VARUTRA℠
An Infoshare Systems, Inc. Company.

Mobile Security Assessment

Case Study

This is a case study of Mobile Security Assessment activities that Varutra has performed for one of its clients. For the privacy concerns certain information in this document has been amended or modified to maintain confidentiality.

Mobile Security Assessment Case Study Report

About Our Client

The client is one of the largest financial service providers and they offer comprehensive suite of financial products and their business includes Retail, Corporate and International Banking services, Insurance, Mutual Funds, Mortgage services and other financial services.

Objective

The client sought Varutra for advice on securing their Mobile Applications from security threats which can lead to loss of **Confidentiality**, **Integrity** and **Availability (CIA)** of the data. Client wanted to ensure that their Mobile Applications meet all the security standards.

The Challenge

Our Client's business requirement was to provide mobility to all their customers for all finances. To fulfil the same, Android & iOS applications were developed to provide mobility to the customers via cross-platform support.

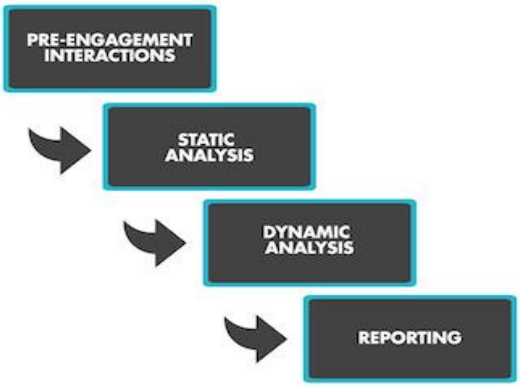
Major concern was to secure the customer's sensitive data, client being from financial background has developed applications considering all secure configurations like SSL Pinning and root detection implemented.

Security Standards followed at Varutra

Varutra's security assessment methodology is in accordance with best standards and follows guidelines from **OSSTMM, OSINT, NIST, ISSAF, CIS and OWASP** for web and mobile and **SANS** for Network Penetration Testing. Varutra follows **Application Security Verification Standard (ASVS)** which helps developers with the requirement for secure development.

Our Methodology

The client application is a complete mobile solution which covers Android and iOS platform. The goal was to understand the current level of external risks which may compromise the sensitive data of the organization. Client authorized to carry out the penetration testing and supplied Varutra with the mobile applications for Android and iOS.



Our Approach

Varutra's methodology involves assessing the security posture of the mobile applications to find out vulnerabilities (if any). To check the security of mobile application and server systems from an attacker's point of view; specifically, as an internet malicious user, determine if the mobile application and server could be compromised to gain access impacting Confidentiality, Integrity and Availability of data.

- Pentest activity started with gathering information for the mobile application and technologies used on frontend and backend systems.
- Reverse engineering the iOS and Android mobile application in order to better understand the interactions between the application layer and server.
- Pentesting via Black box testing methodology which helped to gain more knowledge about technologies used.
- At the end of Black box testing, many critical and high vulnerabilities be discovered which includes authentication bypass and 2FA bypass and others.
- Test cases were prepared by Pentesters to test critical modules of the application.
- Pentesters initiated Grey box testing wherein they checked internal storage and business logic.

• • •

Key Findings and Observations

Varutra, with its skilled Pentesters, was able to break into the mobile application by finding multiple Critical vulnerabilities such as,

- SSL Pinning Bypass
- Improper Export of Android Application Components
- Authentication Bypass
- Sensitive data in local storage and logs
- Application allows runtime debugging
- SQL Injection
- Cross-Site Scripting (XSS)
- Improper Session Management

The complete assessment was done with the automated testing using commercial and open source tools as well as extensive manual testing for verification and validation. This was the most important phase of a penetration test because it effectively demonstrates the impact of breach for the concern organization. Main targets in this phase were sensitive information revealed by the mobile application which includes sensitive API Keys, Hard coded credentials, Credit card details transmitted via logs.

Deliverables

The reports and remediation information provided by Varutra were customized to match the Client's operational environment and requirement. The following reports were submitted to the client:

1. **Executive Report:** Overview of the entire engagement, the vulnerabilities statistics and the roadmap for the recommendations made to mitigate the threats identified.
2. **Technical Report:** Comprehensive information, proof of concept examples and detailed exploitation instructions of all the threats/vulnerabilities identified and remediation for the same.
3. **Mitigation Tracker:** Simple and comprehensive vulnerability tracker aimed at helping the IT asset owner/administrator to keep track of the vulnerabilities, remediation status, action items, etc.

How Varutra Helped

Our Penetration Test helped numerous clients to identify the potential threats / vulnerability that could have compromised entire infrastructure. All of our clients are assisted in assessing percentage of potential business and operational impacts of successful attacks/exploitation. Additionally, the client gained the following benefits:

- **Risk Benefits:** Varutra minimized security risks by assessing and analyzing the client's infrastructure vulnerabilities and recommended solutions and remediation with proven methods to enhance security of organization.

• • •

- **Cost Savings:** Varutra suggested cost-effective risk-mitigation measures based on the client's business requirements that would ensure security and continuity of the business.
- **Customer Satisfaction:** Penetration testing was conducted with minimum interruption and damage across client systems/workstations to identify security vulnerabilities, their impacts and potential risks.
- **Compliance:** As an added bonus, the client was able to utilize the information gained from this Penetration Test to easily gain industry certifications and provide a higher level of service to its customers.

Conclusion

Penetration testing is often done for varying reasons. Two of the key goals we and our client aimed for, were to increase upper management awareness of security issues and to test intrusion detection and response capabilities. After conducting the Pentest and compromising the organization & engaged the client in a controlled offensive/defensive threat detection challenge, allowing the client several days to identify and remediate active threats within their systems.

Post completion of the assessment, Varutra was appointed to **conduct training for the key internal security team like secure code development as well as further advisory on remediation tactics.** In the end our client was able to meet the highest level of compliance and regulation standards, develop better security practices and reassure their customers, employees, and board of their continued dedication to best business practices and continued growth.

After mitigating all security risks by following all remediations suggested by Varutra, the client mobile application was secure from all possible risks uncovered by Varutra and effectiveness of these vulnerabilities can be verified by conducting Reassessment activity on same target mobile applications to analyze strength and the security posture. Upon Reassessing the target scope for all security vulnerabilities following are the vulnerability count for Assessment and Reassessment activities.

About Varutra

Varutra Consulting is an Information Security Consulting, Solutions & Training services firm, providing specialized security services for software, mobile and network. We are motivated to provide our customers with specially tailored services providing protection against external as well as internal threats and reduce business risk to improve security posture, achieve regulatory compliance and increase efficiency.

Under our Process & Compliance Consulting services we provide ISO/IEC 27001:2013, ISO 22301, ISO 20000-1:2011, NIST Cyber Security Framework, GDPR Compliance Audit, Virtual CISO and assist clients in auditing as per RBI IT Framework for NBFC, IRDAI Information and Cyber Security Framework.

At Varutra, we follow a unique methodology that is derived from our expertise, experience and a blend of internationally accepted and acclaimed industry standards in the Information Security domain.

26040 Acero
Suite 111 Mission Viejo
CA -92691, USA

9505 E 59th Street
Suite B Indianapolis
IN-46216, USA

7th floor, Marisoft 3
West Wing, Marigold
Behind Big Cinemas, Kalyani Nagar
Pune, Maharashtra 411014

Unit No 2, 5th Floor
Building No.9
Mindspace Raheja IT Park
Hi-tech City, Madhapur Hyderabad - 500 081