FACULTY OF EGINEERING & TECHNOLOGY
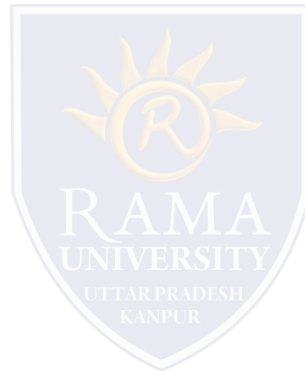
MOBILE SECURITY

LECTURE -28

Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

- **Top Mobile App Security Testing Tools**

- **MCQ**

- **References**

Top Mobile App Security Testing Tools

Enlisted below are the most popular Mobile App Security Testing tools that are used worldwide.

❑ImmuniWeb® MobileSuite

❑ Zed Attack Proxy

❑Kiuwan

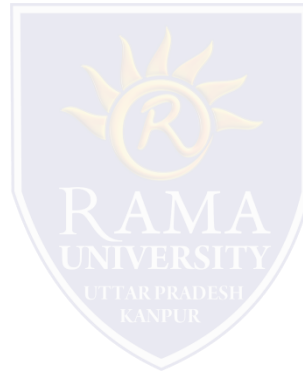❑QARK

❑Micro Focus

❑Android Debug Bridge

❑CodifiedSecurity

❑Drozer

❑WhiteHat Security

❑Synopsys

❑Veracode

❑Mobile Security Framework (MobSF)

❑ImmuniWeb® MobileSuite

Key Features:

❑Mobile app and backend testing.

❑Zero false-positive SLA.

❑PCI DSS and GDPR compliances.

❑CVE, CWE and CVSSv3 scores.

❑Actionable remediation guidelines.

❑SDLC and CI/CD tools integration.

❑One-click virtual patching via WAF.

❑24/7 Access to security analysts.

❑Zed Attack Proxy

Key Features:

❑World's most popular open-source security testing tool.

❑ZAP is actively maintained by hundreds of international volunteers.

❑It is very easy to install.

❑ZAP is available in 20 different languages.

❑It is an international community-based tool which provides support and includes active development by international volunteers.

❑It is also a great tool for manual security testing.

TOP MOBILE APP SECURITY TESTING TOOLS

❑ Kiuwan

Key Features:

❑ Kiuwan provides a 360⁰ approach to mobile app security testing, with the largest technology coverage.

❑ Kiuwan security testing includes static code analysis and software composition analysis, with automation at any stage of the SDLC. Coverage of the main languages and popular frameworks for mobile development, with integration at IDE level.

❑ QARK

Key Features:

❑ QARK is an open-source tool.

❑ It provides in-depth information about security vulnerabilities.

❑ QARK will generate a report about potential vulnerability and provide information about what to do in order to fix them.

❑ It highlights the issue related to the Android version.

❑ QARK scans all the components in the mobile app for misconfiguration and security threats.

❑ It creates a custom application for testing purposes in the form of APK and identifies the potential issues.

TOP MOBILE APP SECURITY TESTING TOOLS

❏Micro Focus

Key Features:

❏Fortify performs comprehensive mobile security testing using a flexible delivery model.

❏Security Testing includes static code analysis and scheduled scan for mobile apps and provides the accurate result.

❏Identify security vulnerabilities across – client, server, and network.

❏Fortify allows standard scan which helps to identify malware.

❏Fortify supports multiple platforms such as Google Android, Apple iOS, Microsoft Windows and Blackberry.

❏Android Debug Bridge

Key Features:

❏ADB can be integrated with Google's Android Studio IDE.

❏Real-time monitoring of system events.

❏It allows operating at the system level using shell commands.

❏ADB communicates with devices using USB, WI-FI, Bluetooth etc.

❏ADB is included in the Android SDK package itself.

❑CodifiedSecurity

CodifiedSecurity

Key Features:

❑It is an automated testing platform that detects security loopholes in the mobile app code.

❑Codified Security provides real-time feedback.

❑It is supported by machine learning and static code analysis.

❑It supports both Static and Dynamic testing in mobile app security testing.

❑Code-level reporting helps to get the issues in the mobile app's client-side code.

❑Codified Security supports iOS, Android platform, etc.

❑It tests a mobile app without actually fetching the source code. The data and source code is hosted on the Google cloud.

❑Files can be uploaded in multiple formats such as APK, IPA, etc.

TOP MOBILE APP SECURITY TESTING TOOLS

❑Drozer

Key Features:

❑Drozer is an open-source tool.

❑Drozer supports both actual android devices and emulators for security testing.

❑It only supports the Android platform.

❑Executes Java-enabled code on the device itself.

❑It provides solutions in all areas of cyber security.

❑Drozer support can be extended to find and exploit hidden weaknesses.

❑It discovers and interacts with the threat area in an android app.

❑WhiteHat Security

Key Features:

❑It is a cloud-b

❑It supports both Android and iOS platforms.

❑Sentinel platform provides detailed information and reporting to get the status of the project.

❑Automated static and dynamic mobile app testing, it is able to detect loophole faster than any other tool or platform.

❑Testing is performed on the actual device by installing the mobile app, it does not use any emulators for testing.

❑It gives a clear and concise description of security vulnerabilities and provides a solution.

❑Sentinel can be integrated with CI servers, bug tracking tools, and ALM tools.

TOP MOBILE APP SECURITY TESTING TOOLS

❏**Synopsys**

❏ **Veracode**

Key Features:

❏Combine multiple tools to get the most comprehensive solution for mobile app security testing.

❏Focuses on delivering the security defect-free software into the production environment.

❏Synopsys helps to improve quality and reduces costs.

❏Eliminates security vulnerabilities from the server-side applications and from APIs.

❏It tests vulnerabilities using embedded software.

❏Static and Dynamic analysis tools are used during mobile app security testing.

Key Features:

❏It is easy to use and provides accurate security testing results.

❏Security tests are performed based on the application. Finance and healthcare applications are tested in-depth while the simple web application is tested with a simple scan.

❏In-depth testing is performed using complete coverage of mobile app use cases.

❏Veracode Static Analysis provides a fast and accurate code review result.

❏Under a single platform, it provides multiple security analysis which includes static, dynamic and mobile app behavioral analysis.

❑ Mobile Security Framework (MobSF)

Key Features:

❑ It is an open-source tool for mobile app security testing.

❑ Mobile app testing environment can be easily set-up using MobSF.

❑ MobSF is hosted in a local environment, so sensitive data never interacts with the cloud.

❑ Faster security analysis for mobile apps on all three platforms (Android, iOS, Windows).

❑ MobSF supports both binary and Zipped source code.

❑ It supports Web API security testing using API Fuzzer.

❑ Developers can identify security vulnerabilities during the development phase.

MCQ

Q 1 - How to get a response from an activity in Android?

A - startActivityToResult()

B - startActiivtyForResult()

C - Bundle()

D - None of the above

Q 2 -How to move services to foreground in android?

A - Services always work in Foreground only

B - No,We can't do this query

C - Using startService(Intent intent)

D - startFordgroud(int id, Notification notification).

Q 3 -What are the functionalities of Binder services in android?

A - Binder is responsible to manage the thread while using aidl

in android

B - Binder is responsible for marshalling and un-marshalling of

the data

C - A & B

D - Binder is a kind of interface

E - None of the above

Q 4 - What is the use of content provider in android?

A - To send the data from an application to another

application

B - To store the data in a database

C - To share the data between applications
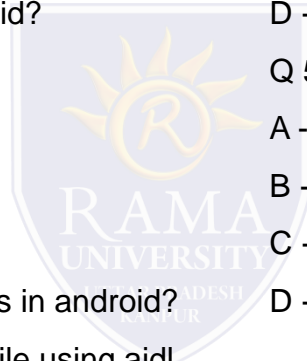
D - None of the above.

Q 5 -What is the 9 patch tool in android?

A - Using with tool, we can redraw images in 9 sections.

B - image extension tool

C - image editable tool

D - Device features

REFERENCES

❑https://www.peerbits.com/blog/security-issues-in-developing-mobile-app.html

❑https://www.softwaretestinghelp.com/mobile-app-security-testing-tools/