CASE STUDY

Large Bank

Automated Static Testing (Software Audit) from Magic Lamp

Static Testing identifies critical reliability, security and performance defects missed by traditional (dynamic) testing and enforces compliance with rules and best practices. Magic Lamp Software provides technologies and services for automating Static Testing or Software Code Audits.

It automatically detects critical errors in applications that use core Java and Java EE, based on an expert knowledge base of thousands of rules, including security, performance, concurrency, resource leakage, Core Java/Java EE/Open Source API usage, and SQL query analysis rules.

Overview

- Top retail and investment bank in India
- Application development done in-house
- CTO concerned about down-time and security issues during financial crisis

Objective

Identify reliability, security and performance issues missed by testing

Application details

- Mission-critical for retail banking, customer support
- Exposed to users on internet, high security needed
- High performance and reliability needed
- Well tested including security penetration testing

Critical issues identified

Security

Cross-Site Scripting, Cross-site Request Forgery

Effect: Steal User ID/Password, see private user data, perform transactions on behalf of other user

Cause: User-input not validated properly

SQL Injection

Effect: Change server logic, change/destroy database

Cause: User-input not validated, incorrect database access

User ID Forging

Effect: See/modify another user's data

Cause: User ID accepted from input after login

Improper Error Handling

Effect: Confidential server data/configuration exposed

Cause: Error messages printed to browser

Concurrency

Data-Race Condition

Effect: See/modify/transact with other users' private data, corruption of customer data

Cause: Private data stored in a location shared by multiple concurrent threads of execution, and accessed without locking

Resource Leakages

Database Connection Leakage

Effect: Performance slowdown, loss of scalability, server hang/downtime

Cause: Database connection starvation because connections are not closed after usage

Category	Priority 0	Priority 1	Total
Security Vulnerabilities (Cross-Site Scripting, SQL Injection, File Path Traversal, User ID Forging, Improper Handling of Confidential Information)	179	694	873
Reliability/Concurrency (Data-Race Conditions, Runtime Exceptions, etc.)	45	318	363
Performance (Resource Leaks, etc.)	69	394	463
Java/J2EE/Open Source/ Custom API Usage	7	262	269
Total Defects	300	1668	1968

Software Audit

Magic Lamp can provide an on-site or off-site audit service that allows clients to reliably and quickly improve quality and security without disturbing existing processes or diverting resources from other commitments.

Customer Testimonial

Magic Lamp's technologies enabled us to discover security, reliability and performance issues much faster with significantly less efforts in several Java-based products.

– SVP, Large IT Services Vendor

Jenesys Technologies Pvt. Ltd.
45/A, 4th Floor, Green Arch
1st Main, JP Nagar 3rd Phase
Bangalore 560 078

E-mail : magiclamp@jenesystech.com
solutions@jenesystech.com

Phone: +91-80-4081 7777

www.jenesystech.com/magiclamp

JENESYS
Making IT Work