Parkeon Chooses Quotium's Seeker

for Agile Code Security and PCI Compliance

Overview

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 multiplication 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.

The need

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 has been using a dynamic application security testing (DAST) tool to validate the security of applications on its integration environment.

> *"The main issue with scanners is that they need a substantial expertise to sort false positive. The correlation between vulnerabilities and impacted source code as well as the analysis to find the right correction is a time consuming task. Neither testers nor developers have security expertise and time to execute these tasks in a regular manner. "*
>
> *L. Porchon MBS Information Security & Banking Certification, Parkeon*

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.

Why Seeker ?

Seeker ensures that the entire system end to end complies with security standards such as PCI-DSS at each release

Seeker follows the data flow throughout all of the application and evaluates 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, unsecure manipulation, unsecure storage - even temporarily - in files or database, unsecure transmission to third parties etc.)

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

Seeker facilitates the communication between test and development teams

Seeker automatically ties vulnerabilities as they appear to a hacker to the originating vulnerable code. It eliminates false positives, pinpoints the vulnerable source code and provides clear remediation tailored to the tested application.

Consequently, it improves security, reduces the time spent on security testing and improves communication between security and R&D:

- Developers focus their time on proven vulnerabilities and source code corrections proposed by Seeker.
- Testers have a clear view of business risks of the application tailored by OWASP Top 10 criteria, Parkeon's corporate security standard.

Seeker improves awareness and training for more secure coding practice

Another reason Parkeon chose Seeker is for the educational value it provides. 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 attacks, explanation of business risks and relevant remediation to apply, Seeker helps the test and development teams to acquire awareness and training in an ongoing manner, thus improving the security of their code.

Conclusion

Parkeon teams needed a security automation process to ensure that each release sent to production is secure and compliant. Seeker successfully fulfills Parkeon's requirements.

> *"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 MBS Information Security & Banking Certification, Parkeon