Beware of Relying on Tools Alone to Secure Web Apps

The demands of regulatory compliance may have you looking to vulnerability scanning tools in the hope of finding a magic bullet to vet your web applications. However, it would be unwise to expect scanners alone to accurately determine the impact of the web application vulnerabilities they detect. While the latest and greatest scanning tools promise the world, the reality is they only function well when configured and utilized correctly.

The scanner can provide clues, but it lacks the ability to determine where those clues lead. Tools are excellent at catching basic cross-site scripting and SQL injection errors, but the report you get back inevitably will contain a high number of false-positives. Without the trained eye of an experienced security auditor to interpret the results, your development staff will be at a loss to prioritize bugs and create an actionable remediation strategy.

Another drawback of automated vulnerability scanners is their inability to string together several low-risk issues to create a high-risk vulnerability. This is where hands-on penetration testing is especially critical. For example, during a recent audit of a client's website we detected two cross-site scripting vulnerabilities, which the scanner flagged as low- to medium-risk. However, the penetration tester was able to combine these code flaws to hijack sessions and manipulate user data.

Like any reporting tool, scanners have programmatic limitations that prevent auditing for logic problems; for example, they generally do not detect when a CAPTCHA image can be bypassed. One of the dangers here is that a malicious user can create multiple new user accounts simply by clicking the browser's Back button repeatedly. Another type of logic problem that isn't detected by scanners involves the ability to change the user ID and return someone else's data by altering the value in the URL. These simple examples illustrate how easy it is to punch holes in an otherwise airtight system.

At this point you may be wondering if it is even worth purchasing a vulnerability scanner. The answer is yes, but look before you leap—tools often get shelved because the IT staff doesn't know how to configure them. If you don't have an experienced security team in place, consider hiring a reputable auditing firm to assist with the selection and implementation of your scan tool. You may be surprised to learn that the best options are often the lowest priced.

Scanners are handy because they provide a record of tests performed. By documenting information—like the exact structure of a query used to produce an SQL injection error—they save valuable time when trying to reproduce the error by hand or across teams. Scanners also provide a degree of confidence for their report results, which helps testers identify areas that deserve a closer look.

All of the popular web application scanning tools on the market profess to be accurate, but unlocking this potential often calls for the trained eye of an experienced penetration tester. Think of your scan tools as the starting point in your security audit: let them do the initial grunt work of sorting through your web application, but don't fall victim to the myth that tools alone can adequately assess your website's security posture.

About IOActive

Established in 1998, IOActive is an industry leader that offers comprehensive computer security services with specializations in smart grid technologies, software assurance, and compliance. Boasting a well-rounded and diverse clientele, IOActive works with a majority of Global 500 companies including power and utility, hardware, retail, financial, media, aerospace, high-tech, and software development organizations. As a home for highly skilled and experienced professionals, IOActive attracts the likes of Barnaby Jack, Ilja van Sprundel, Mike Davis and Michael Milvich—talented consultants who contribute to the growing body of security knowledge by speaking at such elite conferences as Black Hat, Ruxcon, Defcon, BlueHat, CanSec, and WhatTheHack. For more information, visit www.ioactive.com