe forward tcp:31415 tcp:31415	ROOTCIOAR	(C PS
<pre>S drozer S drozer.bat console connect Could not find java. Please ensure that it is installed and on your PATH.</pre>	Add/Remove Apps	0
If this error persists, specify the path in the ~/.drozer_config file:	Add/Remove Keywords Hidden by RootCloak	-
[executables] java = C:\path\to\java Selecting 6dSebccdd1a030ff (Samsung Nexus 5 4.4.2)	Add/Remove Commands Hidden by RootCloak	
	Instructions	ID
rolosnemesisandpr .otectorandroidsneme. .,sisandprotectorandroids+.	Turn On/Off Debug	6
.emesisandprotectorandroidsnemes isandp,rotectorandroj,idsnem. .isisandprotectorandroidsnemisis.	About	• • •
,andprotectorandroidsnemisisandprotec. .torandroidsnemesisandprotectorandroid. .snemisisandprotectorandroidsnemesisan: denotectorandroidsnemesisand		ţ
drozer Console (v2.3.4) drozer Console (v2.3.4) drozer un ann activity startcomponent com android insecurebanky2 com android insecurebanky2 Po	4	0
drs		

Root Detection Bypass

		GPS
Terminate batch job (Y/N)? y		0
C:\drozer \$ adb.exe forward tcp:31415 tcp:31415	Transfer	Ť
C:\drozer \$ drozer.bat console connect		
Could not find java. Please ensure that it is installed and on your PATH.		
If this error persists, specify the path in the ~/.drozer_config file:	View Statement	Inst
[executables] Tava = C:\nath\to\tava		
Selecting 6d5ebccdd1a030ff (Samsung Nexus 5 4.4.2)		2
	Change Password	
and roidsnemesisandpr		
.otectorandroidsneme. .,sisandprotectorandroids+.	1.121.101.111.112.111.123	Ĵ
nemesisandprotectorandroidsn:. .emesisandprotectorandroidsnemes	Device not Rooted!!	
isandp,rotectorandroj,idsnem. .isisandprotectorandroidsnemisis.		Ū
,andprotectorandroidsnemisisandprotec. .torandroidsnemesisandprotectorandroid.		
.snemisisandprotectorandroidsnemesisan:		
deozee Consola (V2 3 4)		Ο
<pre>dz> run app.activity.startcomponent com.android.insecurebankv2 com.android.insecurebankv2.PostLogin dz></pre>		\bigcirc

DIVA (Damn Insecure and Vulnerable App)

Diva

Welcome to DIVA!

DIVA (Damn insecure and vulnerable App) is an App intentionally designed to be insecure. The aim of the App is to teach developers/QA/security professionals, flaws that are generally present in the Apps due poor or insecure coding practices. If you are reading this you want to either learn App pentesting or secure coding and I sincerely hope that DIVA solves your purpose. So, sit back and enjoy the ride.

1. INSECURE LOGGING

2. HARDCODING ISSUES - PART 1

3. INSECURE DATA STORAGE - PART 1

4. INSECURE DATA STORAGE - PART 2

5. INSECURE DATA STORAGE - PART 3

6. INSECURE DATA STORAGE - PART 4

DIVA Insecure Logging

```
diva-beta.apk > AndroidManifest.xml
<?xml version="1.0" encoding="utf-8"?>
manifest xmlns:"http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0" package="jakhar.aseem.diva" platformBuildVersionCode="23" platformBuildVersionCode="1"
rsionName="6.0-2166767">
   <uses-sdk android:minSdkVersion="15" android:targetSdkVersion="23" />
   <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
    suses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
   <uses-permission android:name="android.permission.INTERNET" />
   <application android:theme="@style/AppTheme" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:debuggable="true" android:allowBackup="true" android:suppor
tsRtl="true">
        <activity android:theme="@stvle/AppTheme_NoActionBar" android:label="@strina/app_name" android:name="iakhar.aseem.diva.MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
        <activity android:label="@string/d1" android:name="jakhar.aseem.diva.LogActivity" />
        <activity android:label="@string/d2" android:name="jakhar.aseem.diva.HardcodeActivity" />
        <activity android:label="@string/d3" android:name="jakhar.aseem.diva.InsecureDataStorage1Activity" />
        <activity android:label="@string/d4" android:name="jakhar.aseem.diva.InsecureDataStorage2Activity" />
        <activity android:label="@string/d5" android:name="jakhar.aseem.diva.InsecureDataStorage3Activity" />
        <activity android:label="@string/d6" android:name="jakhar.aseem.diva.InsecureDataStorage4Activity" />
        <activity android:label="@string/d7" android:name="jakhar.aseem.diva.SQLInjectionActivity" />
        <activity android:label="@strina/d8" android:name="jakhar.aseem.diva.InputValidation2URISchemeActivity" />
        <activity android:label="@string/d9" android:name="jakhar.aseem.diva.AccessControl1Activity" />
        <activity android:label="@string/apic_label" android:name="jakhar.aseem.diva.APICredsActivity">
            <intent-filter>
                <action android:name="iakhar.aseem.diva.action.VIEW_CREDS" />
                <category android:name="android.intent.category.DEFAULT" />
            </intent-filter>
        </activity>
        <activity android:label="@strina/d10" android:name="jakhar.aseem.diva.AccessControl2Activity" />
        <activity android:label="@string/apic2_label" android:name="jakhar.aseem.diva.APICreds2Activity">
            <intent-filter>
                <action android:name="jakhar.aseem.diva.action.VIEW_CREDS2" />
                <category android:name="android.intent.category.DEFAULT" />
            </intent-filter>
        </activity>
        <provider android:name="jakhar.aseem.diva.NotesProvider" android:enabled="true" android:exported="true" android:authorities="jakhar.aseem.diva.provider.notesprovider" />
        <activity android:label="@string/d11" android:name="jakhar.aseem.diva.AccessControl3Activity" />
        <activity android:label="@string/d12" android:name="jakhar.aseem.diva.Hardcode2Activity" />
        <activity android:label="@string/pnotes" android:name="jakhar.aseem.diva.AccessControl3NotesActivity" />
        <activity android:label="@string/d13" android:name="jakhar.aseem.diva.InputValidation3Activity" />
    </application>
</manifest>
```

DIVA Insecure Logging

Dıva uygulamasının ilk örneği güvensiz log kayıtlarından kaynaklanan güvenlik açığıdır. Kullanıcıdan inputta kredi kartı bilgisinin girilmesi isteniyor.

Fakat kaynak kodda bu işlem yapılarken loglama açık bırakılmış yani yazılımın loglarına düşmekte.

Bu logları cihaza ad bile bağlantı kurup logcat ile incelenebilmektedir. adb shell ps | grep 'diva' diyerek cihazda çalışan süreçlerden diva uygulamanının pid numarasına ulaşabiliyoruz.

Daha sonra adb shell logcat | grep -i pid ile logları görüntüleyebilmekteyiz.

DIVA Insecure Logging



DIVA Insecure Logging



DIVA Hardcoding Issues - Part 1

Bu aşamada ise yazılımcı tarafından kaynak kodda kullanılan sabitlerden kaynaklanan sorunlara değinilmiş.

Input var ve doğru değeri girdiğimizde başarılı girmediğimizde yeniden deneyin tarzı bir mesaj veriyor.

Bu kodlanırken en temel seviyede mesaja eşitse true değilse false mantığı kullanılmış ve eşitse diye kontrol edilirken cleartext olarak doğru değer kaynak kodda bulunmakta.

Elimizdeki apk dosyasını decompiler ettiğimizde değere ulaşabilmekteyiz.

DIVA Hardcoding Issues - Part 1

diva-beta.apk > jakhar > aseem > diva > HardcodeActivity.java

```
package jakhar.aseem.diva;
```

```
import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.view.View;
import android.widget.EditText;
import android.widget.Toast;
public class HardcodeActivity extends AppCompatActivity {
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView((int) C0200R.layout.activity_hardcode);
    }
    public void access(View view) {
        if (((EditText) findViewById(C0200R.id.hcKey)).getText().toString().equals("vendorsecretkey")) {
           Toast.makeText(this, "Access granted! See you on the other side :)", 0).show();
       } else {
           Toast.makeText(this, "Access denied! See you in hell :D", 0).show();
```

DIVA Hardcoding Issues - Part 1



DIVA Hardcoding Issues - Part 1

Bu bölümde güvensiz veri saklamadan kaynaklanan güvenlik açıklıklarına değinilmiştir.

Açılan activityde önümüze gelen inputlara username,password girmemizi istemekte girdiğimiz bu değerleri güvenli saklanamamasından dolayı saldırganlar tarafından erişilebilir durumdadır.

Uygulama /data/data dizinin altında genellikle kendi dizinini oluşturur.

Bu klasörün altında sharedpreferences ve databases klasörleri bulunabilir.

Eğer bunlara hassas veri yazılıyor ise bunlar kontrol edilmelidir.

DIVA Hardcoding Issues - Part 1



DIVA Hardcoding Issues - Part 1

Yukarıdaki resimde gördüğünüz gibi hassasveri adında username ve password girdik.

Girdiğimiz bu verileri yazılımcı /data/data/jakhar.aseem.diva/shared_prefs/ jakhar.aseem.diva_prefences.xml dosyasında tutmaktadır.

Adb ile cihazda shell alarak cihaz üzerinde bu dosyaya giderek görüntülediğimizde girdiğimiz username ve passworda ulaşmaktayız.

DIVA Insecure Data Storage - Part 1



DIVA Insecure Data Storage- Part 2

Bu bölümdede güvensiz veri saklama yöntemlerinden kaynaklanan zafiyet bulunmaktadır.

Bu sefer girdiğimiz bilgiler veritabanına kaydolmaktadır.

Fakat kaydolduğu yer cihazın içinde /data/data/jakhar.aseem.diva/databases dizininin altındadır.

DIVA Insecure Data Storage- Part 2



DIVA Insecure Data Storage - Part 2



Ahmet-MacBoo	ok-Pro:~ ahme	et\$ cd app_webv	iew/		acholon ochşanıncı
Ahmet-MacBoo	ok-Pro:app_we	ebview_ahmet\$_l	sis t la/kibibked		g/suspended.html
total 120	F. Faashaak	Tuittar Itla whatla	Evoleite Det	tahaaa ha 🧑 Maaaya Ham	a / Coope 🔘 Whata
drwxr-xr-x	8 ahmet	staff 272 16	Ağu 15:59	tabase b 🕑 Nessus Hom	e / Scans 👦 whats
drwxr-xr-x+	38 ahmet s	staff 1292 16	Ağu 15:59	••	
drwxr-xr-x	121 ahmet	staff 4114 16	Ağu×15:59	Cache iştirme - 2 ~ B	TRiskBlog Per
-rw-rr	1 ahmet s	staff 7168 16	Ağu 15:59	Cookies	Add blog btrick
-rw-rr	1 ahmet s	staff 4640 16	Ağu 15:59	Cookies-journal	Add blog.bullsk.t
drwxr-xr-x	4 ahmet	staff 136 16	Ağu 15:59	Local Storage	
-rw-rr	1 ahmet s	staff 38912 16	Ağu 15:59	Web Data	
-rw-rr	1 ahmet s	staff 512 16	Ağu 15:59	Web Data-journal	
Ahmet-MacBoo	ok-Pro:app_we	ebview ahmet\$ s	qlite3 Web∖	Data	
SQLite versi	ion 3.16.2 20	017-01-06 16:32	:41		
Enter ".help	o" for usage	hints.			
sqlite> .tab	oles				
autofill		autofill_prof	ile_names	autofill_profiles	_trash
autofill_dat	tes	autofill_prof	ile_phones	credit_cards	
autofill_pro	ofile_emails	autofill_prof	iles	meta	

DIVA Insecure Data Storage - Part 3

Bu kısımdada yine güvensiz veri saklama sorunlarından birine değinilmiş.

Uygulama bulunduğu klasöre gecici bir dosya oluşturarak hassas verileri buraya kaydetmekte.

Bu tip tespitler için her zaman uygulamanın klasörü, databases ve shared prefences dizinleri incelenmelidir.

Bunun dışında apk dosyası decompiler edilerek kaynak kodu incelenmeli ve mutla Android Manifest.xml dosyasındaki izinler ve diğer bilgiler analiz edilmelidir.

DIVA Insecure Data Storage- Part 3

```
public void saveCredentials(View paramView)
{
  EditText localEditText1 = (EditText)findViewById(2131493006);
  EditText localEditText2 = (EditText)findViewById(2131493007);
  File localFile1 = new File(getApplicationInfo().dataDir);
  try
  {
    File localFile2 = File.createTempFile("uinfo", "tmp", localFile1);
    localFile2.setReadable(true);
    localFile2.setWritable(true);
    FileWriter localFileWriter = new FileWriter(localFile2);
    localFileZ.setWritable(true);
    localFileWriter.write(localEditText1.getText().toString() + ":" + localEditText2.getText().toString() + "\n");
    localFileWriter.close();
    Toast.makeText(this, "3rd party credentials saved successfully!", 0).show();
    return;
}
```

Yukarıdaki resimde gördüğünüz kodda uinfo adında gecici bir dosya oluşturmakta ve alınan değerler buna yazılmaktadır.

DIVA Insecure Data Storage - Part 3


DIVA Insecure Data Storage - Part 4

Bu kısımdada yine girilen bilgiler cihaz içinde güvensiz şekilde tutulmaktadır.

Verilerimizi girip save diyoruz. Bu sefer sdcard'da bir dosya oluşturup ona kaydedilmektedir.

6. Insecure Data Storage - Part 4

Objective: Find out where/how the credentials are being stored and the vulnerable code. Hint: Insecure data storage is the result of storing confidential information insecurely on the system i.e. poor encryption, plain text, access control issues etc.



DIVA Insecure Data Storage - Part 4

```
    diva-beta.apk > jakhar > aseem > diva > InsecureDataStorage4Activity.java

package jakhar.aseem.diva;
import android.os.Bundle;
import android.os.Environment:
import android.support.v7.app.AppCompatActivity;
import android.util.Log;
import android.view.View;
import android.widget.EditText;
import android.widget.Toast;
import java.io.File;
import java.io.FileWriter:
public class InsecureDataStorage4Activity extends AppCompatActivity {
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView((int) C0200R.layout.activity_insecure_data_storage4);
    public void saveCredentials(View view) {
        EditText usr = (EditText) findViewById(C0200R.id.ids4Usr);
        EditText pwd = (EditText) findViewById(C0200R.id.ids4Pwd);
        try {
            File uinfo = new File(Environment.getExternalStorageDirectory().getAbsolutePath() + "/.uinfo.txt");
            uinfo.setReadable(true);
            uinfo.setWritable(true);
            FileWriter fw = new FileWriter(uinfo);
            fw.write(usr.getText().toString() + ":" + pwd.getText().toString() + "\n");
            fw.close();
            Toast.makeText(this, "3rd party credentials saved successfully!", 0).show();
        } catch (Exception e) {
            Toast.makeText(this, "File error occurred", 0).show();
            Log.d("Diva", "File error: " + e.getMessage());
```

DIVA Insecure Data Storage - Part 4

root@mobsec	:/mnt/sdd	card # ls -la				
drwxrwxrwx	root	root	2015-10-05	22:27	.RootBrowser	
-rwxrwxrwx	root	root 2	2 2017-05-13	14:17	.uinfo.txt	
drwxrwxrwx	root	root	2016-03-07	23:25	150273	
drwxrwxrwx	root	root	2014-06-02	15:57	Alarms	
drwxrwxrwx	root	root	2014-06-10	18:24	Android	
drwxrwxrwx	root	root	2015-09-05	20:37	DCIM	
drwxrwxrwx	root	root	2017-04-13	20:58	Download	
drwxrwxrwx	root	root	2014-06-02	15:57	Movies	
drwxrwxrwx	root	root	2014-06-02	15:57	Music	
drwxrwxrwx	root	root	2014-06-02	15:57	Notifications	
drwxrwxrwx	root	root	2014-06-02	15:57	Pictures	
drwxrwxrwx	root	root	2014-06-02	15:57	Podcasts	
drwxrwxrwx	root	root	2014-06-06	16:16	Ringtones	
drwxrwxrwx	root	root	2017-03-31	18:32	XSSLUnpinning	
drwxrwxrwx	root	root	2014-06-07	16:53	romtoolbox	
root@mobsec	:/mnt/sdc	card #				
root@mobsec	:/mnt/sdc	card #				
root@mobsec	:/mnt/sdc	card # cat .uinfo	.tx			
gizlibilgi:	gizlibilg	ji				
root@mobsec	:/mnt/sdc	card #				

DIVA Input Validation Issues – Part 1

Bu kısımda input kontrol eksikliğinden kaynaklanan zafiyetlere değinilmiştir.

Buradaki input girilen değeri aramaktadır.

Varsa ekrana getirmekte yoksa bulunamadı olarak çıktı vermekte.

Sql injection denemesi yapmak için "tırnak kullanıyoruz fakat bize user bulunamadı olarak çıktı vermekte.

' tırnak denediğimizde ise her hangi bir user bulunamadı çıktısı vermemekte boş döndürmektedir.

()

....

DIVA Input Validation Issues – Part 1 Genymotion for personal use - MobSF VM 0.2 (720x12. A # € 2:34 A # 7. Input Validation Issues - Part 1 GPS Objective: Try to access all user data without 0 knowing any user name. There are three users by default and your task is to output data of all the three users with a single malicious search. Hint: Improper or no input validation issue arise when the input is not filtered or validated before using it. When developing components that take input from outside, always validate it. For ease of testing there are three users already present in the database, for example one of them is admin, you can try searching for admin to test the output. SEARCH ſ User: (1) not found

F



```
public void search(View paramView)
  EditText localEditText = (EditText)findViewById(2131493017);
  try
    Cursor localCursor = this.mDB.rawQuery("SELECT * FROM sqliuser WHERE user = '" + localEditText.getText().toString() + "'", null);
    StringBuilder localStringBuilder = new StringBuilder(");
    if ((localCursor != null) && (localCursor.getCount() > 0))
      localCursor.moveToFirst();
      dö
        localStringBuilder.append("User: (" + localCursor.getString(8) + ") pass: (" + localCursor.getString(1) + ") Credit card: (" +
      while (localCursor.moveToNext());
    while (true)
      Toast.makeText(this, localStringBuilder.toString(), 0).show();
      return:
      localStringBuilder.append("User: (" + localEditText.getText().toString() + ") not found");
```







DIVA Acces Control Issues – Part 1

Erişim control sorunları başlıklı bu bölümde activitylerin AndroidManifest.xml dosyasında gerekli şekilde konfigurasyonu ve izinleri ayarlanamadığında activityler dışarıdan butonlara tıklanmadan açılabilmektedir.

Drozer ve adb gibi araçlarla bu işlemler yapılabilmektedir.

Bu kısımda View Apı Credentials a tıkladığımızda yeni bir activity açılarak api bilgilerini getiriyor. Buraya tıklamadan dışarıdan komut ile activity başlatılabilmektedir.

DIVA Acces Control Issues – Part 1

9. Access Control Issues - Part 1

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. **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.

VIEW API CREDENTIALS

DIVA Acces Control Issues – Part 1

	Genymotion for personal use - MoDSF_VM_0.2 (72)	Genymotion for personal use - MoDSF_VM_0.2 (720x12		
	▲ #	•		
	Vendor API Credentials	(îr GPS		
▲ ahmet — -bash — 71×23 Last login: Sat May 13 15:00:26 on console Ahmet-MacBook-Pro:~ ahmet\$ adb shell am start -n jakhar.aseem.diva/.API CredsActivity -a jakhar.aseem.diva.action.VIEW_CREDS WARNING: linker: libdvm.so has text relocations. This is wasting memory and is a security risk. Please fix.	API Key: 123secretapikey123 API User name: diva API Password: p@ssword	۵. ۱۹۹۳ - ۲۹۹۳ - ۲۹۹۳ - ۲۹۹۳ - ۲۹۹۳ - ۲۹۹۳ - ۲۹۹۳ - ۲۹۹۳ - ۲۹۹۳ - ۲۹۹۳ - ۲۹۹۳ - ۲۹۹۳ - ۲۹۹۳ - ۲۹۹۳ - ۲۹۹۳ - ۲۹۹۳ -		
WARNING: linker: app_process has text relocations. This is wasting memo ry and is a security risk. Please fix. Starting: Intent { act=jakhar.aseem.diva.action.VIEW_CREDS cmp=jakhar.a seem.diva/.APICredsActivity } Ahmet-MacBook-Pro:~ ahmet\$				
		Ĵ		

adb shell am start -n jakhar.aseem.diva/.API CredsActivity -a jakhar.aseem.diva.action.VIEW_CREDS

DIVA Acces Control Issues – Part 2

Erişim control sorunlarının ikinci kısmıda illk kısmına benzer sadece bu sefer uygulama açıldığında önümüze iki seçenek suruyor Kayıt ol ve Zaten Kayıtlı Kullanıcıyım tarzında kayıt ol seçeneğine tıklandığı zaman PIN sormakta.

Fakat Zaten kayıtlı kullanıcıyım sekmesinde ise direk activity açılmakta. Bizim amacımız zaten kayıtlı kullanıcıyım butonuna basmadan bu activity'i dışarıdan çalıştırmak.

DIVA Acces Control Issues – Part 2

10. Access Control Issues - Part 2

Objective: You are able to access the Third Party app TVEETER API credentials after you have registered with Tveeter. The App requests you to register online and the vendor gives you a pin, which you can use to register with the app. Now, try to access the API credentials from outside the app without knowing the PIN. This is a business logic problem so you may need to see the code. Hint:Components of an app can be accessed from other apps or users if they are not properly protected and some may also accept external inputs. Components such as activities, services, content providers are prone to this.

O Register Now. O Already Registered.

VIEW TVEETER API CREDENTIALS

Tveeter API Credentials

Register yourself at http://payatu.com to get your PIN and then login with that PIN!

Enter PIN received from Tveeter

TVEETER API CREDENTIALS

DIVA Acces Control Issues – Part 2

Tveeter API Credentials

TVEETER API Key: secrettveeterapikey API User name: diva2 API Password: p@ssword2

DIVA Acces Control Issues – Part 2

Kaynak kod incelendiği zaman check_pin true gibi bir kod satırı görülmekte ve biz bunu adb ile activity'i başlatırken –ez check_pin false parametresini ekleyerek activity'i dışarıdan tetikleyip hiç bir butona basmadan çalıştırılabilmektedir.

DIVA Acces Control Issues – Part 2



DIVA Acces Control Issues – Part 3

Bu kısımda yine erişim control sorunlarına değinilmiş. Kullanıcıdan bir pin kodu girmesi istenmektedir.

Girilen PIN kodu sharedpreferences dizinin altında xml dosyasına yazılmaktadır. Buradan PIN koduna ulaşabilmekteyiz. 11. Access Control Issues - Part 3

Objective: This is a private notes application. You can create a PIN once and access your notes after entering the correct pin. Now, try to access the private notes from outside the app without knowing the PIN.

Hint:Components of an app can be accessed from other apps or users if they are not properly protected and some may also accept external inputs. Components such as activities, services, content providers are prone to this.

Enter 4 Digit PIN CREATE/CHANGE PIN GO TO PRIVATE NOTES

DIVA Acces Control Issues – Part 3



DIVA Hardcoding Issues – Part 2

Bu aşama daha önce değindiğimiz kaynak kodda bulunan parola ve doğrulama değerlerinden kaynaklanan güvenlik açıklıklarıdır.

DIVA Hardcoding Issues – Part 2

```
33
    #include <jni.h>
34
    #include <string.h>
35
    #include "divajni.h"
36
37
    #define VENDORKEY
                        "olsdfgad; lh"
38
    #define CODE
                        ".dotdot"
39
    #define CODESIZEMAX 20
40
    /*
     * Verify the key for access
41
42
     *
43
     * @param jkey The key input by user
44
     *
45
     * @return 1 if jkey is valid, 0 otherwise. In other words
46
     0
               if the user key matches our key return 1, else return 0.
47
     */
48
    JNIEXPORT jint JNICALL Java jakhar aseem diva DivaJni access(JNIEnv * env, jobject jobj, jstring jkey) {
49
50
        const char * key = (*env)->GetStringUTFChars(env, jkey, 0);
52
        return ((strncmp(VENDORKEY, key, strlen(VENDORKEY)))?0:1);
53
    }
54
```

Kaynak kodda bulunan bu key apk decompiler işlemlerinden sonra elde edilebilir durumdadır.

DIVA Hardcoding Issues – Part 2



DIVA Input Validation Issues – Part 3

Input kontrol eksikliğinden kaynaklanan zafiyetlerin üçüncü kısmı bu sefer input uzunluğu kontrol edilmemiş.

10 karakter girildiğinde herhangi bir sorun vermemektedir fakat 40 adet karakter girildiğinde uygulama crash olmaktadır.





Google Play Uygulamaları Gerçek Olmayabilir !

S	AliExpress	••	-
Скай⊓ 2tyivunk ★★★★★	Алиэкспресс 2tyivunk	Авито kovdka	Юла kovdka
Skype - free IM & vic	AliExpress Shoppin	Объявления Avito	Юла – объявления
Skype - free five & Vic Skype	Alicxpress Shoppin Alibaba Mobile	Avito.ru	Mail.Ru Group
****	****	****	****

Google Play Uygulamaları Gerçek Olmayabilir !



Kontrol Listesi (Check List)

- 1. Network Trafiği
- 2. SSL Pinning Kontrolu / Bypass
- 3. Web Servis Kontrolleri
- 4. Yanlış Kimlik Doğrulaması
- 5. Oturum Yönetimi Kontrolü
- 6. IDOR
- 7. MongoDB/NoSQL Injection
- 8. Yönetim Panel Login Brute Force
- 9. Uygulama Komponent Analizi (Drozer)
- 10. File Verification
- 11. Uygulama Yetkilendirmeleri ve Kriptografik Kontroller
- 12. Lokal Veri Analizi
- 13. Veri Sızıntısı Android Backup
- 14. Tersine Mühendislik Hardcoded Credential Kontrolü
- 15. Patching/Modification
- 16. QRCode Backdoor
- 17. Subdomain Keşif
- 18. Email Keşif
- 19. Github vb. Siteler ile Hassas Veri Kontrolü

info@gurelahmet.com

