Effective Application Security Testing at High Velocity: Keeping up with Agile/DevOps

February 28, 2017

Q: Do we have fortify plugins for Visual Studio too?
A: Yes. Visit the Fortify Ecosystem for the latest plugin's and more.

Q: Do you recommend using both SAST and DAST? Or do we really need one or the other?
A: Yes. SAST is meant for source code while DAST tests a working application. Each can find vulnerabilities that the other may not.

Q: What about IAST? Do you recommend using IAST?
A: IAST is a great tool to provide greater insight back to the developers than what DAST alone could provide. WebInspect customers can use the WebInspect Agent for IAST testing.

Q: What is the difference between Security Assistant and SCA scan IDE?
A: Security Assistant is a feature found in SCA and DevInspect, a stand-alone developer workbench. Security Assistant provides spell-check-like functionality to help the developer find and fix vulnerabilities as they write the code – all without leaving their IDE. The plug-in is available on the Fortify Ecosystem.

Q: Is Dynamic Analysis more effective than PEN Testing?
A: Dynamic Analysis is essentially automated Penetration testing but DAST is much more scalable and cost effective than scarce and expensive pen testers. Typically organizations will still pen test critical applications on an infrequent basis but will rely on automated dynamic testing to more frequently test a larger set of their applications.

Q: Can FOD log bugs/defects directly to ALM Quality Centre?
A: Yes.

Q: Is the speaker saying RASP? Runtime Application Self-Protection?
A: Yes, Runtime Application Self-protection (RASP)

Q: Why is the IDE scan lightweight compared to SCA scan on server?
A: Some enterprises will use a lightweight scan, stand-alone on the developer's workbench because they are just beginning an app sec journey and want to quickly arm developers with helpful information and tools. Others want to extend the reach of their existing app sec program getting more developers engaged via lightweight scans without enlisting them in the full breadth of app sec.

Q: When should DAST start in SDLC? Is this a tool primarily for developers or app sec team?
A: DAST requires a working application. That would be the earliest you could apply it. Developers really need to take a greater role in the security of their applications. Typically app sec is the champion but dev and QA are the users.

Q: What was the name of the article by Jason Schmidt in dark reading?
A: http://www.darkreading.com/application-security/software-security-is-hard-but-not-impossible/a/d-id/1321726