

Course Syllabus

Intro to Mobile AppSec/Penetration Testing with Corellium

This, highly interactive and engaging, course is designed to give an overview of using the Corellium platform to perform mobile app penetration testing. Students will get first-hand knowledge of tools, tactics and techniques used to discover app vulnerabilities. Students will also get a crash-course in the OWASP Mobile App Verification Standard (MSAVS) V1-V8 test cases and experience live demonstrations of the Corellium platform to perform MASVS. Students are highly encouraged to engage with our expert app pen test instructors to ask questions, give feedback and make sure they get the most from the class.

What is Corellium?

Quick overview of the Corellium platform and what it offers

Using the Corellium Platform

Replace your existing physical device(s) with virtual

- **Creating a virtual device**
 - Selecting device type (iPhone, Android, IoT, etc.)
 - Selecting model (e.g., iPhone 13 Pro)
 - Selecting OS version
 - Selecting jailbroken or stock
- **Using the virtual display**
- **Using the console**
- **Corellium device settings**
- **File and Apps review**
- **Network Monitor**

Interacting with the device

- **Connecting to the SSH tunnel or VPN (cloud only)**
- **USBFlux**
- **SSH into the device**
- **Snapshots – taking/restoring/deleting**

Application Signing and Installing

- **iOS Signing and Troubleshooting Errors**
 - Third-party tools
- **Android Signing**
- **Installing applications (IPAs and APKs)**

Certificate Pinning/Certificate Validation

How to test applications with these implementations

Break #1 (15-30 minutes depending on class)



Timing

This course is designed to fit into a half-day session (3-4 hours depending on breaks/engagement).



Target Audience

Mobile AppSec/DevOps personnel, app pen testers, service provider/system integrator engineers, reverse engineers, security and/or malware researchers and forensics experts interested in mobile appsec on iOS and Android.

Mobile AppSec Verification Standard

- Mobile Security Standards
- Mobile Security Testing Guide
- Mobile Security Testing Checklist
- Google App Defencse Alliance

MASVS V1-V8 Overview

- Test Cases and Examples

Break #2 (15-30 minutes depending on class)

Mobile Penetration Testing with Corellium

- Using DVIA iOS application to solve some common vulnerabilities
 - Detailed descriptions and demos
- Android Uncrackable application to solve common vulnerabilities
 - Detailed descriptions and demos
- Android OWASP “Crack me if you can” vulnerable application
 - Detailed descriptions and demos

Pentesting with Corellium Overview

Closing/final questions – next steps

