SYNOPSYS®

SOFTFLOW

WhiteHat DAST

웹 프레임워크 및 애플리케이션 모두에 적합한 최신 웹 애플리케이션 보안 진단 도구

최근 기업들은 홈페이지와 고객포털, 쇼핑카트, 로그인 페이지부터 기업내부 HR 시스템까지 다양하게 웹 애플리케이션을 활용합니다.

웹 애플리케이션은 해커에게 매력적인 공격 타켓이 됩니다. 이와 같이 비즈니스와 직결되는 웹 애플리케이션의 취약점이 악용되면 기업의 백엔드 데이터베이스에 엑세스가 가능해지기 때문입니다.

WhiteHat DAST

WhiteHat™ DAST는 SaaS(software-as-a-service) 기반의 DAST(dynamic application security testing) 솔루션입니다. WhiteHat DAST를 이용하면 확장 가능한 웹 보안 프로그램을 빠르게 도입할 수 있습니다. 웹페이지가 아무리 많아도, 또 아무리 자주 바뀌어도 WhiteHat DAST라면 수요에 맞춰 얼마든지 확장이 가능합니다. 보안 개발팀은 QA와 프로덕션 중에 애플리케이션의 취약점 평가를 해커들이 취약점을 찾는 것과 동일한 방법을 적용하여 신속, 정확하게 지속적으로 할 수 있습니다. 따라서 해커보다 먼저 취약점을 발견하여 수정할 수 있습니다.

WhiteHat DAST는 클라우드 기반 솔루션으로 별도의 하드웨어나 스캐닝 소프트웨어를 설치할 필요가 없습니다. 주요 특징은 다음과 같습니다.

- 무제한 지속되는 전체 분석
- 웹 애플리케이션의 코드 변경 자동 탐지, 분석
- 오픈 API 통합 : 보안 정보 시스템, 이벤트 관리 솔루션, 버그 추적 시스템, 웹 애플리케이션 방화벽

WhiteHat DAST는 어떤 환경에든 적용하여 확장 가능하며 수천 가지 웹사이트를 동시에 분석합니다. 또한 취약점은 모두 Synopsys 전문가가 검증하므로 오탐 가능성이 사실상 제로입니다.

인공지능과 머신러닝 기능

WhiteHat DAST는 머신러닝(ML)과 인공지능(AI), 전문가 취약성 분석을 결합하여 최고 수준의 정확도를 가진 동적 애플리케이션 보안 테스팅 결과를 산출합니다. 따라서 오탐으로 인한 개발속도 저하 없이 웹 애플리케이션의 보안을 검증할 수 있습니다.

DAST 분야의 숙련된 보안 전문가가 다년간 수집한 데이터 기반 AI/ML 모델을 개발하여 적용하였습니다. 이러한 방식은 결과 도출이 빠르고 자동화되며 여기에 전문가 검증까지 더해져 사이버 공격을 초기에 탐지, 대응할 수 있습니다.

WhiteHat DAST의 원리

WhiteHat DAST은 자동 애플리케이션 스캐닝 시스템과 세계 최고 보안 전문팀이 검증한 취약점과 조치가능한 결과를 제공해 드리는 솔루션입니다.

온보딩

고객 URL과 로그인, 일정 제공

최초 스캐닝

발견, 미세 조정, 구성

웹사이트 분석

무제한 분석, 취약점 탐지, 검증

보고

커스텀 결과 보고서와 함께 포털에 표시

요구사항에 가장 잘 맞는 WhiteHat 에디션을 선택하세요

WhiteHat PE (프리미엄 에디션)	WhiteHat SE (스탠다드 에디션)	WhiteHat BE (베이직 에디션)
• 엄격한 컴플라이언스 요구사항과 멀티스텝 형식의 웹 애플리케이션 비즈니스 고객에 적합 • SE 기능과 비즈니스 로직 분석 모두 포함	• 일반 웹사이트 비즈니스 고객에 적합 • BE기능 및 멀티스텝 형식과 로그인 테스팅 모두 포함	• 비즈니스 중요도가 낮은 일반 웹사이트용 기본 솔루션 • 자동 스캐닝과 취약점 검증 실시. 위험도가 낮은 사이트에 적합

특징	설명	PE	SE	BE
지속 분석	웹사이트를 상시 스캐닝하여 웹 애플리케이션의 코드 변경을 자동으로 탐지합니다.	●	●	●
보안 취약점 검증	모든 보안 취약점은 보안전문가가 일일이 검증하고 AI로 보강하므로 오탐율이 사실상 제로입니다.	●	●	●
요청시 리테스팅	탐지된 취약점이 시정된 후 요청하면 사이트를 재시험하여 교정 여부를 검토할 수 있습니다.	●	●	●
프로덕션 무해성	프로덕션에 해가 없는 페이로드만 이용하므로 성능 저하가 없습니다.	●	●	●
WhiteHat 보안 엔지니어	포털을 통해 보안 전문가를 제한 없이 직접 요청하여 시정 지침을 받을 수 있습니다.	●	●	●
WhiteHat Security Index (WSI)	하나의 점수로 웹사이트 보안성을 눈으로 즉시 확인할 수 있습니다.	●	●	●
내부 QA/스테이징 환경 테스팅	내부 프리프로덕션/스테이징 환경을 세부적으로 테스팅하여 프로덕션에 도달하기 전에 취약점을 잡아냅니다.	●	●	●
유연한 보고형식과 분석 및 동종 업계 비교	엔터프라이즈급 기업의 사업부서별 데이터 보고 및 분석을 유연한 형식으로 집계합니다. 따라서 전체 웹사이트의 보안 현황이 한눈에 들어오고 업계 평균과도 쉽게 비교 가능합니다.	●	●	●
싱글 페이지 애플리케이션	싱글 페이지 애플리케이션도 프로덕션에 지장이 없도록 자동으로 스캐닝합니다.	●	●	
구성과 형식 교육	웹사이트 형식과 로그인 설정을 통해 사이트를 안전하게 스캔하도록 스캐너를 구성할 수 있습니다.	●	●	
전체 설정 및 형식 관련 교육	다중요소 인증을 요구하는 사이트를 포함해 자동으로 인증을 마친 후 사이트를 스캐닝합니다.	●	●	
비즈니스 로직 분석	애플리케이션 레이어에 대해 수동으로 침투 테스팅을 하여 스캐너만으로는 드러나지 않는 논리적 취약점을 검출합니다.	●		

WhiteHat DAST만의 장점

엔터프라이즈급 비즈니스 보고서 - 유연한 형식

강력한 보고서 생성 기능으로 보안 프로그램의 성능을 파악하고 애플리케이션 보안을 개선할 수 있습니다. 고급 분석 기능으로 수정 완료 비율, 수정 소요시간, 취약점의 노출기간 등 추이와 주요 통계를 모니터링할 수 있습니다. 추이 분석이 실시간 이력 데이터를 추적하므로 시간 경과에 따른 보안 위험 노출을 평가하고 이를 통해 안전한 사이트와 그렇지 않은 사이트를 한눈에 파악할 수 있습니다.

WhiteHat Security Index

WhiteHat Security Index(WSI)는 애플리케이션의 전반적 보안 상태를 나타내는 점수로 이를 통해 웹사이트 보안성을 즉시 눈으로 판단할 수 있습니다. 이 점수는 여러 산업 내 방대한 지표 데이터와 인텔리전스 메트릭스 분야에서 쌓은 경험을 토대로 계산돼 웹사이트 전체의 애플리케이션 보안 현황을 정확히 보여주는 잣대가 됩니다. WSI가 제공하는 인사이트를 통해 보안 위험 감소, 시간 절약, 우선순위 선정, 전체적인 보안 개선이 가능합니다.

간편한 배포, 동시성, 확장성

WhiteHat DAST는 배포가 간편한 클라우드 기반의 동적 보안 테스팅 솔루션으로 속도 저하 없이 1만개 이상 웹사이트를 동시에 온보딩하고 테스팅 가능합니다. 확장성이 좋아 어떤 환경에도 적용 가능하여 개발 속도에 맞춰 조절도 가능합니다.

연속 분석 방법

WhiteHat DAST는 연속 분석을 통해 웹사이트의 변경에 따라 상시 스캐닝합니다. 웹 애플리케이션에 대한 코드 변경을 자동으로 탐지, 분석하고 취약점이 새로 발견되면 경고를 합니다. 또한 처음부터 테스팅하지 않고 취약점만 다시 테스팅하므로 "상시" 위험 분석이 가능합니다.

프로덕션 무해성

WhiteHat DAST는 성능 저하 없이 프로덕션 웹사이트에 안전하게 적용할 수 있습니다. 실제 코드 대신 테스트용 Injection 사용으로 데이터 무결성을 보장하며, 스캔 내용을 커스텀 튜닝하여 성능 저하 없이 전체를 커버할 수 있습니다.

검증되고 조치 가능한 결과 - 제로에 가까운 오탐

모든 보안 취약점은 보안전문가가 일일이 검증하고 AI로 보강하므로 오탐율이 사실상 제로입니다. 이를 통해 시정 프로세스를 간소화하고 심각도와 위협에 맞춰 보안 취약점 우선순위를 정할 수 있습니다. 결과적으로, 시정과 전체적인 보안에 더 집중할 수 있습니다.

오픈 API 통합

WhiteHat DAST는 자주 사용되는 버그 추적 시스템, 보안 정보 시스템와 이벤트 관리 솔루션, 거버넌스/위험/컴플라이언스 제품, 웹 애플리케이션 방화벽(WAF)과 통합이 가능합니다.

웹보안 전문가에게 상시 요청 가능

WhiteHat DAST을 도입하면 웹 애플리케이션 보안 테스팅 전문가에게 제한없이 요청하여 분야별 시정 지침을 제공받을 수 있습니다. "Ask a Question" 기능으로 보안 전문가를 언제든 포털에서 바로 만날 수 있습니다.

PCI 컴플라이언스

WhiteHat DAST는 내부 웹사이트와 공개 웹사이트에 대해 검증된 취약점 분석을 수시로 실시하므로 PCI DSS 3.1의 요구사항을 여유롭게 충족합니다. WhiteHat PE에서는 PCI DSS에서 요구하는 비즈니스 로직 분석과 침투 테스팅을 모두 실시합니다. WAF와 통합하여 가상패치를 만들어 보안 취약점을 수정하고 감사에 필요한 보고서를 제공합니다.

싱글 페이지 애플리케이션 전체 자동 스캐닝

WhiteHat DAST는 싱글 페이지 애플리케이션과 기존 애플리케이션을 전체 자동으로 스캔하고 테스팅합니다. 웹 애플리케이션을 브라우저로 로딩한 후 사용자와 같은 방식으로 처리합니다. 프로덕션에 지장을 주지 않고 분석하여 기존 스캐닝 도구가 놓치기 쉬운 취약점을 찾아냅니다.

WhiteHat DAST | 탐지 가능한 취약점

기술적 취약점

WASC Threat Classification 2.0

- 애플리케이션 구성 오류
- 디렉토리 인덱싱
- HTTP 응답 스머글링
- 부적절한 입력 취급
- 불충분한 트랜스포트 레이어 보호
- OS 커맨딩
- 원격 파일 포함
- SQL Injection
- XML 외부 개체
- XQuery Injection
- 콘텐츠 스푸핑
- 핑거프린팅
- HTTP 응답 분할
- 부적절한 출력 취급
- 메일 명령 Injection
- 경로 조작
- 라우팅 우회
- SSL Injection
- Injection
- 크로스 사이트 스크립팅
- 포맷 스트링 공격
- 부적절한 파일 시스템 권한
- 정보 유출
- 널 바이트 Injection
- 예측 가능한 리소스 위치
- 서버 설정오류
- URL 리디렉터 오용
- XPath Injection

OWASP Top 10

- A1- Injection
- A2 - 인증과 취약한 인증과 세션 관리
- A3 - 민감한 데이터 노출
- A4 - XML 외부 개체(XXE)
- A5 - 취약한 접근 통제
- A6 - 잘못된 보안 구성
- A7 - 크로스 사이트 스크립팅(XSS)
- A8 - 안전하지 않은 역직렬화
- A9 - 알려진 취약점이 있는 구성요소 사용 (DAST지원영역 외)
- A10 - 불충분한 로깅 및 모니터링 (DAST지원영역 외)

주: 제품 에디션별 자세한 지원 목록은 요청시 제공 드립니다.

Synopsys의 차별성

Synopsys는 위험을 최소화하고 속도와 생산성은 극대화하여 개발팀이 안전한 고품질 소프트웨어를 개발할 수 있도록 지원합니다. 애플리케이션 보안 분야의 리더로서 Synopsys는 정적 분석, 소프트웨어 구성 분석, 동적 분석 솔루션을 제공합니다. 개발팀은 이를 활용하여 자사코드, 오픈소스 컴포넌트, 애플리케이션 동작의 취약점과 결함을 빠르게 발견하고 보완할 수 있습니다. 업계 최고 수준의 도구, 서비스, 전문성을 겸비한 Synopsys와 함께라면 DevSecOps 및 소프트웨어 개발 주기 전체에서 보안과 품질을 최적할 수 있습니다.

자세한 정보는
www.synopsys.com/software에서
확인할 수 있습니다.

Synopsys, Inc.
경기도 성남시 분당구 판교역로 235
에이치 스퀘어 N동 5층
(우)13494 시높시스코리아

Contact us:
대표 번호: (82) 2-3404-2700
Email: sig-info@synopsys.com