Application Security Assessment Profile: Payroll and Employee Benefits Management Software

1.1 About the Client

The customer for this project were a payroll outsorucing firm based out of India who had their own application that manages the payroll and employee benefits management function as outsourced to them. The customers are various kind of firms both based out of India and outside India.

1.2 Project Description

The client had a payroll management application solution developed in Microsoft Technologies. The software is accessible to all customers over the Internet. Customers and their employees can access the application to input various data as required in various forms so that payroll can be processed on time and payslip and other reports as required by the management of relevant customers can be provided. The application solution also provided mechanism to input various benefits as provided to the various employees and one single view of remunerations and benefits management of employees.

1.3 Business Challenges

The customers of the firm in question required the payroll processing solution to provide security of data as captured in the payroll application solution and also to reasonably address the various security risks within the application software and associated infrastructure so that their data is not at security risk.

1.4 Our Role

We performed the following functions:

- Studied and Analyze the business information flow within the application from security perspective
- Performed security assessment of application from a black box(ethical hacker's perspective testing for issues like authentication risks, data disclosure risks, data corruption risks, application denial of service attacks, specific targeted attacks etc).
- Performed security assessment of application from an application controls perspective(Input controls, processing controls, output controls, database controls and interface controls).
- Performed white box testing from security perspective including tests from an internal intruder perspective, architecture review, cryptographic controls, selective security code reviews)

- Provided a report on security risks assessment within the application from various perspective as mentioned above along with recommendations.

1.5 Resources used

- CISSP/CISA certified professional
- OWASP Reference framework
- Acunetix, Nessus and various tools
- Reference best practices COBIT, ISO27001

1.6 Business Benefits Delivered

- Project execution followed onsite and offshore model due to various tests.
- Security of application was improved as many of the security risks identified resulted in making code changes, architectural improvements and new way of doing things to address the risks.