Acunetix Web Vulnerability Scanner

A comprehensive set of security tools in one package, with a convenient and easy-to-use interface

An organisation’s web presence can be a source of problems as well as revenue. Some problems such as site defacement are obvious and easily dealt with, but others may not even be noticed, and these can do far more damage. A successful SQL injection attack will leave few traces, but it can hand the contents of your company’s database over to the attacker. New vulnerabilities come to light almost every day, and keeping on top of them can be difficult. The Acunetix Web Vulnerability Scanner software runs security scans against a website, testing for known vulnerabilities. Operating in much the same way as a hacker, it can mount attacks based on what it finds.

We tested the scanner on some websites that were under active development but not yet live. The results were surprising, and at first sight depressing, with one site returning no less than 138 alerts, of which 39 were classified as “high”. However, not all alerts are equal, and several were potential rather than actual problems. As with all security scans, the results need to be interpreted, and the software went to great lengths to explain what the risks might be. Even more information and suggested remedies were provided in the reports generated by the system, backed up by links to useful reference sources on the web.

The software can scan for a wide range of known security flaws, ranging from simple version checks and parameter manipulation exploits, such as HTTP splitting, to cross-site scripting and SQL injection vulnerabilities. It also checks the site structure, looking for broken links, weak directory permissions and other potential security gaps. AJAX applications aren’t ignored, and the site crawler will analyse and execute JavaScript files as it builds up the site profile. Acunetix also makes use of the hacking database maintained at http://johnny.ihackstuff.com, which contains lists of search queries that can return data useful to hackers.

Scanning is controlled by profiles that can be used to restrict it to relevant operations. The default profile will scan for everything, while other options will concentrate on specific areas such as version checks or SQL injection. Automated scanning will detect most problems, but Acunetix has provided tools to help construct more specific tests. The HTTP editor can be used to build SQL injection or cross-site scripting attacks. The HTTP sniffer can record web traffic for use in more complex attacks. The HTTP fuzzer checks for buffer overflows and flaws in input validation scripts, while the authentication tester tool can access the strength of any passwords used to validate users through HTML Forms or HTTP Authentication.

Evaluating website security is never easy, and Acunetix has provided a range of tools to help. Hackers almost certainly can and will run similar scans against your website at some time, and they won’t share the results with you. With this software you can know what they know and act accordingly.

IAN PARSONS