



SECURE ENTERPRISE

BUILDING TRUSTED BUSINESS

WWW.SECUREENTERPRISEMAG.COM | VOL.2 ISSUE 9 | SEPTEMBER 2005

EASY TARGET

Web application vulnerability scanners make your sites harder to hit. We tested three products. See how they scored



EASY TARGET

If you aren't performing regular Web vulnerability testing, your company's sites are sitting ducks. Trust us—this is the voice of experience talking **BY JEFFREY H. RUBIN**

Two weeks too late! Just before we began testing Web application vulnerability-assessment tools, three of our servers two Windows 2000 boxes and one Windows 2003 box were successfully attacked.

All three reside at Internet Consulting Services, a Web application development company located on the Syracuse University campus and affiliated with our Real-World Labs®. One Windows 2000 box was running Microsoft IIS 5.0 and had about 150 Web profiles on it; the other 2000 server was running Microsoft SQL Server 2000 with about 75 databases. The Windows 2003 mail server runs Microsoft Exchange 2003. Had we started testing a couple of weeks earlier and addressed the vulnerabilities these products revealed, we could have saved a lot of time and money.

We're like most Web developers who use the Microsoft platform: Our Web applications are written mainly in ASP and, more recently, ASP.Net. Although we try to stay up to date with patches and services packs, we realize attackers often go after application, rather than network, vulnerabilities. A colleague suggested we install a hardware firewall to prevent future attacks. Not a bad suggestion, but hardly a cure-all given that we have Ports 21, 80 and 443 and our SQL server (on a nonstandard port) wide open for development purposes. After all, we're in the business of developing dynamic Web pages, and our clients are all over the country.

Any organization that sets up a Web site, whether it's static or dynamic, assumes a certain amount of risk. Yes, a dynamic site is a greater liability than a static one because of its server-side programming and database components. Regardless, learn from our pain: Consider implementing one of the three Web application vulnerability products we tested.

Better Late Than Never

We sent out a call for vulnerability-testing software for Web applications. We wanted products that perform vulnerability testing on database and Web servers and on custom Web programs, and that create custom policies and/or have extensive policy libraries. We told the vendors we would be performing vulnerability testing against Web servers and Web applications written in a variety of programming languages, including .JSP, .Net, .ASP and Cold Fusion, in our office at Syracuse University.

Any organization that sets up a Web site, whether it's static or dynamic, assumes a certain amount of risk.

Cenzic, SPI Dynamics and Watchfire agreed to participate. Kavado declined, saying it plans to sell its intellectual property and get out of the race.

We downloaded Watchfire's AppScan Audit 5.0 and SPI Dynamics' WebInspect 5.5 from the vendors' sites and installed Cenzic's Hailstorm 2.6 from CD. Interestingly, we found out while testing that Watchfire had sold its application firewall to F5 Networks in May but had kept its application scanner.

We rated each offering on functionality, policy management and vulnerability testing, reporting, and price; see "Methodology," page 3, for further information.

THE ESSENTIALS

We tested Web vulnerability scanners at Internet Consulting Services, a Web application-development company affiliated with our Syracuse University Real-World Labs®. There was a bittersweet quality to our evaluations because just two weeks before testing commenced, three of our servers were successfully attacked. Not surprisingly, we strongly recommend that you consider one of these scanners. All perform vulnerability testing on database and Web servers and custom Web apps written in a variety of programming languages, plus they provide policy editors to create rules.

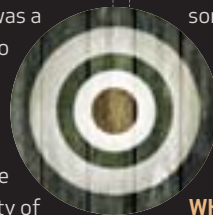
PRODUCT CATEGORY: Web vulnerability-assessment tools

PRODUCTS TESTED: Cenzic Hailstorm 2.6, SPI Dynamics WebInspect 5.5 and Watchfire AppScan Audit 5.0. Kavado declined to partici-

pate, saying it plans to sell its intellectual property.

WHO WON AND WHY: Watchfire AppScan could easily be used by someone with little or no security background, but in terms of functionality, it's not as powerful as its rivals. Cenzic Hailstorm is plenty powerful, but you'll need serious security chops to use it. Our Tester's Choice, SPI WebInspect, strikes a perfect balance between ease of use and powerful protection.

WHAT HAPPENS NEXT: Through the second half of next year, fewer than 20 percent of successful Web server attacks will take advantage of vulnerabilities in Web server code, according to Gartner. A key factor in Web server security: The quality of enterprise vulnerability-management processes for the OS used to host Web servers. So run these scanners, but pay attention to patching too.



Let the Games Begin

We began our tests by banging on the policy editors included in each product. With these tools, policy management entails setting up rules and tests for specific vulnerabilities that might be found in Web applications. Cenzic's Hailstorm led the pack here because it let us edit the actual JavaScript code of the product's numerous canned policies (after making a copy of the original, of course). We didn't quite have the nerve to really dive into the JavaScript code, but we did review the JavaScript policies and were impressed with the comments and details Cenzic provides.

SPI's WebInspect Policy Manager was a strong finisher here as well, thanks to its flexibility—we could drill down to a specific type of vulnerability for which we wanted to test. For example, we started with the OWASP (Open Web Application Security Project) Top 10 Web application vulnerabilities, then drilled down to cross-site scripting

Reporting is an essential component of any vulnerability scanner, particularly when you're running hundreds of tests against each Web application.

flaws. We were amazed to find that we could tell WebInspect to run checks using only single quotes, double quotes or various JavaScript injections.

In contrast, Watchfire's AppScan let us choose attacks on a group basis only. Specific details were scant. We used a global preference in the software to choose from one of 16 groups of tests that would be performed; however, we couldn't find a way to view the details of what would be performed in each group test. Watchfire representatives explained that this setup contributes to the product's ease of use.

Once we defined the policies or checks for which we wanted to test, we started scanning. WebInspect's performance is similar to Cenzic Hailstorm's—both provide an interactive results pane that shows what's happening during the scan. Unfortunately, Watchfire AppScan kept us in the dark until after the scan had completed. In addition, though the other two products offer some type of HTTP editor, WebInspect's is the most intuitive and powerful; we could change the URL parameters and content length, and even try to *put* (upload) a file through a Web page and see the results.

Post-scan processing of results was good across the board. This was AppScan's strongest area. For example, where the results showed that we may have cross-site scripting vulnerabilities, AppScan did a good job explaining the impact and recommended fixes, though we preferred the level of detail and recommendations provided by Cenzic Hailstorm, where for a particular potential vulnerability, we could

click into manual testing to change HTTP headers, query parameters, cookies and body information. We could then retest the application and compare the new results to the initial response, and continue making adjustments.

Reporting is an essential component of any vulnerability scanner—when you're running hundreds of tests against each Web application, it's important to have reports detailing the severity and risk of each potential vulnerability. Again, WebInspect led the pack, providing plenty of predefined reports as well as seven customizable templates, ranging from a comprehensive report to a basic one. We also could create a template based on the categories and subcategories of information we wanted to include. Hailstorm and AppScan lack flexibility here, allowing for only minor configuration changes in their plain-vanilla reports. Still, both Hailstorm and AppScan let us export reports to a range of options, including Crystal Reports, whereas WebInspect was limited to exporting to a PDF file.

Clear Choices

We were pleased that all three products returned few false positives. If your environment is new to vulnerability testing, you won't go wrong with any of them. Cenzic's Hailstorm is the most in-depth and therefore is recommended for the hard-core Web security analyst, who will appreciate its granularity and customization options. Hailstorm is quite powerful, and we were impressed with its configuration, reports and overall management. However, its new GUI still has a way to go.

On the other end of the complexity spectrum is Watchfire's AppScan. Although not as detailed or as customizable as Hailstorm or WebInspect, AppScan is simple to use. Watchfire has tried to make AppScan accessible, but the product has paid a price for this simplicity, lacking the vulnerability and security assessment detail most IT analysts look for.

Like baby bear's porridge, SPI Dynamics' WebInspect is just right and wins our Tester's Choice award. From installation to reporting, the product is both powerful and easy to use. The GUI is functional, and the software is feature-rich and extensible. Updates are abundant, and no restart is required afterward.

One note: Cenzic has announced a new managed version of its software, unique among the products we tested. Organizations simply supply the host name of the Web application they want to test and work with Cenzic's specialists to pick out the policies they want to run. Cenzic then runs a managed version of Hailstorm against the Web application. Once the scan is completed, Cenzic produces a report and sets up an information session with the organization on its findings. Pricing for this service starts at \$6,000 per Web application.

Speaking of pricing, note that what's listed for all three products we

REAL-WORLD
LABS®

REPORT CARD / WEB VULNERABILITY SCANNERS

	SPI Dynamics WebInspect 5.5	Cenzic Hailstorm 2.6	WatchFire AppScan Audit 5.0
MANAGEMENT AND CONFIGURATION (35%)	4.5	3	2.5
POLICY EDITING (25%)	4	5	2
PRICE (20%)	4	3	2
REPORTING (20%)	5	2.5	3
TOTAL SCORE (100%)	4.38	3.30	2.38

A≥4.3, B≥3.5, C≥2.5, D≥1.5, F<1.5
A-C GRADES INCLUDE + OR - IN
THEIR RANGES. TOTAL SCORES AND
WEIGHTED SCORES ARE BASED ON A
SCALE OF 0-5.

A⁻

C⁺

D

Customize the results of this report card using the Interactive Report Card®, a Java applet, at www.secureenterprisemag.com.

tested is yearly—you must make the financial commitment to keep these testers up to date. Otherwise, it's like running last month's antivirus signature.

SPI Dynamics WebInspect 5.5

by performing a smart update, which is similar to a virus-definition update in that it downloads new components of the software. Over our two-week testing period, we received 302 updates: 234 updated vulnerabilities, 39 new vulnerabilities, 15 new attack agents and four new server types. At one point, we stopped testing, went to lunch and came back an hour later to find a new vulnerability definition waiting for us. Impressive.

WebInspect offers three types of assessments: a single assessment covering one Web site; an enterprise assessment, which let us specify a range of IP addresses; and a Web service assessment, where we pointed at a WSDL (Web Services Definition Language) file. Although the other products we evaluated support Web service vulnerability testing, only WebInspect has this capability built into its wizard, making it a breeze to use. We pointed to a WSDL URL or a local WSDL file, and WebInspect then connected to the Web service and scanned the app. In addition, WebInspect was the only product that let us enter a range of IP addresses and scan the ports on those IPs looking for Web applications.

Policy management is another strong point of WebInspect. If the hundreds of vulnerability tests the Policy Manager offered were not enough, the "Create a Custom Check" wizard let us set a specific vulnerability test to run. In addition, we could see all the tests that would run against our Web server environment, in this case IIS 5.0. The icing on the cake was that we could save our custom test sets to run again at a later date.

When we started scanning, WebInspect was again the class of the group. We especially liked that WebInspect not only showed what was happening in real time, but also let us use its built-in HTTP editor to adjust the HTTP request and see instant results based on our changes—all while the scan was running.

WebInspect was the only product in this review that tested and reported useful, though nonvulnerability-oriented, information about our Web sites. For exam-



ple, we could see all pages that contained HTML comments, cookies, broken links and more. Sure, these items don't necessarily have an impact on security, but it's information that many organizations will be interested in and typically would have to buy a separate product to find.

As for reporting, WebInspect provides a variety of templates, and we could build new templates based on the categories and subcategories of information we wanted to include in the report. We would, however, like to see support for Crystal Reports added to this product.

Standard WebInspect support is your basic 9-to-5, five days, but 24-hour support is available. Overall, we were pleased with WebInspect and wish we'd had it in-house a few weeks earlier.

WebInspect 5.5, single-server perpetual licenses start at \$6,000 for one server (one host). SPI Dynamics, (866) 774-2700, (678) 781-4800. www.spidynamics.com

Cenzic Hailstorm 2.6

When we tested Hailstorm 2.0 in March, we bemoaned the lack of a user interface. So when we booted up 2.6, we were happy to see that Cenzic has added a wizard-based GUI. After testing, though, we were less thrilled—though it's better than nothing, the GUI needs to be better integrated with the rest of the product before Hailstorm is accessible to the average IT practitioner.

Still, what Hailstorm lacks in ease of use it makes up for in iron-fisted control of policy building, earning Cenzic a perfect score in this category. We not only could edit policy parameters, we also could go right down to the JavaScript code and make modifications. Wisely, Cenzic doesn't allow editing of original policies; rather, we copied the code to create policies. IT departments replete with security experts and programmers will love this capability.

Like WebInspect, Hailstorm has an auto-update feature. Cenzic's standard Hailstorm Enterprise product comes with all updates (every two weeks) of the assessment objects library. For customers that want the basic product, called Hailstorm Core, Cenzic provides fewer assessment objects to start with and then fewer updates. The price for the core product is much lower, designed for customers with minimum requirements for application security testing. For example, Hailstorm Core product customers might not get all the application-logic, session-management and compliance



METHODOLOGY

We installed and tested each product using Windows XP Professional on a Dell Dimension with 512 MB of RAM. We pointed each product to our development Web server, which was running IIS 6.0 and SQL 2000. Specifically, we tested each product against two Web applications: a Web site that receives approximately 5 million page views per month and that was built using ASP, and a second site that receives about 300,000 page views and was built using ASP.Net. Both Web sites are dynamic, complete with shopping-cart applications, content-management components and multitier user groups.

Within each product, we tried to set up a custom policy or use a built-in policy to test for cross-site scripting and SQL injec-

tions. After these tests were completed, we undertook a more comprehensive test by firing all vulnerabilities against both sites. In addition, we tested specific portions of both sites using the manual browse feature rather than the automatic spider.

All SECURE ENTERPRISE product reviews are conducted by current or former IT professionals in our own Real-World Labs®, according to our own test criteria. Vendor involvement is limited to assistance in configuration and troubleshooting. SECURE ENTERPRISE schedules reviews based solely on our editorial judgment of reader needs, and we conduct tests and publish results without vendor influence.

tests. We evaluated the Enterprise version.

Cenzic calls its spidering process a traversal. As with the other products tested, we could traverse our Web application automatically and then switch to mixed mode, which let us record specific steps to get past the registration and login process on our Web site. We found the process confusing, however: First, we started an interactive traversal of our Web site, then decided we'd rather do a spidered traversal—no dice. We were stuck, unable to close the interactive traversal browser window. Finally, we resorted to the task manager to kill the process. We later learned there's a tool to close all browser windows, but we'd rather just click on "X" already.

Hailstorm and AppScan both traversed our site before conducting vulnerability assessments. When we asked Cenzic about the benefit of this method, the company said it lets users run new tests against a traversal that is already completed. If pages change, Hailstorm will recognize the changes and index the new pages.

Next, we added a job in which we ran Cenzic's best-practices policies against the traversal we had just created. Hailstorm's built-in

browser let us watch each page being traversed—a cool feature for those with time on their hands to watch a spider do its work. While the tests were being performed, we could use the product's HTTP editor to edit any portion of the vulnerability test, then retest that page. This was similar to the capability in WebInspect, but the process was not as intuitive.

Overall, we found Cenzic's reporting interface weak. Although it does export to PDF, Word, Crystal Reports and other formats, and we could view comparisons between two sets of tests, the overall interface and available customization features are minimal. And Hailstorm Enterprise is priced higher than competitors, at \$35,000 per year for the first application, though deep discounts are available for several Web apps. For example, organizations with more than 500 Web apps could receive pricing as low as \$1,000 each. Standard support is offered from 5 a.m. to 5 p.m. EST, and 24-hour support is available.

Cenzic Hailstorm 2.6, starts at \$35,000 per application, per year for one application. Cenzic, (866) 423-6942. www.cenzic.com

WEB VULNERABILITY SCANNER FEATURES

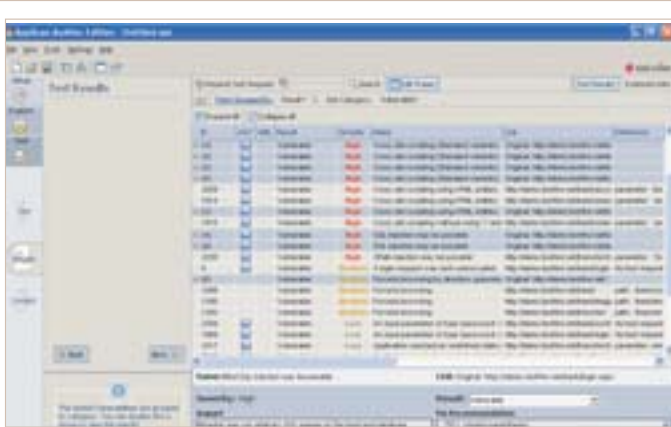
	Cenzic Hailstorm 2.6	SPI Dynamics WebInspect 5.5	Watchfire AppScan Audit 5.0
Supports parametered URIs	Y	Y	Y
Supports SSL	Y	Y	Y
Configurable number of threads	N*	Y	Y
Supports standard proxy	Y	Y	Y
Scans for Web services (supports SOAP)	N	Y	Y
Logs activity	Y	Y	Y
Parsing/crawler			
Parses HTML/CSS/JavaScript	Y/Y/Y	Y/Y/Y	Y/Y/Y
Detects hidden form fields	Y	Y	Y
Tests cookie values	Y	Y	Y
Looks for common backup files (.bak)	Y	Y	Y
Looks for server misconfiguration	Y	Y	Y
Looks for SSL warnings	Y	Y	N
Looks for cross-site scripting	Y	Y	Y
Looks for SQL injections	Y	Y	Y
Parses flash links	N	Y	N
Detects error codes by HTTP status	Y	Y	Y
Crawler can be restricted to specific part of site	Y	Y	Y
Links can be added manually to crawl	Y	Y	Y
Crawls forms	Y	Y	Y
Crawl depth can be limited	Y	Y	Y
Takes note of Web server and OS	Y	Y	Y
Authentication			
Basic	Y	Y	Y
Digest	N*	Y	N
Form-based	Y	Y	Y
Client certificate	Y	Y	Y
NTLM	Y	Y	Y
Reports on broken links	N*	Y	Y
Can apply tests relevant to Web server	Y	Y	Y
Scans			
Can be saved/scheduled	Y/Y	Y/Y	Y/Y
Can be exported via API/XML	Y/N*	Y/Y	Y/Y
Reports			
Can produce PDF/Word/HTML	Y/Y/Y	Y/Y/Y	Y/Y/Y
Support multiple report templates	Y	Y	Y
Support compliance testing	Y	Y	Y
Can include multiple scans	Y	Y	Y

Y=Yes, N=No *Available fall 2005

FYI



There's been significant growth in the use of non-Internet-Explorer browsers, primarily Firefox, according to Gartner. Although Firefox's growth-rate percentages in absolute terms are still in the single digits, in relative terms they exceed 50 percent per year.



The most powerful portion of Watchfire's AppScan is its results. For every potential vulnerability, we were given detailed information and retesting flexibility. It's a shame the same level of detail is not shown throughout the product.

Watchfire AppScan Audit 5.0

D AppScan is easy to use but not as powerful as Hailstorm or WebInspect. We never felt we had real control over the product. Still, those who want to secure their Web apps but prefer to have few buttons to click will like that the product takes you through a controlled process, from setting up the scan to reading a report. AppScan subscription updates are scheduled for every four weeks, plus any critical updates within 24 hours. Watchfire products check for updates and notify users when updates are available. For example, every time AppScan is started, it will detect the last time an update check was performed.

We started out by entering the information needed to create a session to scan one of our Web applications. We started with the automatic scan and could pause the scan to record interactive steps we wanted our application to go through, such as a checkout process. The good news is that within two or three clicks of the mouse, we were scanning our site for vulnerabilities. The bad news? We had no idea what AppScan was scanning for. As the explorer crawled through our site, it gave us an overview of how the scan was going—how many pages it scanned, how many links it has to follow and how many potential vulnerabilities it found. However, we couldn't see what type of vulnerabilities were being found until the scan was complete. Cenzic Hailstorm and SPI WebInspect both let us interact with the scanned vulnerabilities, drilling down for more info, as the scan was taking place.

Once the scan finished, we could view high-level results, including potential vulnerabilities and the types of vulnerabilities found. We appreciated that. Rather than just tell us a cross-site scripting vulnerability existed, it gave us the details of every potential vulnerability. For example, we could see that there were hundreds of potential JavaScript Context Cross Site Scripting vulnerabilities, but only a handful of those could affect ASP.Net. This could lead to information overload, though—when all was said and done, we went from 18,253 potential vulnerabilities to 205 actual vulnerabilities. In addition, at this stage

AppScan did nothing more than list potential vulnerabilities. We would have liked to be able to drill down for further details on a specific potential vulnerability or even use an HTTP editor to perform further tests.

With the exploration process completed, we moved on to testing. Again, we had very little control, and a handful of group filters, such as "Send Application Specific," offered no explanation. We had to read the documentation to determine what each filter would test. After selecting the group of tests we wanted to run, we started the vulnerability scans and could see a limited amount of data about the tests being performed. For example, we could see and highlight the specific URL being tested, but we couldn't double-click to see additional information. We missed seeing a specific test with results in real time. Heck, we couldn't even pause the tests and see specific results.

One nice feature of AppScan is its ability to generate only those tests relevant to the application being tested. For example, after exploring our Web site, the product recognized which version of IIS we were running and that we used ASP and ASP.Net, and it tailored its testing, helping to reduce the number of false positives. We accomplished a similar test using the drill-down approach that WebInspect offered.

AppScan redeemed itself after testing was done. Our results initially were sorted by severity and by "filter group." For every potential vulnerability, we had quite a bit of information and retesting flexibility. We wish AppScan showed this level of detail and control from the beginning.

Once testing was complete, we were off to the reporting process. Reports come in just two flavors, detailed and executive-style. After building a report, we could export it to an XML file, CSV files or Crystal Reports. In addition, we could save the report as a PDF or HTML file.

One impressive feature of AppScan is its built-in Port Listener with which AppScan can act as a server, listening on a port and waiting for specific messages or data to be returned from the Web application. This feature allows for more accurate testing and validation of tests for specific vulnerabilities, such as blind SQL injections. Watchfire told us that one of AppScan's differentiators is its ability to compare two saved sessions. However, we found that both Cenzic Hailstorm and SPI WebInspect have similar processes.

AppScan Audit 5.0, starts at \$15,000 for a yearly subscription. Watchfire, (888) 245-5550, Ext. 1, (781) 810-1450. www.watchfire.com

JEFFREY H. RUBIN



is a senior instructor with the School of Information Studies at Syracuse University and president of Internet Consulting Services Inc. Send your comments on this article to him at jhrubin@internetconsult.com.



115 Perimeter Center Place N.E., Suite 1100, Atlanta, GA 30346
Telephone: 678.781.4800 • Toll-Free: 1.866.774.2700
www.spidynamics.com