

SECURE CODE AUDIT

With the increased exposure of firms to online presence comes a barrage of security concerns to be addressed. As more and more people join the online community, web applications and network dependent software fall under heavier scrutiny by all types of people. This adds a heavy burden on companies that choose to develop in-house software since the sole responsibility of the security of such software weighs only upon the said company's shoulders.

So, is the threat large enough to be considered in your security model? According to a September, 2004 press release by Gartner, "Organizations that don't include security as a criterion when building or buying software will see system downtime caused by security vulnerabilities grow from 5 percent of downtime in 2004 to 15 percent of downtime in 2008", thus keeping security in mind while developing applications is the first step to dispelling future security concerns and costs.

Security steps into your Software Development Life Cycle (SDLC), and thus your application, through Source Code Security Audits. A source code audit allows you to locate and root out possible security concerns in your software; a task that most developers are not adept at performing because their focus is upon the software's functionality and the scheduled release date. A separate team-usually a consulting group-is ordained to validate the development effort from a security perspective.

Through their extensive research and knowledge in software vulnerabilities and exploitation methods, our consultants are able to best utilize code auditing tools to weed out the vulnerabilities in developed software. After analyzing the code in question, our consultants present their findings to the development team in a report outlining all the security threats found in the code along with possible remediation methods for each threat. Security issues found by our consultants are rectified by the development or support team and another code audit is run to ensure that no new vulnerabilities were introduced during the modification of the software.

The code audit becomes an integral part of the SDLC from then on. For as long as the software is in use and supported, support personnel develop patches and consolidate the changes into new versions. A code audit should take place before each new version of the code is released to ensure that no security issues were introduced after any major modifications.