CYBERSRC®
CONSULTANCY
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

MOBILE APPLICATION SECURITY TESTING SERVICES

MOBILE APPLICATION SECURITY TESTING SERVICES

OVERVIEW

Security testing of Mobile application focuses on the software security built on different platforms like Android, iOS, and Windows Phone. It includes analysing and assessing applications for security related issues with respect to the platforms they are built on and developed with, the designated set of different users. These days, mobile applications are the crucial part of any organization or business's presence in the online world.

In the research, it has also been found that users are dependent and rely more on mobile applications rather than using desktop applications. With such growth and users having access to mobile applications, it is evident that there is large amount of user data, much of which is sensitive data and must be protected from unauthorized access.

COMMON ISSUES THAT AFFECT MOBILE APPLICATIONS INCLUDE

1. **Storing or unintentionally leaking sensitive data in ways that it could be read by other applications on the user's phone.**
2. **Implementing poor authentication and authorization checks that could be bypassed by malicious applications or users.**
3. **Using data encryption methods that are known to be vulnerable or can be easily broken.**
4. **Transmitting sensitive data without encryption over the Internet.**

CHALLENGES IN MOBILE APPLICATION SECURITY TESTING

1

PLATFORM, OS AND DEVICE FRAGMENTATION

Mobile application testing needs to cover a multiplicity of mobile devices with different capabilities, features, and limitations. Identification of security vulnerabilities specific to devices makes performance testing a difficult task. There are different versions of each Operating System (OS) which have a different set of vulnerabilities. Testing of the app on each version is time-consuming and requires the application tester to be aware of the loopholes.

2

MOBILE DEVICE'S PHYSICAL CHARACTERISTICS

There are three approaches to mobile app architecture: native, Web/HTML5 and hybrid apps. Test case scenarios differ for each, especially for stress, performance, conformance and compatibility testing. While Native apps have a reduced testing scope, Web and hybrid apps need both on-/off-platform test cases, thereby leading to back-end issues. While Web-only apps need to be tested more rigorously for the choice of browser versions, Native and hybrid apps must be tested for successful download, execution, platform interaction, and updates.

3

DIFFERENT MOBILE AUTOMATION TESTING TOOLS

Fragmentation requires considerable knowledge about the use of automation testing. Since cross-platform minds were not used for designing traditional testing tools like QuickTest Professional (QTP) or Selenium, hence different automation tools are used for mobile apps and web applications altogether. Even after the emergence of a number of test automation and testing tools for Android and iOS, the availability of full-fledged standard tools for security testing is still scarce.

4

PERFORMANCE & SECURITY

With so much of personal data being stored and shared across apps and devices, it has become imperative that performance and security testing of apps on a public cloud is given a very serious consideration, and all possible tests conducted to ensure the data privacy.

OUR DETAILED APPROACH

There are 3 approaches to security testing:

GREY-BOX TESTING

This one is the most common approach in security testing. With it, some information (like the credentials) is provided, but the rest is to be discovered by the tester.

BLACK-BOX TESTING

With this approach, the tester has no prior knowledge of the app, which allows them to behave like a user (or hacker) and exploit the publicly available info.

WHITE BOX TESTING

This method implies that the tester knows the app’s ins and outs and has access to the source code and various documentation. White-box testing allows for faster testing and more sophisticated test cases.

VULNERABILITY ANALYSIS

This self-explanatory procedure is usually automated and done with various scanners, although it can also be done manually. There are two approaches to vulnerability analysis

STATIC ANALYSIS

Static analysis is the process of analyzing an application without actual executing the application. Static analysis will review code of an application to find known or suspicious function calls or permissions that deem malicious.

DYNAMIC ANALYSIS

It is the process of analyzing an application while executing the app in a controlled environment. Dynamic analysis will monitor network traffic and other communications to catch malicious activity. With a powerful dynamic analyzer, applications that attempt to connect out to unknown or malicious sites, or send SMS messages without authorization will be flagged as malicious and consequently be reported as threats.

SOME OF THE TOOLS USED

- Frida
- Dex2jar
- Drozer
- Mobsf
- Objection
- Apktool
- Burpsuite

KEY AREAS COVERED IN MOBILE APPLICATION SECURITY

1 Code Quality

While mobile apps are less susceptible to traditional injection attacks and memory management issues, you can’t afford to produce sloppy code. This is a perfect opportunity to introduce the security as code culture to your team and implement the DevSecOps methodology.

2 Interaction with Platform

Platform-specific features like app permission systems that control access to APIs or inter-process communication (IPC) facilities, which let apps exchange data, have underlying potential problems.

3 Local Data Storage

Taking extra care with data storage means better protection to the users’ sensitive data. Misuse of the local storage or IPC, it might expose sensitive data to other apps on the device and unintentionally leak data to backups, keyboard cache, or cloud storage.

CASE STUDIES

Background

- Client is one of the leading E sign service provider company
- The client has been in the industry for over 10 years with a global presence including India, California and New Jersey
- Mobile application VAPT was crucial to prevent any monetary loss and any reputational loss

Objectives

- Assessment of both android as well as iOS Mobile Application
- Identify the vulnerabilities like XSS, SQLi, etc. during the dynamic analysis
- Identification of the any API keys, hard coded credentials logs revealing critical information etc. during static analysis.

Challenges

- The client did not have any expertise for security testing of mobile application
- The client lacked required knowledge of tools used for security testing of both android and iOS application

Our Role

- Performing static and dynamic analysis of the application using various tools
- Retesting of Application and Network
- VAPT reporting and legal advisory
- Expert recommendations and guidance to cover up gaps and improve information security posture

Result/ Benefits

- Successful security testing of both Android and iOS Application
- Detailed report of VAPT and recommendation with preventive measure
- Consultancy on action items required to cover up identified gaps

Industry Sector

E-Sign Service Provider

Service Utilized

Android Application VAPT

iOS Application VAPT

Business Areas Addressed

IT
&
Technology

HOW CAN CYBERSRC® HELP?

Our mobile security assessments take various attack vectors and threats into consideration, which includes Jailbroken iOS and rooted Android devices. By comparing the vulnerabilities of both options, we can demonstrate the security risk from multiple user types, including dedicated attackers and everyday use.

ABOUT US

CyberSRC® forays into domains of Cyber Security, Data Privacy, Assurance and Governance. Our aim is to assist enterprises, MSMEs, SMEs & others enhance their capabilities for cybersecurity defence, minimise enterprise security and assurance risks, manage security operations and achieve regulatory compliance. Our team consists of several consultants and advisors. We have collaborated with multi-partners in order to provide support for end-to-end security solutions and implementation support.

WHY CYBERSRC®?

We are team of qualified professionals with rich experience of multiple industries such as Manufacturing, BFSI, Insurance, Healthcare, NBFCs & others. Our consultants are industry experts and have proven track records, some of the renowned certificates that our consultants hold such as CISA, CISSP, COBIT, CEH, CCNA, OSCP, ISO 9001 LA/LI, ISO 27001, ITIL LA/LI, PMP, to name a few. We believe in adding value to your business which is enabled through our Centre of Excellence (Coe) and, we have end-to-end capability for Program Build – Operations – Transformation. We have the ability to jump start and execute projects in Managed Services mode globally and flexible delivery models. Our Vision is to be one of the World’s most trusted advisory & solution provider for Cyber Security, Data Protection an Assurance practices.

WHAT WE DO

SECURITY ASSESSMENT SERVICES

1. Vulnerability and Penetration Testing Services

- Web Application VA/PT
- Mobile Application VA/PT
- Network Security VA/PT
- Database Security Assessment
- Cloud Security Assessment
- Wireless/WIFI Devices Assessment
- API & Web Services

2. Source Code Review

3. Configuration Review and Hardening Testing

4. Firewall/ Network Devices Security Review

SPECIALISED CYBER SECURITY SERVICES

1. External Threat Intelligence

- Phishing Domain Detection
- Rogue Applications Detection
- Source Code Leaks
- Social Media Abuse
- Brand Abuse
- Dark Web Monitoring
- Take Down support

2. Phishing Campaigns/ Stimulation

- Phishing
- Smishing
- Vishing

3. Incident response & Malware Analysis

4. Forensics Analysis

5. Root Cause Analysis

6. Red Teaming Exercise

7. Honeypot as Service

- Web Attack Mitigation
- Network Attack Mitigation
- Shadow Surveillance

CONSULTING, COMPLIANCE AND & AUDIT SERVICES

1. ISO Compliance

- ISO 27001 ISMS
- ISO 9001 QMS
- ISO 27701 PIMS

2. Information System Assurance & Audit

- **RBI**
  - Payment & Settlement Systems (PSS)
  - NBFC
  - Co-Operative Banks
  - Prepaid Payment Instruments PPI
  - CISA
  - P2P Lending
- **IRDA ISNP**
- **SEBI**
- **AADHAAR**
  - UIDAI AADHAAR
  - ESIGN ASP
- **OTHER**
  - GST SUVIDHA PROVIDER
  - NPCI

3. Regulatory Compliance

- PCI DSS
- SOX
- SOC 1, SOC 2 & SOC 3

4. Privacy Compliance

- General Data Protection
- Regulation (GDPR)
- ISO 27701 PIMS
- California Consumer Privacy Act (CCPA)
- Brazilian General Data Protection Law (LGPD)
- Personal Information Protection and Electronic Documents Act (PIPEDA, Canada)
- Singapore Personal Data Protection Act (PDPA)
- Health Insurance Portability and Accountability Act (HIPAA)

5. Risk Management

- Virtual Chief Information Security Officer (V-CISO)
- Third Party Risk Management
- IT Risk Management

CONTACT US

CYBERSRC®
CONSULTANCY
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

☎ **+91 9718933141, 0120-4160448**

✉ **info@cybersrcc.co**

🌐 **www.cybersrcc.com**

📍 **Head Office:** Unit 605, 6th Floor, World Trade Tower, Sector 16, Noida (UP)- 201301
Other Office:
London (UK): Kemp House 152-160 City Road, London, UK (EC1V 2NX)