웹 자산을 위한 전략적 보호 귀사의 비즈니스 목표를 지원합니다.

Rational. software

IBM

IBM Rational AppScan 라이프사이클 솔루션:
소프트웨어 및 시스템 제공 시 웹 응용 프로그램 보안 구축

온라인 취약성으로 비즈니스가 위험에 처한 상태입니까?

오늘날 많은 조직에서는 웹 기반 소프트웨어와 시스템을 사용하여 자신의 비즈니스 프로세스를 실행하고, 공급업체와 거래를 수행하며, 고객에게 고급 서비스도 제공하고 있습니다. 온라인으로 배치되는 모든 응용프로그램에 보안을 구축하는 문제는 관리 수준이 높은 조직의 소프트웨어와 시스템을 제공하기 위한 비즈니스 프로세스의 핵심 부분 입니다. 그러나 많은 기업들은 경쟁에서 앞서기 위해 새로운 제품 출시를 서두르느라 이러한 문제는 소홀하게 다루어지고 있습니다. 이에 따른 보안 취약성은 해커가 기업이나 개인의 데이터를 액세스하거나 도용할 수 있는 많은 기회를 제공할 수 있으며, 잠정적으로 전체 비즈니스를 위험에 빠뜨릴 수 있습니다.

IBM Rational® AppScan®은 조직이 이와 같은 심각한 문제를 해결하는 데 필요한 가시성과 관리 능력을 제공하는 업계 선두의 웹 응용프로그램 보안 솔루션 제품군 입니다. IBM Rational® AppScan® 제품군은 다음 제품으로 구성되어 있습니다.

- **IBM Rational AppScan Standard Edition** (데스크탑 응용 프로그램 또는 SaaS (서비스 개념의 소프트웨어)로 제공)
- **IBM Rational AppScan Tester Edition** (데스크탑 응용 프로그램으로 제공)
- **IBM Rational AppScan Enterprise Edition** (웹 기반 솔루션 또는 SaaS로 제공)

이 종합적인 솔루션에서는 검사, 보고 및 수정 권장사항을 제공하고, 응용 프로그램 개발자, 품질 보증(QA) 팀, 모의 해킹 테스터(Penetration Tester), 보안 감사자 및 수석 관리자 등의 다양한 사용자의 모든 유형의 보안 테스트에 적합한 솔루션입니다.

IBM Rational Software Delivery Platform의 다른 라이프사이클 솔루션처럼 Rational AppScan 제품은 주요 QA 도구와 IDE(통합 개발 환경)과의 완벽한 통합을 제공함으로써 사용자가 익숙한 기술 환경에서 작업할 수 있도록 해줍니다. 또한 지속적인 보안 감사를 수행할 수 있도록 해주고, 소프트웨어 제공 팀이 웹 응용 프로그램에 보안을 구축할 수 있게 해주며 응용 프로그램을 배치하기 이전에 비즈니스 위험을 완화시킬 수 있도록 해 줍니다.

중요한 웹 기반 비즈니스 자산의 보호

복잡한 웹 사이트에 대한 종합적인 보안 서비스를 제공하는 Rational AppScan Standard, Rational AppScan Tester 및 Rational AppScan Enterprise 솔루션은 WASC(Web Application Security Consortium) 위협 분류에 의해 식별된 취약성을 포함하여 일반적인 웹 응용프로그램 취약성을 검색 및 테스트합니다. Rational AppScan 솔루션은 광범위하고 강력하며 유연한 핵심 기능을 공유함으로써 종합적인 Ajax 프로그래밍 언어 지원 및 Flash 및 고급 JavaTM Script 언어에 대한 향상된 지원을 비롯한 최신 웹 2.0 기술에 대한 강력한 응용 프로그램 검색 서비스를 제공합니다. 여기에는 JSON(JavaScript Object Notation) 및 웹 서비스 매개 변수에 대한 전용 테스트도 포함됩니다.

검색 효율성과 용이성을 위한 Rational AppScan 핵심 기능은 다음과 같습니다.

- 응용 프로그램 트리, 계층 구조의 보안 문제 결과 목록, 개발자 개선(Developer Remediation) 보기 및 세부사항 영역에 대한 보기 선택기가 있는 사용자 인터페이스
- 응용 프로그램 매개 변수를 분석할 수 있으며, 개발 프로세스를 방해하지 않는 관련 테스트만 선택할 수 있는 맞춤형 테스트 프로세스
- CAPTCHA(Completely Automated Public Turing Test to Tell Computers and Humans Apart) 개선 인증, 다원적(multifactor) 인증, 일회용 암호, USB(Universal Serial Bus) 키, 스마트 카드 및 상호 인증을 포함한 웹 응용 프로그램의 다단계 인증 절차에 대한 테스트를 수행할 수 있는 복합 인증 지원
- 필요한 경우 자동 재로그인을 수행하는 고급 세션 관리
- 검색이 완료되기 전에 문제에 대처할 수 있게 해주는 실시간 결과 보기
- 신용카드 번호, 주민등록번호 또는 기타 번호에 대한 보안 테스트를 용이하게 해주는 패턴 검색 규칙

사용자 정의 및 제어를 위한 Rational AppScan 핵심 기능은 다음과 같습니다.

- **Rational AppScan eXtensions Framework 기술** – 테스트 기능을 확장해주는 강력한 추가 프로그램을 작성, 공유 및 로드할 수 있게 해줍니다.
- **Pyscan –** Rational AppScan을 Python 스크립트 기능과 결합하여 사용자 인터페이스의 제한 없이 검색 기능을 사용할 수 있도록 해줍니다. 그래서 이전에 보안 전문가 및 모의 해킹 테스터가 사용할 수 없었던 사용자 정의 수준을 구현할 수 있게 되었습니다.
- **Rational AppScan SDK(소프트웨어 개발 키트) –** 장기 검색 실행에서부터 사용자 정의 테스트 제출에 이르는 작업들을 호출할 수 있습니다. SDK 인터페이스는 Rational AppScan eXtensions Framework 및 Pyscan 옵션과 함께 통합을 용이하게 하고 검색 엔진의 사용자 정의 사용을 지원하도록 설계되어 있습니다.

취약성 탐지를 위한 Rational AppScan 핵심 기능은 다음과 같습니다.

- 실수로 트리거된 문제, SSL(Secure Sockets Layer) 테스트(SSL 인증서 유효성 테스트) 및 CSRF(Cross-Site Request Forgery) 테스트에 대한 테스트 응답을 분석하는 글로벌 검증 서비스
- OWASP(Open Web Application Security Project) 상위 10개 취약성 및 SANS(System Administration, Networking, and Security Institute)의 상위 20개 취약성에 대한 해커 시뮬레이션
- Rational AppScan 제품을 시작할 때 자동으로 업데이트되는 최신 위협에 대한 정보
- 모의 해킹 테스터 및 보안 컨설턴트가 웹 응용 프로그램을 개발, 테스트 및 디버그할 수 있게 도와주는 번들형 유틸리티 제품군

보고 및 개선을 위한 Rational AppScan 핵심 기능은 다음과 같습니다.

- NIST SP(National Institute of Standards and Technology Special Publication) 800-53 및 OWASP 상위 10대(2007년 업데이트)를 포함하여 40개 이상의 글로벌 규제 컴플라이언스 문제 및 표준과 관련된 테스트. Rational AppScan 버전 7.7에는 FERPA(Family Education Rights and Privacy Act), FIPPA(Freedom of Information and Protection of Privacy Act) 및 PABP(Payment Application Best Practices)에 대한 서비스도 포함됩니다.
- 취약성이 포함된 HTML 코드를 지적하고 문제를 설명하는 유효성 검사 하이라이팅. 차이점이 수정된 HTML 코드로 표시됩니다.
- PHP(Hypertext Preprocessor) 수정 권장사항 및 개발자 작업 목록이 포함된 개선 보고서. 이 보고서를 통해 응용프로그램 관련 문제나 인프라 문제를 확인하고, 변형을 삭제하거나 나중에 검토하기 위해 취약하지 않음으로 표시할 수 있습니다.
- HTML 주석에 들어있는 민감한 데이터뿐만 아니라 의심스러운 컨텐츠에 대한 HTTP 활동 등의 항목을 나열하는 의심스러운 컨텐츠 상세 보고서
- 취약성 데이터베이스의 CVE(Common Vulnerabilities and Exposure)에 대한 ID를 포함하는 테스트 설명
- Rational AppScan 내부 브라우저의 스크린샷을 보고서에 통합하고, 특정 테스트에서 일반적인 정보를 추출, 압축 및 암호화하여 전자우편으로 보낼 수 있는 기능. Rational AppScan 소프트웨어를 사용하면서 오판율 인시던트를 IBM Rational AppScan 보안 연구팀에 보고하여 연구팀이 제품의 정확성을 지속적으로 개선하도록 할 수 있습니다.

IBM Rational AppScan 보안 문제 보기

IBM Rational AppScan 개선 보기

Rational AppScan Standard Edition 소프트웨어를 사용하여 보안 감사 및 프로덕션 모니터링 수행

보안 감사자 및 모의 해킹 테스터를 위해 웹 응용 프로그램 테스트를 자동화하려면 정교하고 지능적인 검색 기술이 필요합니다. Rational AppScan Standard Edition에는 일반 사용자와 고급 사용자를 지원하기 위해 설계된 다음과 같은 기능이 있습니다.

- 검색 전문가 기능은 검색을 작성하고 베스트 프랙티스에 기반해서 셋업을 하는 지침을 제공하며, 추가적인 도구도 사용하실 수 있습니다. 사용자는 대상 응용 프로그램을 프로파일링하는 사전 검색을 승인하고 성공적인 검사에 필요한 조치를 권고할 수 있습니다.
- 상태 발생기(State Inducer) 기능은 다단계 온라인 쇼핑이나 추적과 같은 복잡한 비즈니스 프로세스를 검색 및 테스트하고 매개 변수 값과 쿠키 처리량을 관리합니다.
- 사전 정의된 검색 템플리트 기능은 사용자가 구성 옵션을 신속하게 선택하고 실행할 수 있게 해줍니다.
- 신속한 검색 구성 마법사 기능은 사용자에게 중요한 설정들을 가이드 해주며, 프록시/플랫폼 인증 및 세션 탐지 정보를 위한 조건부 단계도 가이드를 해줍니다.
- 새로운 요청/응답 탭 기능은 구문 강조, 요청/응답, 축소/확장, 입력 검색 및 추가 오른쪽 클릭 옵션을 제공합니다.
- 기업 표준을 준수하는 사용자 정의 형식을 설계하기 위한 Microsoft® Word 템플리트 기반 보고. 템플리트에는 목차, 검색 시작 및 종료 시간, 그래픽 기능이 있습니다.
- 문제에 대해 설명하고 사용법을 보여주는 임베디드 WBT(웹 기반 교육) 모듈과 함께 취약성을 이해하고 의사소통을 쉽게 할 수 있도록 해주는 결과 검증 기능

Rational AppScan Tester Edition 소프트웨어를 사용하여 품질 관리 프로그램의 일환으로 보안 테스트 수행

Rational AppScan Tester Edition을 사용하면 QA 팀이 보안 테스트를 기존 품질 관리 프로세스에 통합하여 보안 전문가의 부담을 덜어줄 수 있습니다.

업계 최고의 테스트 시스템들과 통합되기 때문에 QA 전문가는 익숙한 테스트 환경에서 Rational AppScan 기능을 사용하여 스크립트 테스트 및 보안 검사를 수행할 수 있고, 기능 및 성능 테스트시에 보안 테스트를 채택하는 것을 용이하게 합니다.

Rational AppScan Enterprise Edition 소프트웨어를 사용하여 전사적으로 응용프로그램 보안 테스트를 확장

웹 기반 아키텍처를 통해 Rational AppScan Enterprise Edition 소프트웨어는 기업이 보안 테스트에 대한 책임을 여러 책임자들에게 분배하고, 웹 응용 프로그램 제공 라이프 사이클 초기(수정하기 쉽고 비용 효율적인 시점)에 취약성을 발견할 수 있도록 설계 되었습니다.

중앙 집중식 관리의 편리성과 확장성 외에도 Rational AppScan Enterprise Edition은 다음과 같은 이점을 제공합니다.

- 복잡한 웹 사이트에서 수천 개의 응용 프로그램을 동시에 검색 및 테스트하고, 응용 프로그램의 변경에 수반하는 빈번한 재 테스트를 수행하는 기능
- 개발자나 다른 비 보안 전문가를 위해 관리자가 정의한 검색 템플리트를 데스크탑 설치나 구성없이 실행할 수 있는 단순하고 빠른 검색 테스트 도구
- 전사적인 접근과 다중 뷰를 위해 테스트 결과들을 자동으로 저장 및 집계하는 중앙 데이터 저장소. 비즈니스 단위, 지역 또는 타사 공급업체별로 취약성을 구분 및 추세화할 수 있습니다.
- 보안 보고서에 대한 접근을 역할 기반으로 가능하게 하고 전사적 커뮤니케이션을 용이하게 하는 웹 기반 보고 콘솔. 문제를 필터링하고 우선순위를 지정하며, 상태(미결, 진행 중 또는 마감)를 지정할 수 있습니다.
- 임원 대상 대시보드 및 델타 분석 보고서는 수정된 문제, 보류 중인 문제, 새로운 보안 문제를 포함하여 검색 간의 변경사항을 강조표시합니다.
- 웹 응용 프로그램 취약성 테스트를 전사적으로 모니터링 및 제어하기 위한 중앙 집중식 관리
- 문제에 대해 설명하고 사용법을 시연하는 임베디드 WBT 모듈과 함께 취약성을 쉽게 이해하고 전달할 수 있는 결과 검증

IBM Rational AppScan Enterprise Edition 대시보드 보기

SaaS로 제공되는 Rational AppScan Standard 및 Rational AppScan Enterprise 기능

관리 대상 서비스로 Rational AppScan 기능에 액세스하여 직원이나 하드웨어의 추가 비용 없이도 제품의 이점을 활용할 수 있습니다.

최신 보안 환경

운영 환경 보호에 초점을 맞추면서 이 서비스는 고급 보안 도구와 기술로 통합되어 있습니다.

전용 보안 및 컴플라이언스 전문가를 가지게 됨

Rational AppScan Standard 또는 Rational AppScan Enterprise 고객은 IBM Rational 보안 분석가를 통해 다음을 지원 받을수 있습니다.

- 각 응용 프로그램을 포함하도록 검색을 구성하고 조정합니다.
- 오판율을 제거하고, 패턴을 식별하며, 주요 문제점의 우선순위를 지정하고, 주요 개선 작업을 강조 표시하도록 결과를 검토 및 분석합니다.
- 동향 데이터를 유지 관리하고, 검색간 주요 문제의 해결책을 추적하며, 개선 효과를 보고하여 개선 진행 과정을 추적합니다.
- 웹 응용 프로그램 제공 라이프사이클 내내 Rational AppScan을 사용하도록 QA 직원을 훈련시키고 응용 프로그램에 보안 및 컴플라이언스 관리를 철저히 구현하도록 합니다.

웹 기반 교육을 통해 조직의 보안 및 컴플라이언스 관리 문제 해결

IBM Rational AppScan 제품군에는 10년간의 전문 지식을 기반으로 한 온라인 자습용 교육 커리큘럼의 웹 기반 교육과 복잡하고 어려운 웹 환경의 실제 고객의 경험으로부터 수집된 베스트 프랙티스가 포함되어 있습니다. 서비스에서는 기본 제품 지침 외에도 개발자, QA 팀 및 보안 전문가를 대상으로 한 자문을 제공합니다.

15분 간격으로 온라인으로 제공된 후 보관되는 서비스 모듈은 언제 어디서든지 액세스할 수 있습니다. 특별 전문가 실습 시간 동안에는 Rational AppScan 보안 전문가의 실시간 가이드에 접근할 수 있습니다.

교육 프로세스 중에 3가지 레벨의 제품 지식 인증에 대한 온라인 테스트를 사용할 수 있고, 관리자는 Rational AppScan Enterprise Edition에서 온라인으로 제공되는 관리 대시보드를 통해 직원의 진행 상태를 추적할 수 있습니다.

시스템 요구사항

프로세서	Intel® Pentium® P4, 1.5GHz (2.4GHz 권장)
메모리	512MB RAM (대형 사이트를 검색할 경우 1GB 권장)
사용 가능한 디스크 공간	1GB (대형 사이트를 검색할 경우 10GB 권장)
네트워크	구성된 TCP/IP와의 네트워크 통신용 10Mbps의 NIC (네트워크 인터페이스 카드) 1개 (100Mbps 권장)
운영 체제	Microsoft Windows® XP, Windows 2000, Windows 2003 Enterprise Edition, Windows Vista
웹 브라우저	Microsoft Internet Explorer 5.5 이상 (6.0 이상 권장)
	Microsoft.NET Framework 2.0 이상
	JRE(Java Runtime Environment) 5.0 (Rational AppScan HTTP 프록시 전용)

추가 정보

IBM Rational AppScan 제품에 대해 자세히 알아보려면 IBM 담당자 또는 파트너에게 문의하거나 다음 웹 사이트를 참조하십시오.

ibm.com/software/rational/offerings/testing/webapplicationsecurity

(135-270)서울시 강남구 도곡동 467-12
군인공제회관빌딩

한국아이비엠주식회사
고객만족센터

TEL: (02)3781-7114
www.ibm.com/kr

2008년 2월
Printed in Korea