SYNOPSYS® | PARKEON

CASE STUDY

Parkeon Delivers Secure Payment Solutions With Seeker

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 3,000 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 point-of-sale (POS) terminals, such as curbside parking meters or "pay and display" and "pay on foot" car parks.

The rapid growth of e-commerce and remote (POS) security breaches led Parkeon to increase the security of their applications to the highest possible level, regardless of the deployment's geographical location.

Parkeon's IT department chose Seeker by Synopsys, our interactive application security testing (IAST) tool, to validate end-to-end security and PCI (Payment Card Industry) compliance of their main electronic ticketing and transaction product, ArchiPEL. Seeker was chosen due to its unique combination of accurate vulnerability detection, PCI compliance capabilities, integration into development processes, and ease of use for developers and testers without security expertise.

"We chose Seeker because 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

Solution evaluation

Parkeon builds complete payment solutions that centralize electronic payment flows on behalf of their clients. Both activities require overall solution architecture compliance 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 in their integration environment, but the solution was not working as they had hoped.

The application is developed using agile development methods and is updated in production five times per quarter. Parkeon needed a tool that integrates security validation into existing automated processes and is easy to operate by developers and testers who are not security experts.

Deployment and benefits realized

While using Seeker, Parkeon has identified three key benefits.

First, Seeker understands and verifies how data flows through the application, ensuring that the entire system, end to end, complies with security standards such as PCI DSS. It also identifies vulnerabilities in relation to their impact on sensitive data.

Seeker provides testing that helps meet PCI DSS Section 6 requirements. By automatically tracking critical data, such as credit card information, through various components of the payment chain, Seeker verifies that there are no vulnerabilities, such as forgotten debug data, insecure manipulation, insecure storage—even temporarily—in a file or database, insecure transmission to third parties, and so on, that may compromise it. With Seeker, Parkeon can automatically ensure that the overall system complies with security standards at each release.

Business benefits

Seeker ensures that the entire system, end to end, complies with security standards at each release

By focusing on data, Seeker provides testing 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 secure coding practices

By teaching developers how to fix problems in their own code, Seeker allows them to learn secure coding practices.

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

Using Seeker, Parkeon improved security, reduced the amount of time spent on security testing, and improved communication between security and R&D:

- Developers focus their time on proven vulnerabilities and source code corrections recommended by Seeker.
- Testers gain a clear view of the application's risk posture in relation to the OWASP Top 10 criteria and Parkeon's corporate security standard.

Third, Seeker improves security awareness and trains developers to exercise secure coding practices as outlined by the OWASP Top 10. By explaining business risks and providing detailed contextual remediation suggestions, Seeker has helped Parkeon's test and development teams acquire awareness and training in an ongoing manner, thus improving the security of their code.

> *"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

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.

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

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

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com

SYNOPSYS®
Silicon to Software™