Seeker – Best Quality Application Security

ACCURACY   **CLARITY**   **SIMPLICITY**

Table of Contents

1 Introduction

In the modern cyber era business data must be protected from application security threats. Seeker brings a novel approach to application security, an approach based on decades of experience in application security and consulting to organizations large to small. Seeker focuses on the data in applications and the impact applications have on sensitive processes and information, addressing application security from the business impact and threat perspectives. Unique technology makes Seeker a real alternative to expensive and nonscalable manual testing, while delivering top quality results.

Seeker is an automated application security testing solution. It tests applications and identifies application security vulnerabilities that pose real threats. It then prioritizes these vulnerabilities according to their business risks. Seeker does this by correlating run-time code and data in response to simulated attacks.

Seeker is an industry recognized solution, developed to integrate into the software development lifecycle and facilitate application security testing as a natural part of the development and testing processes. Seeker does not require change to the normal procedures of the organization, but rather adapts itself to the organization and integrates itself within existing processes. Seeker is simple to operate and still provides the highest level of application security without disrupting existing workflow.

To deliver best quality application security, Seeker is supported by three pillars – Accuracy, Clarity and Simplicity.

2 Accuracy – Identify Vulnerabilities Posing a Real Threat

Seeker identifies vulnerabilities that pose a real threat to business critical data, and only those vulnerabilities. By eliminating false positives and delivering relevant results prioritized by business risks, Seeker enables an efficient application security plan which focuses on issues that matter.

Seeker utilizes a unique technology which correlates end-to-end flow of data and run time code analysis with simulated attacks. Seeker analyzes the actual code as it reacts to attack attempts. Seeker also tracks data throughout the application and learns how it is processed and how it is affected by attacks. Seeker analyzes business processes and data in order to better understand the application and the potential threats. Finally, Seeker develops actual exploits which take advantage of identified vulnerabilities.

This unique combination of technology and functionality allows Seeker to not only find vulnerabilities and eliminate false positives, but also assess the actual impact of vulnerabilities, making it much easier for organizations to prioritize their resources and build an efficient remediation plan.

3 Clarity – Everything Required for Effective Security

Seeker identifies application security threats in an effective manner however, identifying security problems is meaningful only if findings are presented clearly so that risks are easy to understand. Seeker delivers results in a

"what-you-see-is-what-you-need-to-fix" manner, false positives eliminated. Results are delivered in a variety of methods, tailored for different functions in the organization, allowing for quick assessment of security status, and easy, cost effective remediation.

Seeker shows an overview of the application security status to allow management and security to understand the risks, provides technical vulnerability information, as well as making available video clips that capture the exploitation process. The videos show step-by-step exploitation of the tested application to demonstrate how a vulnerability could be used by an attacker, and explain its impact.

To assist developers, Seeker provides all relevant information for understanding and remediation of vulnerabilities. This includes the vulnerable code segment, technical information on the vulnerability, including code, data and memory status during exploitation. Seeker also provides context-based remediation instructions including an explanation on how to fix the problems as well as providing sample secure code in the relevant programming language.

4 Simplicity – Easy to Deploy and Operate for Immediate Results

On top of accurate technology and clear results, Seeker is easy to deploy and run. Members of the SDLC are occupied with development and need security efforts to be kept to a minimum. Seeker provides just that with an easy, intuitive graphical interface, and an abundance of ways to integrate into existing processes for full automation without manual intervention.

5 Seeker in the Organization

Seeker fits as an integral part of software testing in the organization, and interacts with it seamlessly. Seeker can be used for manual testing by quality assurance professionals, but it can also be easily integrated into automated testing and continuous integration processes. Seeker is designed to be used by professionals who are not security people.

While the operation of Seeker is part of the testing processes, the results are eventually presented to developers to address vulnerable code. Seeker's results are tailored for this use. Fixes suggested by Seeker are easy to understand and apply. The information can be provided to the developers through the bug tracking system being used, an approach used by many organizations, as Seeker integrates with all common bug tracking software.

In addition, developers can use Seeker's proprietary reporting mechanisms. Developers are not required to have any prior security experience.

Seeker is a best quality application security solution for any organization.

6 About Seeker

Seeker is the leader of the new generation of application security testing software. Easily integrating with existing software testing processes, Seeker allows developers to efficiently develop secure applications.

7 About Quotium

Quotium Technologies is a specialist in the development of innovative software solutions to guarantee the security and performance of business critical applications throughout their lifecycle.