FLYERALARM

RIPSTECH

CASE STUDY

LEADING GERMAN E-COMMERCE COMPANY SECURES WEB SHOP AND CUSTOMER DATA

SUMMARY

- PHP e-commerce software with up to 2.5 MLOC
- Security scans in less than 20 minutes
- Easy integration into Bamboo, JIRA, PhpStorm
- Multiple developer hours saved per day
- Only 1-2% false positives

PROFILE

FLYERALARM was founded in 2002 and is one of the leading online printing companies in the B2B market in Europe and is one of the largest e-commerce companies in Germany.

FLYERALARM now employs over 2,300 staff and generated a turnover of more than 350 million euros in 2018.

Today, FLYERALARM not only supplies print products, but also marketing services and advertising media of all kinds in 15 European countries.

SOLUTION

FLYERALARM selected RIPS On-Premises as their static application security testing solution and integrated its efficient code analysis into their SDLC.

THE CHALLENGE

At FLYERALARM, around 15,000 products and 24,000 dispatches are coordinated on a daily bases by a PHP-based web shop and backend that drives the major revenue of the company. Every day, the complex code base is customized and advanced by 80+ developers to meet new customer needs. All code changes require a security assessment to ensure the highest standards in data privacy, integrity and availability, including GDPR and PCI DSS requirements. A breach of personal data and payment information or a shop downtime would put the company's reputation and business at risk.

THE ALTERNATIVES

FLYERALARM previously used Dynamic Application Security Testing (DAST) solutions, such as OWASP ZAP and Burp Suite, to automate the error-prone and time-intense manual code review. But unfortunately, the tools' runtime and involved staff resources to deploy and scan all code changes became highly inefficient. Moreover, not all code parts and issue categories were covered. At the same time, the progress in security could not be permanently measured. Slowing down in innovation and development or relaxing the company's high security standards was not an option.

THE REQUIREMENTS

FLYERALARM sought a static application security testing (SAST) solution to fully automate the security reviews of their source codes. The SAST software was required to have strong support for the dynamic PHP language, run on-premises and have the ability to detect a broad spectrum of critical security issues across a large code base. Further, for an easy adoption among the developers, it should seamlessly integrate into the existing CI pipeline and IDE, provide a user-friendly interface and easy to follow remediation instructions for developers with different skill sets in security.

FLYERALARM

RIPSTECH

CASE STUDY

THE SELECTION OF RIPS

After an evaluation, FLYERALARM selected RIPS On-Premises as the only SAST solution with a dedicated focus on the complex PHP language. Already at an early stage, RIPS proved value with lightning-fast scans, meaningful results and accurate detection of selected security issues in historical code bases. With a variety of plugins and an API, good documentation and a straightforward support team, FLYERALARM was convinced that RIPS will be easily integrated into the existing development process to aid code reviews.

THE IMPLEMENTATION

FLYERALARM setup a virtual machine with 32 GB of memory. The initial container-based installation of RIPS completed within 10 minutes. In an initial phase, RIPS API was used to initiate a nightly scan of the source code. While the initial findings were evaluated in the user interface of RIPS, the security architects then integrated RIPS into their IntelliJ PhpStorm IDE to easily patch initial findings. After observing good performance results, FLYERALARM decided to decrease the recommended memory from 32 GB to 16 GB. With the help of analysis settings, warnings in components of external libraries such as debug tools were omitted.

In a second phase, RIPS was integrated into the Bamboo CI/CD pipeline via a plugin that triggers security scans on every build. The plugin was configured to fail a build whenever RIPS detects high-severe or critical security issues in the build‘s code. Finally, RIPS was integrated into the JIRA bug tracker to synchronize all severe security findings in tickets. The integration and configuration took only a few minutes up to 1 hour per integration point. FLYERALARM plans to expand RIPS integration into all developer’s IDE so they can autonomously patch security issues that affect their own components.

THE RESULTS

FLYERALARM scans its large applications with 1.8 and 2.5 million lines of code in only 12 and 20 minutes. Developer mistakes are now reliably detected and reported as early as possible, even when deeply nested within multiple layers of code. With the help of RIPS issue summary and unique context view, the heart of each security issue is easily understood and navigated through in PhpStorm. After an upgrade from RIPS 2.7 to RIPS 3.0, FLYERALARM was happy to use the revised remediation instructions with concrete patch examples. The false positive rate was measured to be at only 1-2%. Further, the usage of RIPS revealed issue categories that are not well known among all developers yet which are addressed with workshops.