Are GlobalSCAPE's applications being developed using common secure coding practices?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- All GlobalSCAPE products

QUESTION

Are GlobalSCAPE's applications being developed using common secure coding practices?

ANSWER

GlobalSCAPE takes application security very seriously, adhering to generally accepted application security standards as set forth by OWASP, Microsoft, and others, in order to prevent common coding vulnerabilities and to minimize security errors.

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

- Follow secure coding practices as recommended by OWASP, Microsoft, and other resources
- Conduct "brown bags" for engineers regarding secure coding practices, including classes offered by third-party security firms
- Provide off-site training for engineers for secure coding practices
- Enable security flags and high warning levels in the development environment to enforce use of secure functions and types
- Maintain and follow a Security Vulnerability Assessment and Response Process
- Monitor security industry watch lists for known vulnerabilities
- Run security scanners/fuzzers against the various protocols and interfaces
- Integrate security verification into the quality assurance process
- Track and monitor potential vulnerabilities in a bug tracking system
- Employ tools such as FindBugs and PMD to automatically catch potential coding and security issues
- Follow a process to review and update third-party libraries for major releases
- Implement security-related unit testing and automated testing to prevent accidental breakage

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11061/Are-GlobalSCAPEs-application...