Mobile application security testing: MobSF

19-April-2024

1RIVET

Pivotal Insights | Focused Solutions

AGENDA

01 Introduction to Mobile application security testing

02 SAST vs DAST

03 Introduction to MobSF

04 Static analysis in MobSF

01

Introduction to Mobile application security testing

Introduction to Mobile app Security Testing

Mobile application security testing involves testing a mobile app in ways that a malicious user would try to attack it. Effective security testing begins with an understanding of the application's business purpose and the types of data it handles.

The testing process includes:

- Interacting with the application and understanding how it stores, receives, and transmits data.
- Decrypting encrypted parts of the application.
- Decompiling the application and analyzing the resulting code.
- Using static analysis to pinpoint security weaknesses in the decompiled code.
- Utilizing dynamic analysis and penetration testing to evaluate the effectiveness of security controls (e.g., authentication and authorization controls) that are used within the application.

Mobile application security testing can be thought of as a pre-production check to ensure that security controls in an application work as expected, while safeguarding against implementation errors.

02

SAST vs DAST

SAST vs DAST

Static application security testing analyzes program source code to identify security vulnerabilities. These vulnerabilities include SQL injection, buffer overflows, XML external entity (XXE) attacks, and other OWASP Top 10 security risks.

The SAST methodology guides developers to begin testing their application at early development stages without executing a functional component. This approach discovers application source code security flaws early and avoids leaving security issues to later development phases. This decreases development time and enhances overall program security.

Dynamic application security testing scans software applications in real-time against leading vulnerability sources, like the OWASP Top 10 or SANS/CWE 25, to find security flaws or open vulnerabilities.

DAST is a form of closed box testing, which stimulates an outside attacker's perspective. It assumes the tester does not know the application's inner functions. It can detect security vulnerabilities that SAST cannot, such as those that appear only during the program runtime.

03

Introduction to MobSF

Introduction to MobSF

Mobile Security Framework (MobSF) is a security research platform for mobile applications in Android, iOS and Windows Mobile. MobSF can be used for a variety of use cases such as mobile application security, penetration testing, malware analysis, and privacy analysis.

The Static Analyzer supports popular mobile app binaries like APK, IPA, APPX and source code.

Source: https://github.com/MobSF

Static Analysis:

Static analysis is a process of analyzing the code of the mobile application without actually executing it. MobSF uses various techniques to perform static analysis of the mobile application, including reverse engineering the application, decompiling the APK, and analyzing the code for vulnerabilities.

Dynamic Analysis:

Dynamic analysis is a process of analyzing the behavior of the mobile application while it is running. MobSF uses various techniques to perform dynamic analysis of the mobile application, including running the application in a simulated environment and analyzing the network traffic generated by the application.

04

Static analysis in MobSF

Static analysis in MobSF

Get MobSF up and running:

```
# Setup
$ git clone https://github.com/MobSF/Mobile-Security-Framework-MobSF.git
$ cd Mobile-Security-Framework-MobSF

# Installation process
$ ./setup.sh # For Linux and Mac setup
$ .bat # For Windows

# Run/Execute
$ ./run.sh # For Linux and Mac
$ run.bat # For Windows
```

Once you have MobSF up and running you can open it in your browser by navigating to http://127.0.0.1:8000.

To perform static analysis of an Android or iOS application, you need to upload the application to MobSF. Once the application is uploaded, MobSF will perform static analysis and generate a report that will show the vulnerabilities found in the application.