



● ABOUT THE CLIENT

IM Your Doc™ is an instant messaging application that aims to enhance the speed of communication between healthcare professionals, their patients and staff. A secure messaging application, IM Your Doc offers the convenience of texting that is secure and follows the compliance laws for healthcare messaging apps. As a HIPAA (Health Insurance Portability and Accountability) compliant application, the users can access rapid and seamless communication.

● GOALS

As an online communications medium, the client had to ensure that the application efficiently and consistently conformed to both the IT and HIPAA compliance standards. The client required the services of a firm that would facilitate them in delivering seamless business and compliance support services, which would further add to the client's expansion plans. A detailed scope of work for the client involved the following practices:

- ✔ Complete software and hardware audit for the application
- ✔ HIPAA Compliance check to be run on all versions of the application – Mobile apps (iOS, Android) and Desktop version
- ✔ Security audit of the application, involving the use of both manual and automated test tools
- ✔ Performance Audit involving load testing and website performance checks. JMeter was to be used as the load testing tool for monitoring the functional behavior of the application and to measure performance.
- ✔ Complete functional test of the IM Your Doc website involving UI test across multiple browser and platform combination to check for compatibility and responsiveness.

INDUSTRY

HealthCare

PARTNER

www.clavax.com

EMAIL

info@clavax.com

PHONE

1-844 425 2829

REACH US @

1754, #210,
Technology Drive San Jose,
CA 95110

● CHALLENGES

For any healthcare application, accuracy of information and efficiency of services are the top priorities. The IM Your Doc client wanted to ensure that their communication platform for users and healthcare providers is secure and verified, conforming to the compliance standards for mobile communication. They wanted to implement a testing environment that would validate the application-user engagement – an aspect in which they were encountering some challenges. The client wanted the QA and Testing team at Clavax to evaluate and eliminate the security loopholes in the website and ensure that the app adhered to the HIPAA compliance act. Additionally, the security audit for the IM Your Doc website included challenges related to compliance, website performance and functioning.



● CLAVAX SOLUTION

Clavax offered a robust and comprehensive solution for auditing the security of the client's application. The QA and testing teams at Clavax analyzed the application and decided on the application of a single test environment that would automate the testing process while simultaneously running manual tests. Mentioned below are the set of test solutions applied in the security audit of IM Your Doc:

- ✔ **Performance Tests** and performance tuning to measure the user response time and throughput of the system, under normal loads conditions
- ✔ **Load Tests** to identify potential bottlenecks in the system
- ✔ **Functional Tests** to determine the conformance of the application to its specifications
- ✔ **Manual Tests** involved the writing of high-level test cases, conforming to the predetermined test plan created with the selection of a general methodology. These detailed test cases enabled the test teams to clearly identify and steps to achieve the expected outcomes. This was further followed by the creation of a detailed test report highlighting the findings of the audit team.



Technologies Used



PENETRATION TESTING – BURP PROXY

An interceptive proxy server for running security tests on web applications; typically functions as man-in-the-middle between the user's browser and the target application.



GCC (GNU COMPILER COLLECTION)

A collection of front-end technologies like C, C++, Objective-C, Fortran, Ada, Java and Go, along with libraries for these languages. Used as the compiler for the system.



NIKTO

An Open Source web server scanner, it performs comprehensive tests for multiple items that include checks for outdated versions of servers, potentially dangerous files or CGI, version-specific problems on over 270 servers.



GOOGLE WEB APPLICATION TESTING TOOLS TAMPER DATA

Another add-on for Mozilla Firefox, with tamper data users can trace and time http response and requests, view or modify post parameters or HTTP/ HTTPS.



XSS ME

With the Cross-Site Scripting (XSS) Me tool, common flaws and XSS vulnerabilities are detected early on to protect the application from unnecessary flaws; test for reflected XSS vulnerabilities.



SQL INJECT ME

Add-on used for SQL Injection testing vulnerabilities on the Mozilla Firefox browser.



SQL INJECTION

An upgrade from the earlier form free, it is a component for transforming radio buttons, checkboxes, or other select elements into input text as well as to enable disabled from all forms in a web page. Identification and testing of SQL Injection vulnerabilities also become easier.



HACK BAR

A simple Penetration test and security audit tool to test for SQL injections, site security and XSS holes.



JAVASCRIPT DEOBFUSCATOR

Allows developers to watch JavaScript codes that run on a web page, whether generated on the fly or obscured, being compiled or executed.



FIREBUG

A tool to edit, debug or monitor any CSS, JavaScript or HTML live in a web page.



ACCESS ME

A Firefox extension to test for Access vulnerabilities is a web application.



NMAP (NETWORK MAPPER)

A free and open source security scanner for security auditing and network discovery.

powered by

Clavax

● OTHER TOOLS:

- ✔ **Proprietary Tools:**
The use of proprietary tools included software exploits, password brute forcers and protocol manipulation tools.
- ✔ **JMeter,**
Open source Java application software, to measure site performance and load test functional behavior was used for Load Testing, Performance Testing and Stress Testing of IM Your Doc.
- ✔ **Selenium** (software testing framework) used for Functional Testing along with manual tests.

● RESULTS

The security audit of the IM Your Doc applications led to the realization of the following results:

- ✔ Boost in user confidence
- ✔ Reduced maintenance efforts
- ✔ Enhanced status reporting along with a dashboard for monthly metrics reports
- ✔ Vast amount of security audits delivered on time, resulting in the increased efficiency
- ✔ The percentage of automated test execution increased from 60% to 95%