AppScan

by Geoff Marshall

Version: 2.5
Supplier: Sanctum, Inc.
Contact: (408) 855-9500
sanctumsales@sanctuminc.com
www.sanctuminc.com

FOR *AppScan* actually tests application vulnerabilities by attacking a web site to avoid time being wasted on 'theoretical' vulnerabilities or false positives.
AGAINST Great care should be taken because full testing must be carried out off-line. *AppScan* is designed as an off-line tool; some of its attacks could adversely affect a live web site.
VERDICT *AppScan's* automation, ease of use and comprehensive reporting already recommend it above other vulnerability scanners, but its key differentiator is its ability actually to attack the web site and thereby identify the real as opposed to 'theoretical' points of risk.

Features	★★★★★
Ease of use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★☆
Value for money	★★★★☆
Overall Rating	★★★★★

AppScan is designed to perform an automated security risk assessment of web-based applications to determine weaknesses that could be exploited by hackers. In this way, it provides the information to enable you to plug the security holes that could otherwise permit defacement or other damage to your web site.

Installation is straightforward as *AppScan* comes with its own copy of the Debian Linux operating system under which it must be installed on a dedicated Intel-based machine. The web-browser user interface makes it easy to configure and use. Before starting an audit session you have to clear your browser's cache as otherwise already cached pages may not be logged in the database. While we appreciate that cache clearing is browser-specific and it is therefore probably impossible for *AppScan* to clear the cache automatically, it would be nice if it provided interactively a warning to the user to do so – the documentation makes this clear, but not everybody reads the manual. *AppScan* then performs the risk assessment in four stages: Crawl, Analysis, Attack and Reporting stages.

Crawl involves *AppScan* discovering web applications and gathering information about them. It identifies bespoke as well as off-the-shelf applications. To start 'crawling,' you simply have to enter a list of the web site URLs to be investigated, and you can append any non-standard port numbers that they may use. Then it explores every link within the target web site, or fewer if configured to do so by filters or other limits. If *AppScan* encounters the sort of forms that many web sites use to register users before allowing them entry, it can even be configured to fill in forms automatically and intelligently with test data which you have supplied during configuration. *AppScan* also supports the delivery of a client certificate that is required by web sites that use SSL to authenticate the user, which in this test scenario would be *AppScan*. During crawling a progress indicator informs you of the current link being crawled, as well as the total of visited, interactive and filtered links.

Analysis requires *AppScan* to use its expert system to identify possible web site vulnerabilities. It does this by creating what it calls 'mutations,' which are attack profiles – the sort of unexpected input that a hacker might try to bring down or break into a web server. Mutations include things such as attempts to cause buffer overflows, direct entry of URLs that should be protected by links from an opening page that demands a password but which may be bypassed.

Attack involves performing tests using the mutations, which have been created from the vulnerabilities identified in the Analysis stage. The success or failure of these test attacks is recorded, together with the assignment of a severity level that indicates the seriousness of the vulnerability. Both the Analysis and Attack stages feature progress indicators to keep the operator informed.

Reporting generates pre-defined reports, which also include advice on how to fix any security problems found. Some of the reports that can be easily produced include Vulnerabilities Highlights and Executive Summary, as well as incredibly detailed reports on vulnerabilities and suggested fixes. Results can also be displayed graphically as pie and bar charts, etc. All reports are generated in HTML format to be displayed, printed or saved. There is a sister product called *AppShield* that can automatically protect your web server from most hacker exploits, and the reporting engine of *AppScan* also informs you whether *AppShield* would be effective in automatically protecting against each detected vulnerability.

All stages can be run automatically or manually. Manual (interactive) mode enables you to be selective in what tests are carried out and to modify your approach as the audit progresses. Even reports can be modified in the light of a manual test if you disagree with *AppScan's* estimated attack success. However, no manual intervention is necessary – it is merely an option to provide experienced users with more control. You can just let *AppScan* run each stage automatically and then look at the reports generated.

Automatic mode offers you the opportunity to specify all the filters and configurations for the Crawl and Attack stages at the outset using a wizard. When completed, the Reporting stage generates the results automatically and displays them. Interactive (manual) mode allows each stage to proceed at your own pace while you fine-tune the process as it progresses and re-run selected tests.

AppScan must be carefully used because it does actually attack the web site to test for vulnerabilities. Some test attacks are categorized as 'safe' and may be used on live servers but a full security audit would require the use also of 'unsafe' tests. So it is not advisable to use it on a live online web server and it is also advisable to have a back up of the web server.

To avoid misuse, *AppScan* is tied by its licensing to scanning certain agreed domain names and IP addresses. *AppScan* itself is further protected from abuse against your own domains by requiring users to log in with username and password. A single installation of *AppScan* can be configured to have a number of users, but these users do not have different permissions – they are there only for tracking who did what in the logs and reports.

Compared with other vulnerability scanners, *AppScan* differentiates itself by actually attacking the site rather than just reporting possible security loopholes. This approach greatly reduces false positives because it reports only vulnerabilities that could be exploited with a high probability of success. *AppScan* is equally suitable for use by corporate IT security managers, service providers and outside security consultants.

Contact Information:

Sanctum Inc.

SANCTUM

2901 Tasman Drive, Ste 205
Santa Clara, CA 95054
408-855-9500
www.SanctumInc.com