

nCircle WebApp360™

Complete Web Application Infrastructure Scanning for Production Environments

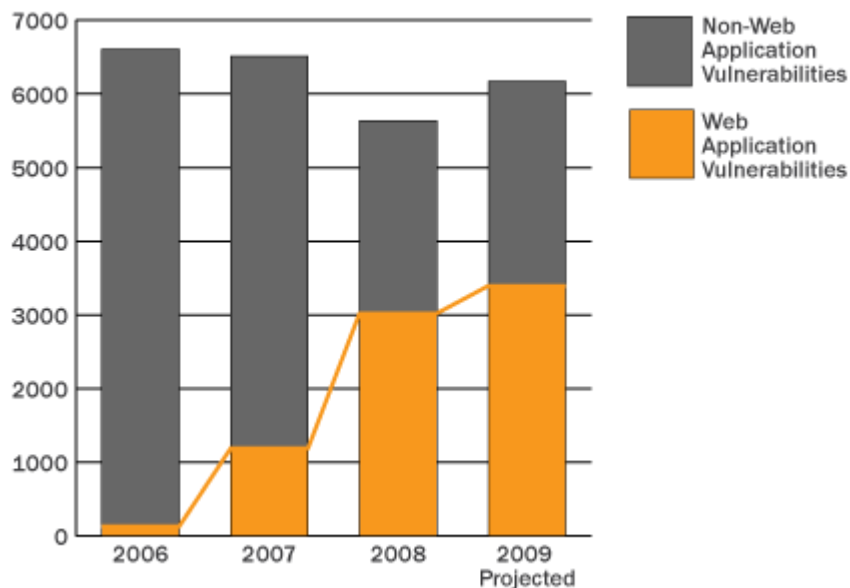
Over the past five years, Web application vulnerabilities such as Cross-Site Scripting (XSS) and SQL Injection attacks have made up an increasing percentage of newly discovered vulnerabilities and actual reported intrusions. Online systems such as banking, healthcare, e-commerce, and customer support portals increasingly collect and provide access to extremely sensitive data and internal systems that provide a juicy target for opportunistic hackers.

At the same time, enterprises have struggled to find solutions that provide a complete assessment of their production Web applications; not only the Web applications themselves but also the underlying operating systems, databases and other IT infrastructure. Additionally, most Web application scanners are stand-alone point-and-shoot products that don't integrate with standard vulnerability scanning, requiring the customer to try and make sense of differing report types and results from multiple vendors. The dramatic growth of Web application deployments and related vulnerabilities has left a significant gap in the market of comprehensive, automated auditing solutions designed to solve these problems.

Web Application Trends

The increase in disclosed Web application vulnerabilities is staggering, to say the least. According to research from nCircle VERT (Vulnerability and Exposure Research Team):

- The number of publicly disclosed web application vulnerabilities grew 1,755% from 2006 to 2009.
- Through September 2009, more than half of the total publicly disclosed vulnerabilities were web application-related.
- While the web application vulnerabilities grew 5% from 2008 to 2009 (projected), the total number of new vulnerabilities (including non-web application vulnerabilities) grew almost 10%.



As the total number of vulnerabilities discovered each year has declined slightly the percentage of Web application vulnerabilities has skyrocketed up to over half of all disclosed vulnerabilities.

It is important to note that these figures deal only with commercial Web applications. When you consider how many organizations are building their own sites and applications, likely without committing the same level of diligence to secure development that commercial vendors employ, it stands to reason that these staggering figures are *understating* the threat.

nCircle WebApp360

nCircle WebApp360 extends nCircle's market-leading vulnerability management platform, nCircle IP360™, to include assessment of production Web applications, offering the industry's most comprehensive view of IT security risk. The integrated solution of IP360 and WebApp360 enables organizations to comprehensively audit their network for vulnerabilities – at a network, system, and Web application level. WebApp360 is the only commercially-developed product with full integration between system and Web scanners.

Automatic, continuous Web application vulnerability detection

Cross-Site Scripting (XSS) Vulnerabilities allow attackers to inject arbitrary html or JavaScript into Web applications and their served Web pages. This malicious code can then be executed in a visiting client's browser, compromising the client's security. WebApp360 utilizes dynamic testing for various types of persistent and non-persistent Cross-Site Scripting vulnerabilities, ensuring that Web applications remain secure.

SQL Injection Vulnerabilities allow attackers to inject SQL commands through Web pages, making changes to stored data or executing commands that were not intended by the application's developers. WebApp360 identifies these vulnerabilities, ensuring that code execution does not occur without proper authorization and data remains uncompromised.

Web Page Implementation Flaws Securing the production implementation of Web applications is just as important as the Web application code itself. WebApp360 ensures that implementation flaws have not been introduced to the Web applications during production rollout, such as password submissions via insecure input fields.

Web Application Infrastructure is only as secure as its weakest link. It is not enough to scan Web applications alone; the underlying infrastructure must also be secure, including critical security assessment of Web servers, operating systems, running services and adjacent systems.

nCircle WebApp360 delivers:

- **Dynamic detection of Web application vulnerabilities** and exposures, such as cross-site scripting and SQL injection
- **Comprehensive network risk analysis**, combining Web application coverage with network, operating system and infrastructure exposure intelligence
- **Consolidated reporting** with standard IP360 reports on the VnE central console or Suite360 Intelligence Hub
- **Normalized risk scoring**, using nCircle's risk metric and CVSS v.2
- **Consolidated infrastructure** utilizing the same nCircle appliances and underlying application code base as IP360
- **Role Based Access Control** allows for re-use of existing IP360 roles and/or creation of new roles specific to management of Web properties

- **Instant Deployment** with license key-based activation
- **Enhanced Operating System detection**, optimized for performance in enterprise Web infrastructures
- **Support for HTTP virtual hosts**

The screenshot displays the nCircle WebApp360 interface. The top section shows 'Host Properties' for 'webapp.ncircle.com'. Below this is a 'Scan History' section with a calendar for January 2008 and a line graph. The main part of the screenshot is a 'Host Composite' window showing a list of vulnerabilities.

Vulnerabilities	Last Seen On
Apache HTDigiest Realm Command Line Argument Buffer Overflow Vulnerability	2008-01-15
Apache WebServer Available	2008-01-15
Basic Image Cross-Site Scripting (XSS) Vulnerability	2008-01-16
Bypass Escaped Quotes Cross-Site Scripting (XSS) Vulnerability	2008-01-16
Bypass Stripped Greater-Than and Less-Than Sign Cross-Site Scripting (XSS) Vulnerability	2008-01-16
Hex Encoding Cross-Site Scripting (XSS) Vulnerability	2008-01-15
HTML Tag Insertion Vulnerability	2008-01-16
Numeric Cross-Site Scripting (XSS) Vulnerability	2008-01-16
Portmapper Available	2008-01-15
Portmapper RPC enumeration	2008-01-15
RPC status Available	2008-01-15
Self-Signed SSL/TLS Certificate Present	2008-01-15
SSH Protocol Available	2008-01-15
SSL Server Supports Weak Encryption	2008-01-15
SSL/TLS Certificate Domain Name Mismatch	2008-01-15
Sun XDR Library Available	2008-01-15
URL Insertion Vulnerability	2008-01-16
Web Server HTTP TRACE Method Supported	2008-01-15

nCircle WebApp360 audits production Web applications and delivers its findings integrated with a full vulnerability assessment of the system and network on which the Web application resides.

nCircle WebApp360 sample Web application vulnerability checks

- Basic Authentication In Use
- Persistent Cookies
- Simple Cross-Site Scripting (XSS) Vulnerability
- Invalid Input Vulnerability
- Numeric Cross-Site Scripting (XSS) Vulnerability
- Persistent Cross Site Scripting
- Plaintext Password Submission Vulnerability
- Basic SQL Injection Vulnerability
- URL Insertion Vulnerability
- Password Field AutoComplete Vulnerability
- Close TextArea Cross Site Scripting (XSS) Vulnerability
- HTML Tag Insertion Vulnerability
- Basic Image Cross-Site Scripting (XSS) Vulnerability
- Persistent Input Validation
- Quoteless Cross Site Scripting (XSS) Vulnerability
- Cross Site Request Forgery (CSRF) (via SSH-DRT)

WebApp360 OWASP Top 10 Coverage

The OWASP (Open Web Application Security Project) Top Ten is a list of the top 10 Web application vulnerabilities, and the de facto standard for comparing vulnerability coverage by Web application scanners. WebApp360 currently identifies vulnerabilities in 7 of the 10 OWASP top 10 categories, with new coverage in development:

Vulnerability Category	Category Description	nCircle Coverage
A1 - Cross Site Scripting (XSS)	XSS flaws occur whenever an application takes user supplied data and sends it to a Web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface Web sites, possibly introduce worms, etc.	✓
A2 - Injection Flaws	Injection flaws, particularly SQL injection, are common in Web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.	✓
A3 - Malicious File Execution	Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework which accepts filenames or files from users.	Future
A4 - Insecure Direct Object Reference	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.	✓
A5 - Cross Site Request Forgery (CSRF)	A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable Web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the Web application that it attacks.	✓
A6 - Information Leakage and Improper Error Handling	Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data, or conduct more serious attacks.	Future
A7 - Broken Authentication and Session Management	Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.	✓
A8 - Insecure Cryptographic Storage	Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud.	✓
A9 - Insecure Communications	Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.	Future
A10 - Failure to Restrict URL Access	Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.	✓

About nCircle Suite360

nCircle provides the world's most comprehensive suite of solutions for agentless security and configuration auditing. nCircle's solutions combine the broadest discovery of networked systems and their operating systems, applications, vulnerabilities and configurations with advanced analytics to help enterprises reduce security risk and achieve compliance. nCircle's solutions include IP360™ for vulnerability and risk management, WebApp360™ for Web application vulnerability auditing, Configuration Compliance Manager (CCM)™ for configuration auditing and file integrity monitoring, Certified PCI Scan Service™ for on-demand self-service PCI scanning, and Suite360 Intelligence Hub™ for IT governance, risk and compliance (ITGRC) reporting and analytics.

About nCircle

nCircle is the leading provider of automated security and compliance auditing solutions. More than 4,000 enterprises, government agencies and service providers around the world rely on nCircle's proactive solutions to manage and reduce security risk and achieve compliance on their networks. nCircle has won numerous awards for growth, innovation, customer satisfaction and technology leadership. nCircle is headquartered in San Francisco, CA, with regional offices throughout the United States and in London and Toronto. Additional information about nCircle is available at www.ncircle.com.