SB SECURITY BRIGADE

Immunity for your IT

Case Study: Source Code Audit for a Private Sector Bank

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 is an Indian Bank, engaged in providing a range of banking and financial services. The Bank's business segments include Treasury, Corporate/Wholesale Banking, Retail Banking, Corporate Finance, Transaction Banking and a host of other Banking services.

The Challenge

Our Client had developed a banking application that assists its customers manage their funds efficiently. Due to the applications connectivity with its main online banking portal it was necessary to verify the applications security posture before deploying it to production. Our team recommended a complete Source Code Security Audit of the application in-order to bring it up to speed with current security practices

The Solution

By using Security Brigade's unique in-house developed EDITE framework, the consultants completed Source Code Audit. Key highlights of the audit are listed below:

1. Interaction with the development team to understand business requirements and data flow of the application.
2. Using automated tools, preliminary scans were performed on the source code to identify all the flaws as per OWASP top 10 and other industry recognized standards.
3. Based on the applications critical function, manual source code audit was performed to identify threats.
4. Assisting developers to fix the vulnerabilities identified during the course of the audit.

In-addition, our team also helped the Customer's development team in implementing patches and fixes for the identified vulnerabilities.

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

By reviewing the application at the source code level Security Brigade was able to assist the client in identifying critical vulnerabilities that would have resulted in serious financial impact on the client.

Additionally, the Client gained the following benefits:

- **Risk Benefits:** Security Brigade minimized security risks by assessing the customer's application vulnerabilities at source code level.

- **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.
- **Compliance:** At the end of the audit the client was complaint to various industry standards including PCI DSS.

SB SECURITY BRIGADE
Immunity for your IT

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