SYNOPSYS®

Parkeon Delivering Highest Security With Seeker®

"Seeker answered our integrations and automation needs. It provides training and knowledge to its users. Seeker is the perfect tool to help us improve our security practice to build excellent software."

L. Porchon
CISO of Managed Business Service division, Parkeon

Business Overview and Challenge

Parkeon is a key player in the urban mobility sector and a global provider of parking and transport management solutions. Parkeon offers a unique range of parking control and payment services in 55 countries and more than 3000 cities around the world.

Parkeon develops real-time payment systems suitable for all sales channels – credit and debit cards, mobile phone accounts, prepaid cards, e-purse schemes and contact/contactless card technology. These solutions are deployed on Parkeon's own POS terminals, such as parking meters at curbside and at "pay and display" and "pay on foot" car parks.

The accelerating growth of security breaches impacting e-commerce and remote POS sales led Parkeon to implement a process to raise the security of their applications to the highest level possible, regardless of geographical location of the deployment.

Seeker® has been chosen by the IT department of Parkeon to validate end to end security and PCI (Payment Card Industry) compliance of their main electronic ticketing and transaction product, ArchiPEL. Seeker has been chosen due to its unique combination of accurate vulnerability detection and PCI compliance capabilities, integration into development processes and ease of use by developers and testers without security expertise.

Solution Evaluation

Parkeon builds complete solutions for payment and offers the possibility to centralize the electronic payment flows on behalf of its clients. Both activities require the overall solution architecture to be compliant to standards and norms in the industry such as PCI-DSS (Payment Card Industry Data Security Standard).

Parkeon had been using a dynamic application security testing (DAST) tool to validate the security of applications on its integration environment, but that solution was not working out as they had hoped.

The application is developed using agile development methods and is updated in production 5 times per quarter. Security validation needed to be integrated into existing automated processes, and be usable by developers and testers who are not security experts.

BUSINESS BENEFITS

- **Seeker ensures that the entire system, end to end, complies with security standards at each release**
  By focusing on data, Seeker provides strong advantage for critical data requirements such as those defined in PCI-DSS Section 6.

- **Seeker facilitates communication between test and development teams**
  Every vulnerability is automatically linked to the offending source code, with relevant remediation suggestions.

- **Seeker improves awareness and training for more secure coding practices**
  Developers don't just fix vulnerabilities. By fixing problems in their own code, they learn how to use secure coding practices next time.

"We chose Seeker because with Seeker testers and developers don't need to invest time or have expertise in order to execute security tasks on a regular basis. Seeker provides correlation between vulnerabilities and impacted source code saving developer effort."

L. Porchon
CISO of Managed Business Service division, Parkeon

Deployment and Benefits Raised

While using Seeker, Parkeon has identified three key benefits that demonstrate that it is the tool for them.

First, Seeker ensures that the entire system, end to end, complies with security standards such as PCI-DSS by understanding how data flows throughout the entire application. It identifies vulnerabilities in relation to their impact on sensitive data.

The data centric approach of Seeker is a strong advantage in testing for PCI-DSS Section 6 requirements. Critical data – such as credit card information – is automatically tracked through the different components of the payment chain to verify that there are no vulnerabilities that may compromise it (such as forgotten debug data, insecure manipulation, insecure storage – even temporarily – in file or database, insecure transmission to third parties, and so on.)

Seeker gives Parkeon the ability to automatically ensure that the overall system complies with security standards - at each release.

Second, Seeker facilitates communication between the test and development teams by linking vulnerabilities back to the offending source code. Unlike other dynamic testing tools which report vulnerabilities by the offending URL, Seeker automatically ties those vulnerabilities back to the source code where the fix needs to be applied. It eliminates false positives, pinpoints the vulnerable source code and provides developers with clear remediation advice tailored to the tested application.

Parkeon is able to improve security, reduce the amount of time spent on security testing and improve communication between security and R&D:

- Developers focus their time on proven vulnerabilities and source code corrections recommended by Seeker.

- Testers have a clear view of business risks of the application tailored by OWASP Top 10 criteria, Parkeon's corporate security standard.

And third, Seeker improves security awareness and helps train developers for more secure coding practices. Parkeon's developers and testers are trained on the basis of OWASP TOP10, but they are not information security experts. By providing a replay of every attack, explaining the business risks and providing relevant remediation suggestions, Seeker helps their test and development teams to acquire awareness and training in an ongoing manner, thus improving the security of their code.

Conclusion

Seeker fits seamlessly into Parkeon's security automation process, ensuring that their development and testing teams deliver frequent, secure and compliant releases to production while improving productivity and security awareness.

SYNOPSYS®

www.synopsys.com/software

Synopsys
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: (800) 873-8193
International Sales: +1 (415) 321-5237
Email: sales@coverity.com