

INFORMATION SECURITY

WWW.INFOSECURITYMAG.COM

Products

WEB APP SECURITY

WebInspect Enterprise Edition 4.0

SPI Dynamics, www.spidynamics.com

Price: Starts at \$4,995 per server

SPI Dynamics' WebInspect 4.0 can assess Web apps for regulatory compliance and scan them against known attack signatures.

WebInspect scans proprietary and commercial Web apps for compliance with enterprise policies and HIPAA, GLBA and Sarbanes-Oxley regulations. The software includes a policy editor and 11 templates, which list government requirements and checks for proper access control, error handling, remote administration flaws, etc. The templates, which can be customized to company content policies, can flag vulnerabilities that would allow unauthorized access to backend databases, for example, to secure credit card numbers by checking for SQL injection vulnerabilities. WebInspect provides a wizard for configuring an audit of an app or a set of Web sites.

Of course, WebInspect is also a QA/troubleshooting tool for development and production apps, although scanning live apps consumes bandwidth and causes latency. You select the app server IP address and the type of scan to identify vulnerabilities to common attacks—such as buffer overflows. You can choose various scan methodologies, including site mapping, with and without attack signature audits, and regulation-specific compliance.

WebInspect's agents catalog all aspects of the application. They evaluate the data and apply attack signatures and heuristics to determine the presence and severity of vulnerabilities, which are rated according to values assigned by organizations such as CERT. A mouse click updates the database with new assessment methodologies and vulnerability signatures from SPI Dynamics.

WebInspect performed admirably in our scanning of Microsoft- and Linux-based development and production apps. Scans took up to 20 minutes and revealed our misconfigurations and missing patches; we created reports with just a few mouse



SPI Dynamics' WebInspect Enterprise Edition 4.0 scans development apps for security vulnerabilities and regulatory compliance.

clicks. You can access templates to create reports by summary, vulnerability and severity levels and graphical site views. You can sort the data by potential risks, such as command injection or path truncation attacks to create reports for specific programmers, auditors, etc.

It also suggests remediation steps, such as not backing up source code in the Web root for correcting "backup file of source found" vulnerabilities. It includes steps for correcting ColdFusion error messages and fixing known vulnerabilities, such as an Ikonboard arbitrary file source disclosure. It even specifies tips for developer vulnerabilities, such as path parameter file source disclosure. WebInspect integrates with Citadel Software Security's Hercules patch manager to automate vulnerability remediation.

WebInspect's ease of use, depth and breadth of assessments and reporting options make it an essential application security assessment tool and a must-have for any app development toolbox. ▀

—MICHAEL D. ROGERS

SPI DYNAMICS

secure. protect. inspect.

SPI Dynamics
115 Perimeter Center Place N.E.
Atlanta, GA 30346

PHONE: (678) 781-4800

FAX: (678) 781-4850

WEB: www.spidynamics.com

EMAIL: sales@spidynamics.com

FREE TRIAL OFFER: Test your web applications for vulnerabilities. Download a free trial of WebInspect™ at www.spidynamics.com/download.html.