SC MAGAZINE REPRINT

WebInspect facilitates the simulation of an advanced web-application attack on your own web site, enabling your IT staff to detect holes in both standard and proprietary applications. *WebInspect* will meander through the entire web site, scanning all known (and some unknown) security vulnerabilities inside web applications, using multiple sources of data to create complex attack scenarios which test web applications. Designed as a single-user desktop application, it can be used by web application developers and testers or network security administrators. Security professionals can use *WebInspect* to scan a system either before release or after it is already in operation. Already you can see that this is an exciting product with something new to offer in Internet security.

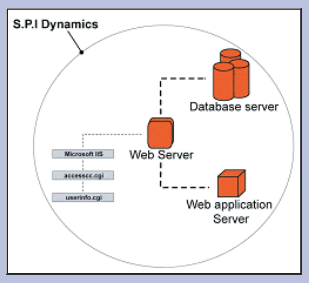
WebInspect gleans its knowledge from three important sources in order to fulfill its somewhat onerous task. Firstly, it utilizes the SPI Dynamics security vulnerabilities database, which contains fingerprints of known attacks running from the last three years up to the present. SPI can configure this database to automatically check for, and download new risks and exploits each time customers run *WebInspect* and this ensures that the product is always current and abreast of hacking techniques.

Secondly, *WebInspect* draws on the expertise of third-party organizations such as Security Focus and the FBI's InfraGuard, which specialize in identifying, collecting, and distributing information and alerts on security risks and exploits. Thirdly, *WebInspect* ascertains the remainder of security risk data from the customer's own web server, learning and remembering through the use of artificial intelligence agents. This information is subsequently used against the web server while *WebInspect* runs. It is important to realize that *WebInspect* includes in its scans the web site content also, encompassing web pages, web scripts, proprietary applications, cookies and other web servers.

The product employs a number of impressive tactics that cannot all be mentioned here. Hidden Manipulation accesses hidden fields that contain confidential information, Cookie Poisoning breaks in through non- or weakly encrypted cookies, and Stealth Commanding plants trojan-horse commands to execute unauthorized codes. Everything is clearly laid out on the screen and it is simple to start a new scan. You simply select the protocol you want to use (http or https), type the host you want to scan, and select the port on which the web server is running in the port box (80 or 443). Alternatively you can put the protocol, host name and port number, separated by colons, into one box using the create scan site wizard, select quick, medium or full scan and proceed.

Quick Scan scans for commonly known vulnerabilities, directories and the IIS UNICODE exploit. Medium Scan covers quick scan and additionally 'crawls' the web site simulating the actions a normal user would perform. Then *WebInspect* checks for vulnerabilities that are commonly part of custom web-based applications. Full Scan performs a full scan of the web site using all of *WebInspect's* algorithms and vulnerabilities. Finally, you can generate a summary report for the issues found during the scan, which contains the information necessary to systematically address and correct any security vulnerabilities that have been identified.

WebInspect



Version: 1.1.35
Supplier: SPI Dynamics
Price: from $7,000 per server
Contact: +55-11- 5052-4733
clm@clm.com.br
www.clm.com.br

FOR Allows for manual intervention during all phases of its operation, after which time, the scanner automatically resumes.
AGAINST None.
VERDICT A well-designed product, allowing you to perform an important task easily, that up until recently would have been impossible to achieve so quickly.

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

A well-designed product, allowing you to perform an important task easily, that up until recently would have been impossible to achieve so quickly.