Global IT Solutions
An ISO 9001:2015 & ISO/IEC 27001:2013

# Security Testing: Background Screening and Immigration Compliance Web App

## About The Client

The client is a global provider of specialised Primary Source Verification solutions along with background screening and immigration compliance services. They partner with clients across the public and private sectors to assist them in mitigating potential risk by exposing fraudulent education degrees, employment certificates, practice licenses, work permits and passports.

## Client's Technology Requirements

The prime objective of application's security testing is to find out the vulnerability of the system and to examine if the data and resources are protected from potential intruders. Online transactions have increased rapidly making security testing as one of the critical testing areas for such applications. Security testing is more effective in identifying potential vulnerabilities when performed on a regular basis. The different attributes verified included:

- Authentication
- Authorization
- Confidentiality
- Availability
- Integrity
- Non-reputation
- Resilience

## Key Challenges

- Frequent changes in application: The development team was constantly releasing new builds and testing the application's security regularly was cumbersome activity.
- Application had detailed info: This required thorough testing of the application both manually and through automation tools against different vulnerabilities and threats.
- Complex user classification: The users had different authority rights and tests were conducted for any loopholes at all user levels. This couldn't be checked with automation tools alone and required manual testing also within specified timelines.
- Implementation of AJAX: Although AJAX allows users to mould the application as per their requirements on regular basis, it also possess numerous security threats with upgradations. The tools for AJAX security testing are still under development.
- Automated Security testing is in primitive stage: The existing tools are not capable to detect all security breaches or loopholes present in the application.

## Solution Approach & Methodology

- Study of Security Architecture: The first step is to understand the business requirements, security goals and objectives in terms of the security compliance required by the organization
- Analysis of Security Architecture: Understanding and analysing the requirements of the application under test
- Classify Security Testing: Collect all system setup information and list out the Vulnerabilities and Security Risks
- Prepare Threat Profile: Developing a detailed threat profile, with clear illustration of the threats enables to implement a proactive incident management program

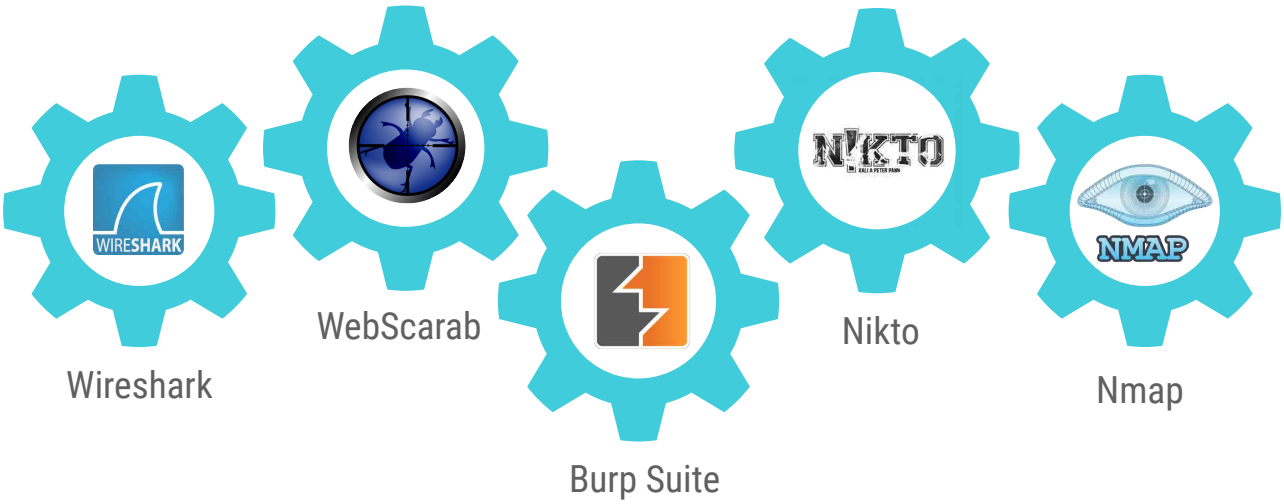
- Test Planning: Based on identified Threat, Vulnerabilities and Security Risks, prepare test plan to address these issues
- Traceability Matrix: For each identified Threat, Vulnerabilities and Security Risks, prepare Traceability Matrix
- Security Testing Tool: Identify the tool to execute security test cases faster & more reliably
- Prepare Test Cases: To determine whether the application satisfies the requirements
- Test Cases Execution: Execute the Security Test cases and retest the fixes along with Regression Test cases
- Reports: Prepare detailed reports of Security Testing with Vulnerabilities, Threats, Risks, and other open issues

## Achievements

We could identity major security threats in the product and made it OWSAP compliant in security paradigms.

- Firewall Configuration: Test firewalls and all identifiable services be it email, VPN, file transfer and remote administration testing
- Network Scanning: Check open, closed and filtered network services
- Network Service Identification: Fingerprinting tools and hands on testing to validate accessible service version and platform information
- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Components with Known Vulnerabilities
- Invalidated Redirects and Forwards

# Testing Tools Used




## Project Highlights

| | |
|---|---|
| **Client** | Due Diligence & Verification Company based in Middle East |
| **Location** | India |
| **Industry** | Background Screening and Immigration Compliance Solutions |
| **Project Duration** | 1 month |
| **Team Size** | 1 person |
| **Delivery Model** | Offshore |
| **Engagement Model** | Turnkey |

## About PSI

Pratham Software (PSI) is a global IT services company (with established ISO 9001:2015 & ISO/IEC 27001:2013 practices) providing software product development, consulting and outsourcing solutions to enterprises worldwide. While providing a wide range of solutions, we focus on Outsourced Product Development (OPD), Business Process Management (BPM), Application Development and Maintenance (AMD) and Content Engineering. Our extensive experience in OPD helps us build strong relationships with Independent Software Vendors (ISVs), as we work with them throughout the product development lifecycle. In terms of technology and platform, we work across all major technologies such as Microsoft, Java and Open source and have capabilities and experience in developing solutions for web, mobile, Cloud and social media. For Enterprise customers, in addition to Process Automation, we also offer development and support services in BI and DWH.

US Office: 21860, Via Regina, Saratoga, California 95070 USA | Ph:(408) 898-4846 | Fax: (408) 867-0666
India Development Center: G1-265-266, RIICO Industrial Area, EPIP, Sitapura, Jaipur 302022, India | Ph: (91)141-6690000
www.thePSI.com