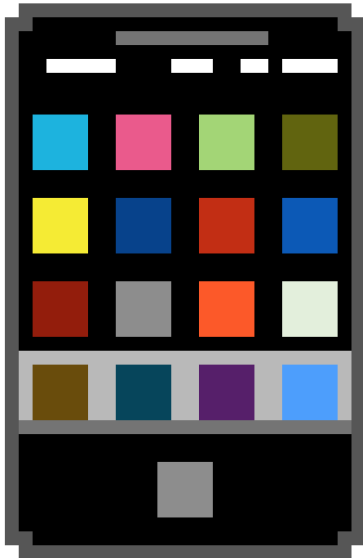


Root Detection Bypass with frida-push + Objection for iOS and Android



OBJECTION
RUNTIME
MOBILE
EXPLORATION
[GIT.IO/OBJECTION](https://git.io/objection)

AHMET RECEP SAĞLAM

Root Detection Bypass with frida-push + Objection for iOS and Android

Frida ve Objection nedir ?

Frida'nın nasıl çalıştığını daha iyi anlamak için ilk önce **DBI** (Dinamik İkili Enstrümantasyon)' i bilmemiz gerekmektedir. Enstrümantasyon, bilgisayar programlamada bir uygulamanın performans ölçümü veya hatalarını tespit etmek demektir. DBI bu enstrümantasyon yaklaşımlarından bir tanesidir. DBI ile çalışan uygulamalardaki işlemler analiz edilebilir ve değiştirilebilir. Frida bir DBI aracıdır ve dinamik olarak uygulamanın işlemlerinde değişiklik yapmaya yarayan bir araçtır.

Objection ise frida ile yazılmış bir uygulama olup frida gibi aynı şekilde dinamik analiz yapmaya yarayan bir araçtır. Frida' dan farkı ise sık kullanılan scriptleri içerisinde bulundurmasıdır.

Frida'nın veya objection'ın cihaz ile haberleşmesi için kurulması gereken frida-server adında dosya mevcuttur. Bu dosya android sürüm ve mimarilere göre değişiklik göstermektedir. Bunun kurulumunu basitleştirmek için geliştirilen aracın adı ise frida-push'dur.

Kurulum

```
pip3 install frida-push  
pip3 install objection
```

Root Detection Bypass

Frida-push aracımız ile cihazımıza frida-server yüklüyoruz.

```
(*)  
(12:27:27) → frida-push  
[2021-04-27 12:28:49,522] [frida-push: INFO]: Devices: emulator-5554  
[2021-04-27 12:28:49,523] [frida-push: INFO]: Current installed Frida version: 14.0.8  
[2021-04-27 12:28:49,554] [frida-push: INFO]: Found arch: x86  
[2021-04-27 12:28:49,555] [frida-push: INFO]: Using frida-server-14.0.8-android-x86 from downloaded  
[2021-04-27 12:28:49,656] [frida-push: INFO]: File pushed to device successfully.  
[2021-04-27 12:28:49,682] [frida-push: INFO]: Killing all frida-server on device.  
[2021-04-27 12:28:49,723] [frida-push: INFO]: Executing frida-server on device.
```

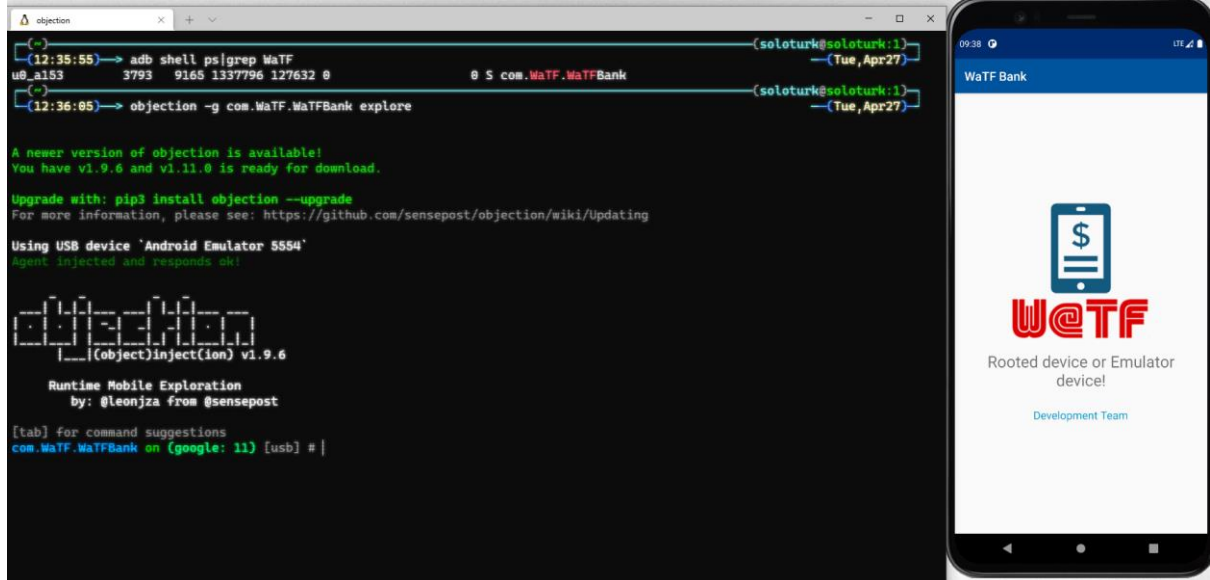
Daha sonra adb Shell ile cihazımıza bağlanıp /data/local/tmp dizininden frida-server'ı çalıştırıyoruz.

```
Adb Shell  
Cd /data/local/tmp  
./frida-server &
```

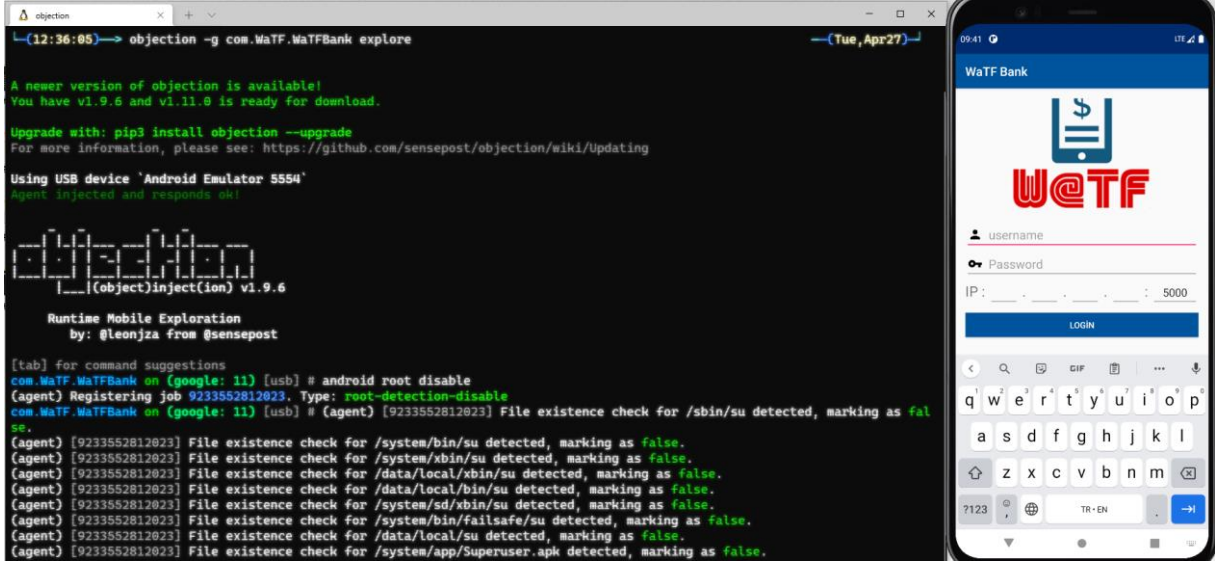
```
(~) (12:30:58) -> adb shell  
generic_x86_arm:/ $ su  
generic_x86_arm:/ # cd /data/local/tmp  
generic_x86_arm:/data/local/tmp # ls  
cert-der.crt frida-server re.frida.server  
generic_x86_arm:/data/local/tmp # ./frida-server &  
[1] 3753  
generic_x86_arm:/data/local/tmp # Unable to start:  
  
[1] + Done (3) ./frida-server  
generic_x86_arm:/data/local/tmp # |
```

Daha sonra uygulamayı başatıp adb ile processler listelendiğinde uygulamanın adı ve pid numarası tespit edilir. Objection -g [uygulamaismi] explore komutu ile objection çalıştırılır.

```
adb shell ps| grep WaTF  
objection -g com.WaTF.WaTFBank explore
```



Objection aracının içinden android root disale komutu çalıştırılarak root bypass işlemi gerçekleştirilir. Uygulama arka plana atılıp tekrar çağrıldığında root kontrolünün bypass işlemi başarıyla gerçekleşmiş olacaktır.



```
objection -g com.WaTF.WaTFBank explore

A newer version of objection is available!
You have v1.9.6 and v1.11.0 is ready for download.

Upgrade with: pip3 install objection --upgrade
For more information, please see: https://github.com/sensepost/objection/wiki/Updating

Using USB device 'Android Emulator 5554'
Agent injected and responds ok!

Runtime Mobile Exploration
by: @leonjza from @sensepost

[tab] for command suggestions
com.WaTF.WaTFBank on (google: 11) [usb] # android root disable
(agent) Registering job 9233552812023, Type: root-detection-disable
com.WaTF.WaTFBank on (google: 11) [usb] # (agent) [9233552812023] File existence check for /sbin/su detected, marking as false.
(agent) [9233552812023] File existence check for /system/bin/su detected, marking as false.
(agent) [9233552812023] File existence check for /system/xbin/su detected, marking as false.
(agent) [9233552812023] File existence check for /data/local/xbin/su detected, marking as false.
(agent) [9233552812023] File existence check for /data/local/bin/su detected, marking as false.
(agent) [9233552812023] File existence check for /system/sd/xbin/su detected, marking as false.
(agent) [9233552812023] File existence check for /system/bin/failsafe/su detected, marking as false.
(agent) [9233552812023] File existence check for /data/local/su detected, marking as false.
(agent) [9233552812023] File existence check for /system/app/Superuser.apk detected, marking as false.
```

The image shows a terminal window on the left and a mobile emulator on the right. The terminal window displays the Objection framework's command-line interface. It shows the command 'objection -g com.WaTF.WaTFBank explore' being executed. The terminal output includes a notification about a newer version of Objection (v1.11.0) being available, instructions to upgrade using 'pip3 install objection --upgrade', and confirmation that the agent was injected into the Android emulator. Below this, a list of file existence checks is shown, all of which returned 'false', indicating that the root detection bypass was successful. The mobile emulator on the right displays the 'WaTF Bank' login screen, which has a blue header, a logo with a dollar sign and '@TF', and input fields for 'username', 'password', and 'IP' (set to 5000). A 'LOGIN' button is visible at the bottom of the screen.