DATASHEET

WVSS

Web Vulnerability Scanning System

NSFOCUS

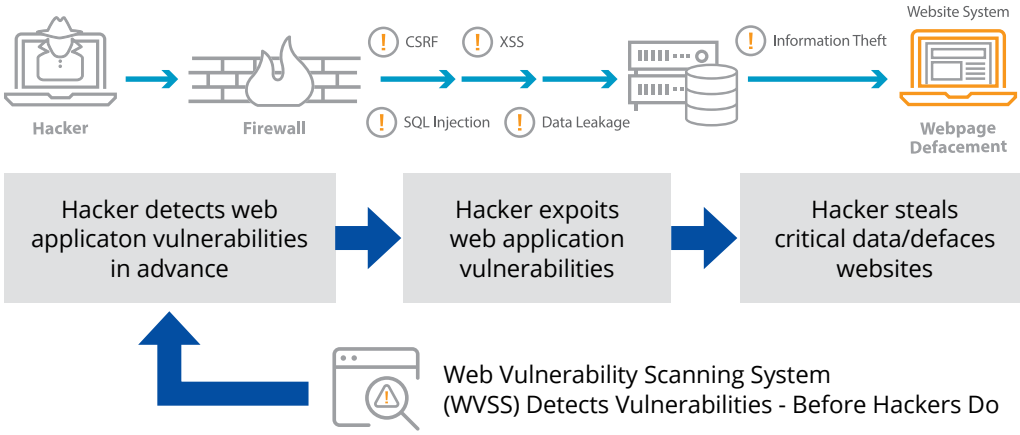
OVERVIEW

Complex attacks on web-based applications are on the rise, accounting for approximately 40 percent of all data breaches in 2016. As organizations rely more heavily on critical web-based applications and continue to migrate valuable and sensitive data to the cloud, the number of security risks they face continues to grow exponentially.

To combat this growing threat, NSFOCUS provides its Web Vulnerability Scanning System (WVSS) to help ensure enterprises are equipped with the most comprehensive application-layer protection against web attacks. In order for organizations to meet compliance requirements like PCI-DSS, they must have a web application security strategy that includes Web Vulnerability Scanning technologies.

The NSFOCUS WVSS protects websites by identifying vulnerabilities in web applications that can be exploited by hackers. Following identification, it provides the NSFOCUS WAF with actionable analysis and reporting, including a remediation plan to improve the overall security of the website.

WHY VULNERABILITY SCANNING



Comprehensive Security Testing

- Full coverage for OWASP and WASC categories
- Intelligent identification of web applications
- Immediate web incident response
- Multi-perspective risk assessment reporting

Efficient and Stable Scanning

- Robust and stable scanning engine
- Intelligent webpage crawling technology
- Multi-node, distributed clustering
- Patented URL webpage load balancing

Closed-Loop Management

- Vulnerability lifetime tracking
- Vulnerability verification and scenario reproducing
- Remediation suggestions with low learning cost
- Automation with NSFOCUS WAF

Closed-Loop Management

- Flexible deployment in virtualization environment
- Effectively use of the virtualized resource pool
- Excellent defenses for all types of data centers
- Supports software deployments

BENEFITS

Vulnerability Identification and Management

WAF and WVSS are Fully Integrated

Enables Automated Smart Patching

Identifies OWASP Top 10 and WASC Vulnerabilities on Web Applications

Safe, Accurate, and Complete Protection

Best Price/Performance for Complete Web Application Security Scanning

Meets PCI requirements and provides audit trail to help ensure compliance with PCI-DSS 3.2 and beyond

KEY FEATURES

WVSS easily scans over 100,000 web pages per day – multi-level clustering enabled

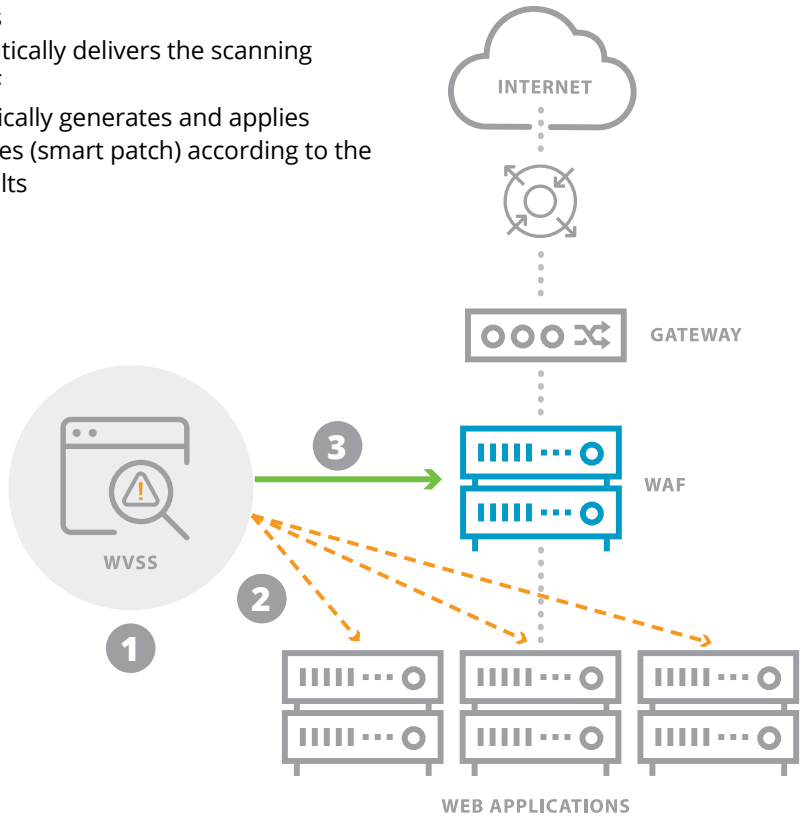
Leverages next-gen technology such as intelligent page crawling, proxy caching, URL-level load balancing, and more

Vulnerability verification and scenario reproducing module to verify vulnerabilities and reduce false positives

NSFOCUS APPLICATION SECURITY IN ACTION

WVSS and WAF Integration

1. WVSS identifies and detects web application vulnerabilities
2. WVSS automatically delivers the scanning report to WAF
3. WAF automatically generates and applies protection rules (smart patch) according to the scanning results



Benefits

Quick Protection

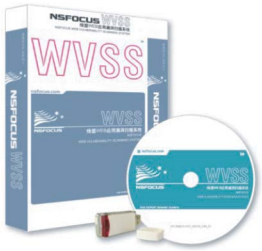
- WAF flexibly dispatches the scanning results and automatically generates protection rules (smart patch)

Continuously website security enhancement

- WVSS scans the target website regularly, and delivers the latest vulnerability information to WAF to update protection rules (smart patch)

VURTUAL WVSS REQUIREMENTS

- Does not rely on operating system
- Virtualized security requirements
- Portal can be installed on a laptop



VM System Requirement	Minimum Requirement		Recommended
Hardware	CPU	Intel X86 (2.46, dual core)	Intel X86 (3.2G, quad core)
	Memory	4GB	Above 8GB
	Hard Disk	500G	
	NIC	10/100/1000 Mbps	
Software	Operating Platform	VMware Player 5.0 or later VMware Workstation 9.0 or later VMware ESXi 5.0 or later	