

Case Study: Mobile Application Security for an Online Travel Company

Date: 23rd October 2013

Confidentiality Notice

This document contains information, which is proprietary to Security Brigade InfoSec Pvt. Ltd. and should be treated as strictly private & confidential. The recipient agrees to maintain this information in confidence and not reproduce or otherwise disclose this information to any person outside of the group directly responsible for the evaluation of its contents. Neither this document nor any copy of it may be taken or transmitted to anybody or distributed, directly or indirectly outside the organization.



About the Customer

Our Client with revenue over \$ 124.72 million is a leading Online Travel booking company in India offering varied travel services and products to its customers.

The Challenge

Our client had decided to enter the mobile application arena by introducing a Blackberry application for its users to schedule and book manage travel itinerary. Their main concern was about its usability and security in terms of user account management and payment modules.

The Solution

By using Security Brigade's unique in-house developed EDITE framework, the consultants completed Mobile Application Security Process.

Our technicians downloaded the travel application on one of the test Blackberry phones and subjected it to initial scans to thoroughly understand the application functionality.

1. Reverse engineering the Blackberry mobile application in order to better understand the interactions between the application layer and server.
2. Vulnerabilities were identified and used to bypass user management controls.
3. Understanding of the application's inner-workings.
4. Exploiting the above findings to access the backend server.
5. The testing yielded several key security vulnerabilities related to ticket cancellations and payments.

The Deliverables

The reports and remediation information provided were customized to match the Client's operational environment and development framework. The following reports were submitted to the customer:

- **Executive Report:** Overview of the entire engagement, the vulnerabilities discovered and the recommendations made to mitigate the threats identified on the Client's websites.
- **Technical Report:** Comprehensive information, proof of concept examples and detailed exploitation instructions of all the threats identified and remediation for the same.
- **Excel Tracker:** Simple and comprehensive vulnerability tracker aimed at helping the IT asset owner keep track of the vulnerabilities, remediation status, action items, etc.

The Benefits

Our Penetration Test helped the bank to identify the potential threats / vulnerability that could have compromised their network and systems. We also assisted them in assessing the magnitude of potential business and operational impacts of successful attacks.

Additionally, the Client gained the following benefits:

- **Risk Benefits:** Security Brigade minimized security risks by assessing the mobile applications vulnerabilities and recommended solutions with proven methods to enhance security.
- **Cost Savings:** Security Brigade suggested cost-effective risk-mitigation measures based on the customer's business requirements that would ensure security and continuity of the business.

- **Customer Satisfaction:** Security Brigade identified key high risk vulnerabilities which if exploited by an attacker would have compromised sensitive customer information. Thus helped the customer in safe-guarding information.
- **Compliance:** As an added bonus, the Client was able to utilize the information gained from this test to easily gain industry certifications and provide a higher level of service to its customers.



E-mail: contactus@securitybrigade.com

Phone:

Mumbai: +91-022-23532909

USA: +1-34799-ITSEC (48732)

Italy: +39-329-788-6447

Head Office: B-20, Everest Building, 156 Tardeo Road,
Mumbai – 400034
India

Branch Office: Via Magnolie
Pisa, Italy 56100