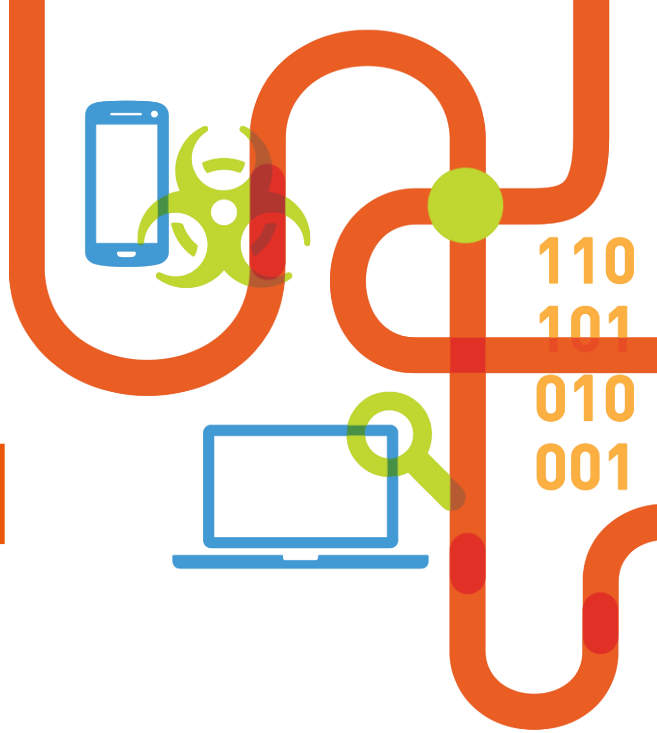
RAPID7



APPSPIDER 특장점 소개

최신 어플리케이션을 이해하는 DAST

㈜인섹시큐리티

INSEC security

appspider

Application Assessment for the Modern World

Know your weak points

Prioritize what matters most

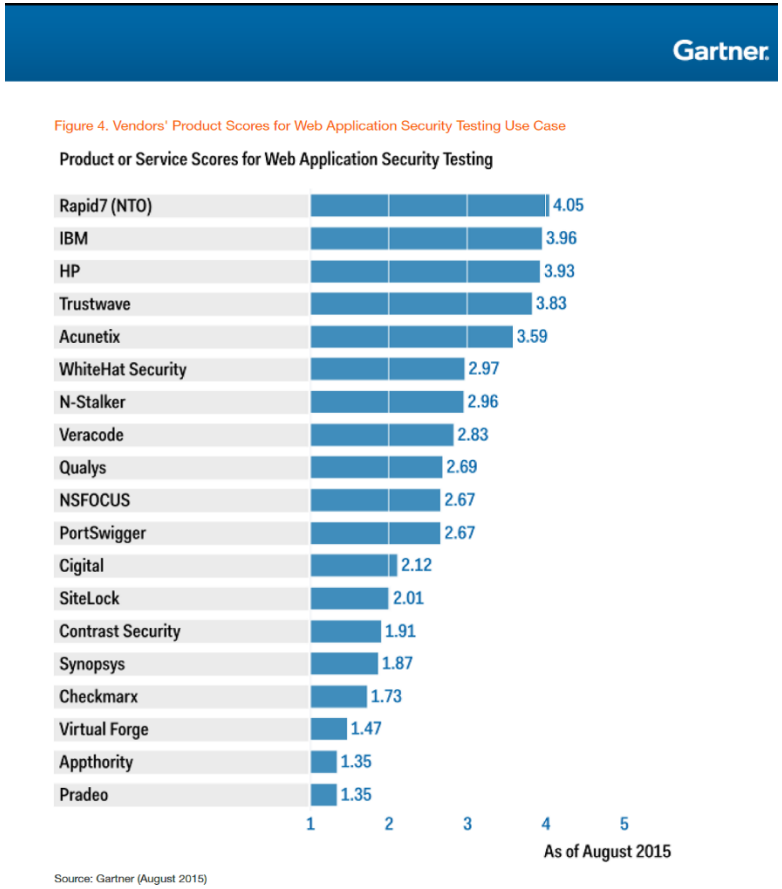
Improve your position

RAPID7

Advanced DAST

appspider

- 2015년 가트너에서 최고의 DAST로 선정
- 최신 웹기술 진단 기술 - JSON, REST, SOAP, XML-RPC, GWT-RPC, AMF, ReactJS, AngularJS, SPA
- 완전히 자동화된 웹앱 스캐너
- 원클릭 취약점 재검증 테스트
- 엔터프라이즈 규모 지원 – RBAC 지원 콘솔, Bug Tracking, SDLC 솔루션과 연동, 신속한 조치를 위해 WAF/IPS에 Virtual patch 제공

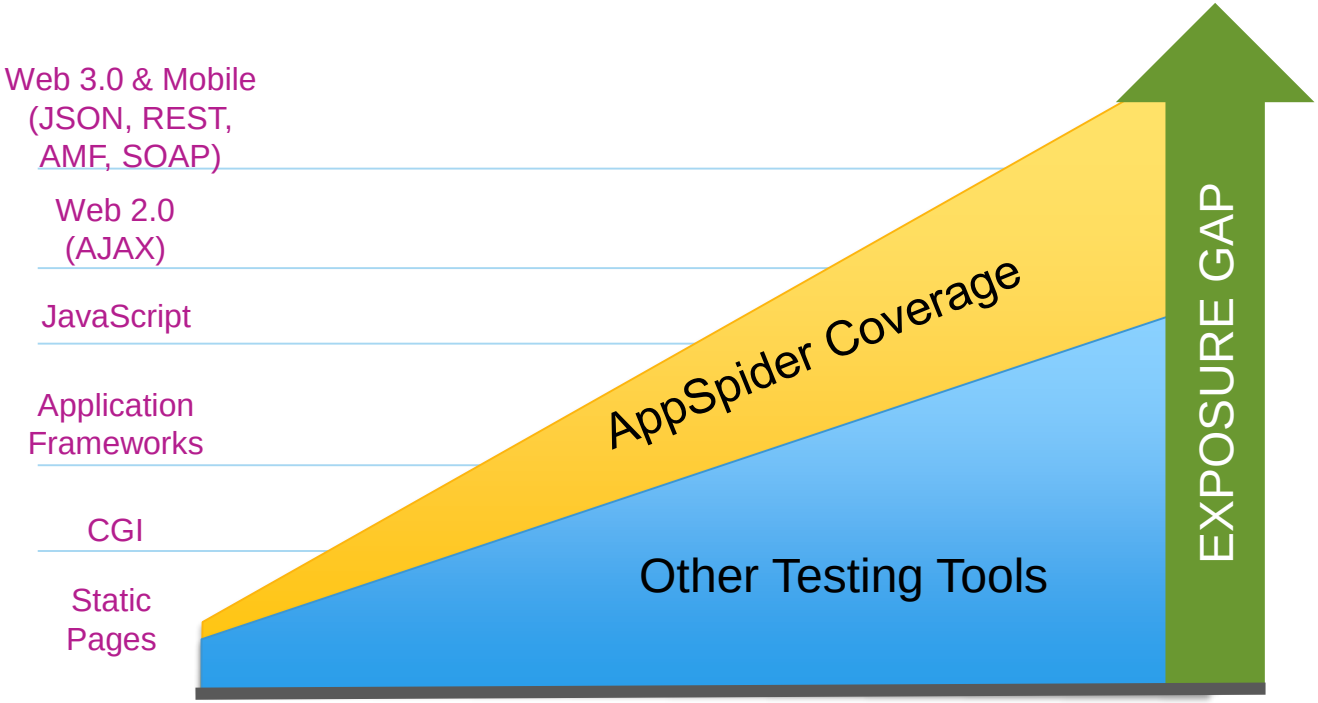


Gartner, Critical Capabilities for Application Security Testing, Joseph Feiman, Neil MacDonald, August 17, 2015

RAPID7

Know Your Weak Points

The Widening Coverage Gap



AppSpider covers more application technologies than any other WAS.

항목	1. 규모의 확장성 - 엔터프라이즈 고객을 위해 준비된 유연한 확장성

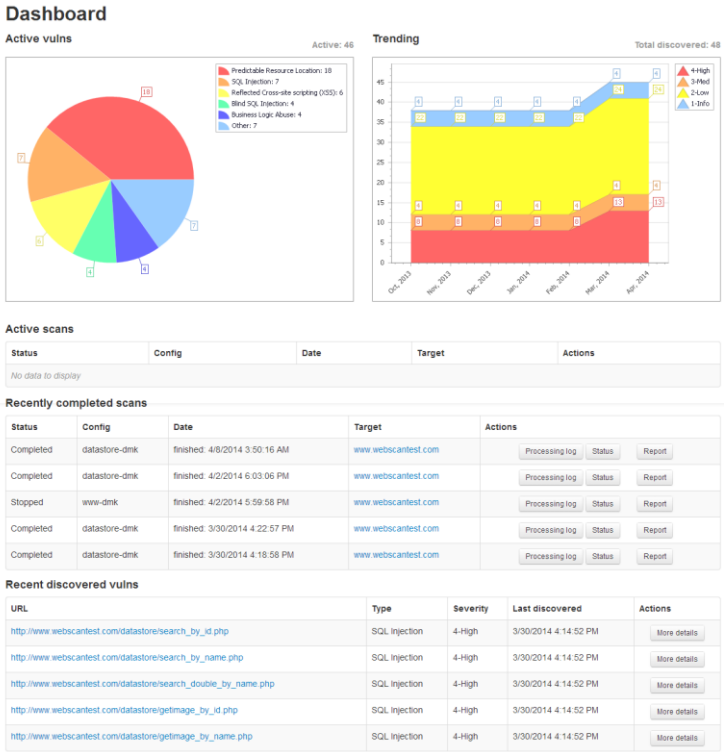
설명

단독형의 Appspider Professional 뿐 아니라 대기업 고객에 적합한 확장형 Appspider Enterprise 버전 제공 :

1. 중앙 통합 관리
   - 통합 관리 데시보드
   - Role-based 접근권한 부여
   - 스케줄링과 리포팅 통합
   - 조직 내부에 데이터 통합 저장 및 관리
   - 지속적인 Site 모니터링 – 마지막 스캔 이후 변화된 어플리케이션 부분만 확인 후 스캔

2. 확장성
   - 내부 사이트 영역별로 스캔 엔진 분리 설치
   - 개별 스캔 엔진들이 여러 영역에 걸쳐 서로 교차 진단 가능
   - 제한 없는 사용자 등록

상세 내용



항목	2. 최신 웹 기술 커버리지 – 최신 웹 기술을 가장 깊이있게 해석하고 진단

설명

AppSpider만의 독보적 기술인 **Universal Translator** 를 통해 AJAX, GWT, REST, JSON등과 같은 최신 웹 어플리케이션, 웹 서비스 그리고 모바일의 새로운 포맷 기술을 이해하고 해당 어플리케이션 영역의 취약점을 상세하게 진단 :

1. Universal Translator 의 새로운 웹 포맷에 대한 이해 능력 :
   - REST
   - JSON
   - AJAX
   - HTML4
   - HTML5

2. Universal Translator 의 해석 영역 :
   - Living in the DOM
   - True Sequence Support
   - XSRF Token Tracking
   - XML-RPC
   - Silverlight
   - Google WebToolkit
   - Flash Remoting (AMF)

상세 내용

항목	2. 최신 기술 커버리지 - 최신 웹 기술을 가장 깊이있게 해석하고 진단

기존 스캐너 수행 방식

RESTful 서비스 : 변형 후 공격하는 복잡한 JSON의 예

한 줄로 변경한 코드


```
{"products":[{"shirt":{"text":"NTO","colors":["blue","red","yellow","
green"],"sizes":["small","medium","large","xlarge"],"price":"19.99"}}
,{"hat":{"text":"NTO","colors":["black","red"],"sizes":["kids","adult
"],"price":"24.99"}}]}
```


기타 스캐너가 한 줄로 변경 후 공격하는 패턴


```
{"products":[{"shirt":{"text":"NTO","colors":["blue","red","yellow",
"green"],"sizes":["small","medium","large","xlarge"],"price":"19.99"
}},{"hat":{"text":"NTO","colors":["black","red"],"sizes":["kids","ad
ult"],"price":"24.99"}}]' OR 1='1}
```


예전 방식으로는 진단 효과가 없음

AppSpider의 수행 방식

RESTful 서비스 : 변형 후 공격하는 복잡한 JSON의 예

한 줄로 변경한 코드


```
{"products":[{"shirt":{"text":"NTO","colors":["blue","red","yellow",
"green"],"sizes":["small","medium","large","xlarge"],"price":"19.99"
}},{"hat":{"text":"NTO","colors":["black","red"],"sizes":["kids","ad
ult"],"price":"24.99"}}]}
```


AppSpider 가 한 줄로 변경 후 공격하는 패턴


```
{"products":[{"shirt' OR 1='1":{"text":"NTO","colors":["blue","red",
"yellow","green"],"sizes":["small","medium","large","xlarge"],"price
":"19.99"}},{"hat":{"text":"NTO","colors":["black","red"],"sizes":["
kids","adult"],"price":"24.99"}}]}
```


성공적으로 취약점 진단 수행


```
{"products":[{"shirt":{"text":"NTO","colors":["blue","red' OR 1='1",
"yellow","green"],"sizes":["small","medium","large","xlarge"],"price
":"19.99"}},{"hat":{"text":"NTO","colors":["black","red"],"sizes":["
kids","adult"],"price":"24.99"}}]}
```

항목	3. 뛰어난 정확성

설명

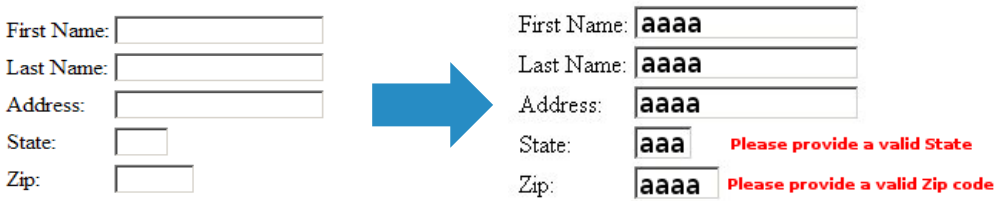
정교한 공격 테스트 기법으로 false positive 와 false negative 를 제거하여 업계에서 가장 정확성이 높음 :

1. 정교한 취약점 진단 알고리즘 적용
   - **폼 필드 입력을 임의의 문자열이 아닌 필드 값의 속성과 근사치 분석을 통해 입력 값 결정**
   - **데이터베이스 패턴 매치 후 입력 값 결정**
   - 취약점 진단을 위한 추가 검증 알고리즘 적용(ex- Blind SQL injection)
   - 잠재적 위험이 있는 XSS 변수 검출(XSS Reflection)

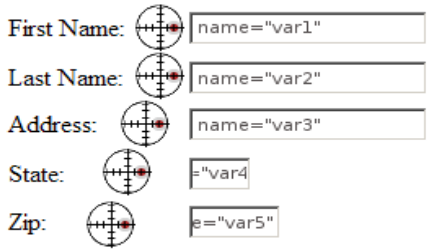
상세 내용

다른 스캐너들은 신뢰할 수 없는 변수나 id에 의존하여 보통 일반적 데이터를 대입함

```
<table>
  <tr><td>First Name: </td><td><input name="var1" /></td></tr>
  <tr><td>Last Name: </td><td><input name="var2" /></td></tr>
  <tr><td>Address: </td><td><input name="var3" /></td></tr>
  <tr><td>State: </td><td><input name="var4" size="2" /></td></tr>
  <tr><td>Zip: </td><td><input name="var5" size="5" /></td></tr>
</table>
```



AppSpider는 정확한 위치와 근사치를 분석하여 데이터베이스의 패턴 매치를 적용하여 대입



Input Name Pattern	Valid Data
/f(irst)?[\s]?name/i	John
/m(iddle)?[\s]?name/i	Paul
/l(ast)?[\s]?name/i	Smith
/address(1)?/i	123 Park Pl
/st(ate)?/i	CA
/zip(-)?(code)?/i	90210

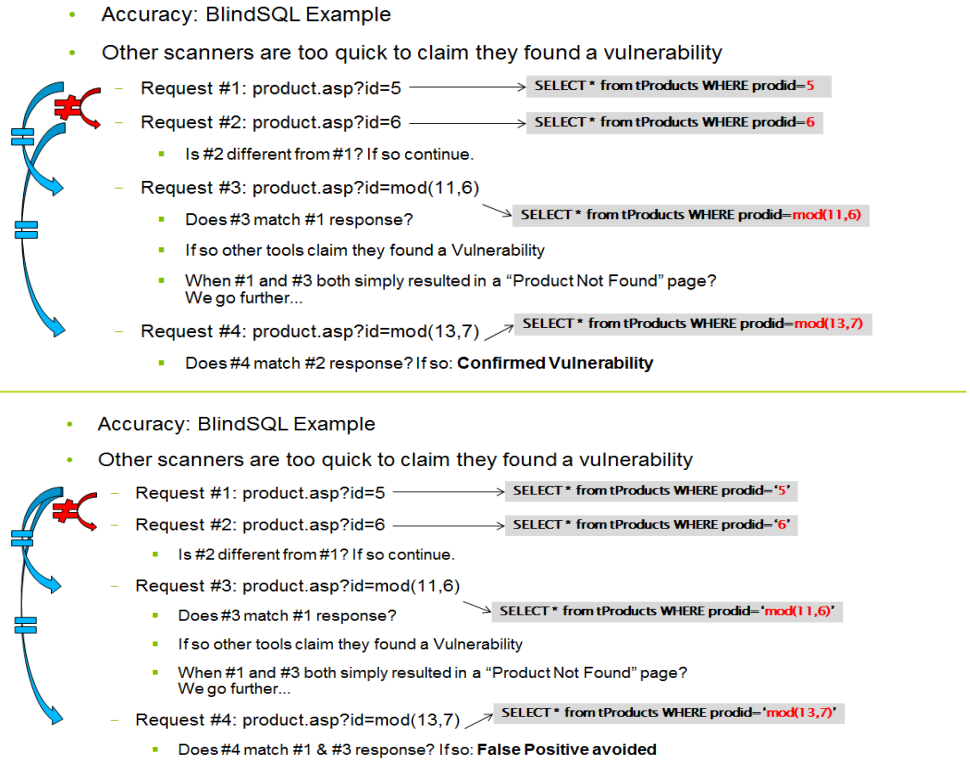
항목	3. 뛰어난 정확성

설명

Appspider 만의 정교한 공격 테스트 방법론으로 false positive 와 false negative 를 제거하여 업계에서 가장 정확성이 높음 :

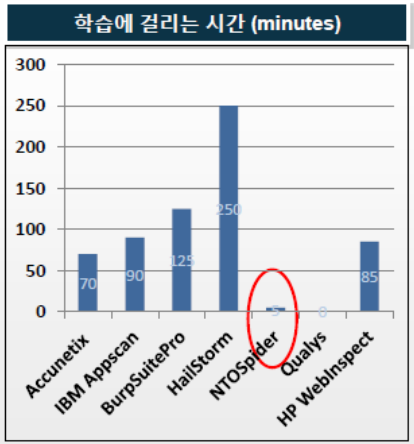
1. 정교한 취약점 진단 알고리즘 적용
   - 임의의 폼 필드 입력 값이 아닌 필드 값의 위치와 근사치 분석을 통한 입력 값 결정
   - 데이터베이스 패턴 매치 후 입력 값 결정
   - **Blind SQL 속성에 따라 다수의 변칙 검증 알고리즘 적용(ex- Blind SQL injection)**
   - 잠재적 위험이 있는 XSS 변수 검출(XSS Reflection)

상세 내용

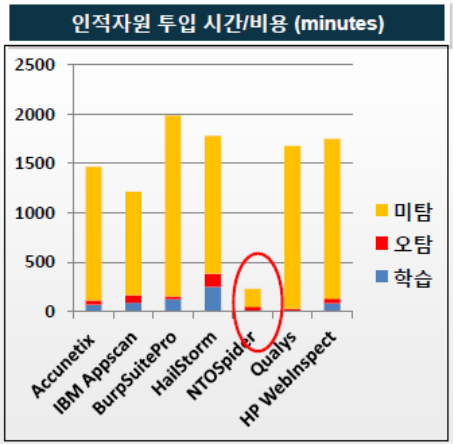


항목	3. 뛰어난 정확성

비교 데이터



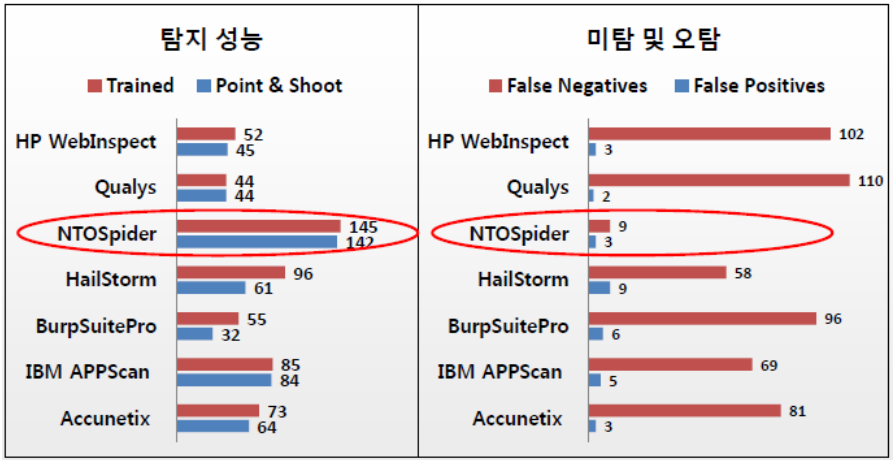
Qualys: Not Applicable



학습시간 + (# 오탐 * 15min) + (# 미탐 * 15min)

Source : 2010 Suto Study (ha.ckers.org/)의 최신 웹 어플리케이션 스캐너 성능 연구자료

비교 데이터



Source : 2010 Suto Study (ha.ckers.org/)의 최신 웹 어플리케이션 스캐너 성능 연구자료

항목	4. 자동화 - 사용하기 쉬움

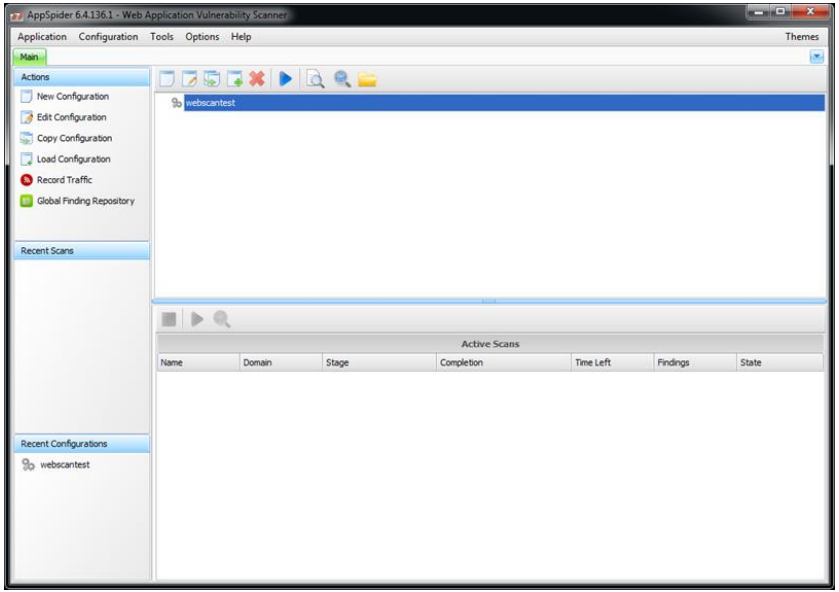
설명

간단히 진단 목표를 선정하고 즉각적으로 테스트를 시작할 수 있고 웹 어플리케이션 구조를 이해하고 취약점을 식별하는데 거의 완전한 자동화 로직을 적용하여 사용하기 쉽도록 설계

1. 자동화
   - 상세한 웹 페이지 크롤링
   - 폼 필드에 유효한 최적의 데이터로 자동 입력 테스트
   - 최소한의 사용자 개입으로 어플리케이션의 깊은 영역까지 자동화 스캔 수행

2. 단순한 메뉴 구성
   - 잘 정의된 기본 정책 설정
   - 핵심 기능 몇 가지로 압축된 Dashboard
   - 웹 형식의 간단한 보고서로 발견된 모든 취약점을 표현

상세내용



항목	4. 자동화 – 다양한 인증 지원 및 세션 관리 능력

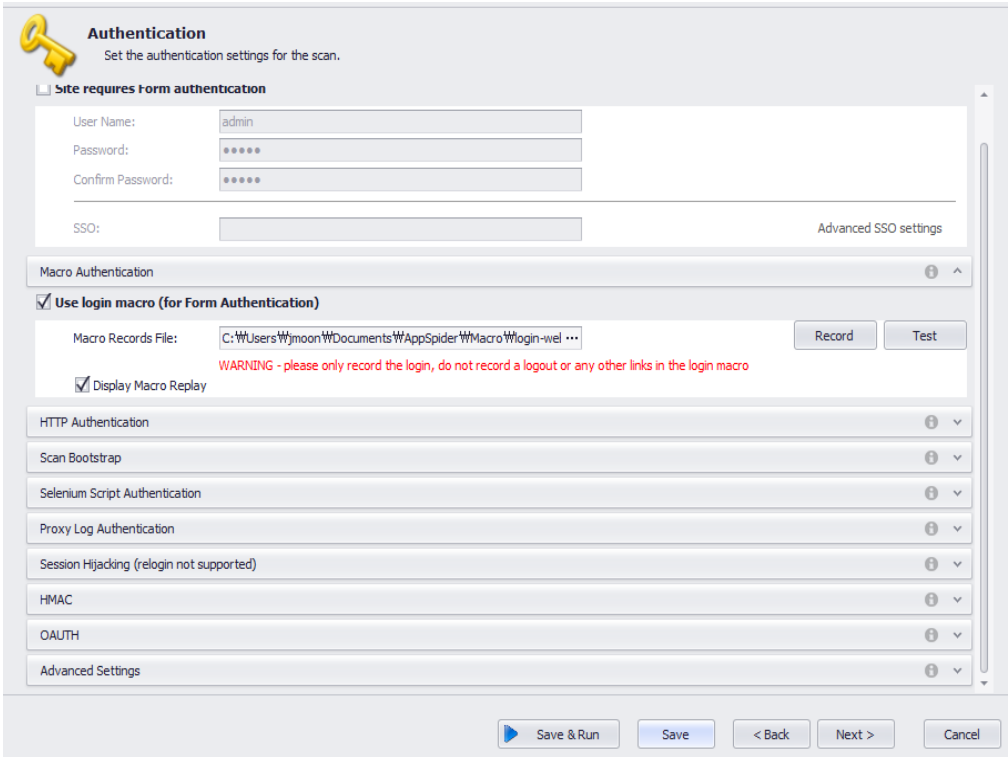
설명

다양한 로그인 인증 환경의 대상 웹 어플리이션에 손쉽게 인증을 수행하고 스캔을 위한 세션을 동적으로 유지하는 능력

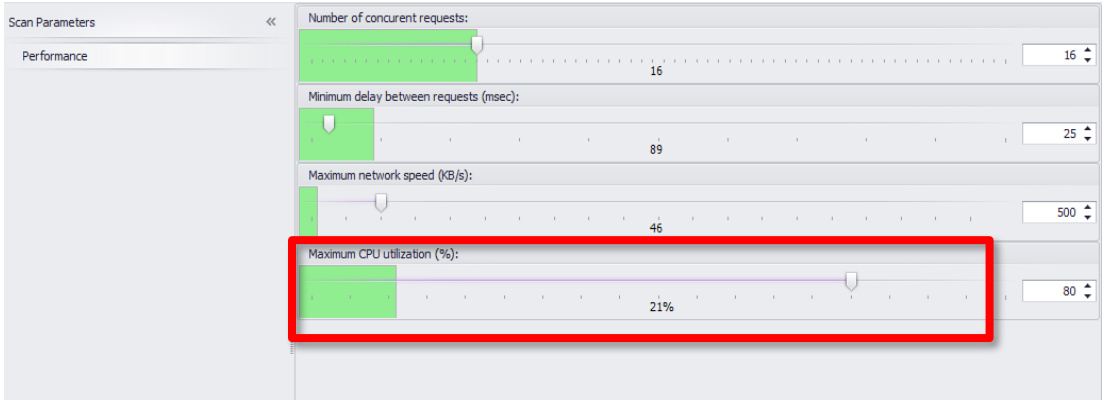
- 다양한 웹사이트 인증 패턴을 지원하기 위한 총 10가지 인증 설정
- 다단계 인증 단계를 기록 저장하여 자동인증 스캔 수행
- 다양한 일회성 토큰 인증의 경우 스캔할 때 수동 인증 설정
- HMAC(해시기반 메시지 인증 코드) 및 OAUTH 표준과 같은 웹 서비스 시스템 연동을 위한 인증 방식 제공
- SSL 인증서 기반 로그인 인증 지원

- 스캔 진행 동안 로그온 과정을 유지하도록 자동으로 세션 관리 수행

상세내용



항목	4. 자동화 - 맞춤형 스캔 성능 조절

설명	상세내용
대규모의 복잡한 웹 사이트도 적은 리소스로 효과적으로 진단 - 어플리케이션 엔진이 스캔 과정에서도 과다한 리소스를 요구하지 않음 - 실시간 성능 모니터링 및 조절 기능 제공	

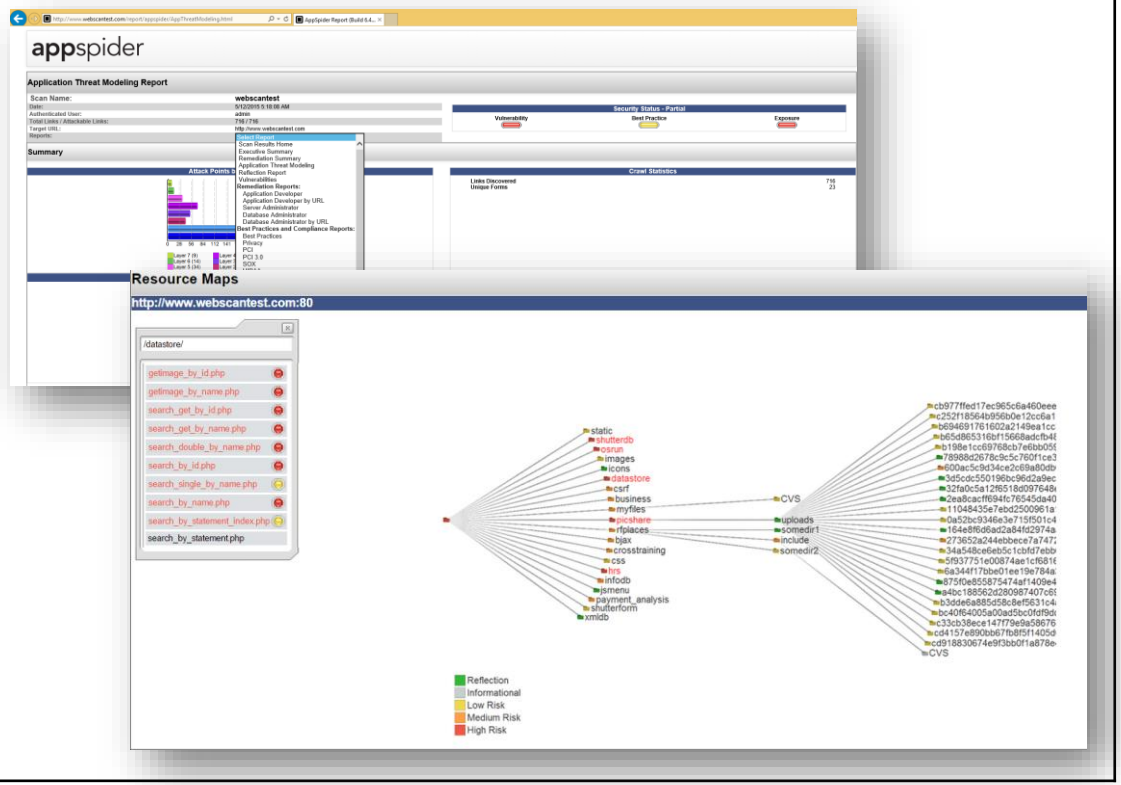
항목	5. 대화형 통합 리포트 – 즉각적인 데이터 접근을 위해 설계된 리포트

설명

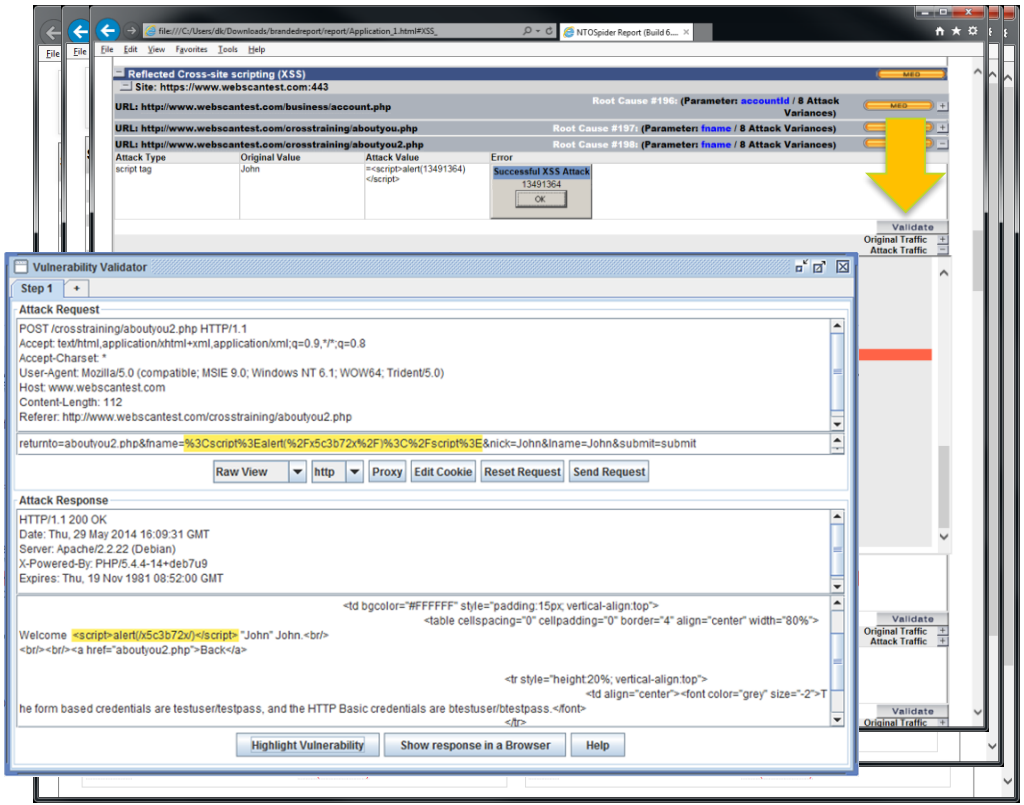
웹 기반의 리포트로 사용자가 클릭하면서 발견된 위험을 검증하고 실시간으로 공격 재현 테스트도 할 수 있는 동적인 인터페이스를 제공

- 전체 세부 리포트를 HTML 형태로 즉각적으로 확인할 수 있는 Live Report 형태로 제공
- 다양한 통계결과 다이아그램 제공
- 다양한 국제 표준 컴플라이언스 기반 리포트 자동 생성
- Resource Maps 기능에서 Crawling 수행 및 취약점이 포함된 분포를 시각적인 전체 웹 사이트 구조로 보여줌
- 개별 취약점 별로 상세한 설명과 근거를 제시하고 리포트 화면에서 사용자가 직접 공격테스트를 재시도 할 수 있음

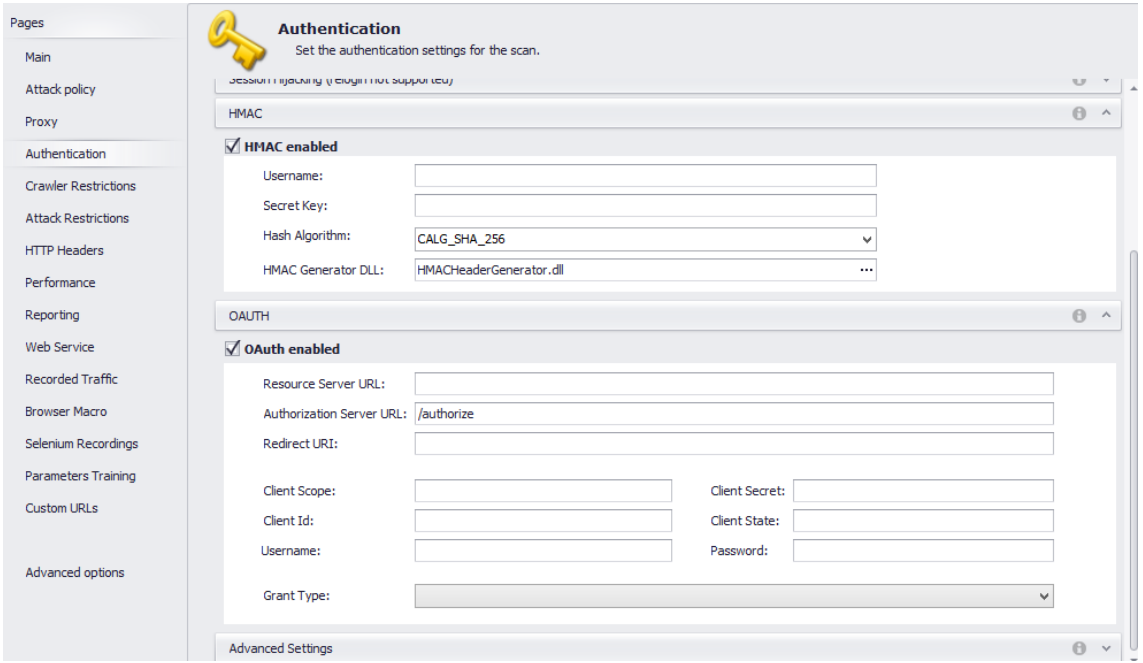
상세내용



항목	5. 대화형 통합 리포트 – 즉각적인 데이터 접근을 위해 설계된 리포트

설명	상세내용
웹 기반의 리포트로 사용자가 클릭하면서 발견된 위험을 검증하고 실시간으로 공격 재현 테스트도 할 수 있는 동적인 인터페이스를 제공 - 개별 취약점 별로 상세한 설명과 근거를 제시하고 사용자가 리포트 개별 취약점 항목에서 직접 공격 테스트를 재시도 할 수 있음	

항목	6. 복잡한 어플리케이션의 이해 - 웹 서비스 인증 지원

설명	상세내용
최근 웹 서비스에서의 인증 기법인 OAuth, 해쉬 메시지 인증 기법인 HMAC, 그리고 웹 사이트별 사용자 정의 인증 방식을 지원함으로써 일반적인 웹 서버 뿐만 아니라 복잡한 웹 서비스에 대해서도 원활하게 진단을 수행	

항목	6. 복잡한 어플리케이션의 이해 - 어플리케이션 워크플로우 상세 진단

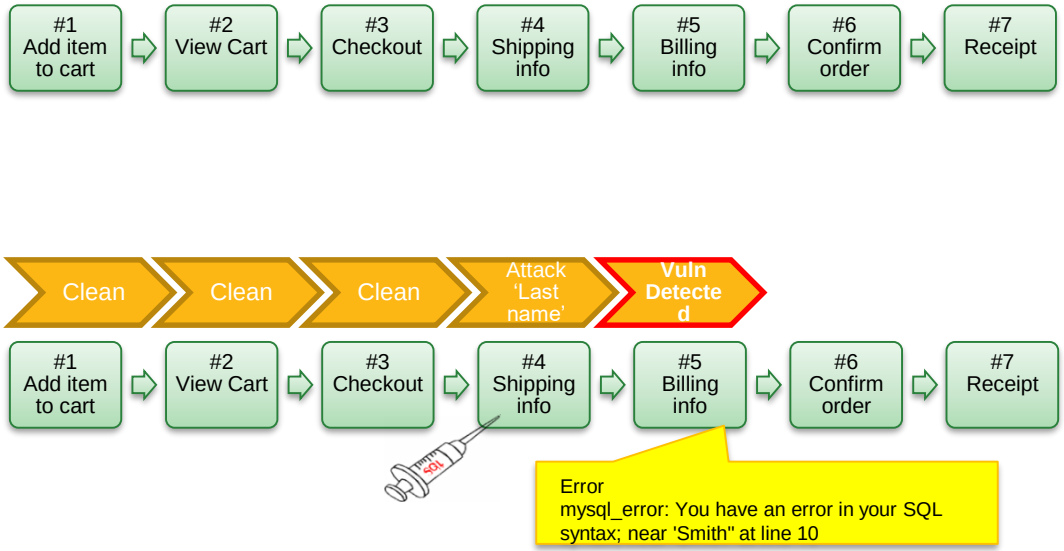
설명

인터넷 쇼핑몰 및 비즈니스 어플리케이션과 같은 복잡한 비즈니스 처리과정을 포함하는 웹 어플리케이션도 정교하게 진단

- 비스니스 처리 단계별로 접근하지 않는 이상 해당 각 단계별 어플리케이션 페이지의 취약점 여부를 진단할 수 없음

- Recoded Traffic 기능으로 비즈니스 처리 과정 단계별로 잠재된 취약점을 상세하게 진단

상세내용



항목	6. 복잡한 어플리케이션의 이해 - 어플리케이션 워크플로우 상세 진단

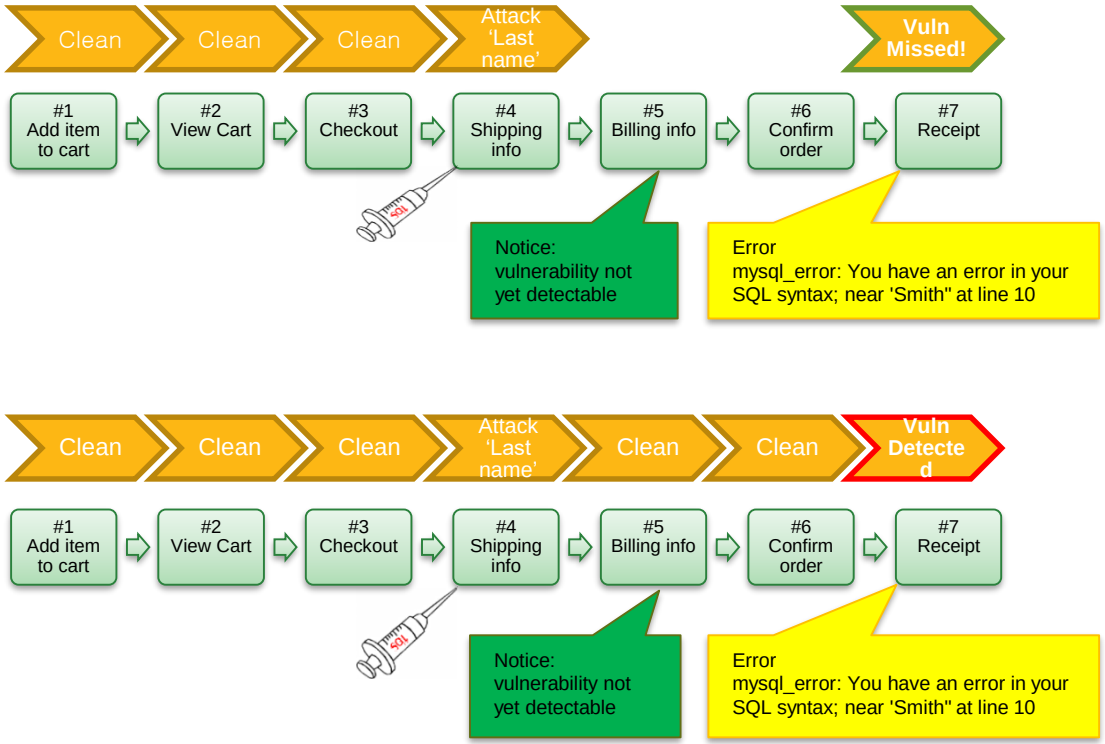
설명

인터넷 쇼핑몰 및 비즈니스 어플리케이션과 같은 복잡한 비즈니스 처리과정을 포함하는 웹 어플리케이션도 정교하게 진단

- 비스니스 처리 단계별로 접근하지 않는 이상 해당 각 단계별 어플리케이션 페이지의 취약점 여부를 진단할 수 없음

- Recoded Traffic 기능으로 비즈니스 처리 과정 단계별로 잠재된 취약점을 상세하게 진단

상세내용



항목	7. 사용자 정의 공격 기능

설명

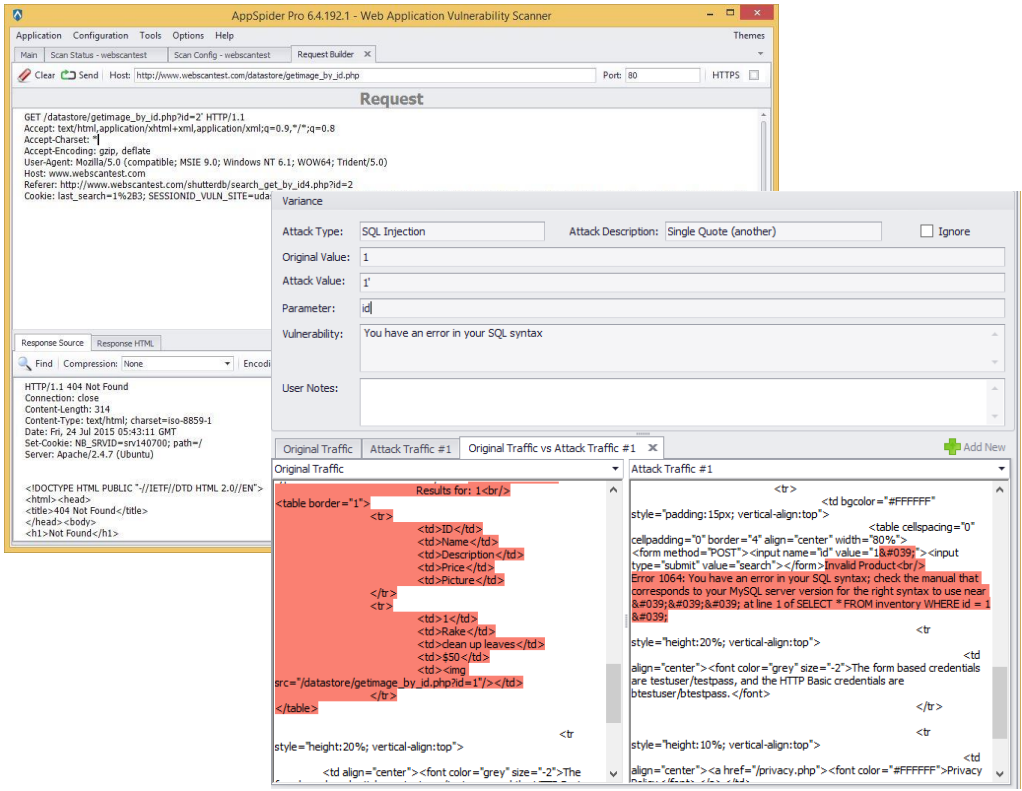
강력한 API 를 이용한 자체 테스트 툴과 연동을 제공하여 사용자가 직접 공격 모듈이나 패이로드를 제작하여 테스트를 수행

- 각종 Parameter 를 추가 및 수정할 수 있는 메뉴

- 리포트 결과 재공격 기능에서 공격 패이로드를 수정가능한 옵션

- 전체적인 사용자 정의 공격 코드로 테스트 가능한 Request builders 툴 제공

상세내용



항목	8. 취약점 차단정책 생성 – 주요 WAP/IPS 솔루션과 연동하여 발견된 취약점 차단정책 생성 전달

설명

웹 진단 후 긴 시간이 걸리는 취약점 조치의 문제점을 극복하기 위해 발견된 취약점에 대한 시그니처를 제공하여 고객이 운영 중인 WAF/IPS가 해당 취약점 시그니처를 기반으로 정확한 탐지 및 차단 정책을 생성할 수 있도록 지원

- 웹 취약점 진단 후 그 결과를 정교한 시그니처로 생성
- 시그니처를 WAF/IPS에 등록하여 보안 정책으로 즉각 적용

국내 솔루션과의 연동 현황

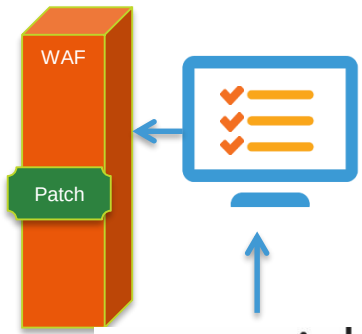
- Secui MFI 제품과 연동 완료
- 국내 주요 WAF 솔루션과 연동 제휴 진행 중

외국 솔루션과의 연동 현황

- Sourcefire, Imperva, NitroSecurity, ModSecurity, DenyAll, Barracuda, F5

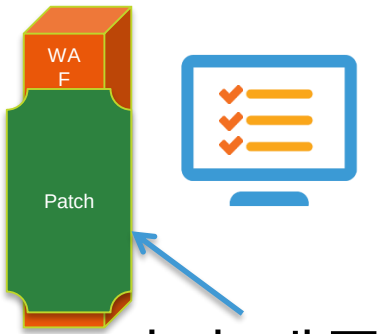
상세내용

Effective custom virtual patch
WAF knowledge + App knowledge



appspider

Ineffective virtual patch
Turn on default WAF rule

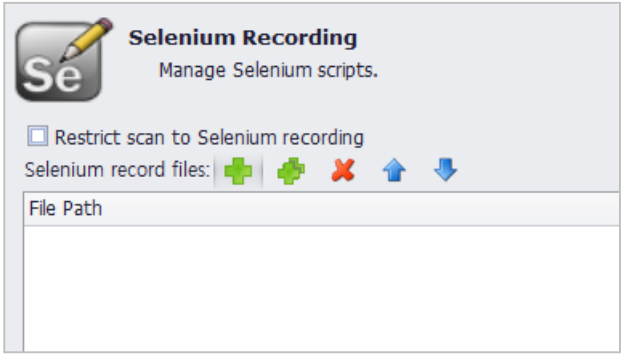


기타 제품

"AppSpider가 생성한 룰들은 다른 WAF/IPS 의 기본생성 룰보다 최소 39% 이상의 향상효과가 있었다."

어플리케이션 시큐리티 컨설턴트 Larry Suto.

항목	9. 3rd party 솔루션들과 연동

설명	상세내용
고객이 보유한 웹 보안 및 개발 관리 솔루션들과 연동하여 웹 보안 프로파일 생성 지원과 자동화된 웹 진단 수행 • **WAF/IPS** - Sourcefire, Imperva, NitroSecurity, ModSecurity, DenyAll, Barracuda, and F5 • **버그 트래킹** – Jira, HP Quality Center, RSA Archer • **DevOps / SDL** - Selenium,, Jenkins, Hudson, Bamboo, Burp, Fiddler, WebScarab, Paros, Swagger, Coverity, Checkmarx	 SOURCEfire® RSA® Archer GRC CHECKMARX


vodafone
Microsoft
Cargill
NETFLIX
bmc
Deloitte & Touche
U.S. DEPARTMENT OF ENERGY
at&t
UNITED STATES NAVY
axway
business. in motion
DEPARTMENT OF HOMELAND SECURITY
zendesk
DELL
CERIDIAN
Trusted Results. Transformative Technology.
Northern Trust
texas.gov
CME Group
NREL
NATIONAL RENEWABLE ENERGY LABORATORY
LOCKHEED MARTIN
IRS
U.S. Department of Veterans Affairs
AXA
HCSC
Health Care Service Corporation
AkzoNobel
monster
proofpoint
Abercrombie & Fitch
COMMERCE.GOV
UNITED STATES DEPARTMENT OF COMMERCE
protiviti
Risk & Business Consulting. Internal Audit.
RAPID7
MUFG
Bank of Tokyo-Mitsubishi UFJ

"In early 2014, Microsoft's Trustworthy computing group decided to do an extensive evaluation of DAST solutions on the market. Due to the fact that Microsoft online services are extremely diverse, we were looking for a solution that had a great deal of flexibility and extensibility. We also wanted to work with a company that would be an agile partner in ongoing engineering efforts. Based on the results of our POC, we selected AppSpider and AppSpider Enterprise as our initial DAST provider platform. We value Rapid7's willingness to partner closely with us to achieve our objectives."

-Microsoft Trustworthy Computing Group

Top 3 Telecommunications Provider

“In 2012 the >>> Digital Technology Services Security Group conducted a POC of the leading DAST tools in the market and selected the NTO Enterprise (AppSpider Enterprise) platform as our DAST provider of choice. We have over >>> applications (including many mobile applications) that we must scan on a monthly basis and AppSpider was found to be more accurate and have the fewest false positives of everyone we tested. We have some of the largest ecommerce sites in the world and AppSpider was able to complete scans within our time frame, which was an issue with several of the other DAST products. We have been very pleased with the support and feature enhancements we have received. NTO’s support is far superior to the other vendors we evaluated.

HP & IBM
Why we beat ‘em

Brandon brought in a deal that encompassed **4800 IPs** for **Nexpose** Enterprise, **AppSpider** Enterprise with an addition **3 ENGINES, custom deployment** and **ASV** scans for **3-years**. That’s what we call a portfolio sell.

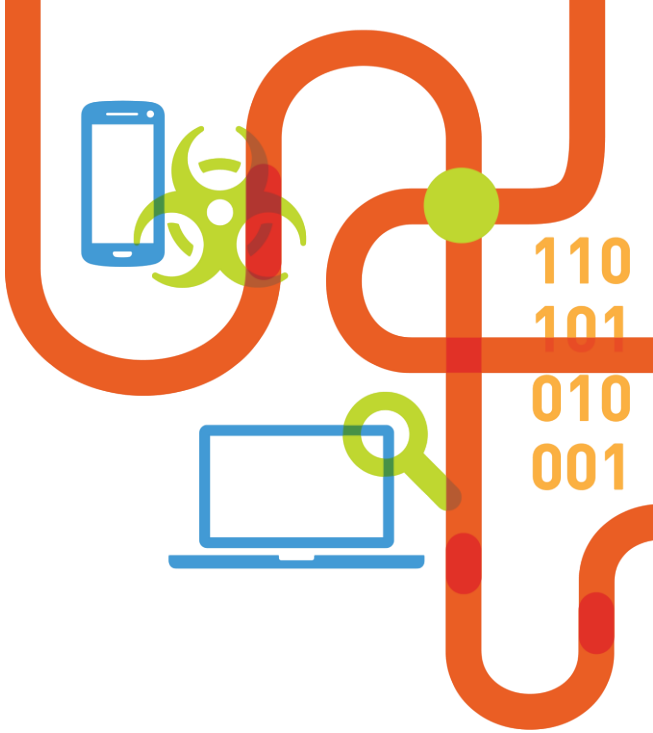
The Highlander started working on this deal back in September 2015, talking about AppSpider and Justin “**The Sharp Shooter**” Warren smashed it out of the park with portraying the value of DAST over SAST.

The Company was familiar with our offensive approach to security and were MSPRO customers previously. The small security team interacted with a ton of developers so the style of reporting out of AppSpider was perfect for both teams to effectively communicate what was needed.

The Problem:

1. With Application scanning, the developers needed to realize their code was flawed and they needed to be clearly shown what needed to be fixed. Burp wasn’t taking the cake from an enterprise scanner standpoint and they liked the scanning technology, reporting and integration with the R7 Suite.
2. With Vulnerability Scanning, they didn’t like the false positive rate with Nessus, the reporting was dubbed “trashy reporting” by the security team. They also needed strong integrations and neither Nessus or upgrading to Sec Center could solve this issue.

RAPID7



감사합니다.

INSEC security