Is PHPKB software developed using common secure coding practices?

240 Ajay Chadha June 29, 2020 Pre-Sales FAQ 1617 0

Our software development team follows industry-standard security programs and follows well-known security best practices to prevent common coding vulnerabilities and to minimize security errors in the PHPKB software. Our development process includes peer review and static code analysis to mitigate the risk of security errors. Our process includes practical validation of security through both automated and manual testing. Our knowledgebase software is periodically subject to external security audits with a rich history of excellent results. We maintain a diligent, pragmatic approach to ensuring high levels of security in the knowledge management software that we deliver.

Specific security tactics include but are not limited to the following:

1. Follow secure coding practices as recommended by OWASP, Microsoft, and other resources
2. Provide training to engineers for secure coding practices
3. Enable security flags and high warning levels in the development environment to enforce the use of secure functions and types
4. Maintain and follow a Security Vulnerability Assessment and Response Process
5. Monitor security industry watch lists for known vulnerabilities
6. Run security scanners against various protocols and interfaces
7. Integrate security verification into the quality assurance process
8. Track and monitor potential vulnerabilities in a bug tracking system
9. Employ tools to automatically catch potential coding and security issues
10. Follow a process to review and update third-party libraries for major releases
11. Implement security-related unit testing and automated testing to prevent accidental breakage

Online URL: https://www.phpkb.com/kb/article/is-phpkb-software-developed-using-common-secure-coding-practices-240.html