CASE STUDY

Briskinfosec secured
The Largest Mobile Application for a Foremost Telecommunication Industry

INDUSTRY
Telecommunication

STANDARDS
OWASP, PTES, SANS, NIST, WASC, OSSTMM, NCDRC MAST

PRIMARY SECTOR
Telecommunication
Internet Service Providers
Digital Television

LOCATION
Worldwide

OFFERED SERVICE
Penetration Test
Security Assessment

TYPE OF SERVICES : **Mobile Application Security Assessment**
(for Fortune 500 Company in Telecommunication Sector)

ABOUT CUSTOMER

Our customer is one of the leading Telecommunication Organization throughout the world. There are more than 100000+ employees in the organization. They have been the pioneers in Telecommunication throughout Urban and sub urban cities by providing their excellent 3G/4G services.

ASSESSMENT SCOPE

To identify and fix the vulnerabilities in the mobile application, the Client wanted us to conduct an effective mobile application security assessment to find out the vulnerabilities and to resolve the issues in the application. As a result of the security assessment, the mobile application is free from all vulnerabilities that makes the application not to get compromised at any cost.

THE SOLUTION

Briskinfosec followed NCDRC MAST (National Cyber Defence Research Center Mobile Application Security Testing Framework) to identify all exposed vulnerabilities in Mobile Application. Briskinfosec consultants mapped all issues with OWASP Mobile Top 10 and recommended perfect fix for identified vulnerabilities.

Key highlights of the Vulnerability fix are as below :

- Serious issues related to Input validation and authorization, session management and cookies handling were identified. The identifies vulnerabilities were fixed by the Development Team.

- Platform level vulnerabilities were identified in the mobile application safeguarding the Source code of the application.

- We completely secured the mobile application from OWASP common attack by hardening the default configuration.

- We performed vulnerability assessment by both automation and manual method to identifying the issues.

- We provided the complete Vulnerability fixing document as a reference to your development team.

THE DELIVERABLE

The reports and remediation information provided were customized to match the Client's operational environment and development framework. Identified security issues were categorized through Code Fix, Configuration Fix and Best Practices to make stakeholders understand the criticality of each vulnerabilities. The following reports were submitted to the customer

Key highlights of the Vulnerability fix is below :

DAILY STATUS REPORT

This mobile security assessment consumed around 1-2 weeks of time including retest. During the process of mobile testing, issues were identified and we shared all identified issues with corresponding recommended FIX over mail on a daily basis. Our prospect looked at the given valid report (XLS) and started working the fix right from Day 1 as they need not work laboriously on the last day when the entire report is given by the security team thus making their final assessment report easier for preparation.

TECHNICAL SECURITY ASSESSMENT REPORT

Complete security testing was carried. All the detected issues and the proof of concept (POC) will be covered with detailed steps in a PDF format.

ISSUE TRACKING SHEET

- All the identified issues were captured and will the be subjected for the retest review in a XLS fomat.
- All the issues will be captured for the reassessment.

SECURITY ASSESSMENT REPORT

Step by step process carried out by the entire team for each vulnerability.

OWASP ASVS MAPPING SHEET

Application Security Verification Standard Checklist was updated and shared the same.

FINAL BUG FIX REPORT

Overview of the entire engagement, the issues that were identified, the recommendations and remediation's which were made to mitigate the threats.

THE CHALLENGE

By conducting Mobile Application Security Assessment and vulnerability fix, Briskinfosec Reduced the Client's risk exposure in the Mobile application in an excellent manner where the Telecom Regulatory Authority of India (TRAI) is taking an extremely strict approach towards security.

RISK BENEFITS

Briskinfosec alleviated the security risks by assessing the customer's infrastructure vulnerabilities and recommended solutions with proven methods to enhance security.

COST SAVINGS

Briskinfosec suggested cost-effective measures based on the customer's business requirements that would ensure security and continuity of the business.

CUSTOMER SATISFACTION

Mobile Application Security Assessment was conducted with minimum interruption and damage across customer systems to identify security vulnerabilities, impacts, and potential risks.

SUPPORT

We have offered 1 year support with periodic security assessment to maintain mobile app security on highest standard.

CONCLUSION

We advised stakeholder on the measures they should take to remedy the various deficiencies in their systems and processes. As part of the remediation stage, we recommended that their day to day network is segregated from the network that stores sensitive personal information and financial systems. We also worked closely with our client to improve the policies, procedures, and employee awareness programmes to increase their cyber maturity. Stakeholder got impressed with our Zero Trust Cybersecurity Framework (ZCF) and they are looking forward to adapt it.

BRISK INFOSEC

CYBER TRUST & ASSURANCE

BRISKINFOSEC

TECHNOLOGY AND CONSULTING PVT LTD

+91-8608634123
044 - 43524537

contact@briskinfosec.com
www.briskinfosec.com