Improving Web Application Security

Success Story - April 2015

Customer & Product

The customer is a leading organization that provides occupational safety hazard software solution. The company holds the vision of eliminating deaths on the job, and to do so they predict the workplace injuries by performing careful calculations on observation data. The application hosted as a SaaS solution combines more than 130 million unique observations and nearly 40,000 reported incidents from 15,000 work sites.

The application provides option to record observable indicators, identify leading vulnerable indicators, identify likelihood of next incident, report and eventually measure the effectiveness of organization's complete safety programs. The web application has multiple interfaces to meet distinct needs of each client. An administrative interface is also provided for creating, configuring and monitoring the clients' data. The application also maintains each organizational detail including running projects, associated company information, resources' contact details and incidents/observation records.

The need to protect application functionality and organizational data motivated our client to engage us to conduct security testing of this application. The testing has been performed on yearly basis.

Challenges

We performed the security testing on the web application to comply with one of the renowned web application security vulnerability reference, OWASP top 10 vulnerability list. The testing was conducted on different versions of the vulnerability list including 2010 and 2013. During the multiple iterations of security testing we faced following key challenges:

- Developing understanding of application functionality was one of the key challenges because the functionality was not documented properly and only few basic use case scenarios were provided.
- Security requirements were also not available for the application other than the requirement of testing against OWASP top 10 vulnerability list. Secondly, OWASP top 10 vulnerability list document identifies just the list of vulnerabilities and does not have all the requirements for all vulnerabilities in a single location or a document.
- Due to continuous updates in OWASP security requirement and references, we had to manage security requirement updates, new skill acquisition, and new/updated security testing tools.
- Sharing the daily/weekly progress of security testing was a challenge because execution of most of the test cases spanned over a long period of time and its status remains In-Progress until all the pages of the interfaces are tested.

Solutions

Most of these challenges were not new to the security testing team of SQA Consultant, and therefore we were able to handle all challenges effectively and efficiently.

- To develop the application understanding, the client gave an initial demonstration session that comprised of an overview of basic application functionality. The client also gave credentials to the test environment; in this way, the security testing team developed application understanding by exploring the application. We also prepared a list of open questions majorly focusing on critical information that was needed to understand the application behavior. We were able to completely cover the application

functionality understanding in a short period of time, before starting testing activities.

- We had to compile the security requirements against OWASP top 10 vulnerability list. Therefore, to extract security requirements we used following strategy:
  - For each OWASP top 10 vulnerability list we compiled a list of requirements extracted from the reference documents and other OWASP security projects including OWASP cheat sheets, development guides and testing guides. We prepared a generic security testing requirements based on these and got them approved from the customer.
  - Next, we inter-related the vulnerability requirement with application functionality to identify test scenarios that were to be tested based on application's functional requirements.
  - As the functional requirements were not available, we worked on the assumption that application is functioning as per requirements. Therefore, we tested security vulnerabilities against the current application functionality.

- OWASP top 10 list and other reference documents are continuously maintained by the OWASP organization, and therefore needed to be tracked and monitored by the security testing team. The security testing team prepared a strategy to monitor any updates in the OWASP project.

  In case of any changes in security requirements, they update their documents, configure required testing tools and develop new skill, if required. SQA Consultant security testing team frequently undertakes this activity, whether the project is running or not.

- During any testing activities, the testers need to share the execution status for progress tracking, monitoring and risk assessment. Similarly, we have to track progress of security testing; however, for most of the test cases, execution time may span over weeks as they need to be tested on different pages, and with different techniques and tools. Therefore, to track the testing of this project we compiled following status trackers in a single Excel document:
  - Test case status tracking sheet
  - Checklist matrix sheet mapping different security requirements to all application pages and representing the percentage coverage of execution
  - Reported issue tracker

Achievements

Here is a summary of our accomplishments during this security testing project:

- Security testing team was able to develop application understanding with limited information in specified time period by manually exploring the application.
- A set of security requirements was prepared for the client which was then used by the client for tracking application's security features and integrating the application's security and functional requirements.
- We kept our security testing training and expertise up-to-date so that our team and testing environment were ready for upcoming security testing projects.
- Our team identified major vulnerability issues that existed in the application. The identified issues were related to injection, XSS, misconfigurations, improper implantation of transport layer protections (HTTPS), authentication and authorization, session management, etc.
- We prepared a concise and effective status tracking document that helped us to monitor progress and identify risk factors and delays at earlier stages of the project.

Contact Us

Explore ways to use our expertise in growing your business while establishing a valuable partnership with us.

Contact our consultants at:

Phone: +1.412.533.1700 (Ext: 585)
E-mail: info@sqaconsultant.com
Website: www.sqaconsultant.com