

Asking the Right Question: Penetration Testing vs. Vulnerability Analysis Tools, Which Is Best?

Over the past several years I have heard people asking the question “should I use vulnerability analysis tools to assess my web based applications or should I look to penetration testing?” I think we, as an industry, may be asking the wrong question. First, let’s look at how the web application industry has grown over the years and how penetration testing has scaled to meet that challenge.

Pre-2000

Before the year 2000, some companies had a web site for marketing purposes and a few companies were starting to do a little business on the web. There were of course a lot of DotComs around selling things on the web, but real “brick and mortar” businesses were just using the web as a marketing tool. The brick and mortar businesses who understood security started asking their experts in penetration testing to check out these web applications. Using some simple vulnerability analysis tools, those penetration testing experts did a good job checking for simple web application security issues. There were a few people running around that really knew how to test a web application, but not many. At this time, there were a few open source vulnerability analysis tools in existence, but the market was in its infancy.

Early 2000s

After the DotCom bust, companies actually started to use the web and web-based applications for both internal and external applications. Most applications still existed on non-web-based platforms, but developers started moving their legacy applications into web-based environments. Developers found that creating a web-based application was a bit more complicated, but deploying it via a browser made it all worthwhile. In addition, customers now wanted to transact their business via the web, and as a result, companies started to provide some of their services via a web application.

Security commonly responded to this change in one of two ways. One approach that worked was to hire or contract more penetration testing experts and to try to test all web-based applications before they went live. This worked in some cases, but usually there was not enough support for the penetration testing so only critical applications were tested, leaving non-critical applications open to attack. The other approach was to assess the web-based application with vulnerability analysis tools before it went live. This approach scaled much better than the penetration testing route, but would frequently miss vulnerabilities that really should have been discovered.

Usually, a combination of stand-alone vulnerability analysis tools and penetration testing was used in an attempt to get full application coverage. This yielded good results, but most security organizations were still quickly overwhelmed by the number of web-based applications that needed to be assessed. Also, this approach typically found vulnerabilities after the application had been developed, tested and was ready for production. This frequently caused companies to go live with vulnerable applications or go back to development and fix the issue.

The Right Question (Where we are today)

Today, the problems of the early 2000s have only worsened. The proliferation of web-based interfaces and applications has spread to every part of our lives and businesses. With this growth, we are not only seeing new groups within companies

use web-based applications, but we are also seeing that these same groups are using web-based applications for everything they do on the computer. And these applications are also becoming more complex.

When faced with this type of environment, many web application security experts ask the question, "Should I use vulnerability analysis tools or hire more staff for penetration testing?" I think this is the wrong question. What we should be asking is, "If I have so many people developing web-based applications, how do I get them to do it in the secure way?" The people involved in creating the web-based applications will need to become part of the solution, not the cause of the problem. Developers and QA testers will need to understand how to develop a web-based application that is secure, and they will need vulnerability analysis tools to help them verify that they are doing the right thing. And providing developers with an automated way to test their applications can help them find web application security issues much earlier in the process.

Training for QA professionals is also critical. These professionals need to know how to look for web-based security issues and then need to have vulnerability analysis tools that help them test for security issues. They also need a way to integrate these vulnerability analysis tools into their existing defect tracking systems. This integration allows for tracking of issues as well as generating metrics around what type of issues are being created by the developers.

At the enterprise level, we need ways to assess applications that are in production and understand what the enterprise looks like from a web application security perspective. These tests should include issues resulting from development, QA and production, as well as the in-depth data that penetration testing will continue to generate. Having an enterprise view allows executives to understand where their risks are and what an appropriate response to the risks should be.

As for penetration testing, it will continue to be a core part of the web application security landscape. The fact is that there are some web application security issues that vulnerability analysis tools just don't do a great job of finding. These vulnerability analysis tools get better every day but they have a long way to go before they can be considered a "mature" product family. The web application security assessment industry is still quite young and the security landscape is changing quickly.

The fact is, the need for those experienced in penetration testing will continue to increase. We will need them to continue to do more assessments and to do more in-depth assessments that vulnerability analysis tools will not be able to fully execute. We will also need them to train developers and QA professionals in how to test web-based applications. Web application penetration testing is still a rare skill that vulnerability analysis tools cannot replace, and we need the people that are creating the web-based applications to develop applications more securely and to help develop processes to promote and verify the security of applications.

Summary

This article sought to explain why the question "Should I use penetration testing or vulnerability analysis tools to assess my applications," that is so often asked, is no longer valid. The question is bigger than it used to be and the answer is more complex than ever. It gets down to people and process, and it becomes about making web application security a natural part of the way applications are developed.

About the Author

Dennis Hurst is a Developer Security Evangelist for [SPI Dynamics](#) where he works with development organizations evangelizing the need to integrate [web application security](#) into their Web development processes. A Microsoft Developer Security MVP, Dennis has more than 15 years experience in the Information Systems/Application Development industry, and he is an expert in computer applications and networks.