Executive Summary

- ✓ Business Domain – Education
- ✓ Type of testing required – Web Application Security Testing
- ✓ Total Duration – 15 days
- ✓ Region – US

Client

Client offers student enrollment and school choice software for Pre-K12 schools, in the US. The software is a revolutionary student enrollment and choice software which aims to streamline processes like student recruitment, application and lottery management, registration, school choice and unified enrollment, family communications and year-round digital forms.

This software is available in both web and mobile platforms for district staff and parents. The software helps them access the information with ease anywhere, anytime. Schools from all over the country use our client's software to modernize their student enrollment process.

Business Context

The software captures extensive Personally Identifiable Information (PII) of the users, which include the details about the families, children, their preferred choices of schools, admission application forms and much more.

Various schools could access the data about children and their families without their consent, which turned out to be a major setback for this software.

Large and complex systems increase the probability of vulnerabilities, making the application fragile and easy to attack.

Given the complexity and size of the application, there were many security challenges that were to be addressed:

- Check if data in transit & data at rest is stored in encrypted form
- Shield user data against data breach including data theft, unauthorized access, cyber-attacks, etc.
- Circumvent data sharing between schools
- Maintain privacy

TestOnDemand Solution

- Used Interactive Application Security Testing (IAST) approach that integrated Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) tools, to identify critical vulnerabilities in the application that could have led to significant reputation and revenue loss
- Used the 5-step approach, to perform a complete assessment of the web application as per the security testing standards (such as OWASP Top 10, NIST, SANS 25 etc.), as well as published zero day vulnerabilities
- Used multiple tools for reconnaissance, discovery and exploitation of vulnerabilities and gathered action able intelligence from the logs to determine the strength of the application

The TestOnDemand team ensured seamless communication with the client. Daily summary and detailed weekly reports were shared with the client to help them track the project status. Daily summary report contained identified vulnerabilities whereas the final report contained comprehensive information on the security issues with exploitable vulnerabilities.

Engagement Metrics

- Number of Days – 15 days
- Location – TestOnDemand Office
- Test Areas – Web Application
- Number of rounds – 1

Findings/Error Matrix

- Identified 15 Vulnerabilities
- 12 Vulnerabilities had a CVSS score of 6 and above (on a scale of 1-10)

Key Outcomes

The client's software was under Medium Risk Security Threat profile, which meant the security issues with high probability had to be fixed within a time frame of 1-3 months. A comprehensive list of recommendations to patch each Vulnerability type was also provided.

We helped our Client remediate the critical security vulnerabilities, which otherwise could have helped attackers gain unauthorized access to the application and also perform Denial of Service (DoS) attacks.