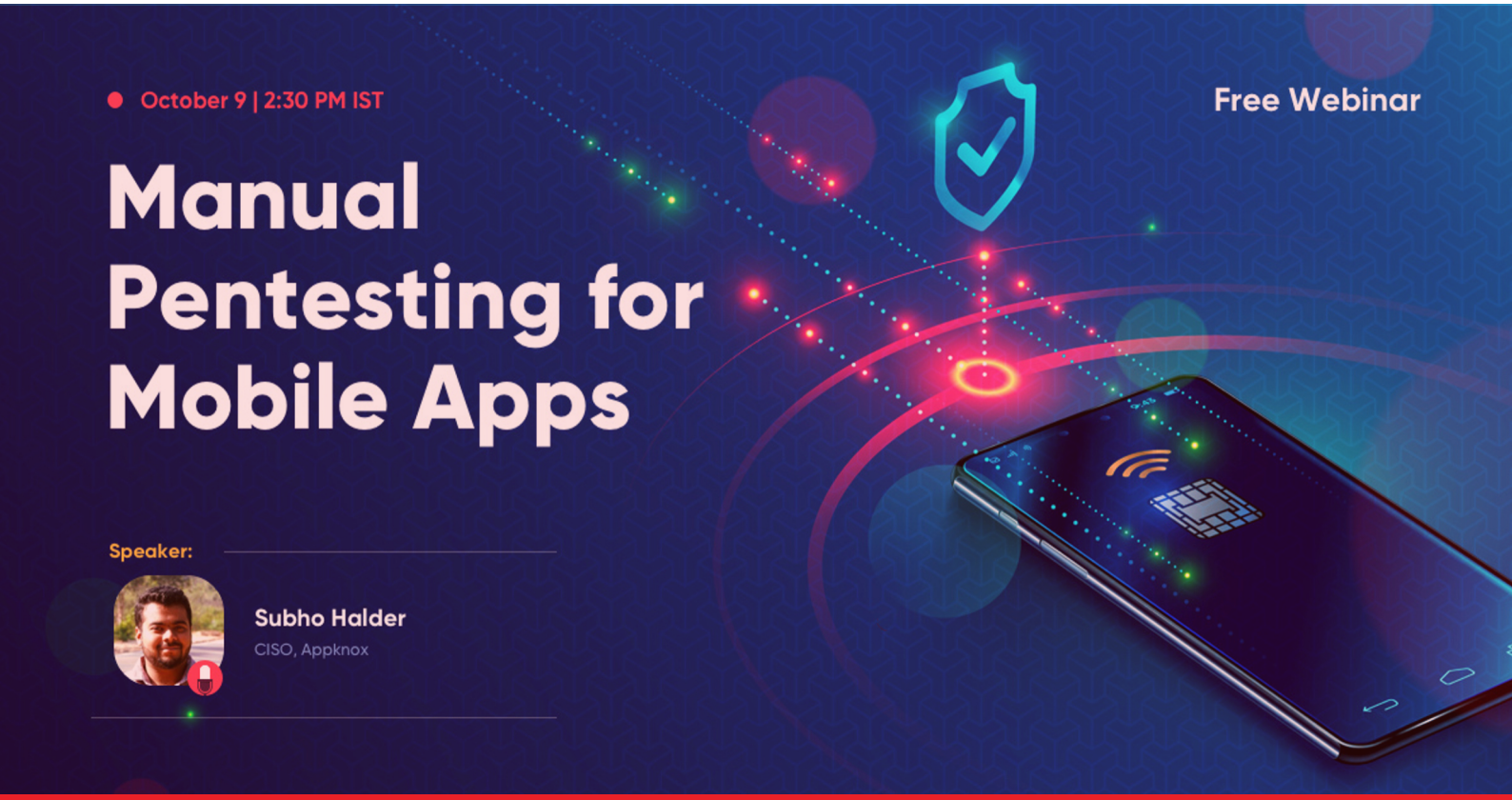
appknox

OCTOBER 2019

HOW TO PERFORM MANUAL PENTEST ON MOBILE APPLICATIONS

Webinar Q & A

Thank You For Joining Our Webinar!



We had a fantastic experience running the webinar on Manual Pentesting on October 9, 2019. Thank you for being there. We've put together all the questions asked during the webinar into a consolidated document that could serve as a good reference for you.

Thanks once again for joining us. We look forward to hosting you on our next webinar soon

You can watch the replay of webinar here

1. How many of them are open-source tools?

Find the below classifications of the tools I showcased

- Apktool - Opensourced https://github.com/iBotPeaches/Apktool
- JADx - Opensourced https://github.com/skylot/jadx
- PassionFruit - Opensourced https://github.com/chaitin/passionfruit
- Burpsuite - Free/Commercial https://portswigger.net
- Drozer - Opensourced https://github.com/FSecureLABS/drozer
- GHIDRA - Opensourced https://github.com/NationalSecurityAgency/ghidra
- Frida - Opensourced https://github.com/fridadn
- SPY - Opensourced https://github.com/0xd4d/dnSpy
- ILSPY - Opensourced https://github.com/icsharpcode/ILSpy
- Xposed - Opensourced https://github.com/rovo89

2. How those tools “you use” are related to the Appknox platform? At what stage of the process do you use them, when we order manual assessment from you?

These are some of the open-sourced tools we use along with our own custom assessment scripts and tools which we have built inhouse

3. Is windows 10 laptop enough for all kinds of android app pentest ? or do we need mac?

For android pentesting, windows laptop is enough, you can also use VMware to run Linux for some of the open-sourced tools which only work in Linux, but apart from that, Windows laptop is enough for Android Pentesting. For iOS pentesting, it is recommended to use Mac OSX.

4. Is this Android device that you are using rooted or is it an unaltered device?

The android device which I'm using is a custom build of LineageOS ROM in a Nexus 6 device. This device is apt for Android Pentesting, but it shouldn't be used for production

5. All these tools will only work with JAVA or Kotlin also?

This question was asked when I was showing the Android Pentesting, all the tools I showcased will work with both since it operates over APK/DEX files. Kotlin internally compiles itself into Java/DEX file. This is however not the case with Xamarin Based application, which would require to analyze the DLL files also. In the case of a hybrid application, you can use any HTML/JS-based security scanner to work.

6. Will these tools work in Kali Linux?

Most of the tools I showed will work in Kali Linux, except for dnSPY which requires a Windows machine. You can probably use WINE to make it work, but I have not tested it out yet.

7. Can passionfruit work on devices without jailbreak?

Yes, PassionFruit can work without jailbreak as well. You can check the documentation which talks about how it works - https://github.com/chaitin/passionfruit#non-jailbroken-device

8. Passionfruit looks like MobSF also?

PassionFruit only works on iOS and not for Android. MobSF is a tool mainly for malware analysis but is not built for vulnerability assessments. MobSF can be used for Application Analysis, but not Vulnerability Assessment as it misses out a lot of issues.

9. Can we extract passwords from the keychain password management system?

Yes we can, that is what a Keychain mainly stores.

10. What tools are recommended to test APIs that are discovered from static analysis of mobile applications?

You can use BurpSuite/ZAP(Zed Attack Proxy) to perform scans on the URLs discovered via static analysis on the mobile application.

11. Share any info on the WIB sim card browser attack which is in news recently. It is hard to dig out info on the web apart from news articles. Also, I would like to know how his approach/resources to learn about new vulnerabilities that come out?

WIB attack is similar to the Simjacking attack. This is not related to mobile application security but related to Platform security. There is a problem with both SIM cards and how Android & iOS communicates with the SIM card in the phone. In short, Simjacking/WIB attack is related to when a flash OTA message is sent with certain encoding, it queries the SIM toolkit service which in turn somehow sends an unauthorized SMS from the victim's phone to another number.

New vulnerabilities and such issues are shared in IRC channels and other groups. CERT-IN also has pieces of information about these new threats/vulnerabilities which are coming.