WEB APPLICATION SCANNING OVERVIEW

Organizations rely on Web applications and Web 2.0 technologies to support key business processes and improve performance. As a result, Web application technology has become pervasive in IT environments, enabling interaction with consumers, partners, employees and other parties.

Web applications have also become a prime vector of attack for hackers and cybercriminals. With secure coding and testing practices often absent or overlooked during the development process, Web applications contain vulnerabilities that are easily exploited by attackers to bypass traditional security measures and damage your organization. Because of this, it is essential for organizations to find weaknesses in their Web applications and remediate them.

Regulators have also recognized the risk that insecure Web applications pose. Many compliance mandates, including PCI, FFIEC, NERC CIP, FISMA and others, now require organizations to secure their Web applications and protect them from attack.

Leveraging SecureWorks' proprietary iScanner™ technology, our Web Application Scanning Service proactively audits the security of Web applications and their backend databases to identify flaws that could be exploited by attackers. Provided on-demand, Web Application Scanning helps organizations safeguard Web applications, protect sensitive data and satisfy regulatory requirements.

Comprehensive Web Application Scanning

As the need to interact with users online has grown, so, too, has the complexity of Web applications. This growing complexity has made finding and auditing all of a Web application's functions – including browser and server-side components – a significant challenge for most scanning technologies.

To ensure that the entire Web application is tested, SecureWorks' iScanner uses advanced Web spidering methods to find and examine websites for Web application components. iScanner then performs deep testing to find vulnerabilities and assess their risk. iScanner also scans for potentially sensitive HTML content on your website, such as credit card data or Social Security Numbers, to protect against attackers and accidental disclosures.

Service Benefits

- Identifies and prioritizes vulnerabilities in Web applications and databases
- Satisfies PCI, and other regulatory mandates for Web application security
- Protects sensitive data and backend systems (databases, servers, etc.)
- Reduces administrative overhead costs
- Key component of comprehensive Web application security program

According to the Web Application Security Consortium, 99 percent of Web applications are not compliant with the PCI DSS standard.

Web 2.0 Support

Technologies such as JavaScript, ColdFusion, PHP, AJAX and Flash have enabled developers to create increasingly sophisticated Web applications to serve business needs. These technologies also introduce potential vulnerabilities that allow attackers to bypass traditional network security controls.

To identify Web application vulnerabilities accurately, you have to know how Web 2.0 technologies interact within Web applications. Using browser emulation techniques, iScanner understands application and session logic which allows it to find all links and components within a website. iScanner then tailors testing methods to your Web application's profile to find hard-to-detect, client-side vulnerabilities such as Cross-site scripting (XSS).

WEB APPLICATION SCANNING OVERVIEW

Integrated Database Scanning

Containing the sensitive data attackers seek to compromise, the backend databases that support Web applications are rich targets for hackers. In addition to security vulnerabilities in database software, attackers can also exploit flaws in database configuration to gain unauthorized access to confidential information.

As part of our Web Application Scanning Service, iScanner also performs comprehensive database scanning to find security, configuration and operational vulnerabilities. iScanner provides broad database coverage, supporting common platforms including:

- Oracle
- IBM DB2
- IBM DB/400
- Informix
- Sybase
- Postgres
- MySQL
- Microsoft SQL Server
- Lotus Notes/ Domino

On-Demand Security and Compliance Reporting

Web Application Scanning features on-demand, asset-based reporting via the SecureWorks Portal. With prebuilt scanning reports ranging from high-level, executive dashboards to detailed scan results that are readily available, you can easily satisfy the information needs of all audiences including management, security, developers and auditors. The SecureWorks Portal also features an easy-to-use reporting wizard that tailors reports to your needs.

Service Features

- Comprehensive Web application scanning
- Finds SQL injection flaws, cross-site scripting, etc.
- Detects sensitive content in HTML (Card data, SSNs, etc.)
- Supports dynamic Web 2.0 technologies including JavaScript, AJAX and Flash
- Uses browser emulation to find and test all links
- Includes database scanning

Part of Integrated Web Application Security Solution

Web Application Scanning is part of our full suite of Web Application Security Services, which also includes Managed Web Application Firewall, Source Code Audit and Log Monitoring. Web Application Scanning integrates seamlessly with our other services to provide end-to-end, comprehensive coverage to protect your Web application infrastructure.