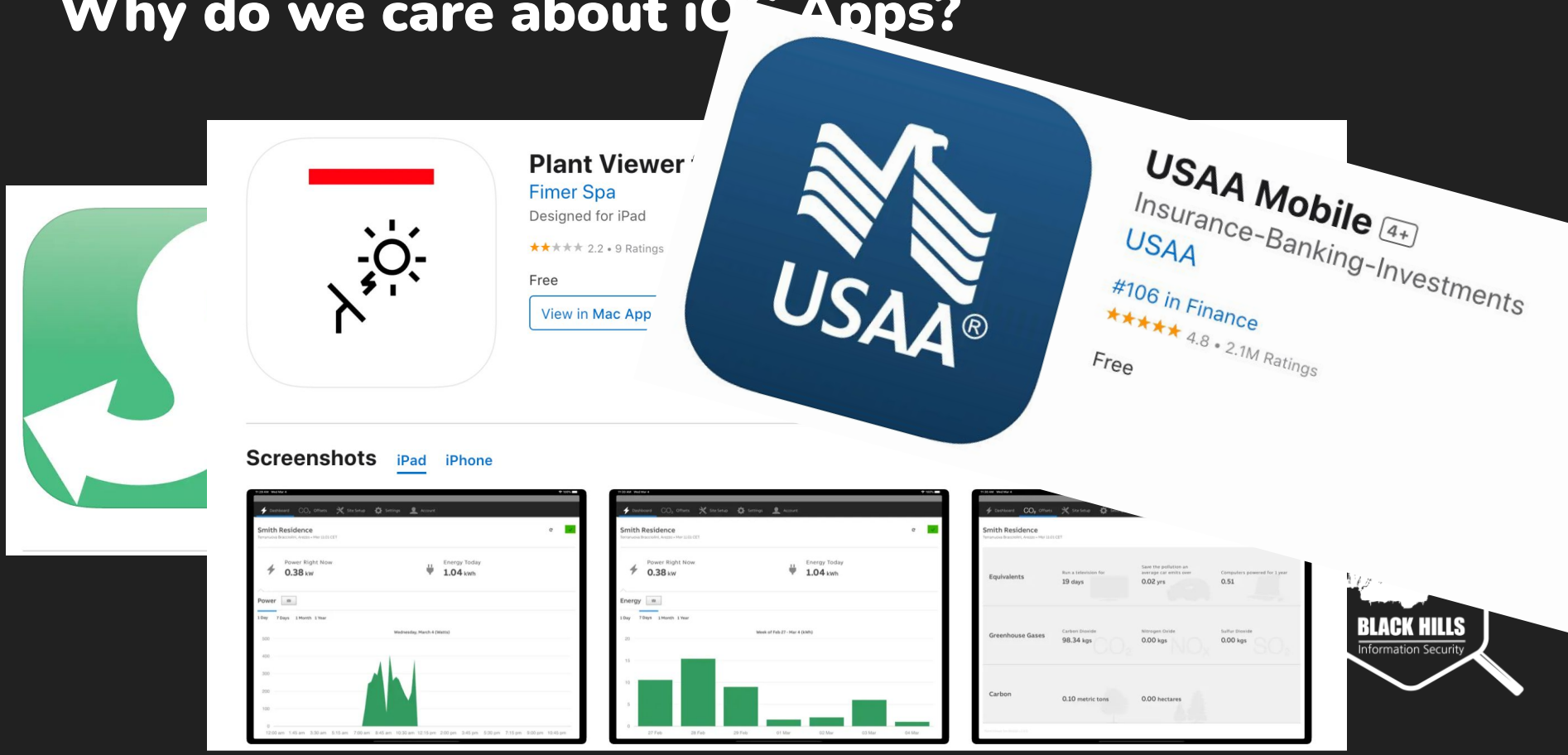
Getting Started in iOS Mobile Application Testing

Cameron & Dave

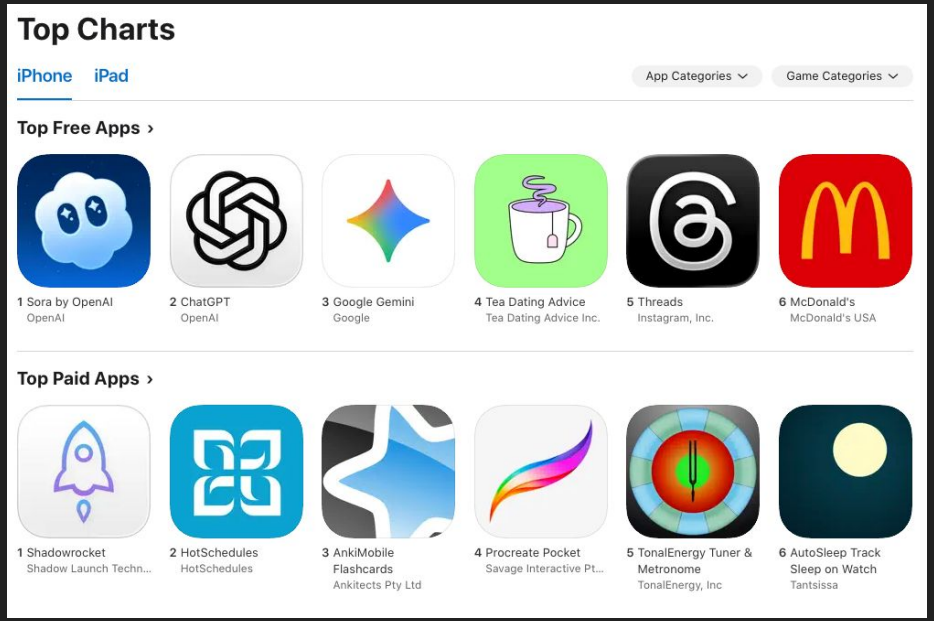
Why do we care about iOS Apps?



IOS Market Share

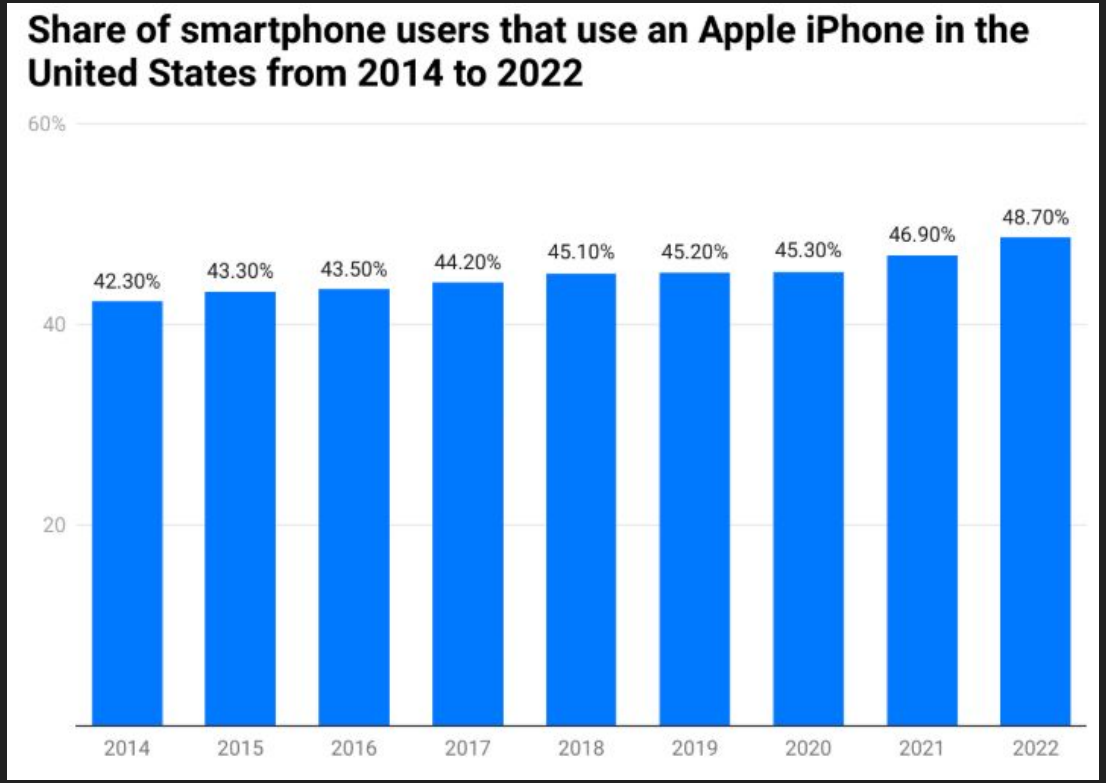
54.76% of North American Smartphone users

27.6% Worldwide



https://www.enterpriseappstoday.com/stats/iphone-usage-statistics.html
https://apps.apple.com/us/charts/iphone

Trending Upwards



statista.com

BLACK HILLS
Information Security

Used by Businesses

According to Computerworld, ¾ of Large US Firms use Apple Devices (2023 Survey)

https://www.computerworld.com/article/1634358/three-quarters-of-large-us-firms-now-using-more-apple-devices-survey.html

What Types of Issues come from iOS

Your Mobile Computer

A small computer that travels with person, connected to internet, emails, calls, messages, banks, carries personal information, etc...

iOS devices have protections (UID, Hardware-backed Keychain, Code Signing and Sandboxing)

When the phone is issued by an employer, access to company resources and internal network

A Quick Look at Bug Bounty Reports

Top Attack Paths -

- Attacker’s app installed on device
- Opening Malicious Page
- Remote Payload
- Hardcoded Secrets and Leakage

Similar order on Payouts - Exceptions:

- MITM
- Client-side Controls Bypass

https://bbre.notion.site/26abfb3c7f4f80e59d7dea9c4de8b06a?v=26abfb3c7f4f8159acc2000cccbdf27f

What Exploits are Being Sought?

Brokers - Buys Exploits and Sells to... Governments

Mobile Exploits in High Demand

Zero Click Full Chains iOS will get ya 5-7 Million

Safari RCE + LPE getcha 2.5-3.5 Million

Sandbox escape worth 500K in Safari

Other iOS Apps as well (Encrypted Messaging Apps...)

When looking at Mobile vs other categories (e.g. Desktop, Enterprise), the payouts are considerably more

https://www.crowdfense.com/exploit-acquisition-program/

Real World Hacks

BLACK HILLS
Information Security

WhatsApp Exploit

In May 2019, a WhatsApp exploit was discovered that allowed malicious actors to remotely install spyware.

The spyware leveraged a bug in the audio call feature of the app to allow the caller to allow the installation of spyware on the device being called, whether the call was answered or not.

ZIP File RCE

NSO’s iMessage Exploit to get RCE through GIFS

The exploit utilized a flaw in Apple's image rendering library (CoreGraphics).

Discovered by Citizen Lab in 2021

Still happening...

CVE-2025-55177 & CVE-2025-43300 - WhatsApp

Seeing a trend... More messaging apps

0-Click Vuln → 2 Issues → Broken logic in validation that message came from approved linked device & memory corruption from DNG file that gives RCE

Exploits as Easy As Making Tea

Unsecured Firebase storage bucket

72,000 images including user profile photos an IDs

A second breach revealed messages, posts, and comments.

Any user could use API key to access other private messages (IDOR)

Resources for Getting Started

BLACK HILLS
Information Security

How is an App Categorized

OWASP MAS Testing Profile is a good place to start

Good to Threat Model the App

MAS-L1 - Essential Security

MAS-L2 - Advanced Security

MAS-R - Resilient Security

Speaking of OWASP

OWASP Mobile Application Security Testing Guide (MASTG)

/h/t Sean Verity - Did a talk on it!
https://www.youtube.com/watch?v=odnip3LL6hc

Great place for beginners to advanced hackers

Covers a lot

Testing Setup

BLACK HILLS
Information Security

Essential Tools

TextMate (or any lightweight text editor) - https://macromates.com/

Burp Suite - https://portswigger.net/burp/communitydownload

Frida - https://frida.re/

Ghidra - https://github.com/NationalSecurityAgency/ghidra

MobSF - https://github.com/MobSF/Mobile-Security-Framework-MobSF

Libimobiledevice - https://github.com/libimobiledevice/libimobiledevice

Jailbreaking

BLACK HILLS
Information Security

Jailbreak Summary

- Run restricted apps, Access/Modify file system, Root access, SSH
- Ability to extract running applications, easily perform runtime analysis with tools such as Frida
- Types: Untethered, Semi-untethered, Semi-tethered, Tethered
- Boot process and chain of trust involved. No time today :(

Jailbreaking Risks

You are willingly downloading unknown code designed to exploit the operating system, which was released online for free.

Be careful out there.

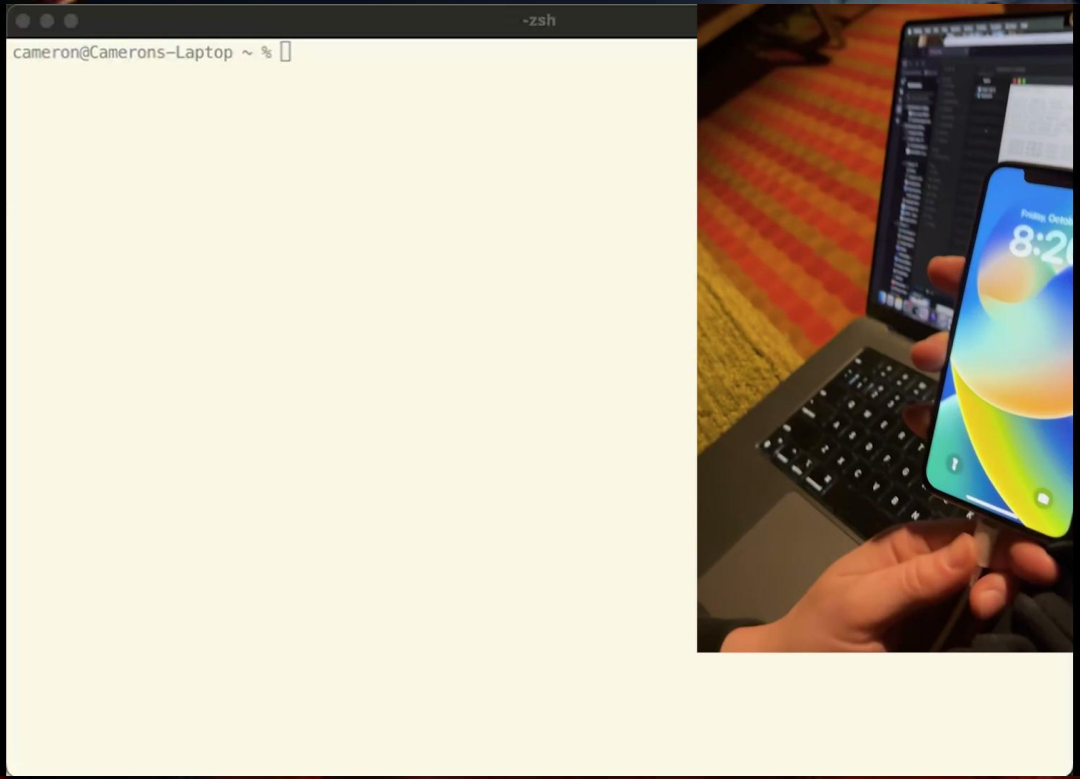
- Malicious Exploits
- Possibility of bricking devices
    - Apple does not need to uphold warranty agreements on Jailbroken devices

Specific Jailbreak Example

CVE-2019-8900 checkm8

BootROM exploit affecting USB DFU stack. iPhone 5s-X. Apple has to support device with updates and can’t patch (Hardware level vuln). So we can use for jailbreaking phones

DEMO



BLACK HILLS
Information Security

Traffic Interception

Intercepting Mobile Traffic

We want traffic to go through an HTTP proxy

Not all applications are proxy aware

Some applications actively try to prevent interception (i.e., cert pinning)

Invisible Proxying for Spooky Season

BLACK HILLS
Information Security

What is an IPA File?

Types of iOS Applications

- Native Apps: Built using the iOS SDK. Implemented in either Objective C or Swift. Performance is good. Platform specific design principles. Close interaction with the operating system and can interact with all peripherals.
- Hybrid Apps: Execute like a native app but rely on WebViews (embedded browser) for much of the functionality.
- Progressive Web Apps (PWAs): PWAs are designed to be run in the browser. Just like a web app. Far easier to build and distribute cross platform. Cannot use system resources the way a Native app can.

Property List Files

Plist file

Main Info.plist gives a lot of information about the app

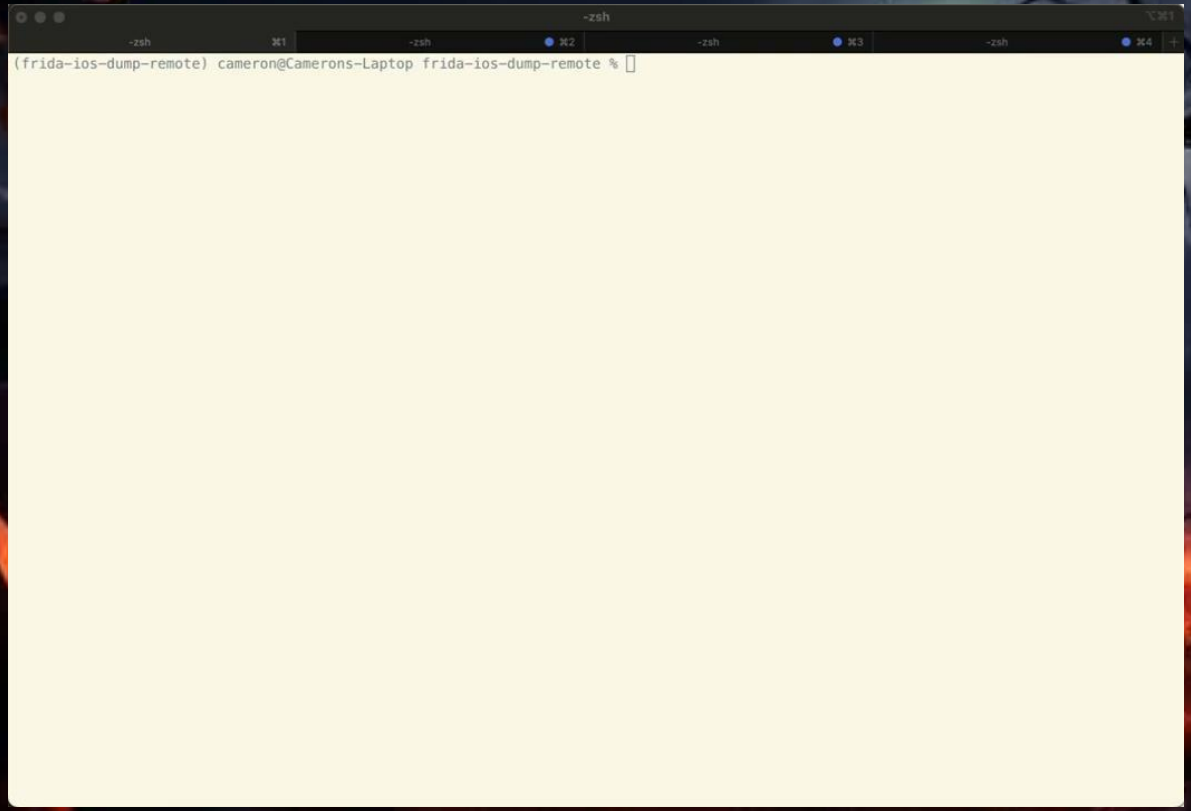
Permissions, background modes, URL schemes, App Transport Security (ATS) settings, how it launches

Review all of them

Extracting an IPA file from Device

- Info.plist - contains configuration information for the application, such as its bundle ID, version number, and display name.
- _CodeSignature/ contains a plist file with a signature over all files in the bundle.
- Frameworks/ contains the app native libraries as .dylib or .framework files.
- PlugIns/ may contain app extensions as .appex files (not present in the example).

Demo



BLACK HILLS
Information Security

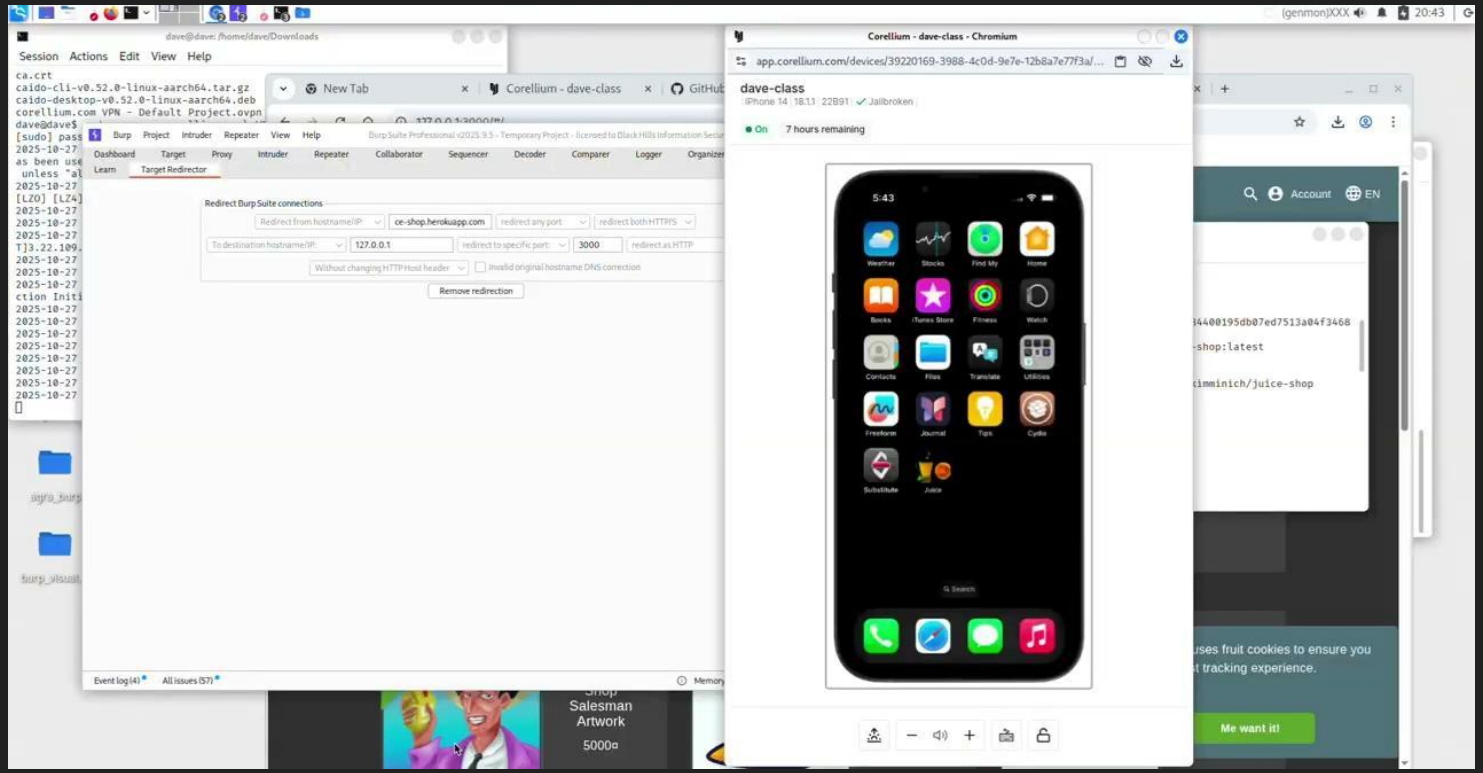
Common API Vulnerabilities

Authentication and Authorization should be implemented following the same best practices as Web Applications.

This is often not the case...

Other common vulnerabilities include typical API exploits such as Information Disclosure, IDOR, and various methods of injection.

API Exploitation



Want to learn more?

Practical iOS Application Security Testing with Cameron Cartier and Dave Blandford

Course Authored by Cameron Cartier and David Blandford.

This course will focus on testing iOS applications. We will give students hands-on experience with both static and dynamic analysis of multiple applications.

Course Length: 16 Hours

Includes a Certificate of Completion

https://www.antisyphontraining.com/product/practical-ios-application-security-testing-with-cameron-cartier-and-dave-blandford/

Questions?