synopsys.com

Badness-ometers are good. Do you own one? | Synopsys

Gary McGraw

4-5 minutes

Posted by on Monday, March 19th, 2007

Badness-ometers, or black box application security testing tools, are good. But you have to do more than just fix the code issues your badness-ometers find.

Never one to mince words, I coined the term *badness-ometer* to describe “application security testing tools” like the ones made by SPI Dynamics and Watchfire. For whatever reason, people read more into the term than I intended. I guess they see the term as having only negative connotations. I stick by my nomenclature —black box application security testing tools are in fact badness-ometers—but badness-ometers are a good thing and everyone should use them!

Here’s part of what I wrote about badness-ometers in my book *Software Security*:

That said, application security testing tools can tell you something about security—namely, that you’re in very deep trouble. That is, if your software fails any of the canned tests, you have some serious security work to do. The tools can help uncover known issues. But if you pass all the tests with flying colors, you know nothing more than that you passed a handful of tests with flying colors.

Put in more basic terms, application security testing tools are “badness-ometers,” as shown in [the Figure below]. They provide a reading in a range from “deep trouble” to “who knows,” but they do not provide a reading into the “security” range at all. Most vulnerabilities that exist in the architecture and the code are beyond the reach of simple canned tests, so passing all the tests is not that reassuring. (Of course, knowing you’re in deep trouble can be helpful!)

I also wrote an article for Dr. Dobbs called Beyond the Badness-ometer. That article stresses the fact that solely relying on a badness-ometer as your only software security activity is a really bad idea.

Why you need badness-ometers

So what’s good about badness-ometers, and why do I think you should buy one right away? Well, many organizations that build software are woefully in the dark about their software security risk. A badness-ometer can do wonders to turn the lights on with respect to software security, especially when it comes to web applications.

The sad fact is that many purveyors of web applications believe that their apps are “bulletproof” if they use simple security features like authentication and SSL. Of course we all know by now that software security goes well beyond security features and deep into enemy territory, concerning itself with things like software defects (bugs and flaws) that lead to software security failure and unacceptable business consequence. Badness-ometers can help expose this "myth of security features" for what it is—a myth—by automatically attacking and taking down web applications through obvious everyday security tests. Automated testing is cheap and sometimes powerful.

The great irony of badness-ometers is that you can be sure that your enemy will use them. In fact, throughout the decade that I have been practicing software security, bad guys have been more adept at adopting advanced tools and techniques than the good guys generally have.

When it comes to deciding whether your organization needs a badness-ometer, you should ask yourself whether you already know your software is at risk or whether you need some more convincing. If you, or anyone else in your organization, need more convincing, grab a badness-ometer and find out whether your code is in "deep trouble." I bet it is.

If you are using a badness-ometer today, and it's finding issues in your code, don't simply fix the issues and call it a day. Never forget that the badness-ometer can't tell you that you're secure. It can only tell you that you're not. To get beyond simple badness-ometer tests or to fix the problems that your badness-ometer is finding, seek professional help from Synopsys.

Learn more about professional services for software security