

Importance of VAPT On Android Application

Subarna Panda¹, Shreyas²

¹ Assistant professor – Department of CS & IT, Jain University, Jayanagar 9th block, Bengaluru, Karnataka, India

² Student, MCA – ISMS, Department of CS & IT, Jain University, Jayanagar 9th block, Bengaluru, Karnataka, India

Abstract - The rapid advancement in the usage of applications and Internet has brought with its challenges of data security and confidentiality. Organizations are investing in Security and Vulnerability Management (SVM) solutions to bring in more intelligence, process consistency, and security awareness to make their applications highly secure and protected against external threats.

Every organization is coming up with their own application to easily manage their clients and processes. Today, there are applications for every operation. These applications can be either web application or mobile application. These applications have made tasks easy. So, the usage of applications is rapidly increasing. Though it makes the work easy, on the other side it is putting user's confidential data at risk. To secure user's data from the access by attacker, trusted and secure applications need to be used.

Security of the application can be improved by performing the VAPT (Vulnerability Assessment and Penetration Testing) of the application. VAPT helps to find out the hidden vulnerabilities inside the application.

Key Words: Vulnerability, Penetration, Testing, Assessment, Security.

1. INTRODUCTION

VAPT is a process in which the Information & Communication Technologies (ICT) infrastructure consists of computers, networks, servers, operating systems and application software are scanned in order to identify the presence of known and unknown vulnerabilities.

Security of the application can be improved by performing the VAPT (Vulnerability Assessment and Penetration Testing) of the application. VAPT helps to find out the hidden vulnerabilities inside the application.

Vulnerability Assessment is the process of systematically scanning an organization's servers, workstations, devices, operating systems, and applications to detect and identify vulnerabilities. Identified vulnerabilities could include missing patches, gaps or loopholes in system design, misconfigurations etc.

Penetration Testing is the process of launching real world attacks on IT infrastructure and applications to help identify the extent of exposures without causing any harm to existing data and systems. Penetration Testing helps detect possible threats by conducting mock attacks within the enterprise IT

framework and helps IT managers identify threats before actual occurrence.

1.1 Android Penetration Testing

Android Penetration Testing is a process of testing and finding out the security issues in an android application. This involves de-compiling, real-time analysis and testing the android application from the security perspective of the application. This involves testing the security issues like - insecure logging, leaking content providers, insecure data storage and access control issues etc.

2. OBJECTIVE

The objective of this Paper is to increase the security of android application by performing Vulnerability Assessment and Penetration Testing (VAPT) of the android application.

VAPT play a very important role in increasing the security of the application. VAPT is always overlooked but it is as important as development and marketing of application. VAPT will help to identify the flaws in the application. Vulnerability Assessment will help to identify the gaps in the application. By this tester can get to know the existence of well-known and some hidden vulnerabilities in the application which can be used by attacker to launch attack.

Penetration testing will help to find out the level of security in the application. In this, the Pen-tester will try to penetrate the application using the vulnerabilities. This attack is launched by the pen-tester with the prior permission from the authority to find out the security level of the application. This will help company to find out how well their application can withstand in the un-secured market. So, it is very important to perform VAPT for application before they are launched to the market.

So, performing VAPT is very important for any application to increase the level of security.

3. SYSTEM ANALYSIS

Vulnerability Assessment and Penetration Testing (VAPT) is the process of testing the security of the application, network, system etc. VAPT is performed with the prior permission from the authority. VAPT is a systematic approach to find out the vulnerability/Vulnerabilities present in the given target. The target can be web application, mobile application, system, server, or network.

The VAPT is performed by the Penetration tester or also called as Security Assessor. This test is performed with the intense care to not to break any agreements signed during the engagement of Security Assessment. Performing VAPT requires relevant knowledge in the field of security.

VAPT is performed with the help of different security testing tools. The test is performed with more than one tool to check for different vulnerabilities and to check the correctness. It is important to check with different tools to check the correctness of the results.

The findings are documented in a standard document structure. The document is re-checked for the correctness of the details mentioned in the document. Document consists of 3 main parts, they are – Executive summary, Vulnerabilities report, & Annexure – A report.

This report is submitted to the authority of the target.

3.1 TOP Mobile application Threats:

1. Insecure Data Storage
2. Client Side Injection
3. Weak Server-Side Controls
4. Insufficient Transport Layer Protection
5. Poor Authorization and Authentication
6. Improper Session Handling
7. Security Decisions via Untrusted Inputs
8. Broken Cryptography
9. Side Channel Data Leakage
10. Sensitive Information Disclosur

4. USEFUL TOOLS

Security Assessment of android application requires lots of tools. Below are some of the important tools used while performing Security Assessment of android application:

- 1. ADB (Android Debug Bridge)** – ADB is a command-line tool that is used to communicate with the device.
- 2. DB Browser for SQLite** – This tool is used to view the database file extracted through ADB.
- 3. Apktool** – This tool is used to reverse engineer the android application. This tool decodes to its almost original form.
- 4. Dex2jar** – This tool is used to convert the .dex file to .jar file to view the source code of the application

5. Drozer – This tool provides huge collection of public exploits for testing the security of the application.

6. MobSF – This tool is a powerful framework for performing static analysis, dynamic analysis of android application.

7. Logcat – This tool dumps the all the system logs.

5. PENETRATION TESTING PHASES



Fig-1: Penetration testing phases

1. Gathering information – This is the first stage in Penetration testing where the basic information and functionalities of the application is gathered.

2. Analysis and Planning – This is the second stage in penetration testing. In this stage the planning is made to carry out the test. This involves deciding the flow of execution.

3. Vulnerability Discovery – In this stage vulnerabilities are discovered either using tool or manually. This stage finds out the vulnerabilities present in the application.

4. Exploitation - In this stage the actual attack is done on the application. In this stage the attack is performed to find out level of severity of the vulnerabilities.

5. Risk Analysis and Recommendation – In this stage the analysis of risk is performed to find out the impact. This stage lists all the vulnerabilities, their severity and appropriate suggestions to mitigate them.

6. Reporting – This is the post stage of testing the application. In this stage a detailed report is prepared on the findings and submitted to the person concerned.

6. CONCLUSION

The Vulnerability Assessment and Penetration Testing (VAPT) is a security testing technique in which the tester tries to find out the vulnerabilities present in the application. VAPT is performed by the penetration tester. Penetration testers are ethical by role. They perform VAPT to check the level of security of the application.

Usage of android application is increasing exponentially. Android apps are being developed and used to carry out every operation. VAPT on android applications will help to find out the vulnerabilities present in the application. By knowing the vulnerabilities, the developer can patch those vulnerabilities.

VAPT on android is as important as marketing of the application. VAPT should be a part of development life cycle. VAPT should be regularly performed before and after the release of the application. Regular testing of application will make the application more secure. So, VAPT on android application plays an important role in securing the application.

REFERENCES

- [1] MobileIron, ' Mobile Security: Threats and Countermeasures', official website
- [2] Android team, ' Android Security White Paper', official website
- [3] Symantec, ' Mobile Security and Management – meeting the enterprise mobility challenge', official website
- [4] Okolie C.C, Oladeji F.A, Benjamin B.C, Alakiri H.A, Olisa O, ' Penetration Testing for Android smartphones', published by students of university of Lagos
- [5] Oburst, ' Mobile Application Security - Best Practices to Optimize Security', official website