



BENEFITS

Secures the complete Web application

NeXpose identifies vulnerabilities throughout the entire application, scanning the browser and server-side components for exposures that other Web application scanners do not find.

Scans Web 2.0 applications

NeXpose is the first vulnerability scanning solution that analyzes JavaScript and AJAX applications in testing, quality assurance, deployment and ongoing management.

Detects more vulnerabilities than traditional Web scanners

The NeXpose collects knowledge on the network environment to accurately scan systems and uncover all vulnerabilities, providing remediation guidance for vulnerabilities that lie deeply under the surface that other scanners miss.

Web Application Scanning

Web technologies have enabled the Internet to develop into an application platform, becoming the platform of choice for both internal and external corporate applications. Today the set of Web technologies and programs known as Web 2.0 is cultivating a social trend of new behaviors enabling real time communication and information sharing.

The popularity of Web applications have made them a choice target for hackers who attempt to corrupt data, crash hosts, gain access to the corporate network and steal valuable information. Because they exist as a conduit between external users and a company's internal databases, Web applications can be one of the biggest IT security risks. For Web sites that take credit cards, the risk transcends the corporation to individuals who conduct e-commerce on the Internet. For these reasons, Web applications need to be regularly audited and closely monitored for changes and improper usage.



Rapid7 NeXpose
Unified Vulnerability Management Solution

Lone Star Bank

"NeXpose gives us a wider view of what's happening as it assesses all IT systems and devices across the organization, including Web applications, databases, firewalls, switches and routers. ... All of these can be scanned for vulnerabilities, a major reason we chose NeXpose."

COMPLEXITY OF WEB APPLICATIONS

To effectively find and remediate vulnerabilities in Web applications, security administrators need reliable scanning solutions that dig deeper into the environment and provide a more complete and accurate picture of what security issues may be lurking inside of a Web application.

Most Web application scanners target the developer, enabling them to find security risks in their code during development. Once the application goes live, Web application scanners struggle to recognize and uncover vulnerabilities in new Web 2.0 functionality such as JavaScript and AJAX.



FEATURES

Browser Emulation Scanning Technology (BEST)

Scans client-side Web applications to find vulnerabilities in Web 2.0 technologies such as JavaScript and AJAX.

Web Application Pass-Through Scanning

Uses found vulnerabilities to scan and report on vulnerabilities that lie deep in the network, providing a more accurate and complete report on Web application exposures.

Batched Scanning

Reduces scan times and allows customers to target specific and mission critical addresses

Content Scanning

Scan applications for specific content such as credit card and social security numbers, ensuring personally identifiable information is not visible to hackers.

ABOUT RAPID7

Rapid7 is the leading provider of unified vulnerability management, compliance, and penetration testing solutions, delivering actionable intelligence about an organization's entire IT environment. Rapid7 offers the only integrated threat management solution that enables organizations to implement and maintain best practices and optimize their network security, Web application security and database security strategies.

Recognized as the fastest growing vulnerability management company in the U.S. by Inc. Magazine, Rapid7 helps leading organizations such as Liz Claiborne, Southern Company, the United States Postal Service, the New York Times, Carnegie Mellon University and the National Nuclear Security Administration (NNSA) to mitigate risk and maintain compliance for regulations such as PCI, HIPAA, FISMA, SOX and NERC . Rapid7 also manages the Metasploit Project, the leading open-source penetration testing platform with the world's largest database of public, tested exploits. For more information, visit www.rapid7.com



DS 12/09

NEXPOSE VERSUS WEB SCANNERS

	Web Scanners	NeXpose
Browser-Based Scanning		√
Web Application Vulnerability Pass-Through		√
Database Scanning		√
Third Party Application and Database Scanning		√
Operating System Scanning		√
Command Execution	√	√
Parameter Injection	√	√
SQL Injection	√	√
Cross-Site Scripting	√	√
Directory Traversal	√	√
Abnormal Input	√	√
Parameter Overflow/ Buffer Overflow	√	√
Parameter Addition	√	√
Path Manipulation/Path Truncation	√	√
Character Encoding	√	√
MS-DOS 8.3 Short Filename	√	√
Character Stripping	√	√
Site Search	√	√
Application Mapping	√	√
Crawl	√	√
Automatic Form-Filling	√	√
SSL Support	√	√
Proxy Support	√	√
Client Certificate Support	√	√
State Management	√	√
Directory Enumeration	√	√
Web Server Assessment	√	√
HTTP Compliance	√	√
WebDAV Compliance	√	√
SSL Strength	√	√
Certificate Analysis	√	√
Content Investigation	√	√
Spam Gateway Detection	√	√
Client-Side Pricing	√	√
Sensitive Developer Comments	√	√
WebServer/Web Package Identification	√	√
Absolute Path Detection	√	√
Error Message Identification Permissions	√	√
Permissions Assessment	√	√
Known Attacks	√	√
Session Hijacking	√	√