31 /12 /2021

IOS App Manipülasyonu

Hazırlayan

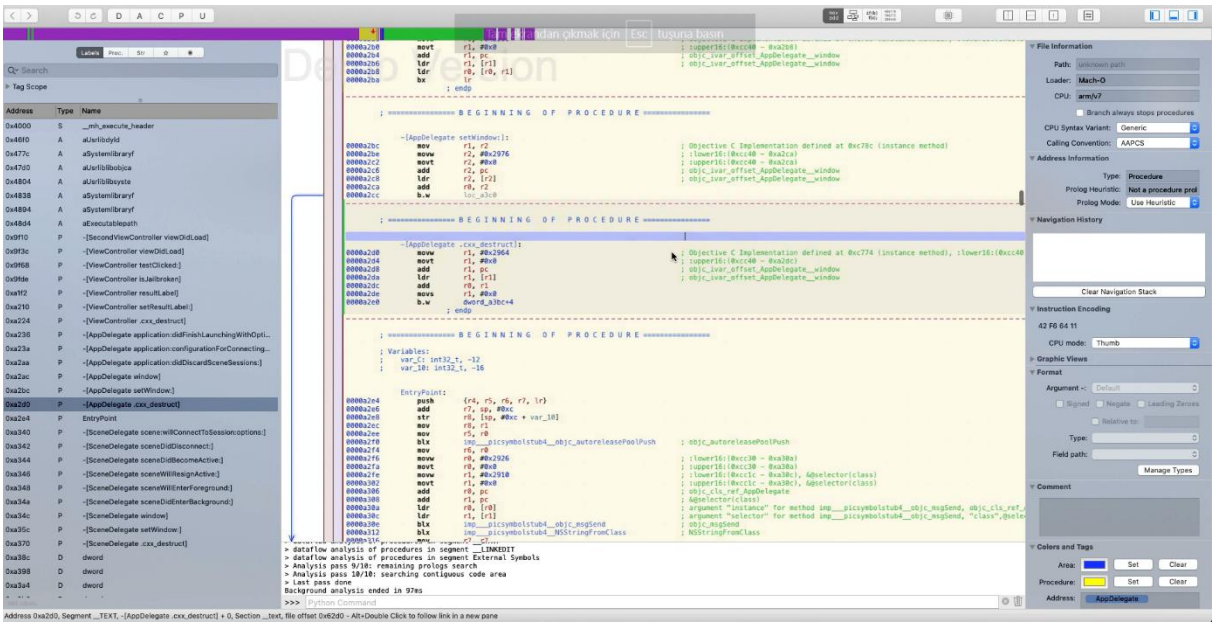
Ümmü Derya Çelik

CTF için hazırlanmış, Başlangıç ekranında ikinci sayfaya yönlendiren bir buton mevcut olan küçük bir uygulamayı manipüle etmeyi deneyeceğiz. Fakat bu uygulama cihazda jailbreak algılarsa ikinci sayfaya yönlendirmeyip erişimi engelliyor. Bu engellemeyi geçerek ikinci sayfaya ulaşmak amacımız.

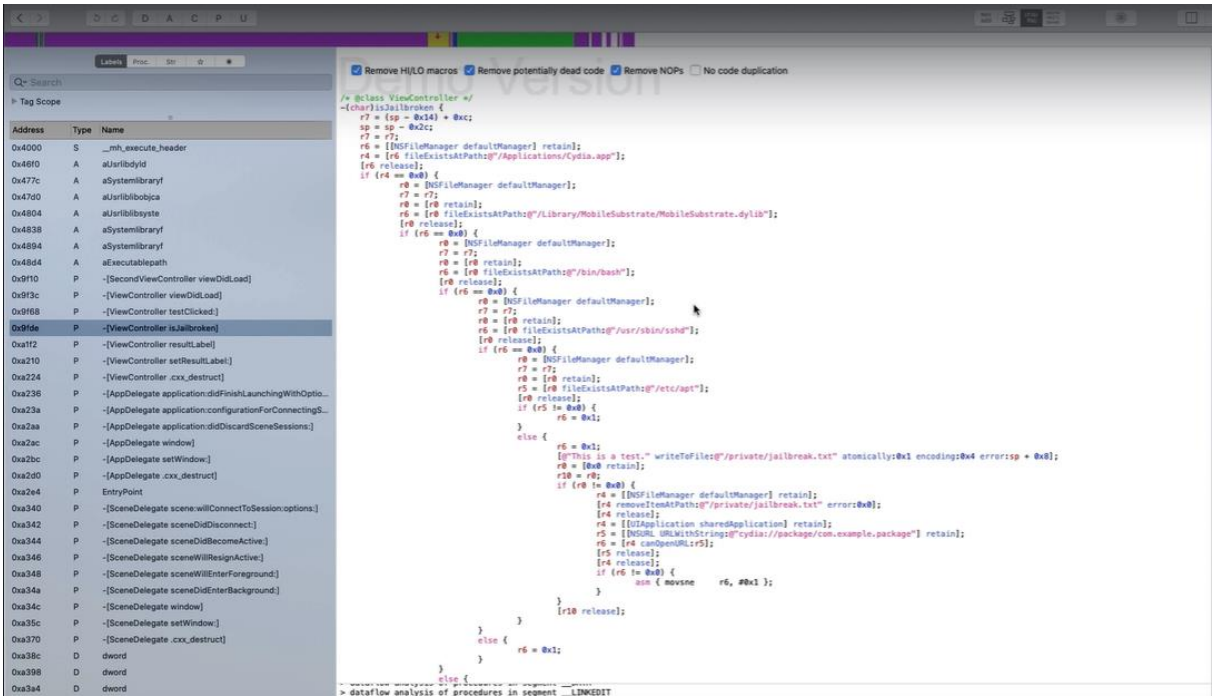
Jailbreakli cihazıma yükleyip uygulamayı açtım. Görünümü şekildeki gibidir;

Uygulamanın ipa dosyasını açıp koddan neler anlayabileceğimize bakalım;

Hopper Disassembler uygulamasını kullarak ipa dosyasını assembly dilinde görüntüleyebiliriz. Hopper uygulamasını açıp ipa dosyasını sayfasına sürükle bırak yaparak ipa dosyasını hopper'da açıyoruz. Ipa dosyasını uygulamasında açtıktan sonra assembly görünümü görseldeki gibidir.



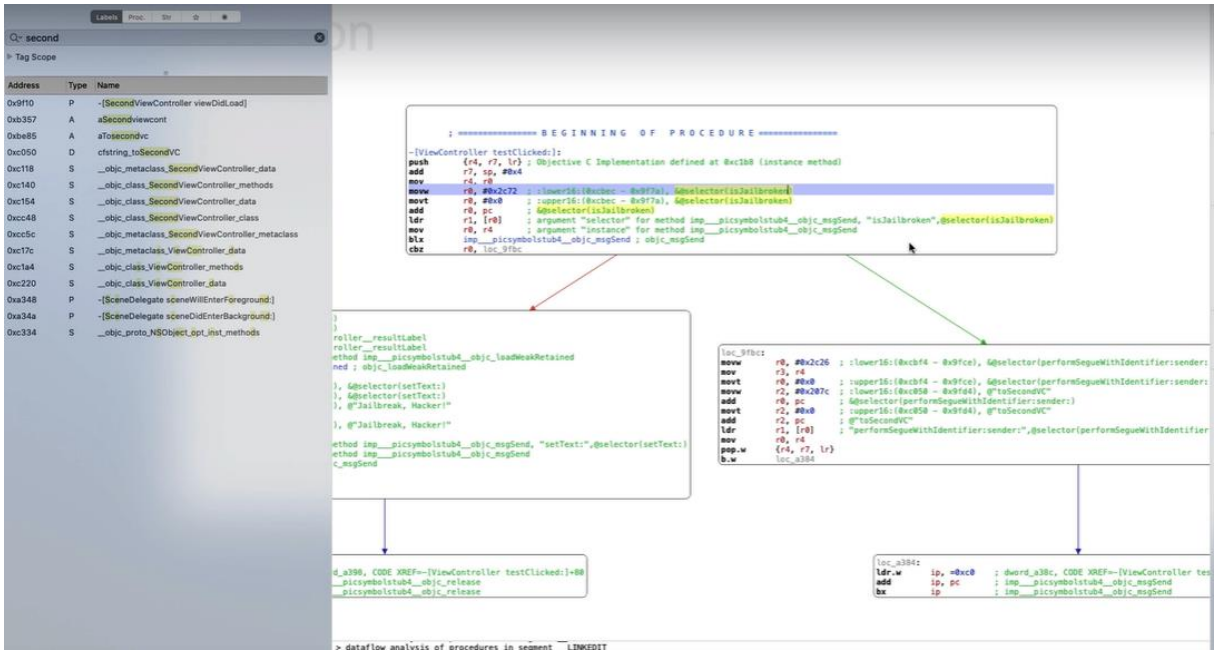
Biraz daha anlaşılabilir koda sağ üstteki görünüm seçeneklerine basarak getirebiliriz.



Bu görünümü if gibi döngüler ekleyerek uygulama kendince bir kod dizini oluşturuyor ve bu sayede biraz daha anlaşılabilir hale gelmekte.

Örneğin görselde gördüğümüz if kontrolünde jailbreakli cihazlarda uygulama yüklemeye yarayan cydia var mı diye kontrol ettiğini ve jailbreak.txt şeklinde bi kontrol dosyasına sahip olduğunu görebiliriz.

Aşağıdaki görselde de görüldüğü üzere view controller ve second view controller olduğunu biliyoruz.



Amacımız Amacımız second view controller'ı görüntülemek. Bunun için kullanacağımız uygulama Cycript. Cycript uygulamasını indirdikten sonra konsolu açıp hedef cihaz ve bilgisayarımız arasında ssh bağlantısı kuruyoruz.

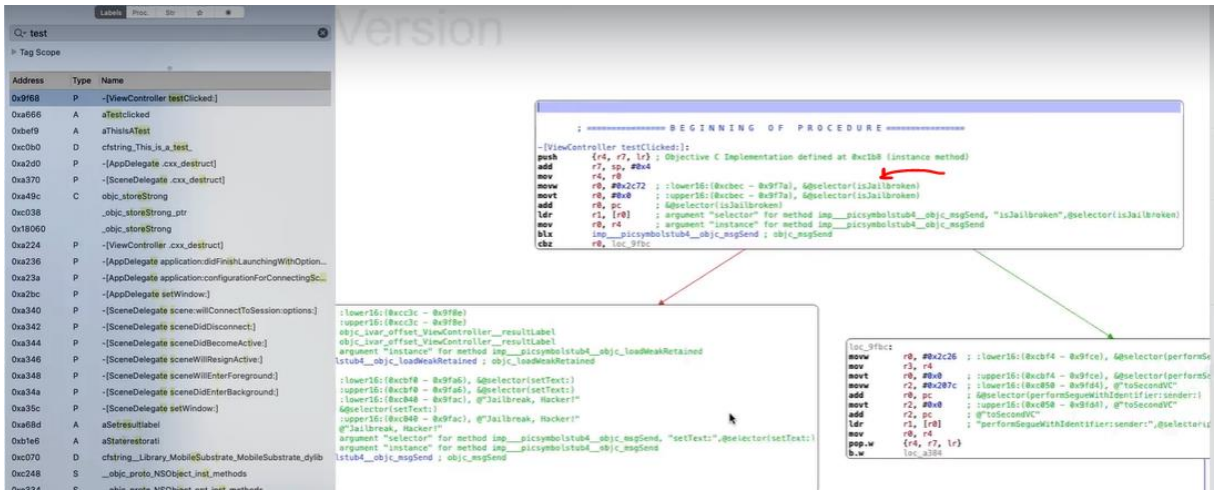
Konsolda " cycript -p DetectJail " komutunu çalıştırıyoruz. Uygulamanın açık olduğundan emin olmamız gerekiyor.

Daha sonra karşımıza çıkan sayfanın adını öğrenmek için " UIApp.keyWindow.rootViewController" komutunu giriyoruz.

```
cy# UIApp.keyWindow.rootViewController
#"<ViewController: 0x1664ae00>"
cy#
```

ViewController'da olduğumuzu gördük. Bizim amacımız önceden de olduğunu gördüğümüz secondViewController'a ulaşmak bunun için hopper uygulamasından assembly şemasına bakalım.

viewController'da bizi yönlendiren true veya false değeri döndüren jailbroken adında bir kontrol görebiliyoruz.



Bu fonksiyonu ne olursa olsun false değerine döndürüp 2. sayfaya yönlendirmesini sağlayabiliriz.

```
cy# ViewController.prototype.isJailbroken = function() {return false;}
function (){return!1}
cy#
```

Bunun için görseldeki kodu yazıyoruz. False değerini döndürmesi için kendimiz java tipinde bir fonksiyon ekledik. Şimdi uygulama da ikinci ekrana gitmeyi deneyelim.

Test butonuna bastık ve daha önce göremediğimiz ikinci sayfayı görüntülemeyi başardık.

Bu işlem sadece o anlık başarılı olmaktadır. Tekrar görüntüleyebilmek için aynı işlemi tekrarlamak gerekmektedir.