Secuguard WSE

Web Application Vulnerability Assessment Tool

GS(GOOD Softward)

CC(Common Criteria)

CVE
(Common Vulnerability Exposure)

As the Internet users are increased and network grows rapidly, hacking/security incidents are rapidly increasing every day. To protect the system from these various external environments, administrators need to run periodic vulnerability assessment scans and update system continuously. However this job requires special knowledge domain and dedicated work hours for administrators to invest newly coming hacking methods and technologies.

Secuguard WSE(Web application Security Explorer) scans various web environment, various worm, DOS,hacking trial and configuration errors on the network. Secuguard WSE is a security solution that provides the methods for found vulnerabilities from its scans for preventing hacking and various IT crimes.

Why web application is vulnerable?

- Web based integration with various services increases vulnerability level
- Web service's accessibility exposes system to worm and DOS attack
- Traditional security system(firewall and intrusion detection)'s limitation and those protocol's bypass attack methods
- Web application's misconfiguration and bugs
- Continuous discovery of new vulnerability and its attacking methods
- Continuous intrusions due to easiness of accessing system

Why web application is needed scanning?

- Increasing damages caused by hacking with web application's vulnerability
- Most secured and safe web site development and integration required.
- Continuous development, update and management required for web applications
- Multiple web servers operation and multiple URLs with multiple applications exist
- Programs coding bug and vulnerability from misconfiguration
- Maintain stronger compliances and preparing the audit

Current Web Applications Vulnerability State

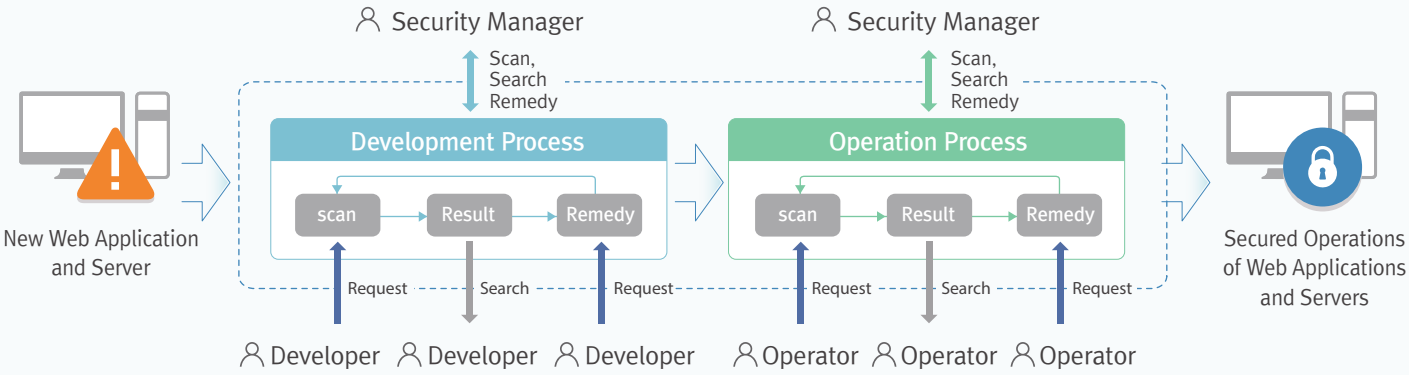
With growth of the internet, most of enterprise and government/public business application system is now developed as web application system form.However, Gartner Group reported 75% of total attack was web application's attacks and Sim Group also reported 97% of more than 300 web sites has web application's vulnerability.

WSE Features

- User friendly GUI based on Windows Explorer-like, and easy installation with InstallSheild
- Hacking simulation with various attacking simulation like XSS, SQL Injection
- Exclusive web browser for vulnerability assessment result and analysis provided
- Testing tool provided for various web tests(hacking simulation) and result report
- Filtering personal information such as personal identification number or matching certain keyword search provided
- Multithread based strong and parallel processed vulnerability assessment
- Console/Agent communication and encryption
- Automatic discovery feature for web server IP, host name and server application information
- Memory queue and table based powerful URL crawler
- Convenient scheduling feature including emailing scan result
- Fast and convenient automated online update based on NVIS
- Various reports such as vulnerability assessment report, assessment report with vulnerability level
- Various reports format conversion provided (DOC, RTF, PDF, XLS, XML)
- Integrated operation with Unified Vulnerability Management system(UVM)
- CVE(Common Vulnerabilities and Exposures) based examination module and vulnerability information
- OWASP TOP 10, SANS TOP 20, WASC TOP 24 vulnerability assessment provided
- Web structure analyzer based on powerful URL crawler

The First step of security, there is WSE!

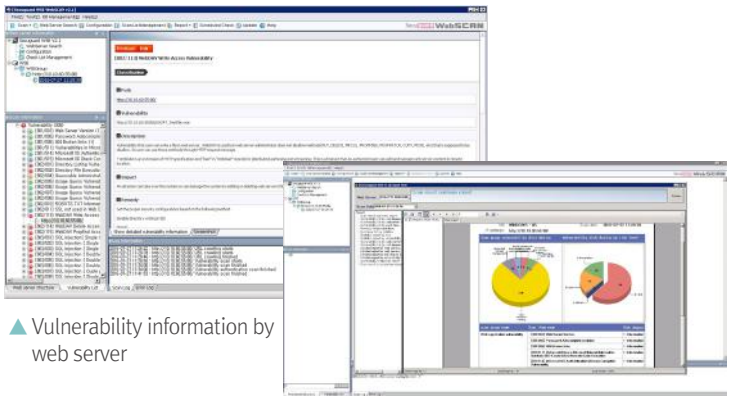
WSE Vulnerability Management Process



WSE Features

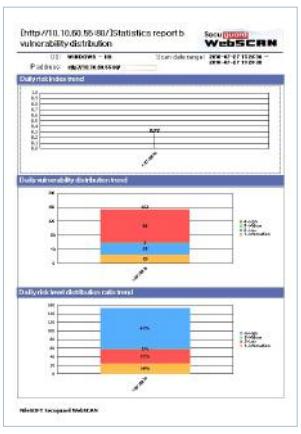
Feature	Description	Feature	Description
Server Detection	· Auto detection of web server IP, hostname · Auto detection of web server's OS and application	Hacking Simulation Tool	· HTTP Login Brute Force tool · HTTP encode / decode tool · HTTP Access trial tool · HTTP Fuzzer and more
Page Analysis	· Web content's structure analysis and auto URL collect feature · URL parsing from JavaScript, AJAX and Flash · User defined URL filtering · Configuration Settings (Proxy, URI Search depth, URI count limit, Etc) · Tree structured URL collector (URL information, HTML Header information, URL Browser)	Report	· Various reports such as vulnerability assessment report, ssessment report with vulnerability level · Various graph and chart based on Crystal Report™ · Various reports format conversion provided (DOC, RTF, PDF, XLS, XML)
		Update	· Update newly updated examination list from update server. · Update scan modules on scheduled time · Offline update for users who cannot access NileSOFT online Update server · For internal network environment, online update through internal update server provided
Assessment	· Parallel Scan : scan multiple target servers simultaneously · Scan History : scan history provided · Vulnerability viewer : Tree structured intuitive vulnerability information for administrator provided · Multithread based fast and string / paralleled vulnerability examination. · Multiple web servers' vulnerability examination in one operation console screen. · Reduced examination time from parallel runs · Server administrators' scan privilege management. · Managing multiple servers' vulnerability scans · Various scan type provided (Group, Batch, By Operation System, Etc.) · Grading founded vulnerability, its content, impact and solution provided	Assessment Items	· Cross Site Scripting, SQL Injection, CRLF Injection, Code Execution, Directory Traversal, File Inclusion, Input Validation, Authentication, Etc · JavaScript, AJAX, Flash File Analysis · Scan with web authentification · Extracting certain information(Credit card number, personal identification number, E-mail) from web pages and attached files. · Keyword filter (Imitated content violation, sexual assault, verbal maltreatment, violation) availablility
		Assessment Policy	· OWASP 10, SANS TOP 20, WASC TOP 24 Vulnerability assessment provided
		Scheduling	· Scheduled Assessment test and E-mail service

WSE Screen Shots



▲ Vulnerability information by web server

▲ Screen of viewing reports



▲ Statistics reports by period

▲ Vulnerability list by web server or risk level

NileSOFT
Kolon Digital Tower Billant 10th Fl. #1004, 30, Digital-ro 32-gil, Guro-gu, Seoul, 08390, South Korea
TEL. +82-2-783-0961 FAX. +82-2-783-0963 e-mail. nileman@nilesoft.co.kr
www.nilesoft.co.kr/eng