

PT APPLICATION INSPECTOR: 보안 진단 분야의 혁신

*“애플리케이션 보안 테스트
시장이 급변하고 있다.
모바일 애플리케이션, 첨단
웹 애플리케이션, 동적 언어
등 여러 기술 경향으로 인해
동적 및 정적 테스트 기술
결합의 필요성이 강조되고
있으며, 이에 따라 전반적인
시장 개편이 진행 중이다”*

Magic Quadrant
for Application Security
Testing,
가트너, 2013년 7월

PT Application Inspector: 보안 진단 분야의 혁신

본격적인 사업에는 최신 소프트웨어 사용이 필수입니다. 하지만 프로그램 수가 증가하면서 취약점 갯수도 따라 증가하고 있습니다. Positive Technologies의 2013년 연구 결과, 인터넷 공격자들이 대기업 91%의 내부 호스트에 접속하는 데 성공했습니다(2011-2012년은 74%). 대다수의 취약점은 공격이 발생하기 훨씬 이전에 발견이 가능합니다. 코드 분석이 사용되는 경우, 10배나 많은 취약점의 탐지도 가능합니다.

결제 애플리케이션에 적용되는 PCI DSS와 데이터 보호지침(Data Protection Directive), 정부 정보, 개인 정보 시스템 등과 같은 규제들의 최근 표준은 취약점의 탐지와 수정을 요구하고 있습니다. 방대한 양의 소프트웨어 사본을 사용하고 있는 기업은 이러한 요구에 부응하기 위해 자동화를 필요로 하고 있습니다. 그렇지만 지금까지 출시된 솔루션들에는 아래와 같은 단점들이 존재합니다.

정적 애플리케이션 보안 테스트(SAST)는 특정 보안 문제 대신 프로그램 오류를 드러내게 되면서 오탐율이 증가하고 별도의 점검을 요구하는 결과를 낳았습니다.

SAST는 프로그램이 구동을 시작할 때에만 나타나는 취약점을 탐지하지 못합니다.

동적 애플리케이션 보안 테스트(DAST)는 시스템 구축을 요구합니다. 기업에서 사용 중인 애플리케이션의 크기가 매우 크고 복잡한 경우, 시스템 구축에 따른 추가 비용이 발생합니다. 이 모델은 애플리케이션이 개발 중인 경우 무용지물이 되고, 애플리케이션이 이미 실행 중인 경우에는 애플리케이션 장애를 발생시킬 수 있습니다. 또한, DAST는 테스트 시간이 상당히 소요되지만 코드의 30%만 다룰 수 있습니다.

PT Application Inspector의 작동 원리

Application Inspector는 Positive Technologies가 구축한 방대한 취약점 기반을 바탕으로 정적, 동적 및 양방향 테스트 방식들의 장점만을 혼합하여 적용합니다.

테스트에는 소스 코드만 필요하며 소스 코드는 부분별 분석이 가능합니다. 따라서, PT AI는 애플리케이션이 개발 중이거나 이미 사용 중인 경우에도 모두 사용이 가능합니다.

가상 샌드박스에서 수행되는 기호 계산과 양방향 추적을 혼합한 고유의 테스트 기술로서, 라이브러리와 프레임워크 고유의 동적 종속성, 함수, 클래스들을 처리하고, 애플리케이션 비즈니스 로직에 영향을 미치는 데이터 흐름을 생성합니다.

추상적인 해석 엔진이 즉각적인 취약점 점검을 허용하고, 개발자들을 위한 단위 테스트를 준비하며, PT Application Firewall이 사용되는 경우에는 애플리케이션 코드 변경 없이 공격을 차단하는 특별 요청인 익스플로잇을 생성합니다.

이와 같은 방식을 통해 기업 웹사이트에서부터 클라우드 서비스, 전자정부 시스템에 이르기까지 다양한 규모의 애플리케이션에 대한 보안 대책 마련과 관련된 비용 절감 등의 효과를 가져올 수 있습니다.

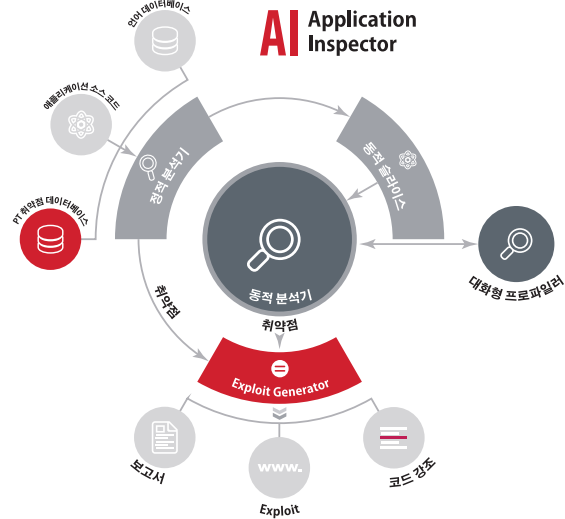
PT Application Inspector의 주요 장점

오탐율의 최소화

개발 단계에서부터 소스 코드 보호

해커가 아닌 기업의 편의를 위한 익스플로잇 생성

보안 전문가, 개발자, QA팀이 모두 사용 가능한 보편성



정보 보안 전문가를 위한 주요 기능

탐지 효율성 제고: PT AI는 DAST, SAST, IAST, 컨텍스트 분석, 서버 및 애플리케이션 설정 분석 등을 혼합한 기술을 사용함으로써 경쟁 솔루션보다 오탐율을 평균 75% 낮추며, 전문가에 의한 수동 점검 비용을 크게 절감시켜 줍니다.

조기 탐지: PT AI는 초기 개발 단계부터 애플리케이션 분석을 보장합니다. QA팀은 애플리케이션의 생산에 앞서 잠재적으로 안전하지 못한 코드에 대해 보고를 받을 수 있기 때문에 공격의 위험이 감소되고 보안 표준 준수 관리에 따른 비용이 절약됩니다.

단일 솔루션: PT AI는 PHP, Java, .NET, SAP ABAP, HTML/JavaScript, SQL 등 다양한 플랫폼과 언어는 물론, SQL Injection(SQLi), Cross-Site Scripting(XSS), XML External Entity(XXE) 등 모든 유형의 취약점을 지원합니다.

위험에 대한 정확한 파악: 익스플로잇 생성 기능을 통해 실제 예가 포함된 취약점 위험 프로파일을 보고함으로써 명확한 코드 패치 작업을 보장합니다.

백도어 탐지: 애플리케이션의 비즈니스 로직을 파악하여 개발자가 남겨 놓거나 해커가 도입한 백도어를 탐지할 수 있습니다.

즉각적인 보안: 일부 대기업에서는 PT AI를 사용하여 PT Application Firewall을 훈련합니다. PT AI에 의해 생성된 익스플로잇을 통해 PT Application Firewall은 소프트웨어 제공 업체가 취약점을 수정할 때까지 가상 패치를 생성하여 애플리케이션을 보호합니다.

표준 규정 준수: SOX, PCI DSS, 안전행정부의 시큐어코딩 가이드 등 다양한 규정의 준수를 증명해 줍니다.

개발자의 편의를 위한 특징

간단하고 안전한 테스트: 실시간 테스트에서 자주 발생하는 테스트 애플리케이션의 설치 및 설정, 또는 복구가 불필요한 솔루션입니다. 애플리케이션 코드나 심지어는 부분적 시스템 코드를 포함하는 폴더에 Application Inspector를 간단히 포인팅하기만 하면 됩니다.

애플리케이션 특정 오류: PT AI가 애플리케이션 기저의 비즈니스 로직을 쉽게 학습할 수 있기 때문에 각 애플리케이션 작동 방식 고유의 취약점들을 탐지할 수 있습니다.

외부업체 구성요소에 대한 지식 기반 탑재: PT AI는 기업의 애플리케이션에서 사용하는 외부업체 구성요소들(예, 오픈 소스 코드)을 검사합니다.

증상 탐지: PT AI는 취약점과 취약점의 증상을 모두 검색하도록 설정이 가능하기 때문에 깊숙이 숨어 있는 취약점으로부터의 보호도 가능합니다.

안전한 SDL 지원: 개발자는 익스플로잇 등 편리한 포맷으로 정확하지 않은 코드에 대한 정보를 수신합니다. PT AI와 개발 주기와의 통합을 통해 안전한 개발 및 테스트 비용의 절감 효과를 얻을 수 있습니다.

Positive Technologies 소개

Positive Technologies는 취약점 진단, 컴플라이언스 관리, 위협 분석 솔루션 분야의 글로벌 리더로서, 전세계 1천 여 고객들에게 솔루션을 제공하고 있습니다. 개발 단계의 애플리케이션 보호, 네트워크 및 애플리케이션 취약점 진단, 규제 요구사항과의 컴플라이언스, 실시간 공격 차단 등 비즈니스와 관련된 모든 보안 문제에 완벽히 대처합니다. 고객 및 연구에 대한 헌신과 노력의 결과, SCADA, 금융, 통신, 웹 애플리케이션, ERP 보안 분야에서 최고의 권위를 가지고 있다는 평가를 얻고 있으며 2012년 IDC 보고서*에서는 가장 빠르게 성장하는 보안 및 취약점 관리 기업으로 선정되기도 했습니다. Positive Technologies에 대한 보다 자세한 사항은 www.ptsecurity.com에서 확인할 수 있습니다.



*출처: Worldwide Security and Vulnerability Management 2013-2017 Forecast and 2012 Vendor Shares, doc #242465, August 2013. 매출 2천만 달러 이상 관련 분야 사업자의 2012년 전년 대비 매출 성장률을 바탕으로 함.
© 2014 Positive Technologies. Positive Technologies and the Positive Technologies logo are trademarks or registered trademarks of Positive Technologies. All other trademarks mentioned herein are the property of their respective owners.