InfoSec Write-ups

Setting Up an iOS Pentesting Lab on a Non-Jailbroken iDevice

Abdullah Khawaja 4 min read · Jan 31, 2024

-- 2

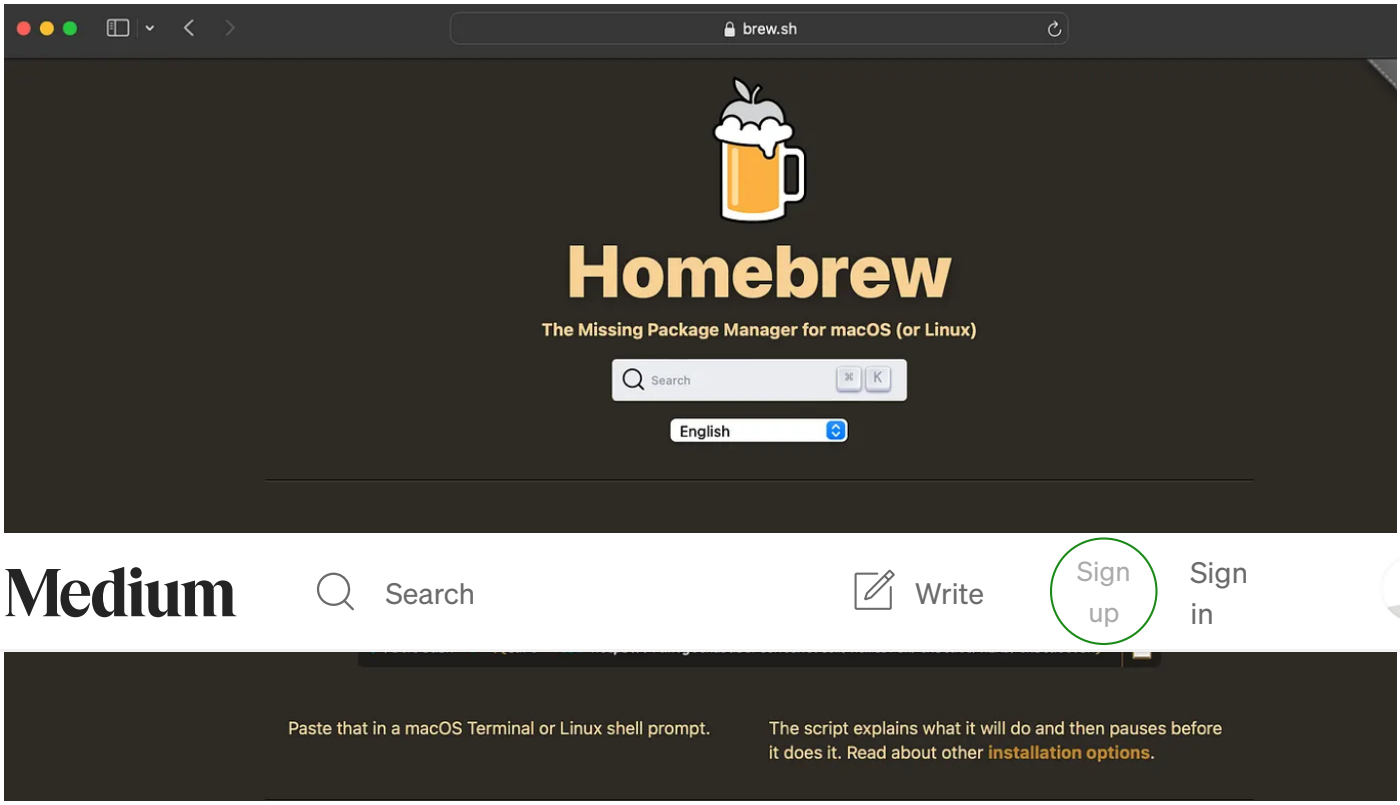
Introduction:

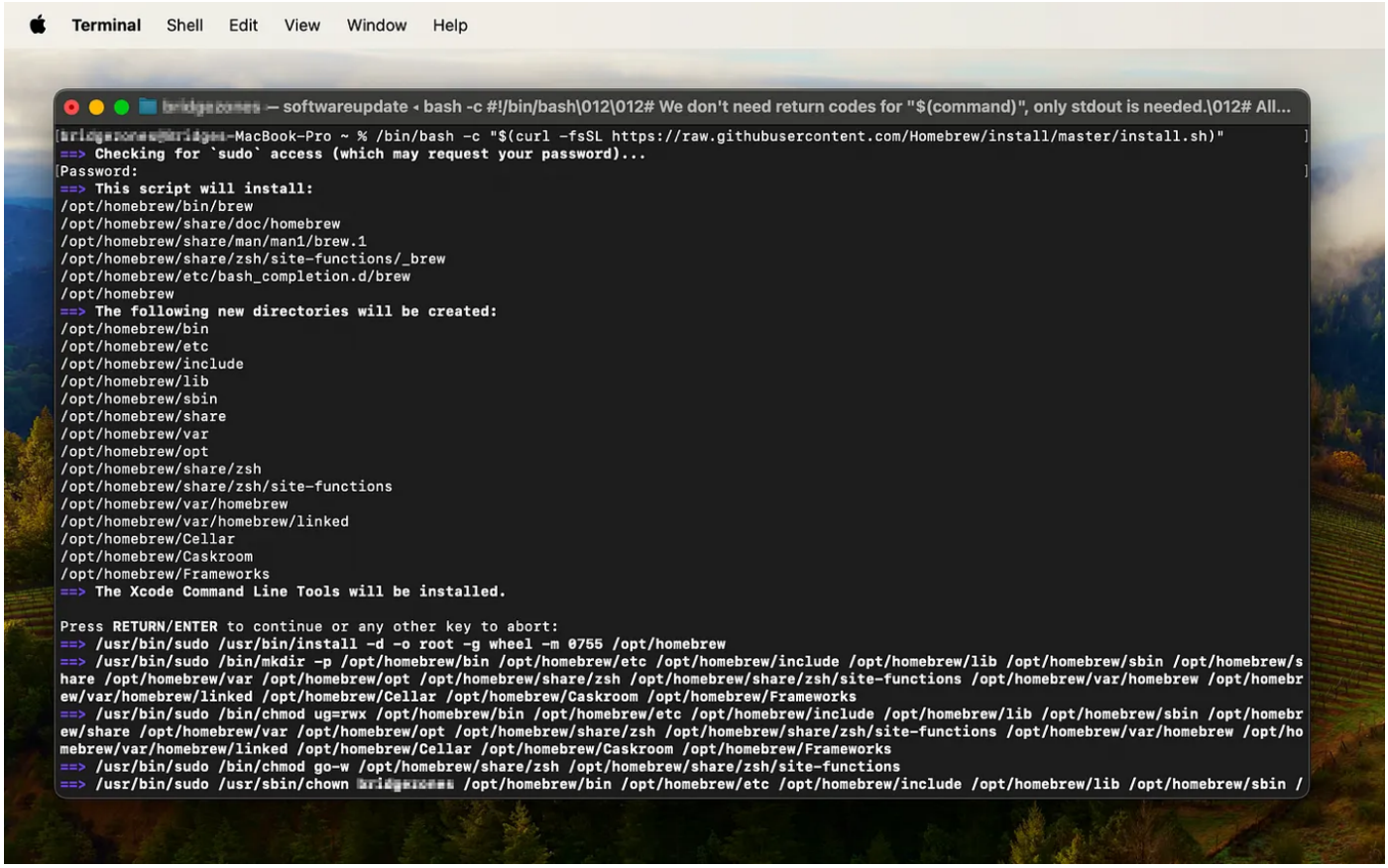
Pentesting iOS apps can be tough when you can't jailbreak your iPhone or if there's no jailbreak available for your iOS version. This stops us from using powerful tools like Frida and Objection. I've been using a method for the past four years to patch iOS apps without jailbreaking my iPhone . These steps let us use FridaGadget easily, unlocking the full power of Frida and Objection for iOS testing. I'm sharing this method to help other pentesters facing the same issues.

Prerequisites and Dependencies:

1. **Install Homebrew**

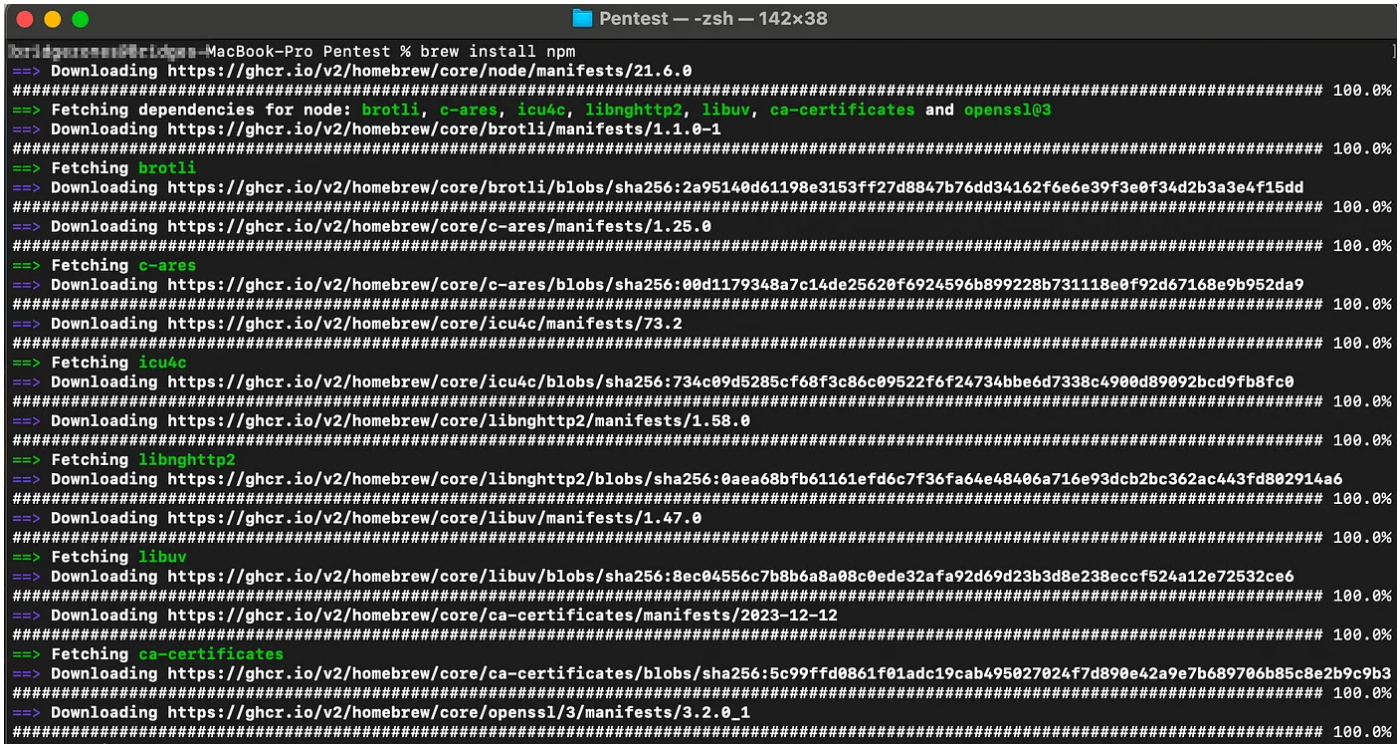
```
/bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/H
```





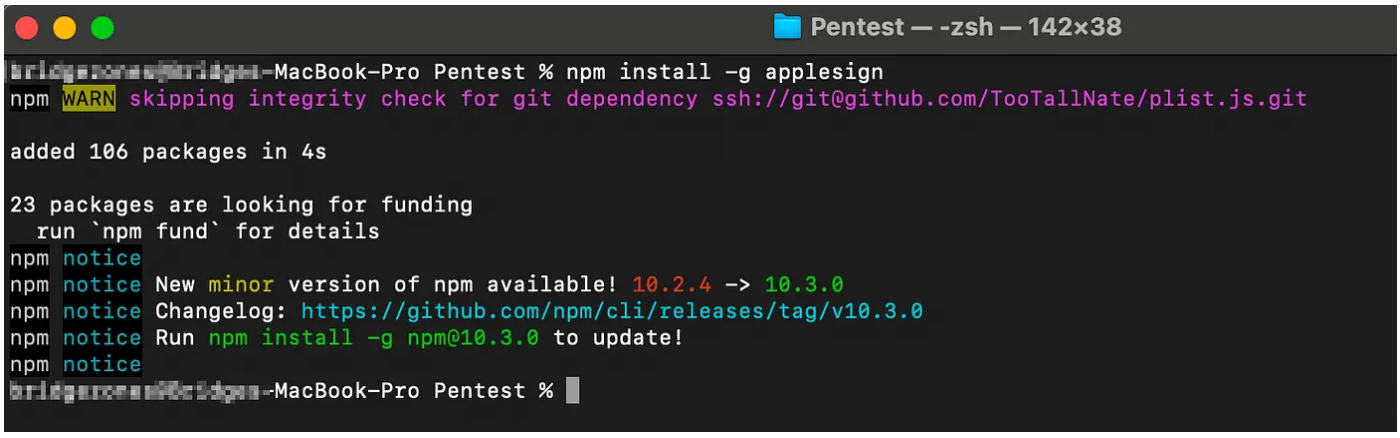
2. Install NPM

```
brew install npm
```



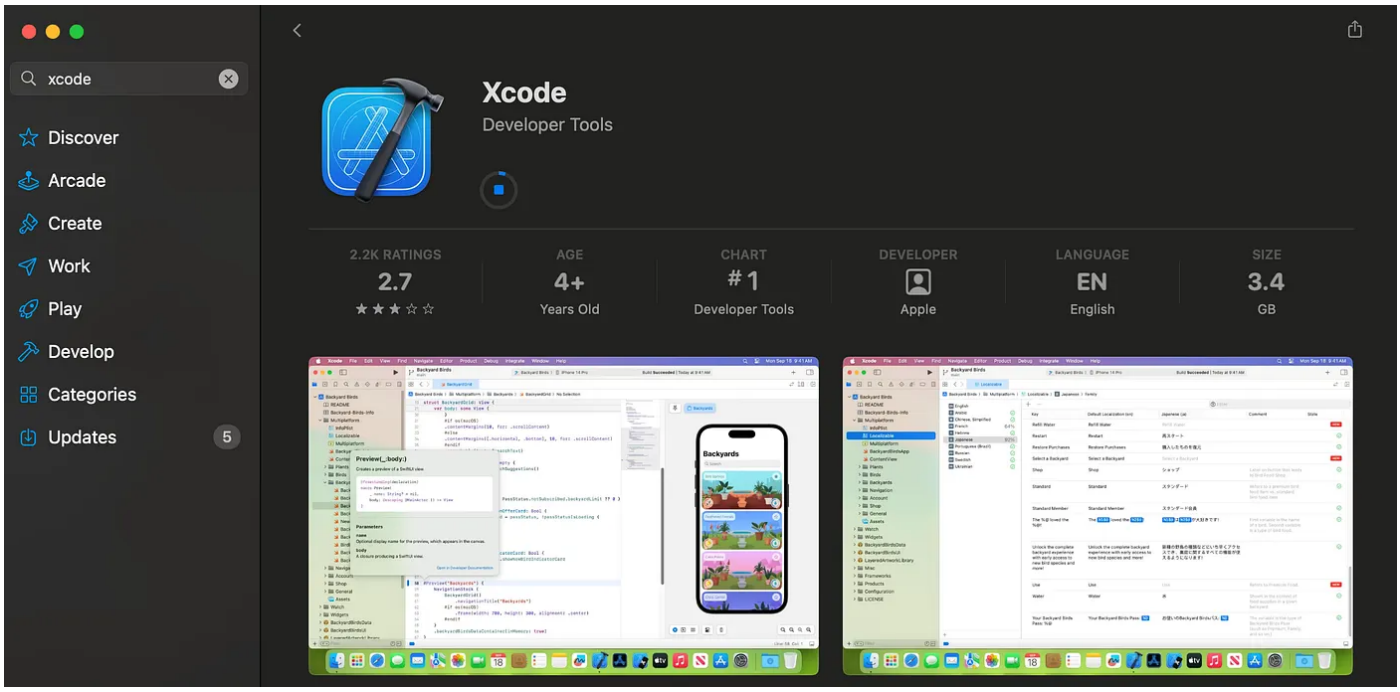
3. Install AppleSign

```
npm install -g applesign
```

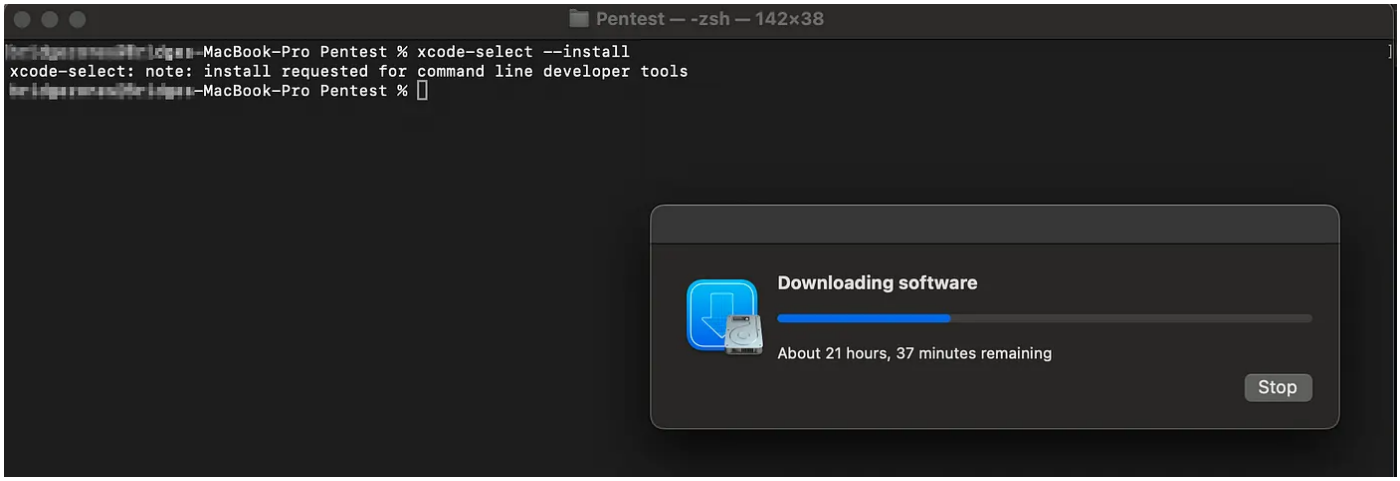


4. Install Xcode

First, install Xcode from the App Store and then install Xcode command line tools:



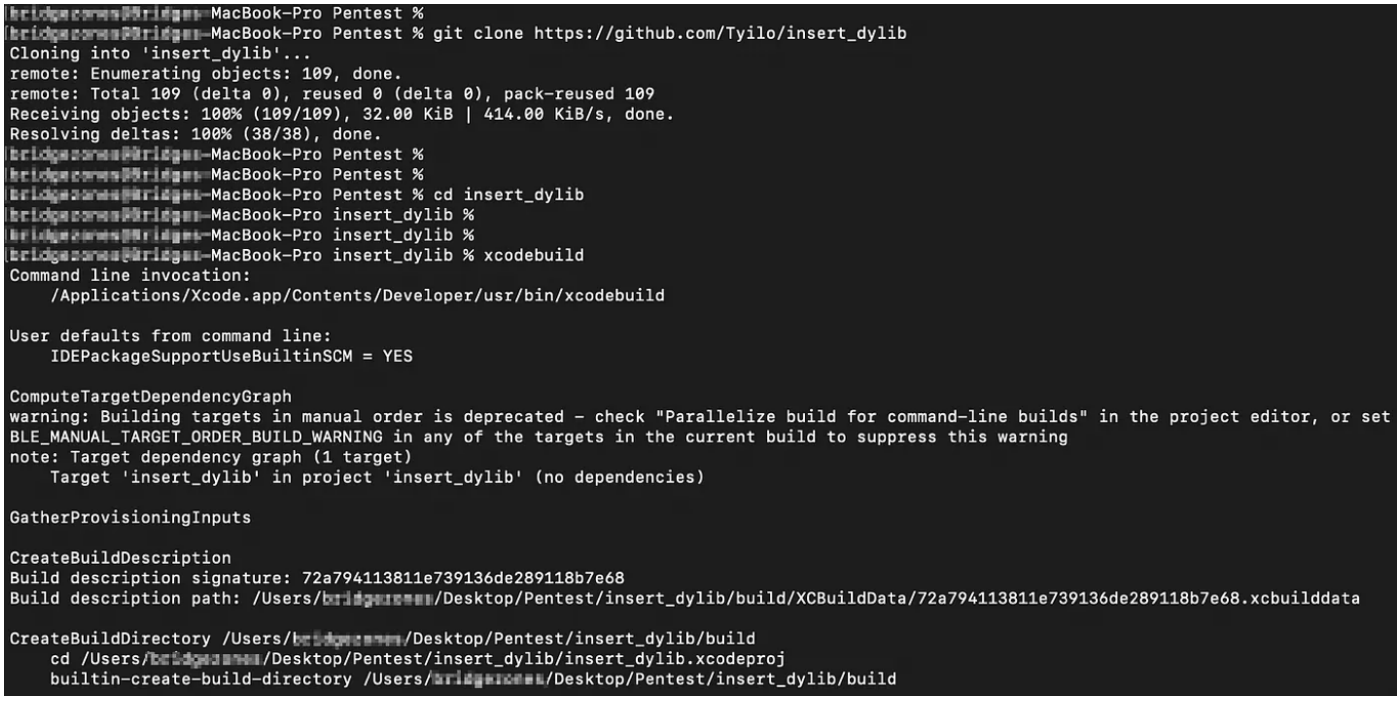

```
xcode-select --install
```



5. Build Insert_dylib

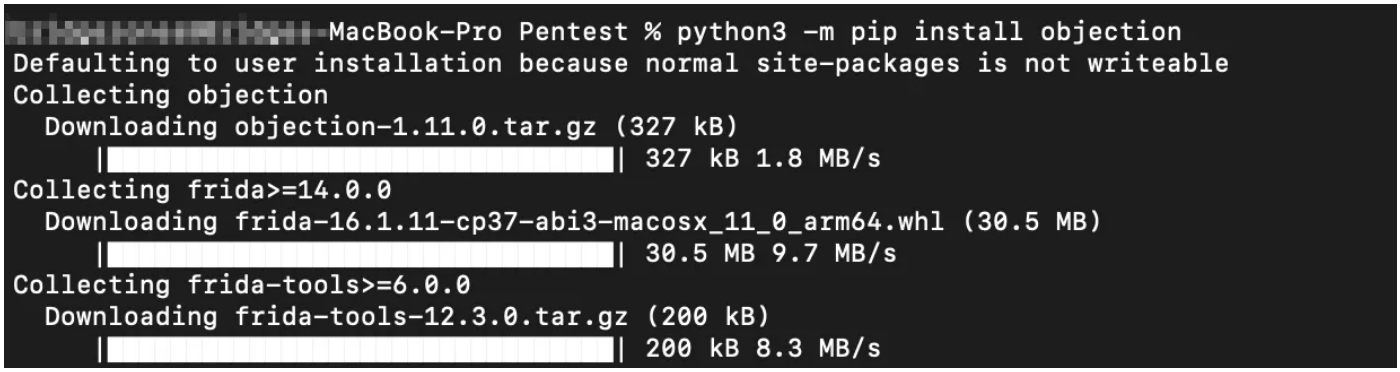
Compile and install insert_dylib from source:

```
git clone https://github.com/Tyilo/insert_dylib
cd insert_dylib
xcodebuild
cp build/Release/insert_dylib /usr/local/bin/insert_dylib
```



6. Install Objection

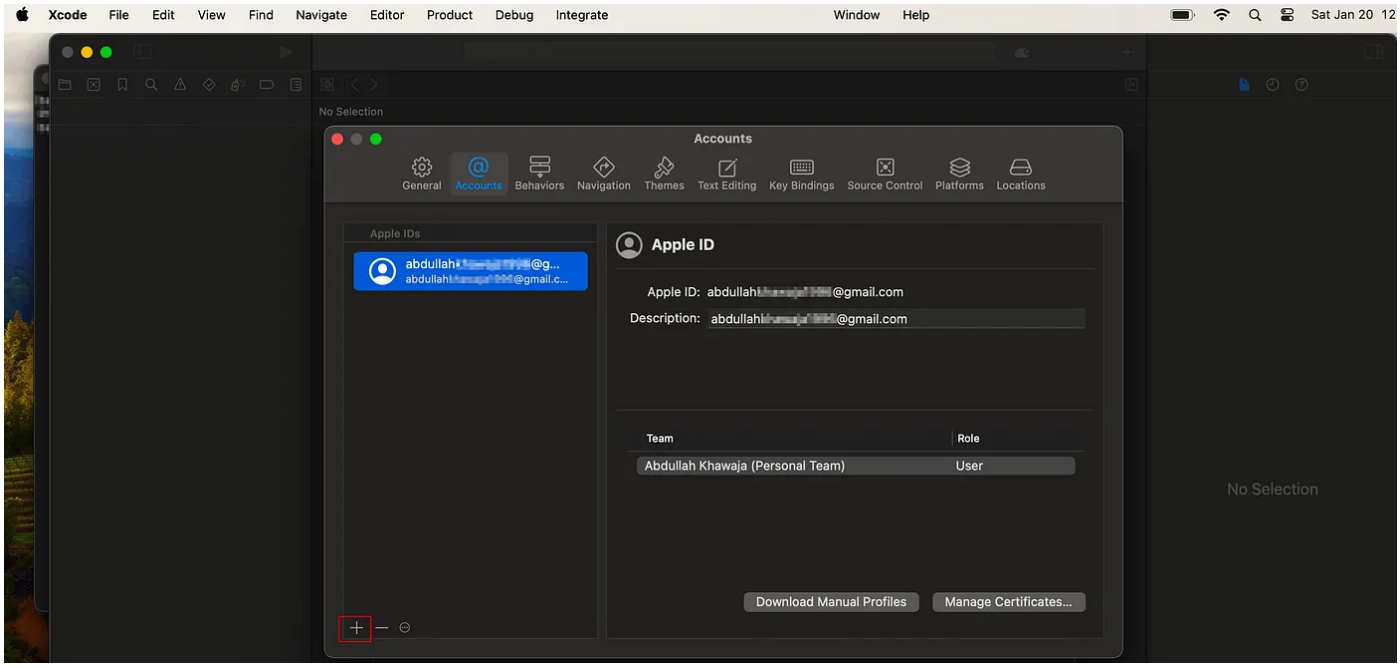
```
python3 -m pip install objection
```

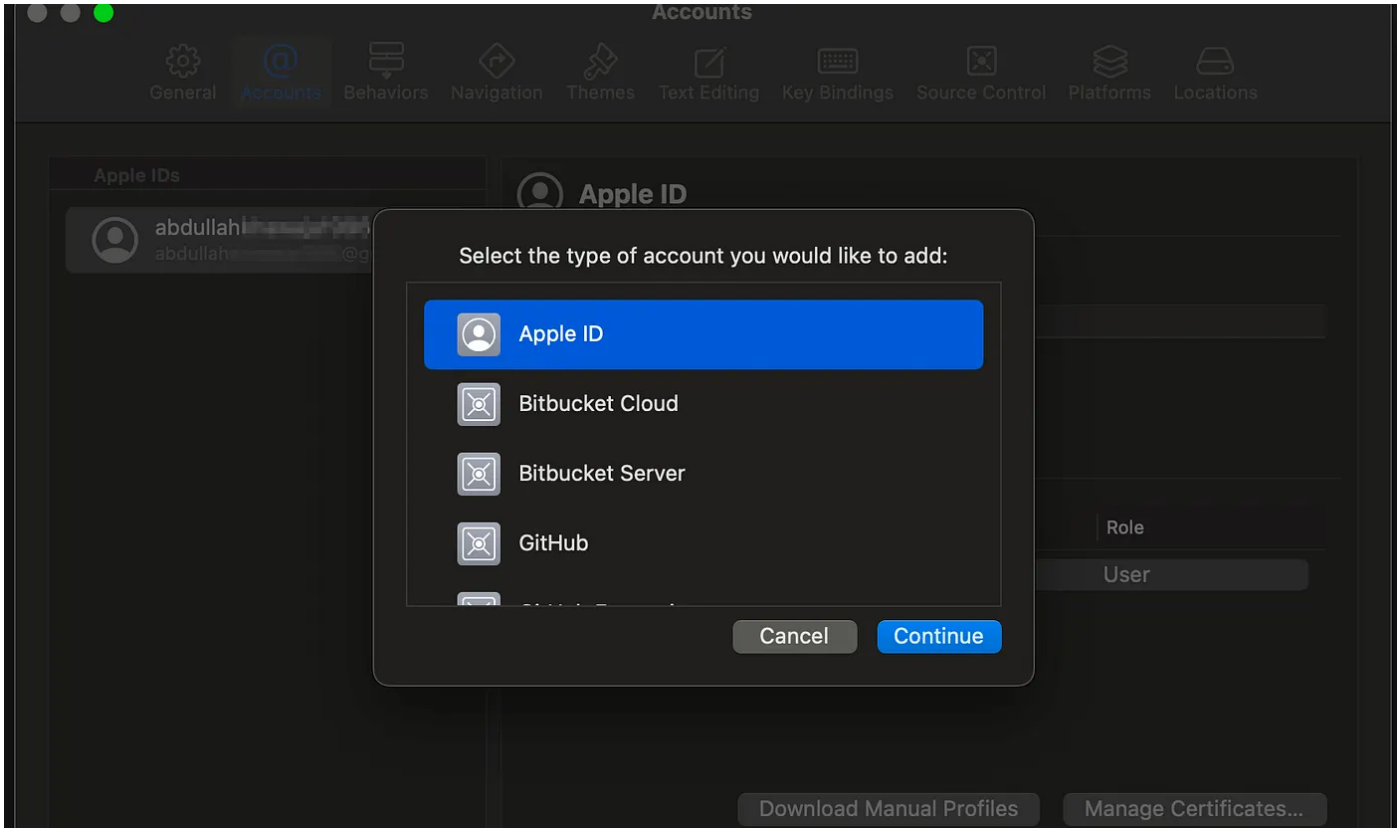


Main Setup

1. Apple Developer Account

1. Open Xcode.
2. Navigate to `Xcode > Preferences`.
3. In the “Accounts” section, click the ‘+’ icon at the bottom left to add your Apple Developer account.

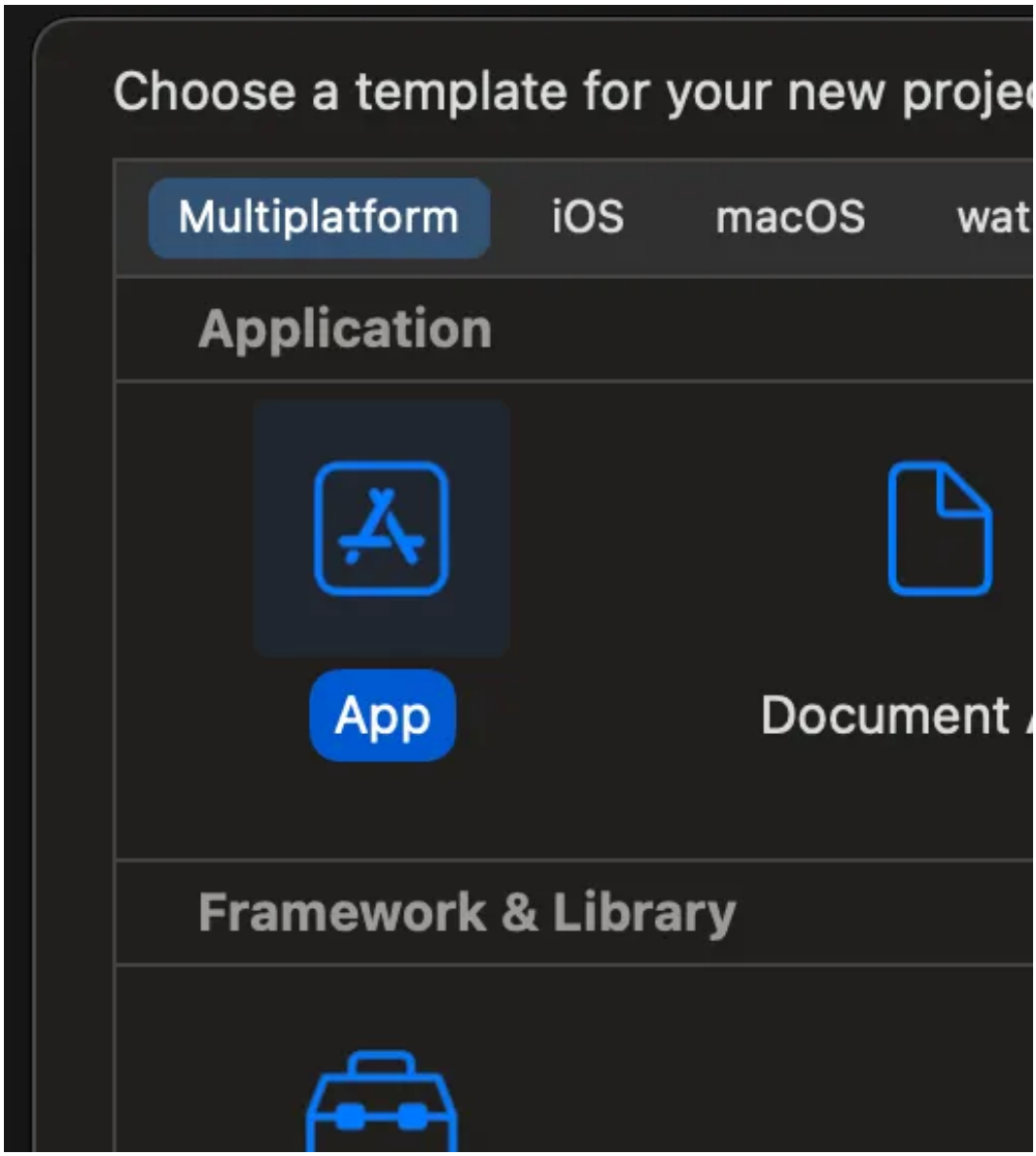


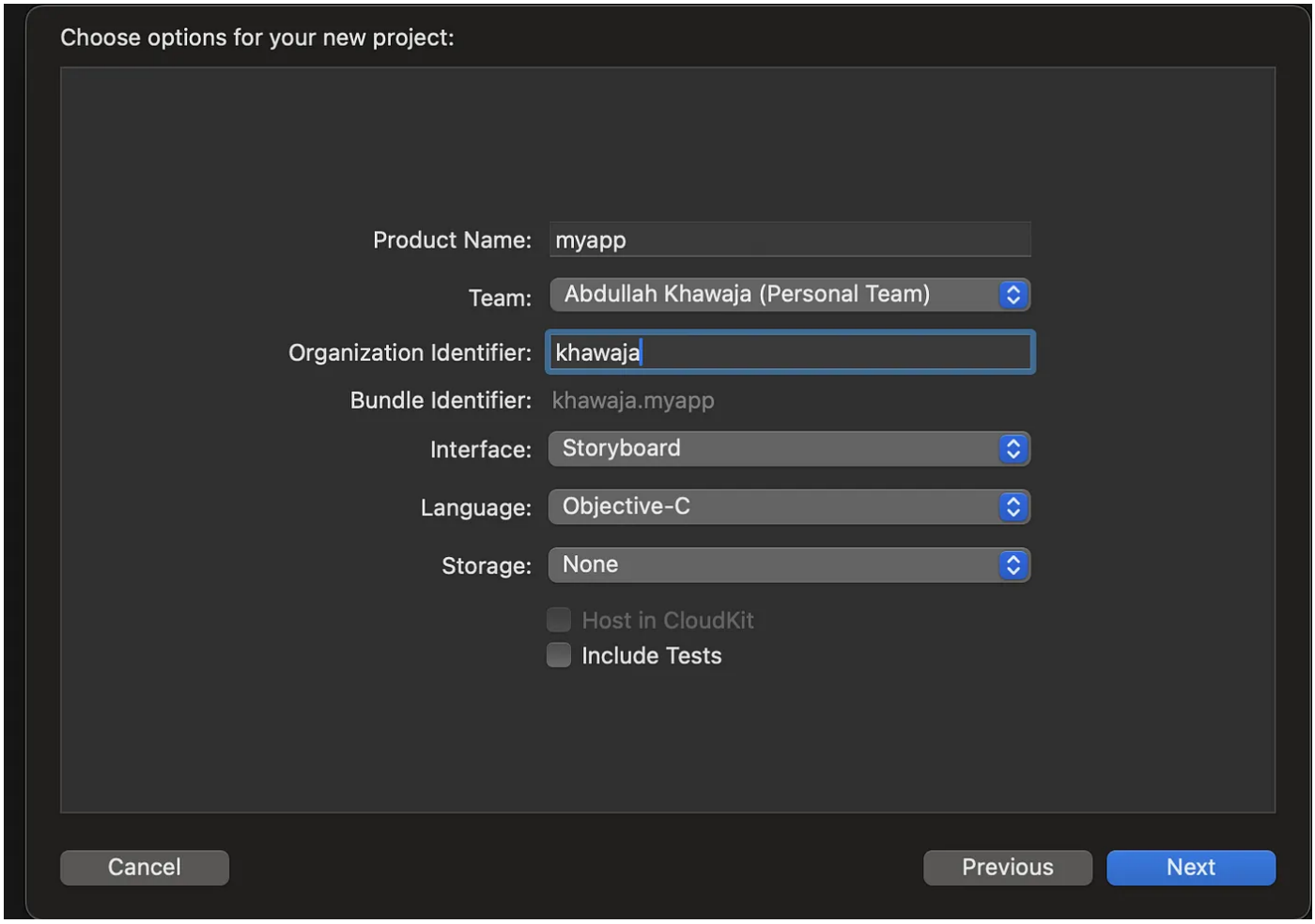


2. Create a Sample Application

1. Open Xcode and go to `File > New > Project.`
2. Select the “App” template.

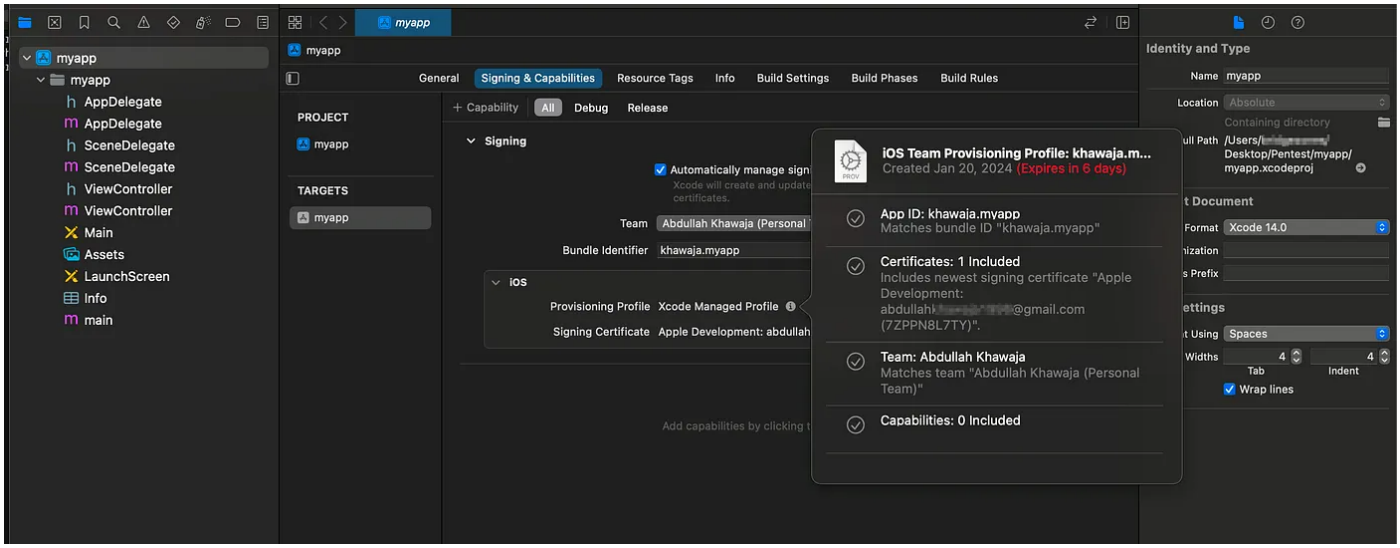
3. Once the project is created, navigate to `Signing & Capabilities`.
4. Verify that your developer account has been added, and you can see the signing certificate.





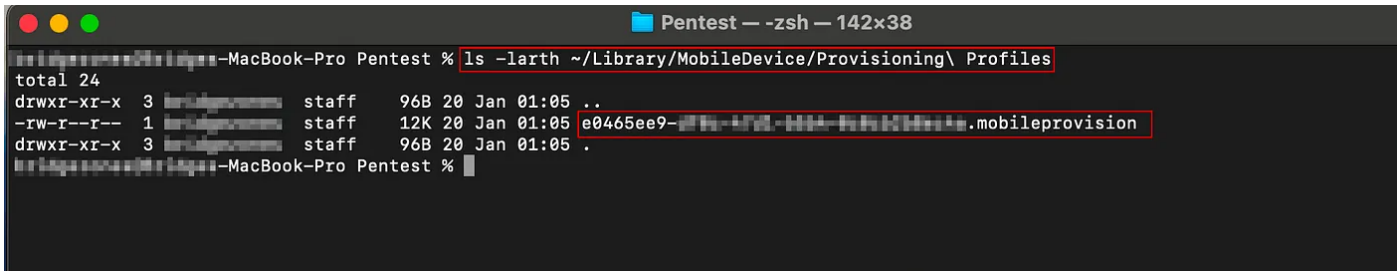
3. Check Provisioning Profile

1. Click on the information icon next to the developer account in `Signing & Capabilities`.
2. Review the properties of the provisioning profile.



4. Provisioning Profile Path

The path for the provisioning profile is `~/Library/MobileDevice/Provisioning Profiles`.



5. Check Signing Identity

Check your signing identity on this device using the command:

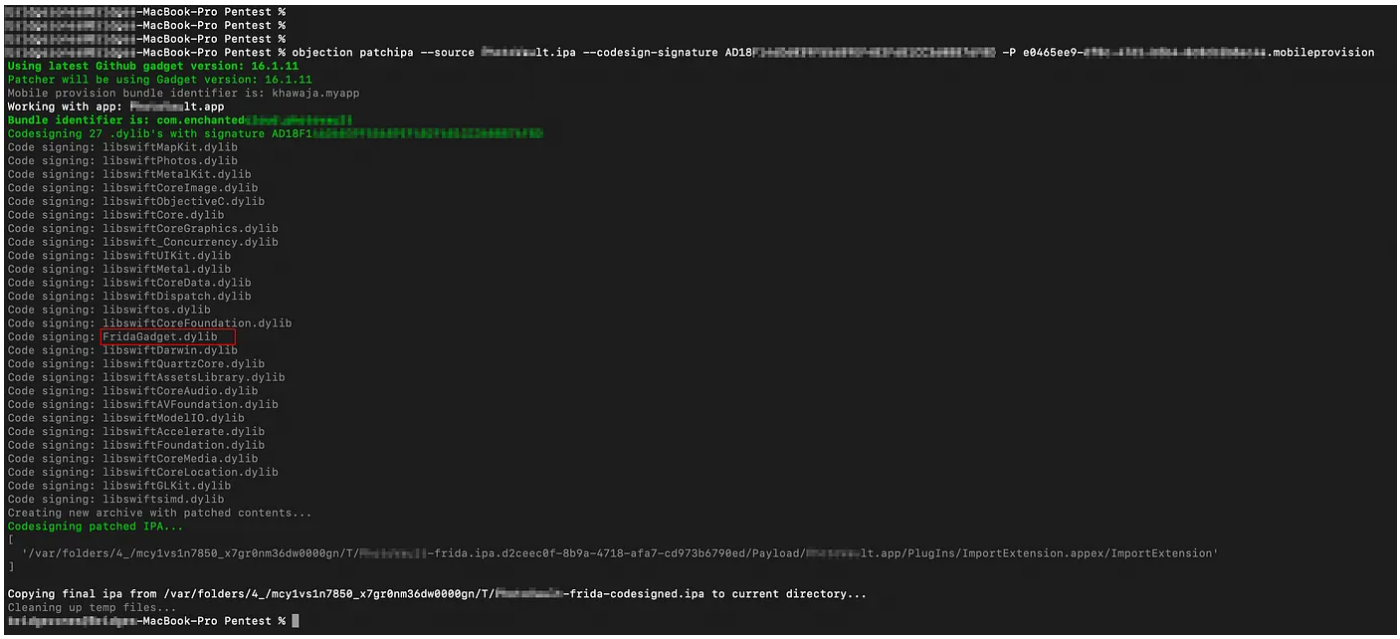
```
applesign -L
```

6. Patch the App

With all dependencies in place, patching an actual IPA is straightforward:

```
objection patchipa --source my-app.ipa --codesign-signature AD18F146xxxx -P e04
```

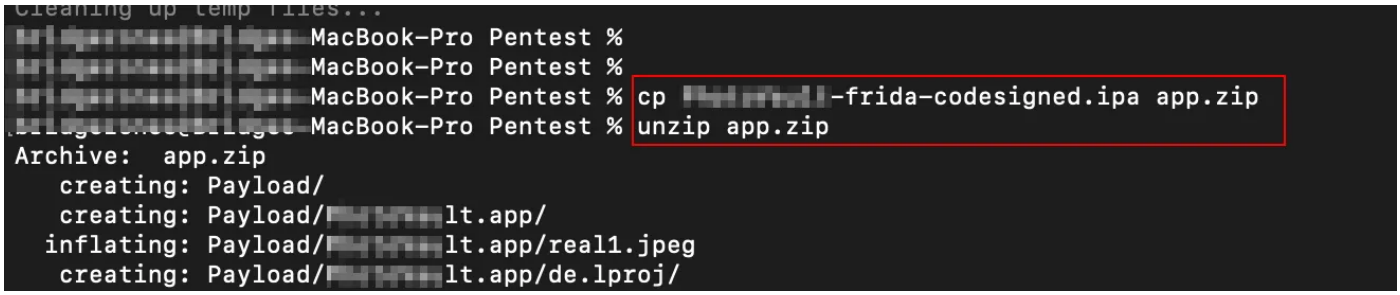
This command will extract the IPA, locate the app binary, patch it to load the FridaGadget.dylib, codesign the dylib and applications binary and repackage it for you.

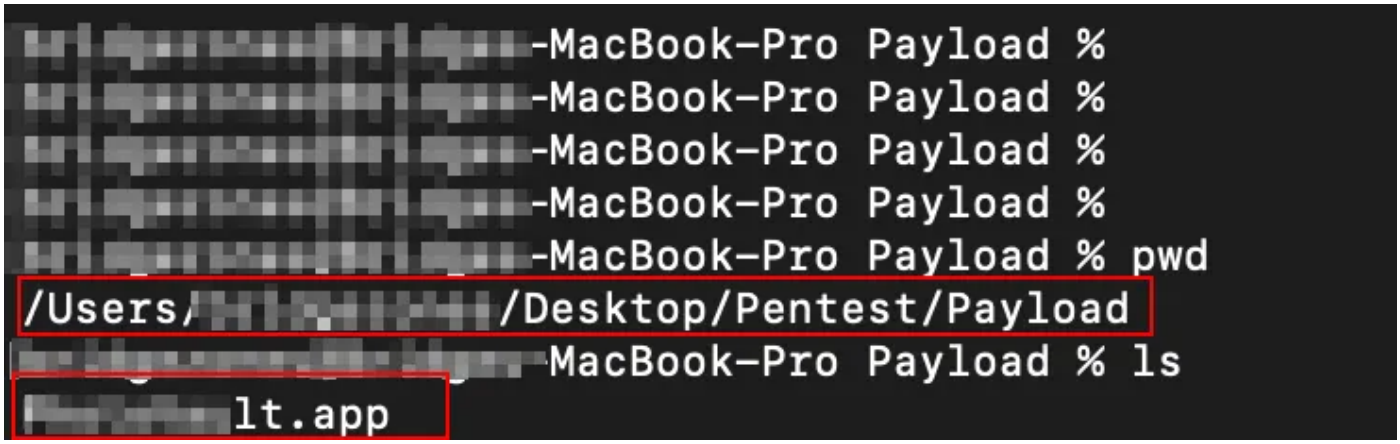


Now, Objection will patch and sign the IPA file, generating a new IPA file named `XXX-frida-codesigned.ipa`.

7. Rename and Execute

1. Rename the newly generated IPA file and change its extension to .zip.
2. Unzip the file to access its contents.
3. Navigate to the Payload directory within the unzipped content.
4. Inside the Payload directory, you will see [bundle-ID].app, where [bundle-ID].app is the folder where your application lives.





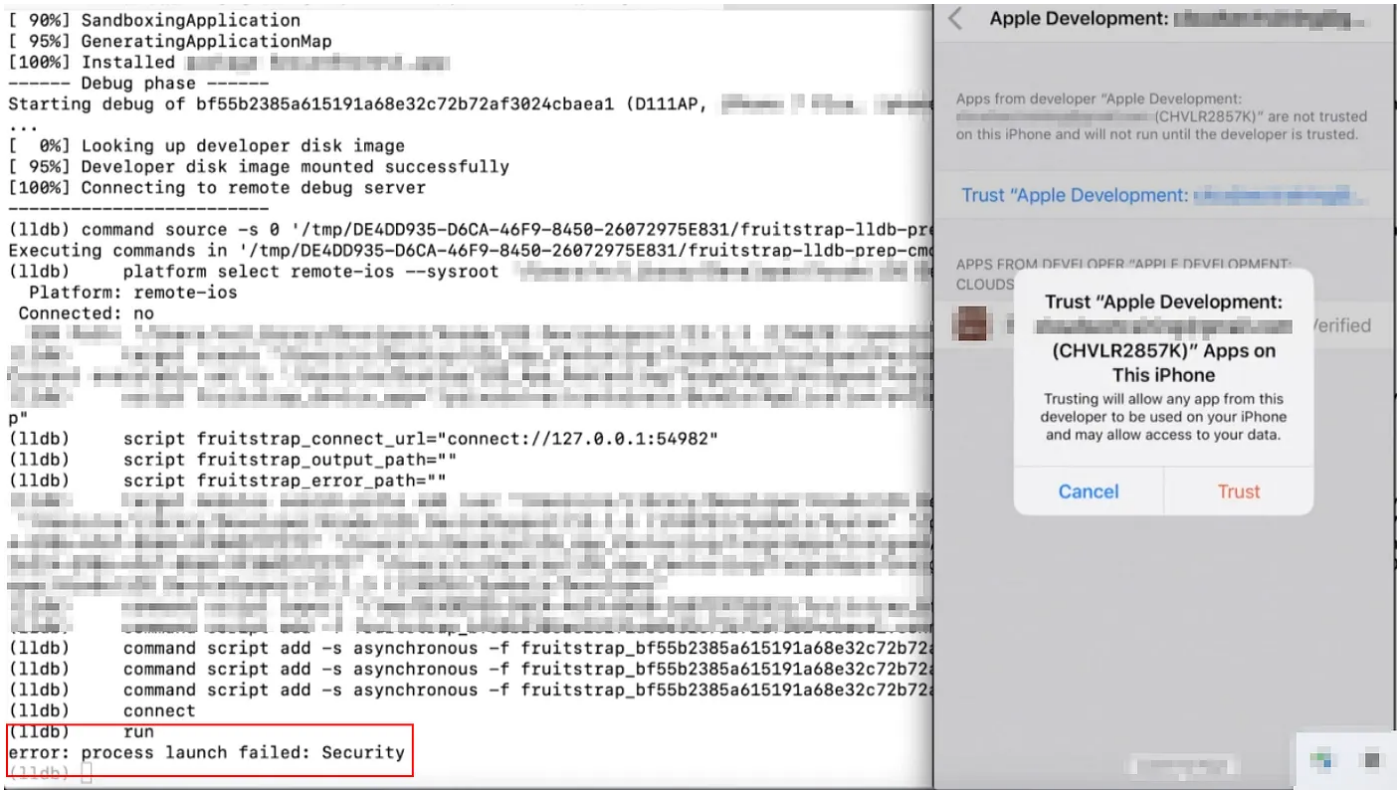
Now, we will deploy this application onto the device using a utility called ios-deploy:

1. Connect your iPhone to your MacBook.
2. Execute the following command in the terminal:

```
ios-deploy --bundle [bundle-ID].app --debug -W
```

Note: If you encounter the error “error: process launch failed,” it indicates that your iPhone hasn’t trusted the developer certificate. To resolve this:

1. Go to General > Device Management on your iPhone.
2. Tap on “Trust Apple Development” certificate.
3. Reinstall the app using ios-deploy, and it should now launch without any issues.
4. You should see the lldb debugger pop up and print out a ‘success’ message.

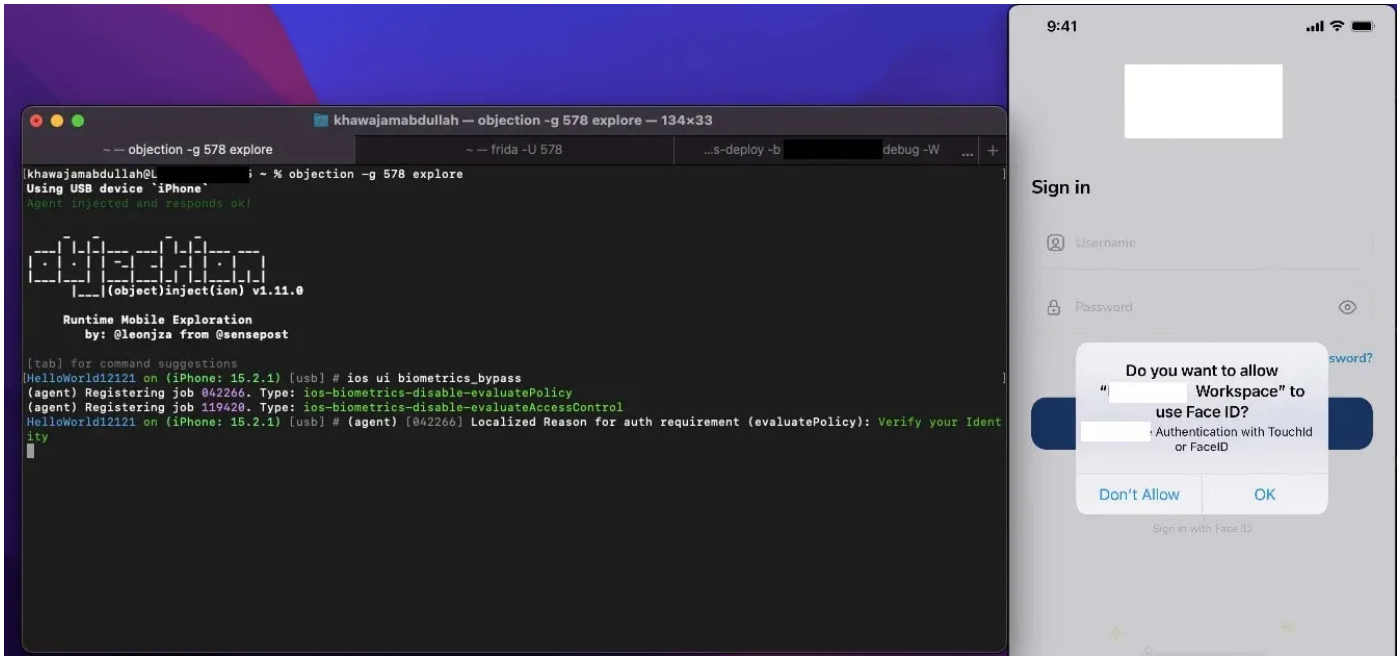


error: process launch failed

```
[ 95%] GeneratingApplicationMap
[100%] Installed package [redacted]
------ Debug phase ------
Starting debug of bf55b2385a615191a68e32c72b72af3024cbaea1 (D111AP, [redacted]) a.k.a. 'iPhone' connect
...
[  0%] Looking up developer disk image
[ 95%] Developer disk image mounted successfully
[100%] Connecting to remote debug server
-------------------------
(lldb) command source -s 0 '/tmp/B86D6B4A-B996-44B4-9951-B69A77176A90/fruitstrap-lldb-prep-cmds-bf55b2385a615191a68e32c72b7
Executing commands in '/tmp/B86D6B4A-B996-44B4-9951-B69A77176A90/fruitstrap-lldb-prep-cmds-bf55b2385a615191a68e32c72b72af30
(lldb)     platform select remote-ios --sysroot [redacted] (17A878)/Symbol
  Platform: remote-ios
 Connected: no
[redacted]
p"
(lldb)     script fruitstrap_connect_url="connect://127.0.0.1:54992"
(lldb)     script fruitstrap_output_path=""
(lldb)     script fruitstrap_error_path=""
[redacted]
(lldb)     command script import "/tmp/B86D6B4A-B996-44B4-9951-B69A77176A90/fruitstrap_bf55b2385a615191a68e32c72b72af3024cb
(lldb)     command script add -f fruitstrap_bf55b2385a615191a68e32c72b72af3024cbaea1.connect_command connect
(lldb)     command script add -s asynchronous -f fruitstrap_bf55b2385a615191a68e32c72b72af3024cbaea1.run_command run
(lldb)     command script add -s asynchronous -f fruitstrap_bf55b2385a615191a68e32c72b72af3024cbaea1.autoexit_command autoe
(lldb)     command script add -s asynchronous -f fruitstrap_bf55b2385a615191a68e32c72b72af3024cbaea1.safequit_command safeq
(lldb)     connect
(lldb)     run
success
2020-05-15 21:24:30.578672+0800 [redacted][913:197282] Frida: Listening on 127.0.0.1 TCP port 27042
(lldb)
```

App Successfully deployed & launched

Now, we can use tools like Frida or Objection to connect to this app.



Objection in Action

Conclusion:

Congratulations! You've set up a non-jailbroken iOS pentesting lab. Make sure to follow ethical guidelines and legal considerations during your testing. Happy testing!

Cybersecurity | Penetration Testing | Bug Bounty | Mobile Security | Ios Penetration Testing

Published in InfoSec Write-ups

Follow

75K followers · Last published 1 day ago

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. Subscribe to our weekly newsletter for the coolest infosec updates: https://weekly.infosecwriteups.com/

Written by Abdullah Khawaja

13 followers · 3 following

Responses (2)

See all responses