

GS(굿소프트웨어)인증
획득제품국제공통평가기준
CC인증 획득제품CVE
인증마크 획득

Web Application Vulnerability Assessment Tool

웹 어플리케이션 취약점 점검스캐너

Secu**guard** WSE



웹 어플리케이션 취약점 점검도구 Secuguard WSE 는

네트워크에 연결된 모든 시스템들의 다양한 웹 어플리케이션에 대한 취약점들을 진단하고 발견된 문제들에 대한 해결 방법을 제공하여 해킹과 컴퓨터 범죄들로부터 보호하고 예방할 수 있는 보안 소프트웨어 솔루션입니다

WSE 필요성

해킹사고가 날로 증가되고 있는 요즘,
외부적 위험 요소로부터 웹서버 시스템을 보호하기 위해
관리자는 웹서버 시스템의 취약점을 주기적으로 점검하고,
조치를 취해야 합니다.

그러나, 관리자가 이런 일을 하기 위해서는
보안에 대한 전문적인 지식과 새로운 해킹 기법의 추적 등을
위해서 많은 시간과 노력을 필요로 합니다!

따라서, 웹어플리케이션에 대한 취약점을 진단하고
발견된 문제들에 대한 해결 방법을 제공하는
보안 소프트웨어 솔루션 Secuguard WSE가
필요합니다!



웹 어플리케이션
취약점을 이용한
해킹 피해 급증



최적의 보안상태를
유지하는 안전한
웹 사이트 구축 필요



웹 어플리케이션은
지속적인 개발 수정,
보완 등의 과정이 반복



프로그램 코딩 및
설정 실수로 인한
취약점 존재



강화된 각종
컴플라이언스 준수
및 감사 대비

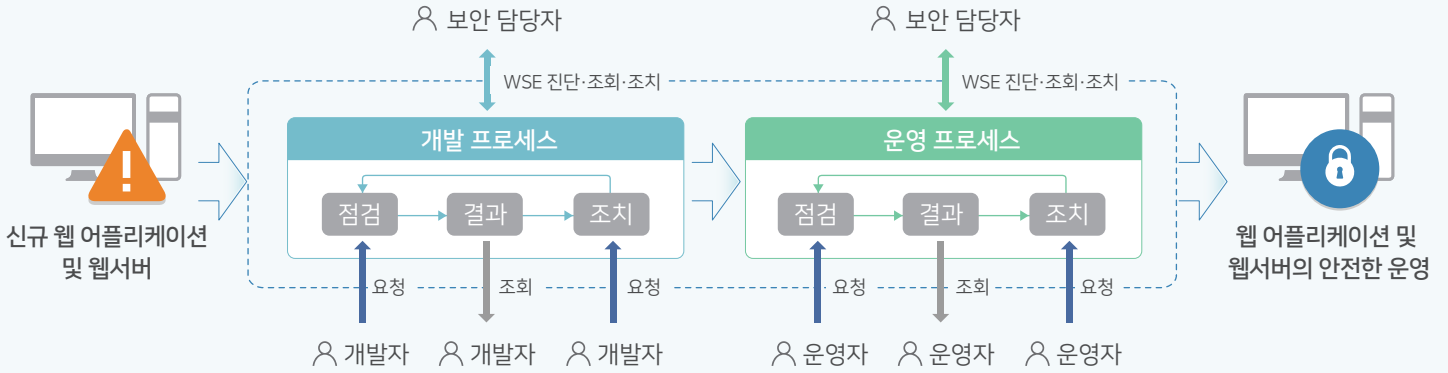


다수의 웹서버 운영 및
웹서버상의 다수의 URL
및 어플리케이션 존재

WSE 특징

- 윈도우 탐색기 형태의 친숙한 GUI 및 Install Shield를 이용한 간편한 설치
- XSS, SQL Injection 등을 포함한 다양한 공격 시뮬레이션으로 모의해킹 수행
- DOC, PDF, XLS, XML, HTML, TXT 등 다양한 파일 형식에서의 보고서 변환 기능
- i-PIN 도입사이트 및 i-PIN 제공기관에 대한 본인인증 취약점 점검 기능
- NVIS(자체취약점데이터베이스)에 기반한 신속하고 편리한 온라인 자동 업데이트
- 다양한 검색기능을 보유한 사용자 기반의 취약점 점검 정책 설정 기능
- 점검결과 자동 E-mail 전송을 포함한 편리한 스케줄링(예약설정) 기능
- 국가정보원 TOP 8, OWASP TOP 10, SANS TOP 20, WASC TOP 24 취약점점검
- CVE (Common Vulnerabilities and Exposures) 기반의 점검 모듈 및 취약점 정보
- 강력한 URL 수집기능을 이용한 웹 페이지 구조 분석
- 주민등록번호를 포함한 개인정보 및 특정용어 포함여부 점검
- 멀티스레드 기반의 빠르고 강력한 동시 다중 보안취약점 점검
- 웹 서버의 IP, 호스트 명, 서버 어플리케이션 정보 자동 인식
- 취약점 목록보고서, 위험도별 취약점 분포 보고서 등 다양한 보고서
- 취약점 결과 및 정보분석을 위한 전용 웹 브라우저 제공
- 다양한 웹테스터(모의해킹) 및 결과 확인을 위한 시험도구 제공
- MS-SQL Server를 통한 대용량 데이터 관리기능
- 통합취약점관리시스템(UVM)과의 연계운영

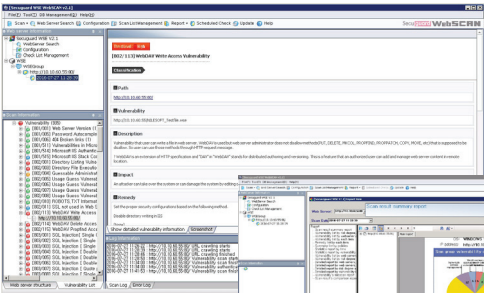
WSE와 취약점관리 프로세스



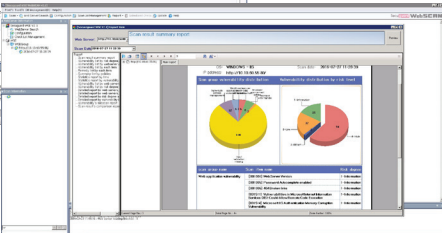
WSE 기능

| 구분 | 설명 | 구분 | 설명 |
|--------|--|----------|--|
| 서버 탐색 | <ul style="list-style-type: none"> 웹 서버의 IP, 호스트명 자동 판별 웹 서버의 운영체제 및 서버 어플리케이션 자동 판별 | 모의 해킹 정보 | <ul style="list-style-type: none"> HTTP 로그인 Brute Force HTTP 인코드 / 디코드 HTTP 접속시도구 HTTP 요청 편집기구 |
| 페이지 분석 | <ul style="list-style-type: none"> 점검 대상의 웹 구조 파악 및 자동 URL 수집 기능 JavaScript, AJAX, Flash 에서 URL 추출 사용자 기반 URL 필터링 기능 환경 설정 (Proxy 여부, URI 점검 깊이, URI 카운트 제한 등) 트리구조로 보여주는 URL 수집기 (URL 정보, HTML 헤더 정보, URL 브라우저 보기) | 보고서 | <ul style="list-style-type: none"> 취약점 목록 보고서, 위험도별 취약점 분포 보고서 등 다양한 보고서 Crystal Report를 이용하여 다양한 그래프 및 표 형태의 보고서 DOC, RTF, PDF, XLS, XML 등 다양한 파일 형식에서의 보고서 변환 기능 |
| | | 업데이트 | <ul style="list-style-type: none"> 업데이트 서버에 접속하여 추가된 취약점에 대한 점검 모듈 업데이트 업데이트 서버에 접근하지 못하는 사용자를 위한 오프라인 업데이트 기능 폐쇄망에 업데이트 서버를 구축하여 온라인 업데이트 지원 |
| 점검 수행 | <ul style="list-style-type: none"> 다중점검 : 점검 대상이 되는 서버들을 동시에 점검 점검이력 : 사용자의 점검 이력을 제공 취약점뷰어 : 점검 대상의 취약점구조를 관리자가 쉽게 파악 할 수 있는 트리구조 정보 제공 멀티쓰레드 기반의 빠르고 강력한 동시 다중 보안 취약점 점검 하나의 콘솔운영화면에서 여러 웹 서버에 대한 취약점 점검을 동시에 수행 동시 점검수행으로 인한 점검시간 단축 웹 서버 다중관리 서버 관리자별 점검 권한 분리 가능 점검 항목 편집기능을 이용한 다양한 점검 가능 발견된 보안취약점의 위험수준, 내용, 영향 및 조치방안을 제시 | 점검 항목 | <ul style="list-style-type: none"> Cross Site Scripting, SQL Injection, CRLF Injection, Code Execution, Directory Traversal, File Inclusion, Input Validation, Authentication 등 JavaScript, AJAX, Flash File 분석등 로그인 정보(계정 및 암호) 입력 웹페이지 혹은 첨부파일 상 신용카드정보, 주민등록번호, E-mail 계정 추출 구글 ADI를 이용한 구글 취약점 점검 |
| | | 점검정책 | <ul style="list-style-type: none"> 금융감독원, 국가정보원 TOP 8, OWASP TOP 10, SANS TOP 20, WASC TOP 24 취약점 점검 |
| | | 예약설정 | <ul style="list-style-type: none"> 특정시간대 점검 및 점검결과 E-mail 통보 |

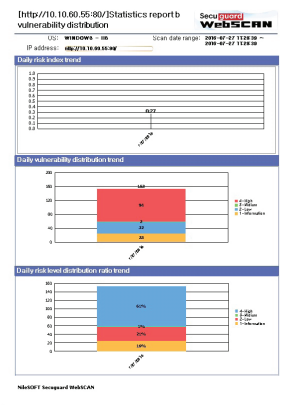
WSE 실행화면 및 보고서



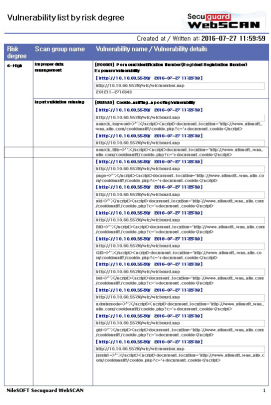
▲ 웹 서버 취약점정보



▲ 보고서 추출화면



▲ 기간별 통계보고서



▲ 웹 서버, 위험도별 취약점 목록