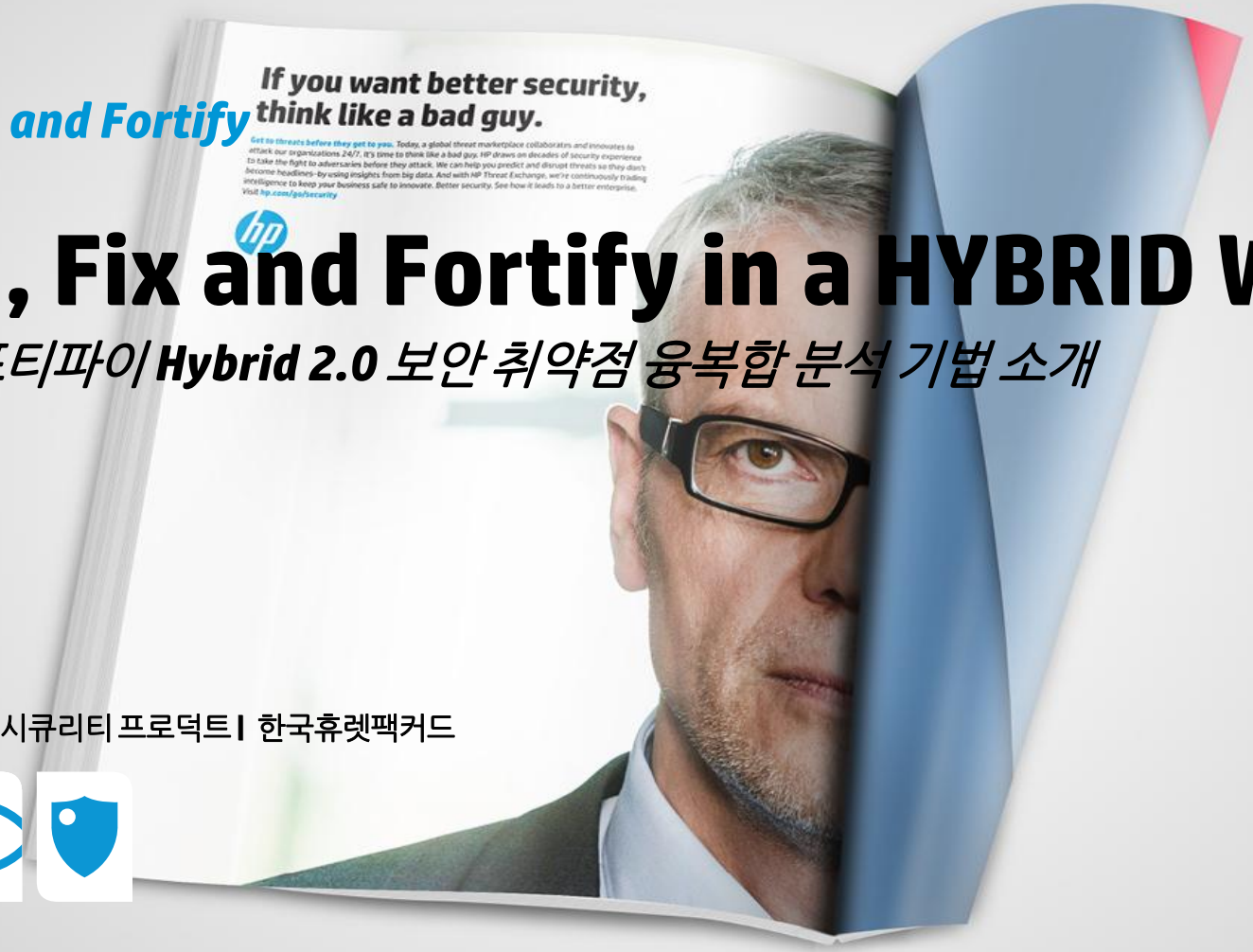
Find, Fix and Fortify



Find, Fix and Fortify in a HYBRID Way

*부제: 포티파이 **Hybrid 2.0** 보안 취약점 융복합 분석 기법 소개*

April 2014

엔터프라이즈 시큐리티 프로덕트 | 한국휴렛팩커드

Find, Fix and Fortify

최근 보안 이슈 분석

보안 취약점 분석 기법 리뷰

Hybrid 2.0 보안취약점 분석

OpenSSL Security Advisory [07 Apr 2014]

==========

TLS heartbeat read overrun (CVE-2014-0160)

==========

A missing bounds check in the handling of the TLS heartbeat extension can be used to reveal up to 64k of memory to a connected client or server.

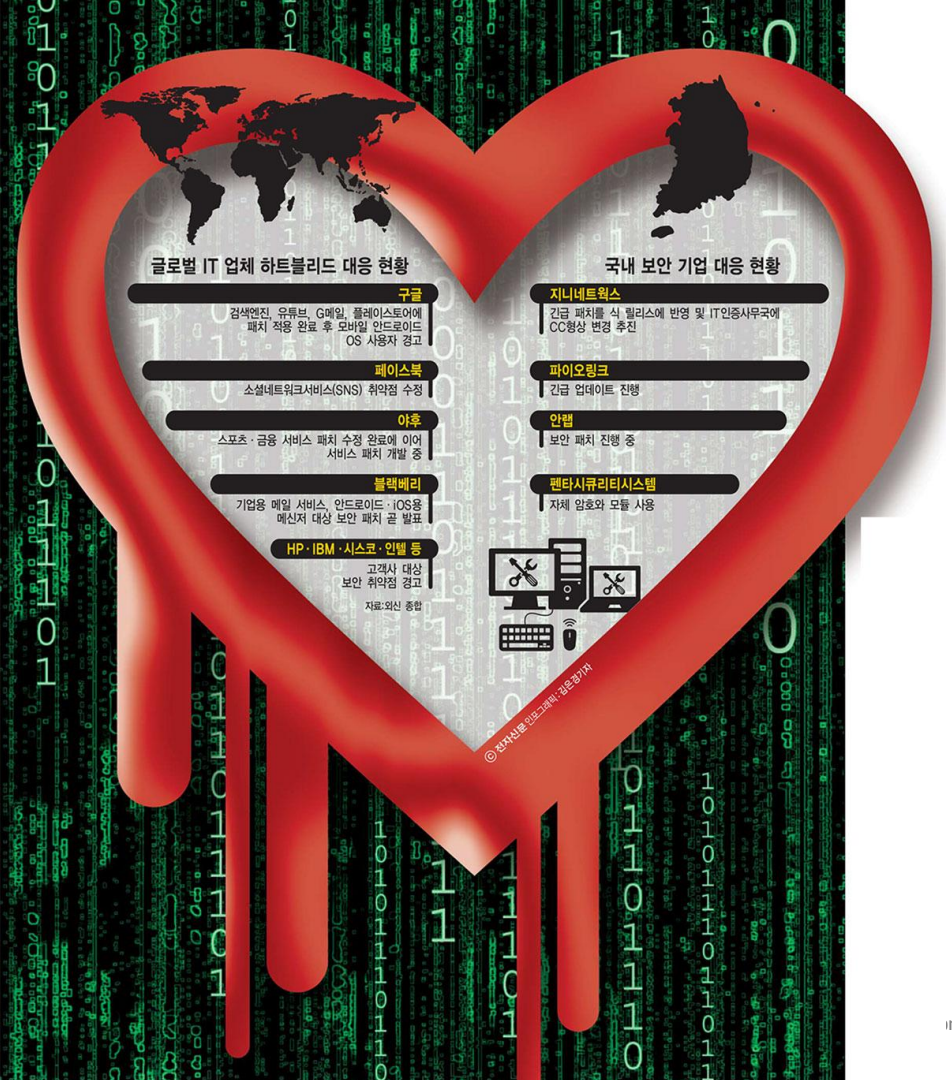
Only 1.0.1 and 1.0.2-beta releases of OpenSSL are affected including 1.0.1f and 1.0.2-beta1.

.....

Affected users should **upgrade to OpenSSL 1.0.1g**. Users unable to immediately upgrade can alternatively **recompile OpenSSL with -DOPENSSL_NO_HEARTBEATS**.

1.0.2 will be fixed in 1.0.2-beta2.

Source : http://www.openssl.org/news/secadv_20140407.txt



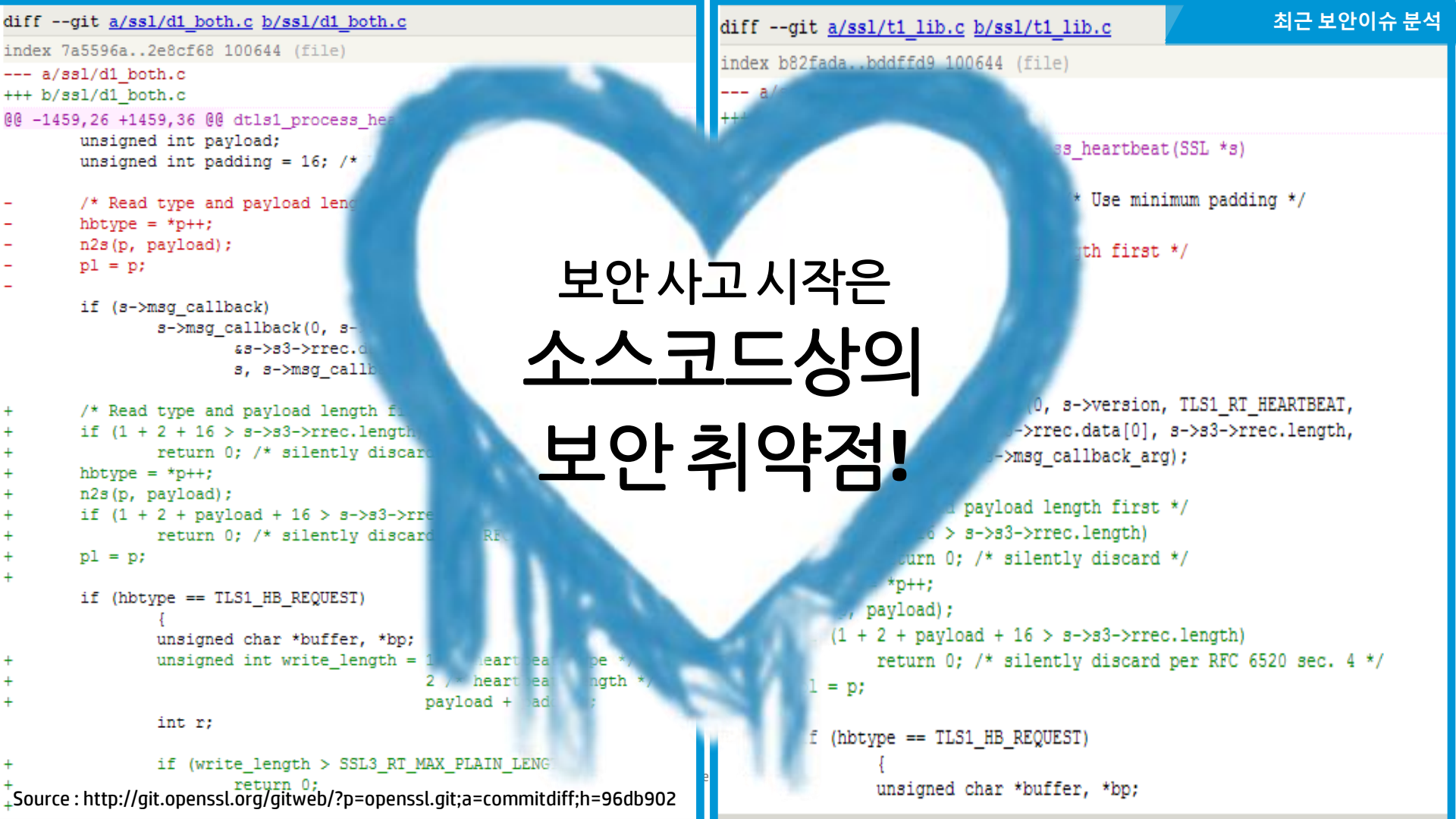
Blog posts for Heartbleed bugs on HP Security Research Blog :

- Heartbleed protection with **HP TippingPoint** : http://h30499.www3.hp.com/t5/HP-Security-Products-Blog/Heartbleed-protection-with-HP-TippingPoint/ba-p/6444226#.U0ilCvmSw-0

- HPSR Software security content update - Heartbleed bug detection (**HP WebInspect**) : http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/HPSR-Software-security-content-update-Heartbleed-bug-detection/ba-p/6445654#.U0ii3vmSw-0

- Heartbleed causes heartache : http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/Heartbleed-causes-heartache/ba-p/6444868#.U0ikJPmSw-0

- Thoughts on the Heartbleed bug : http://h30499.www3.hp.com/t5/Fortify-Application-Security/Thoughts-on-the-Heartbleed-Bug/ba-p/6442708#.U0Xp-_mSw-0



보안 사고 시작은

소스코드상의 보안 취약점!

Source : http://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=96db902

오픈**SSL** 하트블리드 취약점이 세상에 알려지며 보안 제품은 물론이고

모든 소프트웨어 개발에 '시큐어 코딩'을 의무화 해야 한다는 목소리에 힘이 실린다

Source : http://www.etnews.com/20140415000041

Find, Fix and Fortify

최근 보안 이슈 분석

보안 취약점 분석 기법 리뷰

Hybrid 2.0 보안 취약점 분석

소프트웨어 보안 취약점 분석 기법

보안 취약점 자동화 분석 기법

Static 정적분석 1	?	Dynamic 동적분석 2
소스코드	새로운 보안 취약점 분석 기법은?	웹 애플리케이션(침투테스트)
• **White Box Testing** • 보안 취약점 전수검사 (多) • 소스코드 레벨의 보안 취약점 상세결과 제공 • 근원적인 보안취약점 제거방법 제공	• 실제 공격가능한 보안 취약점 우선순위 도출 및 해당 보안 취약점에 대한 소스코드 레벨의 보안 취약점 상세 제공	• **Black Box Testing** • 실제 공격가능한 보안 취약점 검출(小) • 보안취약점 우선순위제공 (제한적인 분석범위) • 근원적인 보안취약점 해결 한계점 보유 • 웹 **Request /Response**를 통한 보안취약점 검출
사용자 : 개발자		사용자 : 보안팀/관제팀

Find, Fix and Fortify

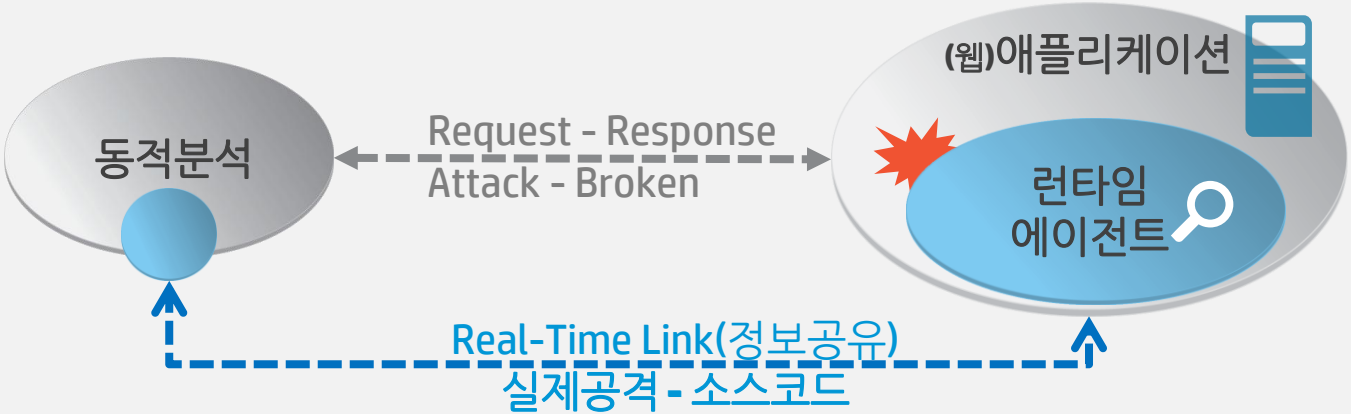
최근 보안 이슈 분석

보안 취약점 분석 기법 리뷰

Hybrid 2.0 보안 취약점 분석

Hybrid 2.0 보안 취약점 분석

분석기법 소개 : 런타임 분석 기법 (Gray Box Testing)



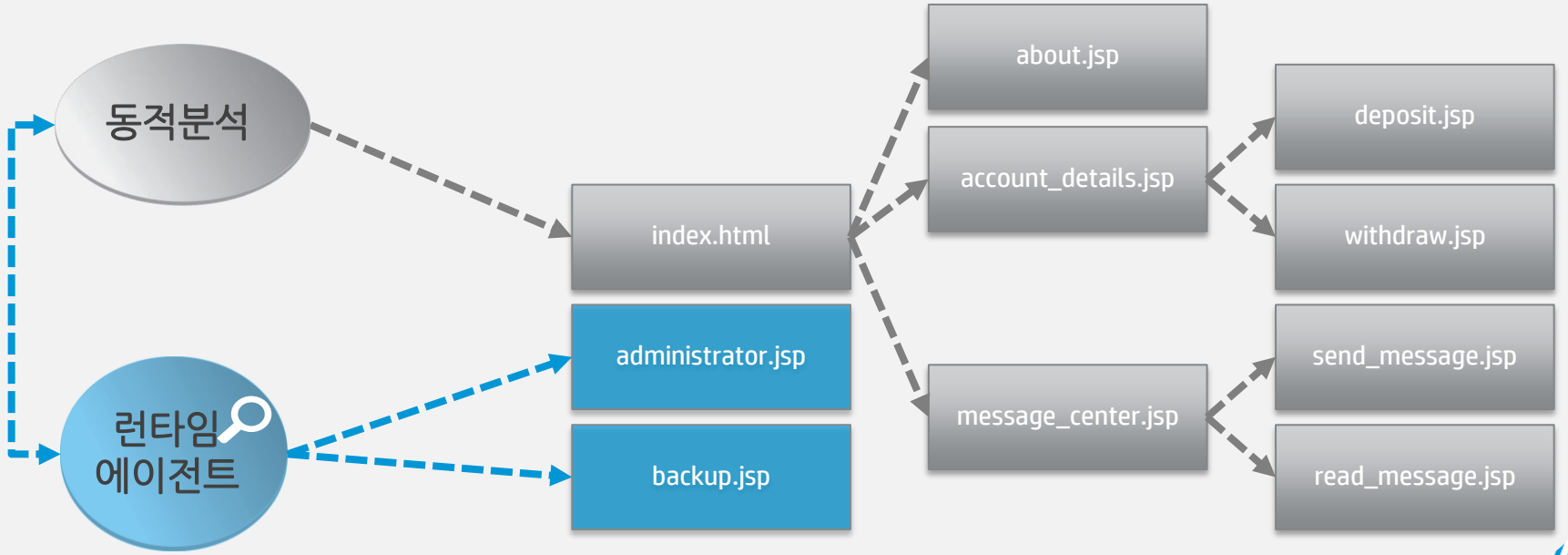
R 동적분석과의 협업을 통한 런타임 분석기법 기대효과

- **Find More** (동적분석에서 놓친) 보안 점검범위 확대(PT)
- **Fix Faster** (실제공격과 소스코드 연계통한) 소스코드 라인상 보안 취약점 정보 제공

Hybrid 2.0 보안 취약점 분석

분석기법 소개 : 런타임 분석 기법 (Gray Box Testing) – Find More(Missing Paths)

R Find More : 런타임 분석기법은 동적분석의 **Crawling**에 의해서 **Missing**되었던 자원을 발견하고 이를 동적분석기에 전달, 보안점검범위를 확대합니다.



Hybrid 2.0 보안 취약점 분석

분석기법 소개 : 동적분석 기법 (White Box Testing)

D 동적분석 예제 : WebGoat 5.4 / WebInspect 10.1 (OWASP Top 10 App Security Policy)

Crawl 983 of 983

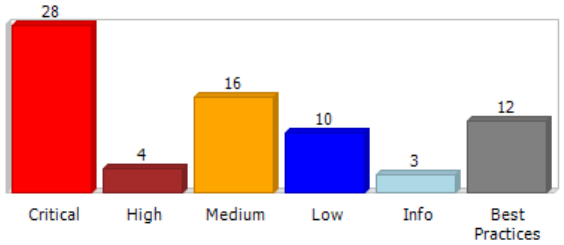
Audit 2,567 of 2,567

Scan Status
Completed

Activity	Req/Sec
Crawling	-
Auditing	-

Other	Evt/Sec
Script Execution	-
SecurityScope	Not Detected

Vulnerabilities



Attack Type	Attacks	Critical	High	Medium	Low	Info	Best Practices
Manipulation	31,571	28	2	9	0	0	0
Exploratory	18,081	0	0	0	1	0	0
Other	30,437	0	2	7	9	3	12

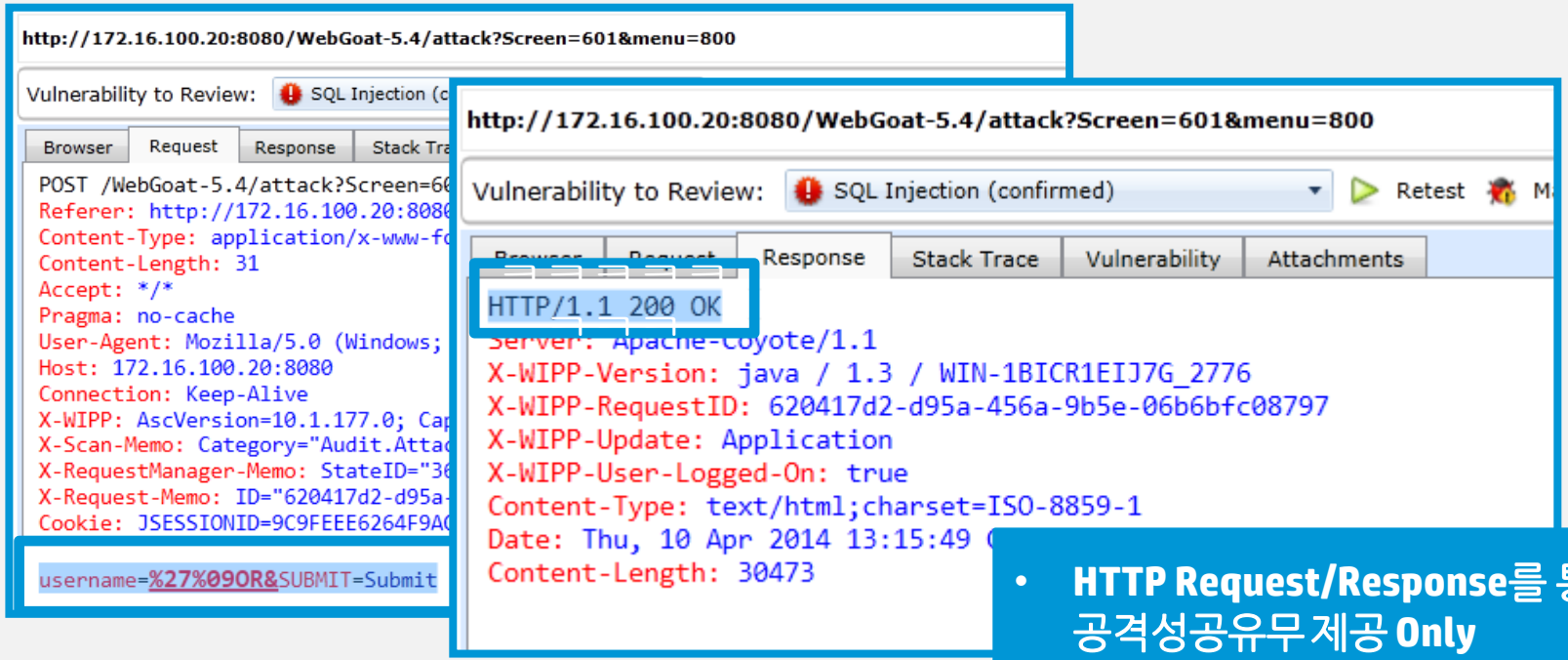
Scan	
Type:	Site
Duration:	08:05:46
Policy:	OWASP...
Deleted Items:	
Crawl	
Hosts:	1
Sessions:	748
Audit	
Attacks Sent:	80,089
Issues:	73
Network	
Total Requests:	81,292
Failed Requests:	4
Script Includes:	15
Macro Requests:	1
404 Probes:	407
404 Check Redirects:	19
Verify Requests:	0
Logouts:	0
Macro Playbacks:	1
AJAX Requests:	2
Script Events:	45,803
Kilobytes Sent:	98,908K
Kilobytes Received:	1,393,9...

- **Crawl(Session) : 748**
- **Issues(보안취약점) : 58**

Hybrid 2.0 보안 취약점 분석

분석기법 소개 : 동적분석 기법 (White Box Testing)

D 동적분석 예제 : WebGoat 5.4 / WebInspect 10.1 (OWASP Top 10 App Security Policy)



- **HTTP Request/Response를 통한 공격성공유무 제공 Only**

Hybrid 2.0 보안 취약점 분석

분석기법 소개 : 런타임 분석 기법 (Gray Box Testing) – Find More & Fix Faster

R 동적+런타임분석 예제 : WebGoat 5.4 / WebInspect 10.1 (OWASP Top 10 App Security Policy)

Crawl 1,751 of 1,751

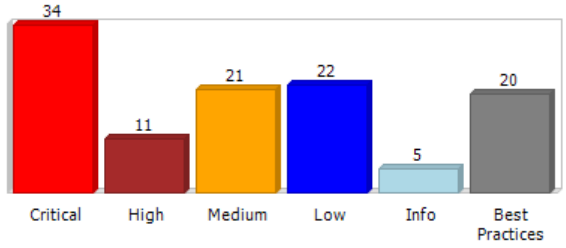
Audit 5,756 of 5,756

Scan Status
Completed

Activity	Req/Sec
Crawling	-
Auditing	-

Other	Evt/Sec
Script Execution	-
SecurityScope	Detected

Vulnerabilities



Attack Type	Attacks	Critical	High	Medium	Low	Info	Best Practices
Manipulation	32,286	34	2	9	0	0	0
Exploratory	385	0	0	0	0	0	0
Other	2,784	0	9	12	22	5	20

Scan

Type:	Site
Duration:	17:38:21
Policy:	OWASP...
Deleted Items:	

Crawl

Hosts:	1
Sessions:	1,288

Audit

Attacks Sent:	35,455
Issues:	113

Network

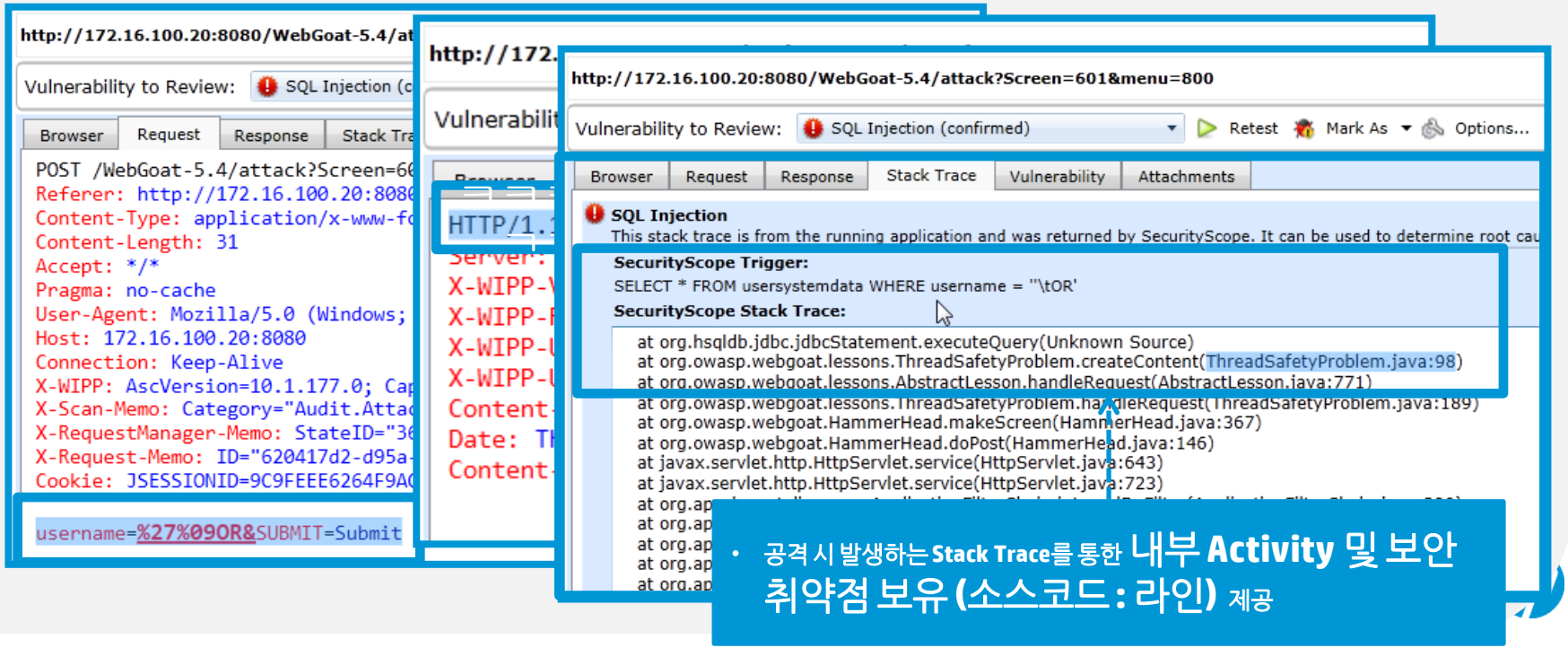
Total Requests:	46,685
Failed Requests:	3
Script Includes:	13
Macro Requests:	1
404 Probes:	476
404 Check Redirects:	23
Verify Requests:	0
Logouts:	0
Macro Playbacks:	1
AJAX Requests:	2
Script Events:	56,525
Kilobytes Sent:	56,963K
Kilobytes Received:	756,998K

- **Crawl(Session) : 1,248**
- **Issues(보안취약점) : 88**

Hybrid 2.0 보안 취약점 분석

분석기법 소개 : 런타임 분석 기법 ***(Gray Box Testing) – Find More & Fix Faster***

R 동적+런타임분석 예제 : WebGoat 5.4 / WebInspect 10.1 (OWASP Top 10 App Security Policy)

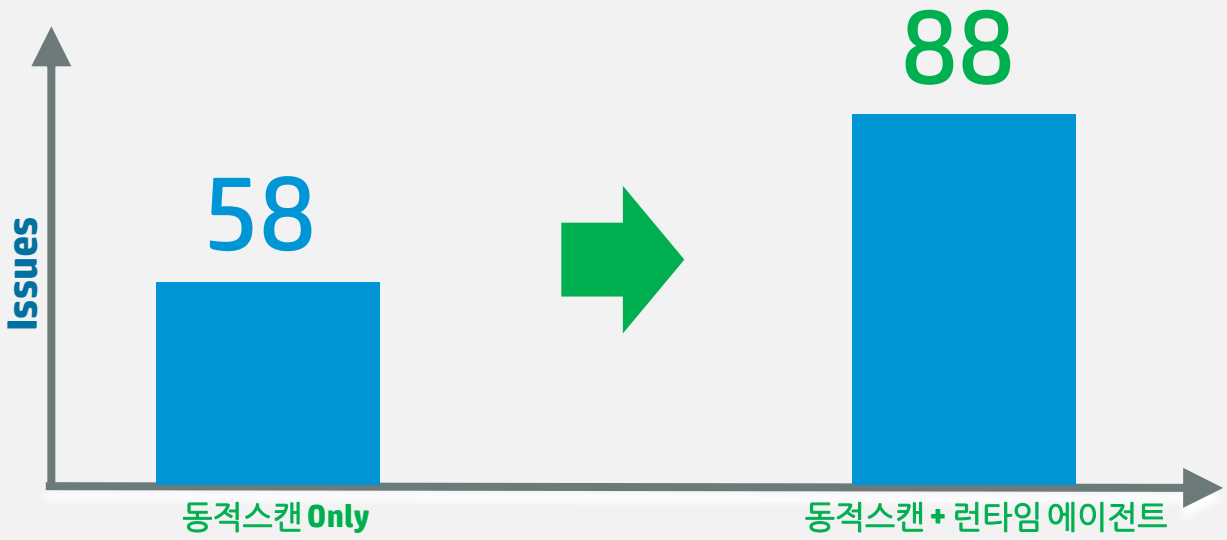


- 공격 시 발생하는 **Stack Trace**를 통한 내부 **Activity** 및 보안 취약점 보유 (소스코드 : 라인) 제공

Hybrid 2.0 보안 취약점 분석

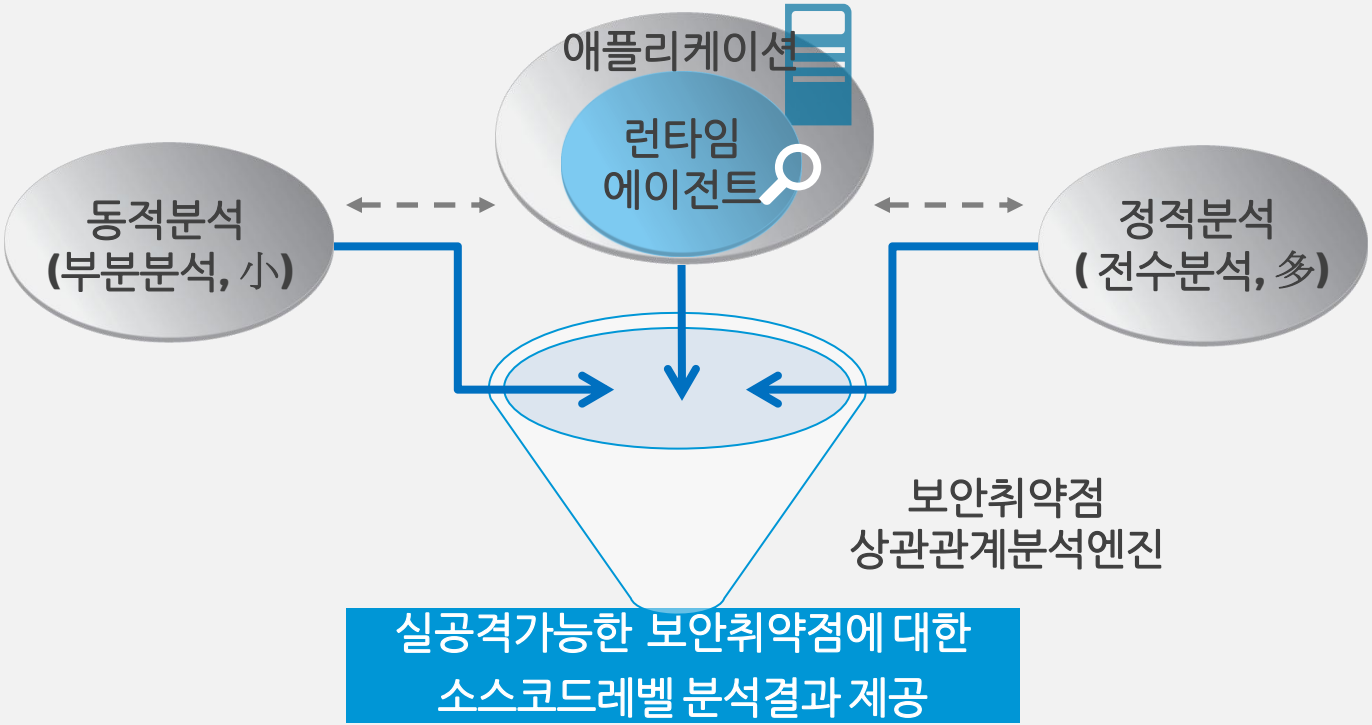
분석기법 소개 : 런타임 분석 기법 ***(Gray Box Testing) – Find More & Fix Faster***

R Find More & Fix Faster: 런타임 분석기법은 동적분석의 **Crawling**에 의해서 **Missing**되었던 자원을 발견하고 이를 동적분석기에 전달, **보안점검범위를 확대**하며 **Stack Trace**를 통해 **보안취약점과 소스코드 라인을** 연결 합니다.



Hybrid 2.0 보안 취약점 분석

분석기법 소개



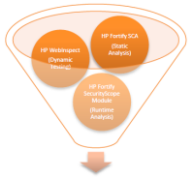
Hybrid 2.0 보안 취약점 분석

분석기법 소개

Static 정적분석	1	Runtime 런타임분석	+	Dynamic 동적분석	2
소스코드		웹 애플리케이션		웹 애플리케이션(침투테스트)	
• **White Box Testing** • 보안 취약점 전수검사 (多) • 소스코드 레벨의 보안 취약점 상세결과 제공 • 근원적인 보안취약점 제거방법 제공	✚	• **Gray Box Testing** • 애플리케이션 내부 실행 프로세스 모니터링 • 동적분석 솔루션과 연계하여 오탐축소, 보안 점검대상 확대(**Hidden applications**) • **Stack Trace**를 통한 새로운 보안 취약점 대상 공격 식별	✚	• **Black Box Testing** • 실제 공격가능한 보안 취약점 검출(小) • 보안취약점 우선순위제공 (제한적인 분석범위) • 근원적인 보안취약점 해결 한계점 보유 • 웹 **Request /Response**를 통한 보안취약점 검출	
사용자 : 개발자		사용자 : 테스팅/보안팀		사용자 : 보안팀/관제팀	

Hybrid 2.0 보안 취약점 분석

분석기법 소개 : Lining up with Attack and Source Code



보안취약점 I		보안취약점 II		보안취약점 III
정적분석	1	런타임분석	+	동적분석 2
• Category : SQL Injection • Package : path8.subdir • Class : Cart • Filename : Cart.java • Line : 359 • ID : 482	✚	• Category : SQL Injection • Package : path8.subdir • Class : Cart • Filename : Cart.java • Line : 359 • ID : 297	✚	• Category : SQL Injection • ID : 297
(1)보안 취약점 그룹핑		(2) 보안 취약점 상관관계 분석		(3) 상관분석된 보안취약점 위험도별 분류 및 소스코드 레벨 취약점 제거방법 제공

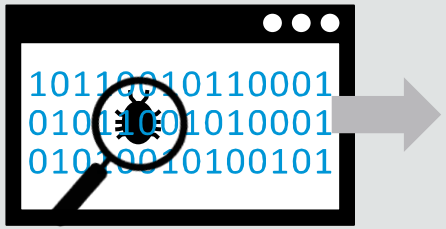
Hybrid 2.0 보안 취약점 분석

구성요소

1

Static Analysis

Fortify SCA/[1]SSC

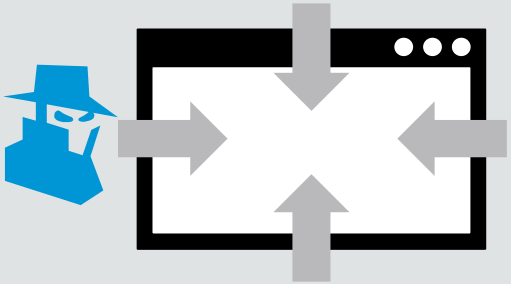


- 소스코드 레벨 보안 취약점 스캐닝
- **Static/WhiteBox/ Internal**
- **21**개의 개발 언어 지원(**Java, Objective-C, ASP.NET, C#, VB.NET, PHP, COBOL, ColdFusion, Classic ASP, ...**)

2

Dynamic Analysis

HP WebInspect/[1]SSC

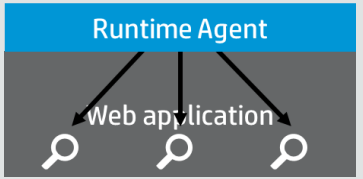


- **Running Application** 대상 보안 취약점 스캐닝
- **Dynamic/BlackBox/External**

3

Runtime Analysis

HP WebInspct Agent (SecurityScope)/[1]SSC



- 런타임분석
- 애플리케이션 내부 실행 모니터링(**Stack Trace** 모니터링)
- **Java, .NET**

Note : [1]SSC (Software Security Center) : 정적/동적/런타임 분석기에 의해 수집된 보안취약점 관리/상관분석 제공 시스템

Hybrid 2.0 보안 취약점 분석

동작원리

동작원리 준비

대상 애플리케이션 :

- **OWASP WebGoat 5.4 (Security Practice를 위해 의도적으로 보안취약점을 탑재한 Open Source)**

단위 보안 취약점 분석 결과물 :

- **정적분석결과(Static) : HP Fortify SCA**
- **동적분석결과(Dynamic) : HP WebInspect**
- **런타임분석결과(Runtime) : HP WebInspect Agent (SecurityScope)**

Fortify Software Security Center(SSC) :

- 정적/동적/런타임 분석기에 의해 수집된 보안취약점 관리 분석 (상관분석) 시스템

Hybrid 2.0 보안 취약점 분석

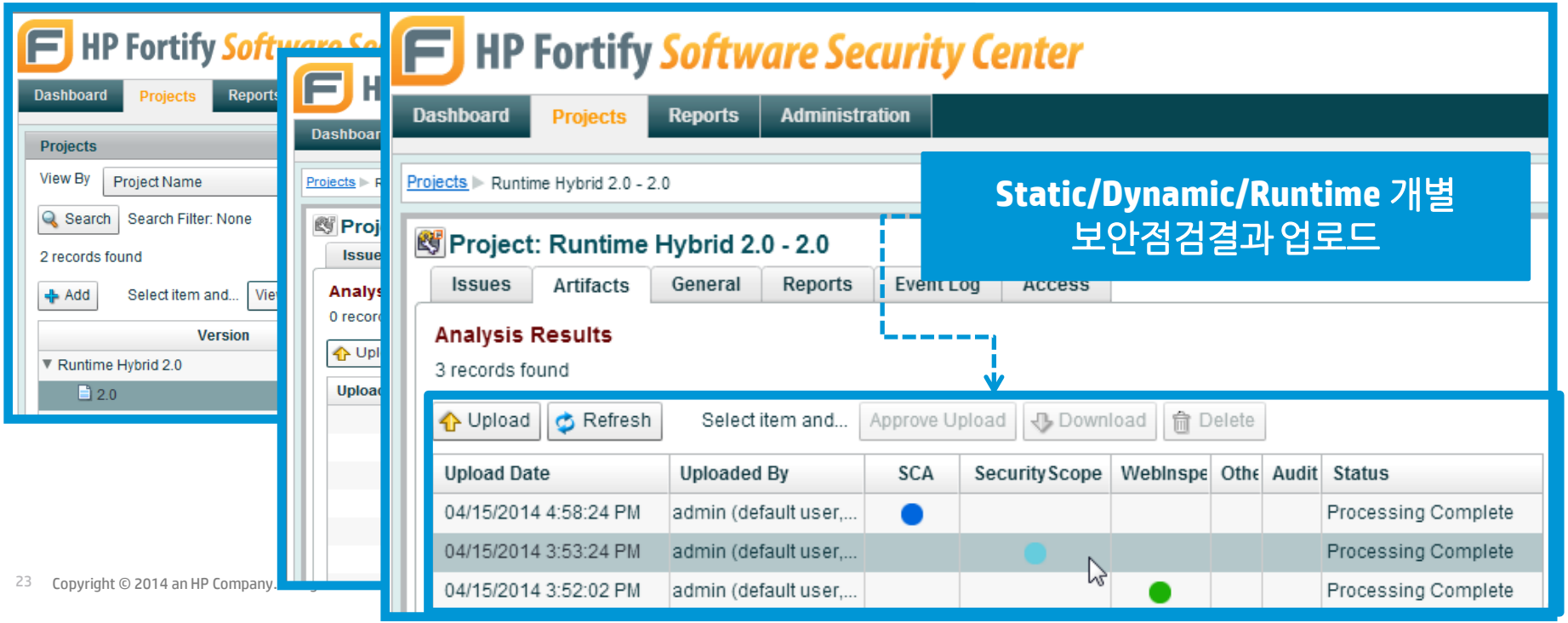
동작원리

프로젝트 생성 : ***Runtime Hybrid 2.0*** 1

Hybrid 2.0 보안 취약점 분석

동작원리

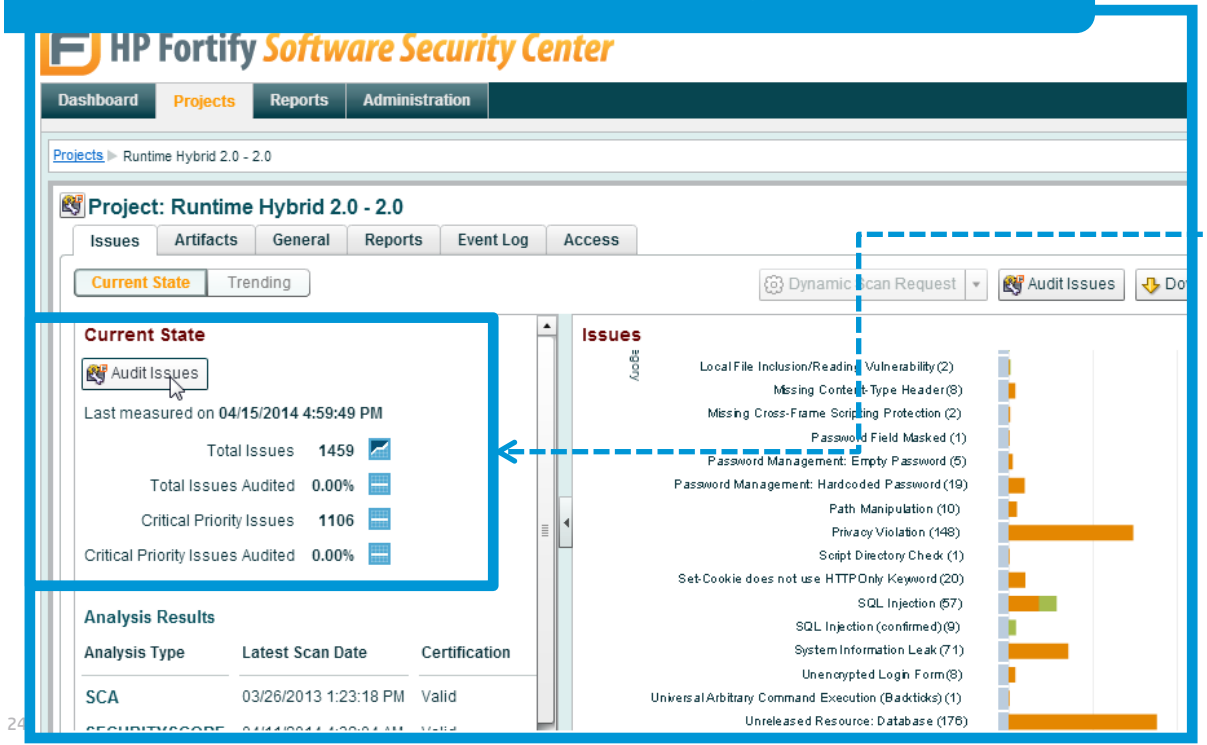
SCA(정적), SecurityScope(런타임), 동적(WebInspect) 단위 보안점검결과 업로드 2



Hybrid 2.0 보안 취약점 분석

동작원리

Audit Issues (WebGoat 프로젝트 보안취약점 현황 개요) 3

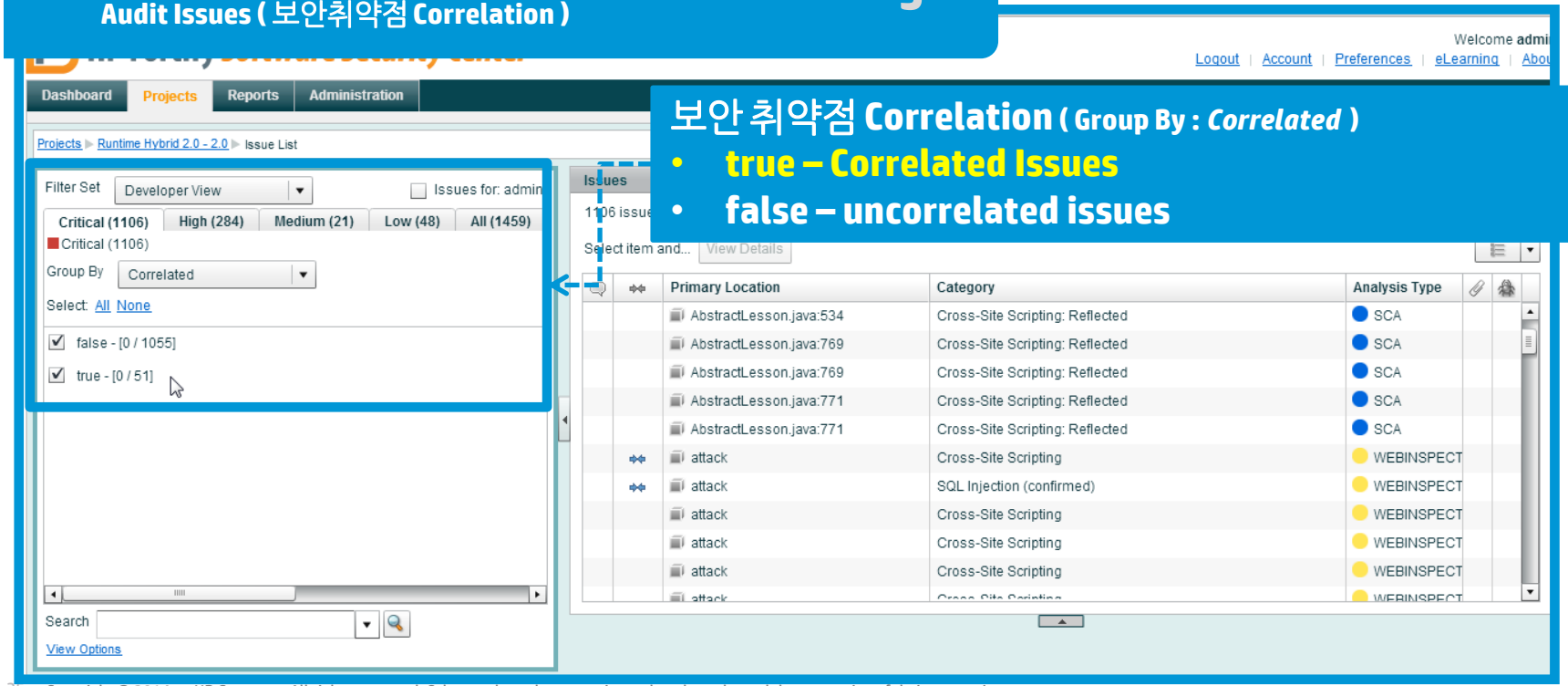


전체 보안 취약점 **1459**개

Hybrid 2.0 보안 취약점 분석

동작원리

Audit Issues (보안취약점 Correlation) 3



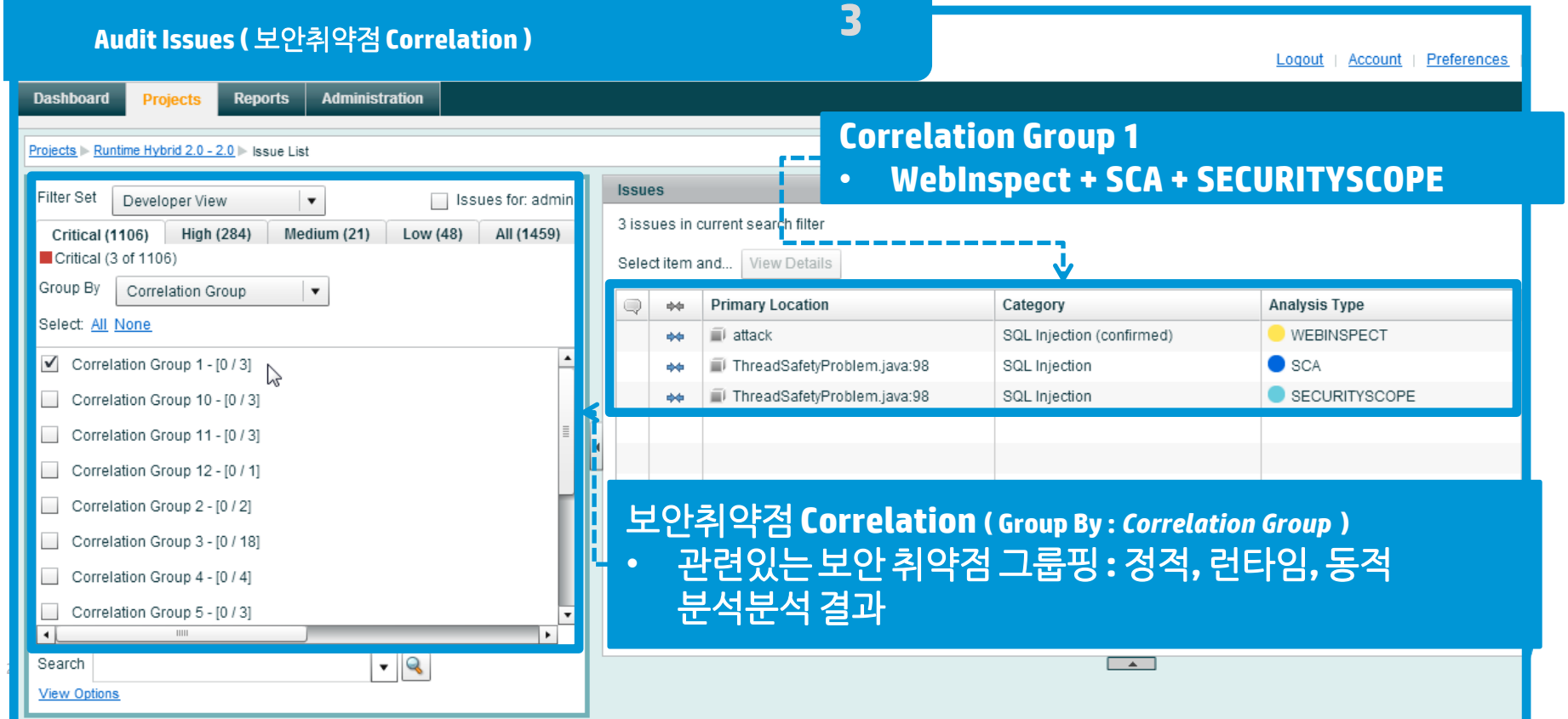
보안 취약점 **Correlation (Group By : *Correlated*)**

- **true – Correlated Issues**
- **false – uncorrelated issues**

Hybrid 2.0 보안 취약점 분석

동작원리

Audit Issues (보안취약점 Correlation) 3



Correlation Group 1

- **WebInspect + SCA + SECURITYSCOPE**

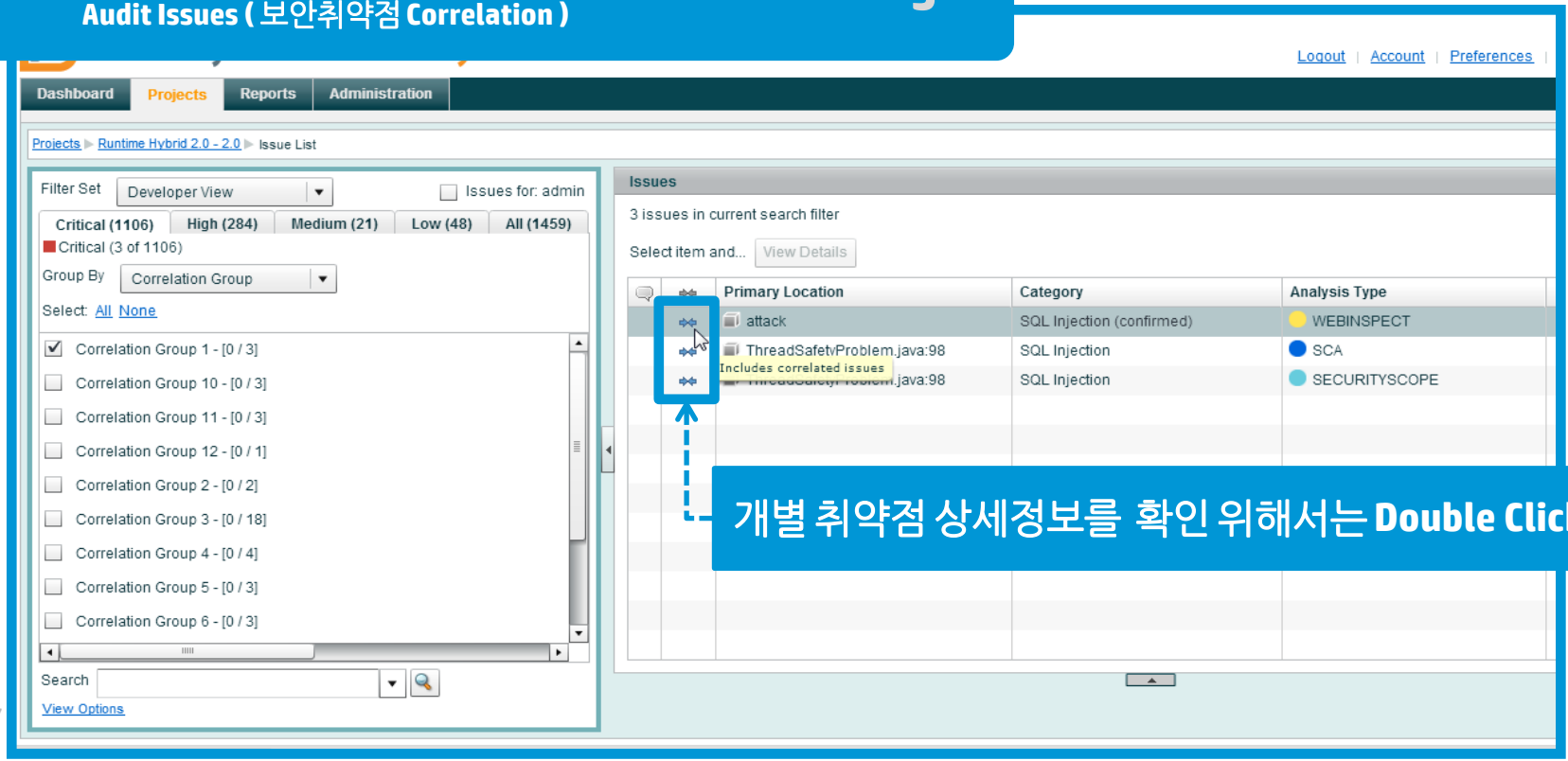
보안취약점 Correlation (Group By : *Correlation Group*)

- 관련있는 보안 취약점 그룹핑 : 정적, 런타임, 동적 분석분석 결과

Hybrid 2.0 보안 취약점 분석

동작원리

Audit Issues (보안취약점 Correlation) 3



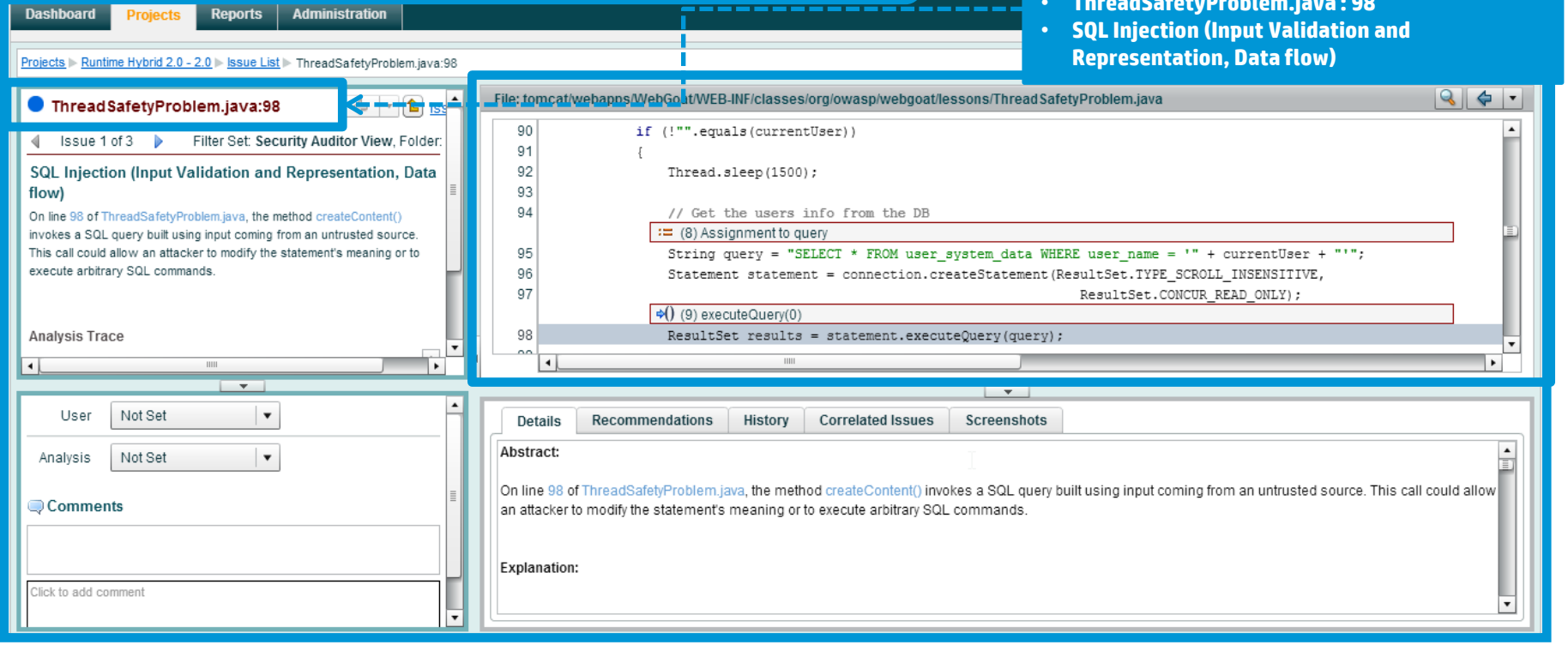
Hybrid 2.0 보안 취약점 분석

동작원리

Audit Issues (보안취약점 Correlation) 3

정적분석 **SCA**

- **ThreadSafetyProblem.java : 98**
- **SQL Injection (Input Validation and Representation, Data flow)**



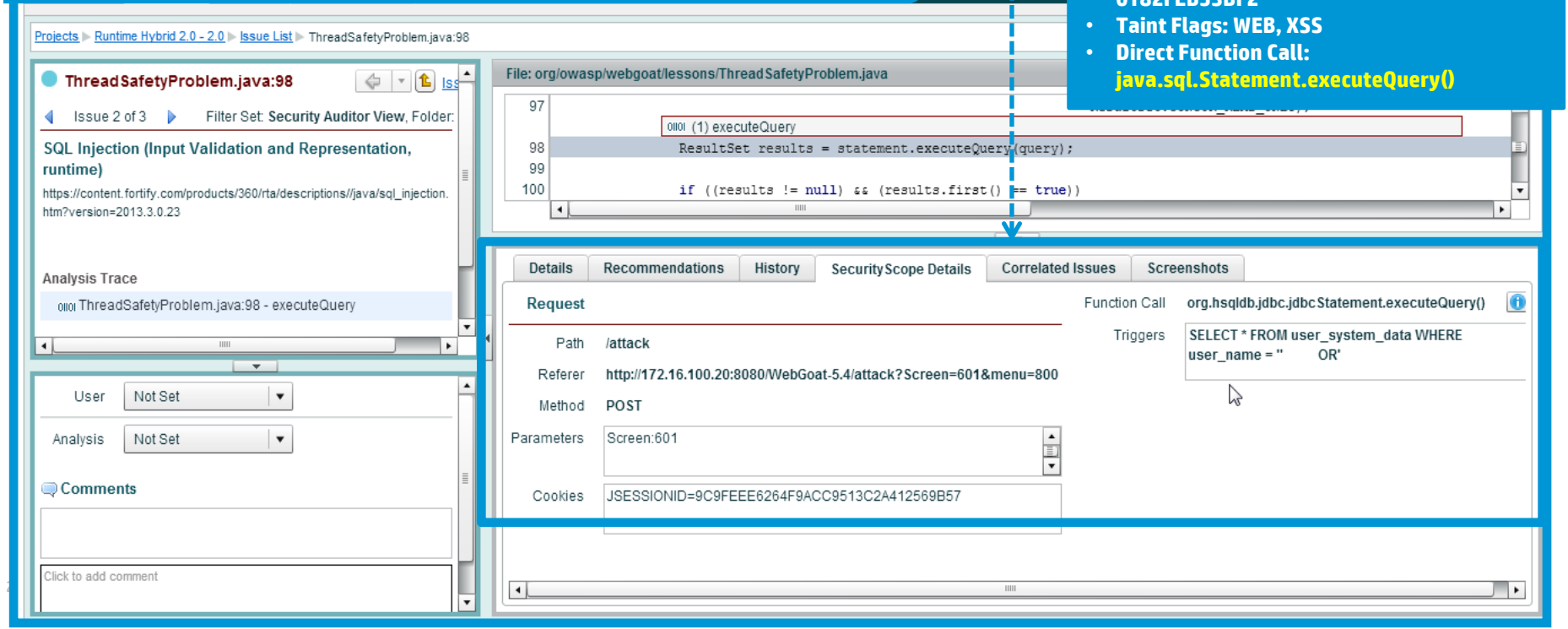
Hybrid 2.0 보안 취약점 분석

동작원리

Audit Issues (보안취약점 Correlation) 3

런타임분석 **SecurityScope**

- **ThreadSafetyProblem.java : 98**
- **Rule ID: 9B5F0161-88EC-4104-B70B-0182FEB53BF2**
- **Taint Flags: WEB, XSS**
- **Direct Function Call: java.sql.Statement.executeQuery()**



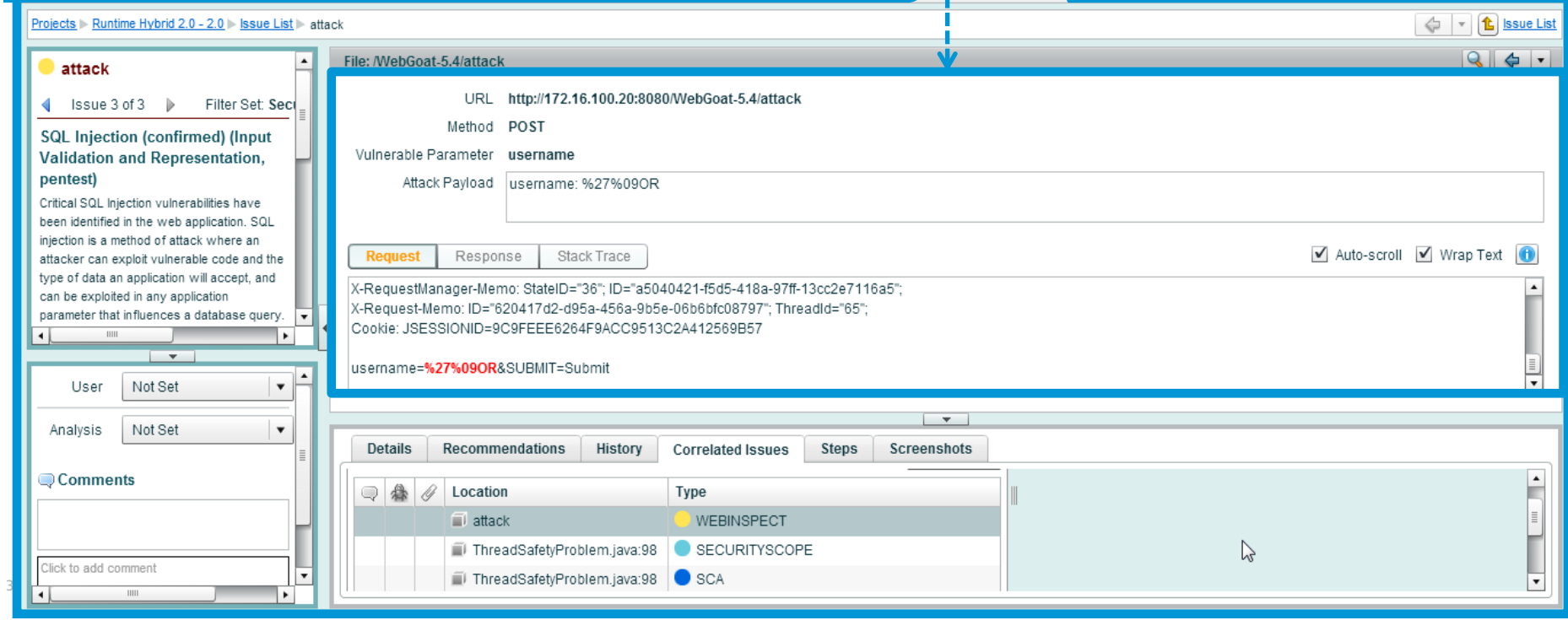
Hybrid 2.0 보안 취약점 분석

동작원리

Audit Issues (보안취약점 Correlation) 3

동적분석 WebInspect

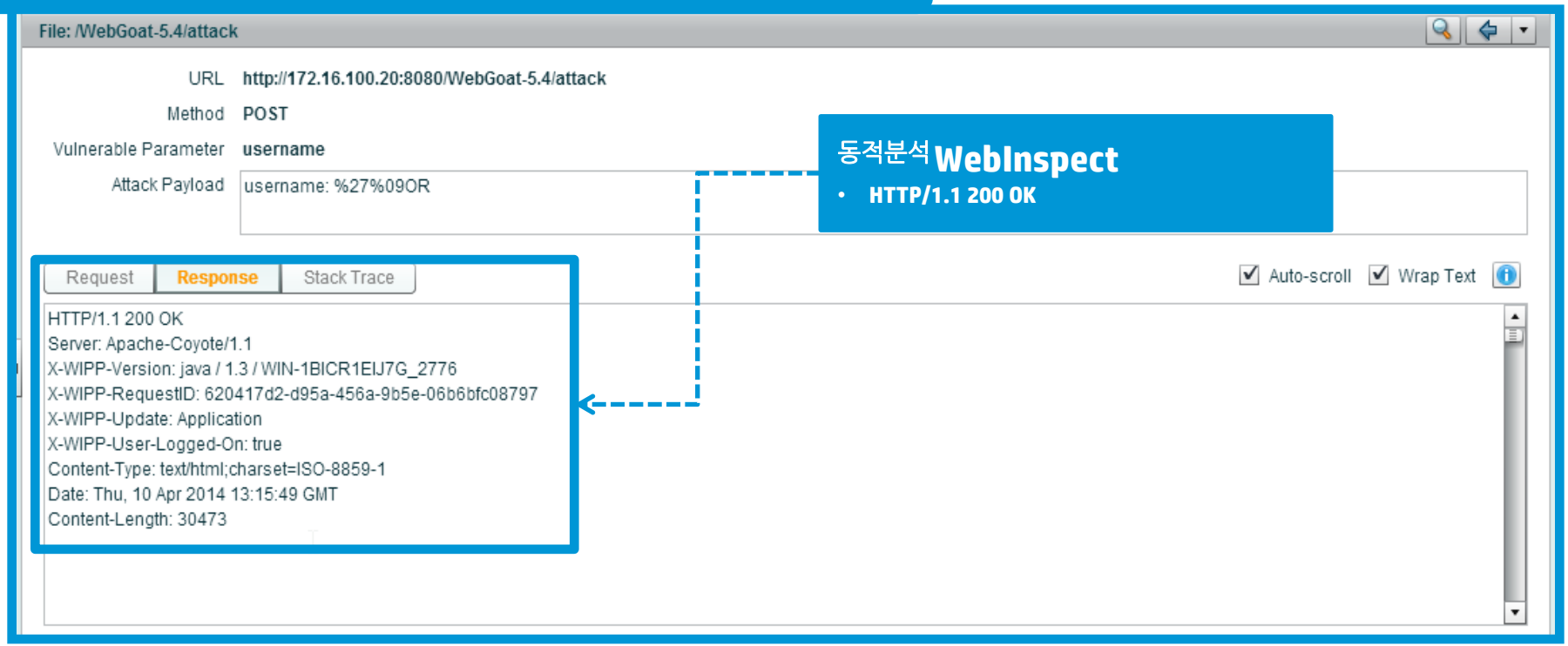
- **SQL Injection (confirmed) (Input Validation and Representation, pentest)**



Hybrid 2.0 보안 취약점 분석

동작원리

Audit Issues (보안취약점 Correlation) 3



Hybrid 2.0 보안 취약점 분석

동작원리

Audit Issues (보안취약점 Correlation) 3

File: /WebGoat-5.4/attack

URL http://172.16.100.20:8080/WebGoat-5.4/attack

Method POST

Vulnerable Parameter **username**

Attack Payload username: %27%09OR

Request | Response | Stack Trace

Security Scope Trigger:

SELECT * FROM user_system_data WHERE user_name = '\tOR'

Security Scope Stack Trace:

at org.hsqldb.jdbc.jdbcStatement.executeQuery(Unknown Source)

at org.owasp.webgoat.lessons.ThreadSafetyProblem.createContent(ThreadSafetyProblem.java:98)

at org.owasp.webgoat.lessons.AbstractLesson.handleRequest(AbstractLesson.java:771)

at org.owasp.webgoat.lessons.ThreadSafetyProblem.handleRequest(ThreadSafetyProblem.java:189)

at org.owasp.webgoat.HammerHead.makeScreen(HammerHead.java:367)

at org.owasp.webgoat.HammerHead.doPost(HammerHead.java:146)

at javax.servlet.http.HttpServlet.service(HttpServlet.java:643)

at javax.servlet.http.HttpServlet.service(HttpServlet.java:723)

at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)

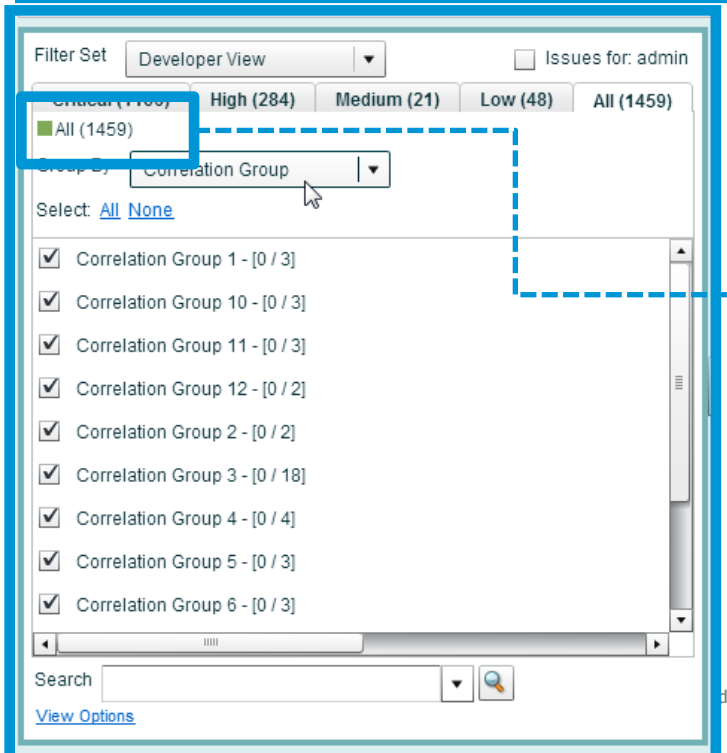
동적분석 **WebInspect**

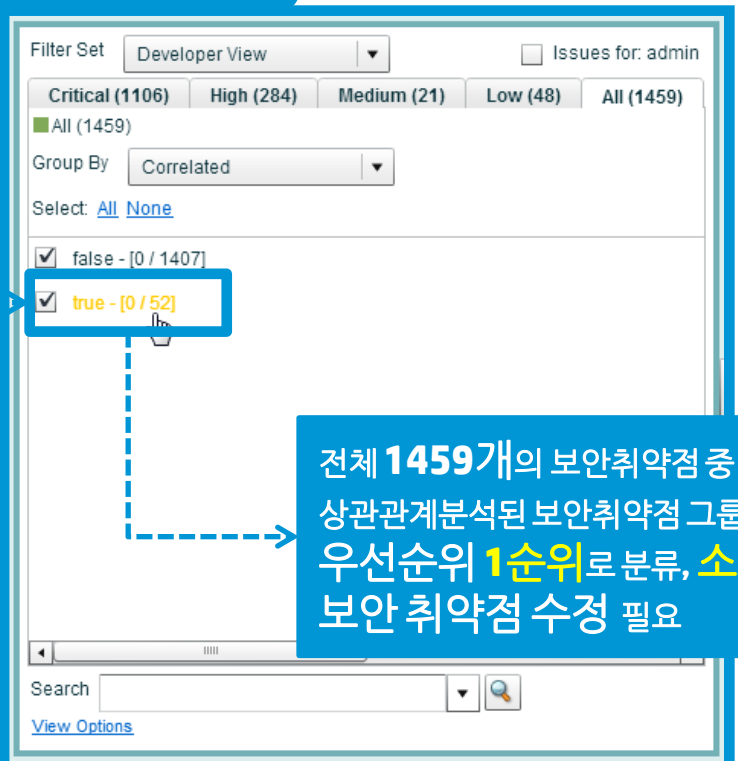
- **StackTrace**
- **SQL Injection (Input Validation and Representation, runtime)**

Hybrid 2.0 보안 취약점 분석

동작원리

Audit Issues (보안취약점 Correlation - All) 3





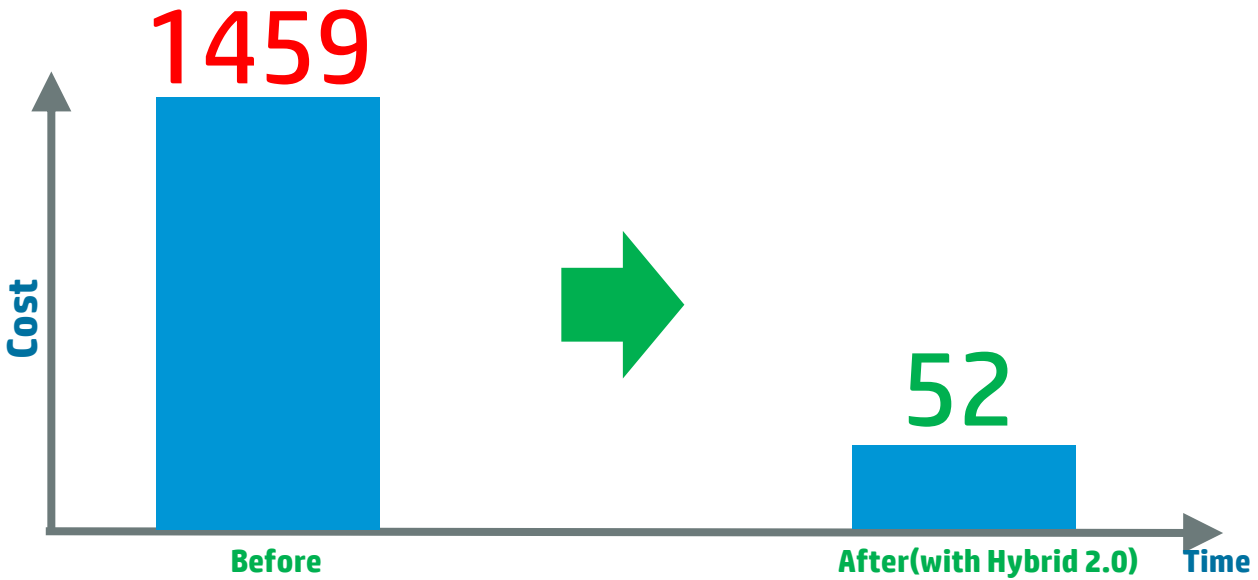
전체 **1459**개의 보안취약점 중 **52**개는 상관관계분석된 보안취약점 그룹으로서 점검 우선순위 **1**순위로 분류, 소스코드상의 보안 취약점 수정 필요

Hybrid 2.0 보안 취약점 분석

기대효과

Hybrid 2.0 분석기법 H

- 소스코드 분석결과와 동적/런타임 분석결과를 연계, 보안취약점에 대한 우선순위화/ 근원적인 보안취약점 제거 방안 제공합니다.



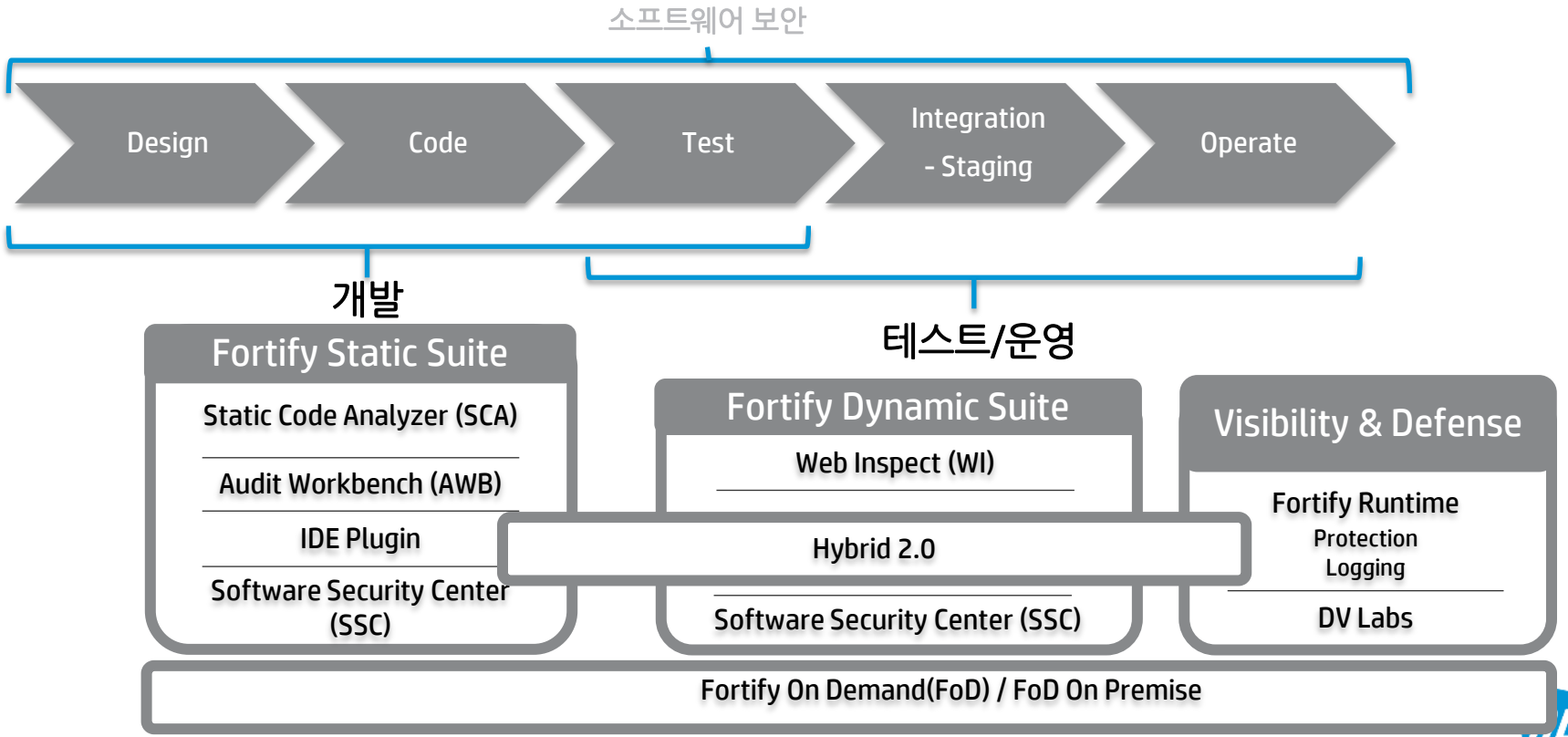
Find, Fix and Fortify

Thank You

보안솔루션 관련 문의처: **espkorea@hp.com**
한국HP | 보안사업부(Enterprise Security Products)

소프트웨어 보안 품질 보증

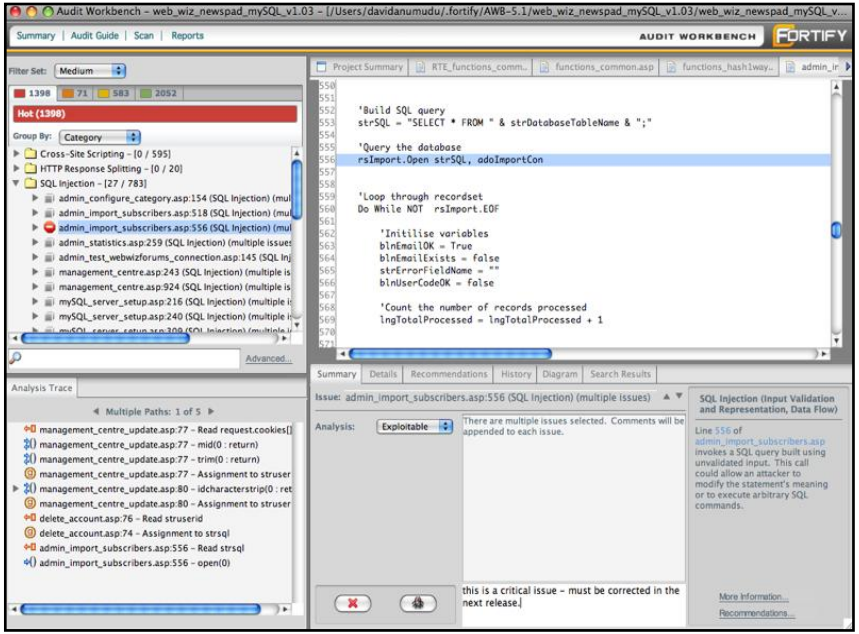
포티파이 애플리케이션 보안 취약점 관리 솔루션



Fortify Static Code Analyzer (SCA)

정적분석기Static analysis –소스코드 보안 취약점 발견 및 조치 가이드

- 소스코드 정적보안취약점 분석 **De facto standard** 제품
- **500**개 이상 보안카테고리 및 업계최다인 **21**개의 개발 언어 대상 코드레벨 정적 보안 취약점 분석지원 **(Java7, HTML5** 포함**)**
- 업계 유일 **Mobile app** 개발 언어 분석지원 **(Apple Objective-C/Xcode, Android Java** 모두 지원**)**
- 업계유일 **Hybrid** 분석 기술**(SecurityScope)** 채용을 통해 **Static/Dynamic** 에만 국한된 분석기법의 한계 극복**,** 보안취약점에 대한 우선순위기반 보안취약점 관리 제공
- **On-Premise/On-Demand** 솔루션지원 통한 유연성 제공



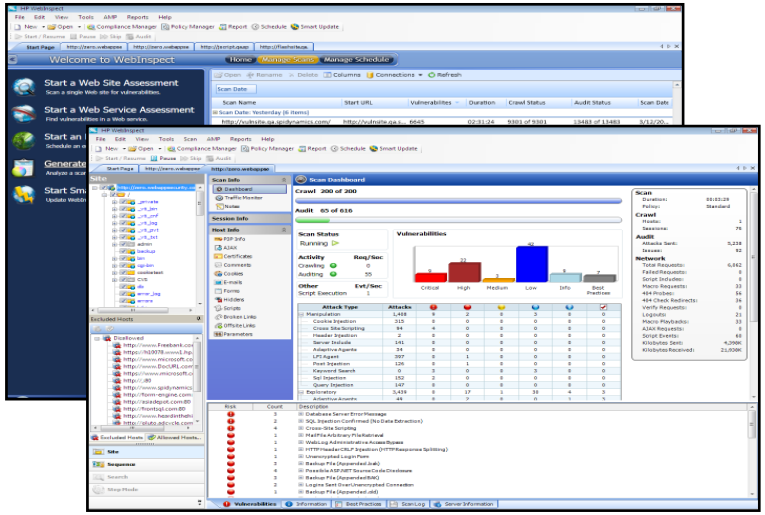
WebInspect

동적 분석기Dynamics analysis – 웹애플리케이션 보안취약점 발견 및 조치가이드

- *네트워크*를 통한 웹서버 대상 보안 스캐닝을 수행해 짧은 시간안에 고위험도 웹애플리케이션 보안취약점 탐지 및 조치 가이드

- 개발 프로젝트 진행, 보안검수시점과 운영 중 웹보안품질 측정을 실시해 보안취약점에 대한 상시 점검

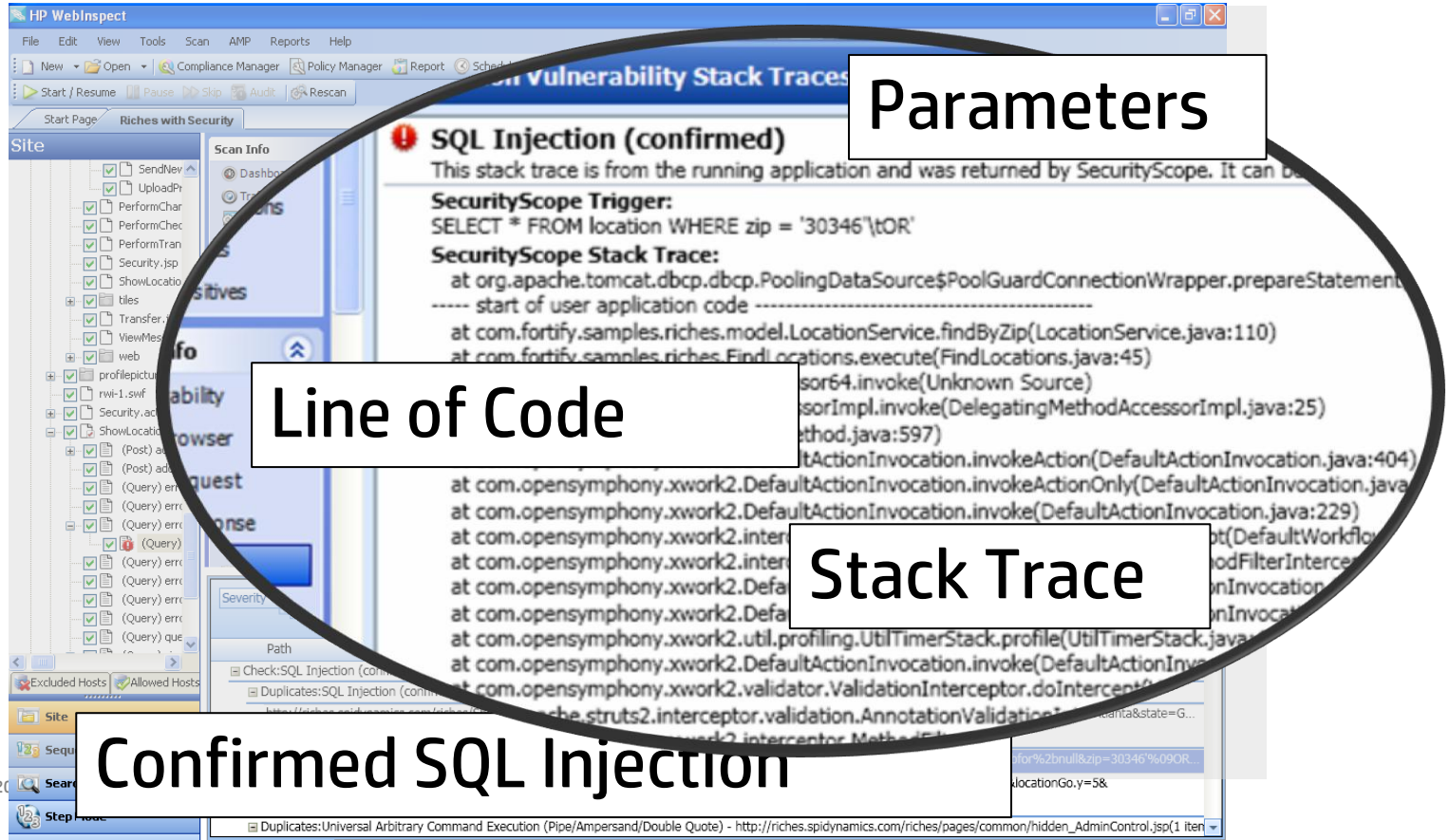
- [1]**Hybrid** 분석 기술을 채용해 소스코드 분석결과와 동적 분석결과를 연계, 보안취약점에 대한 우선순위기반 보안취약점관리방안 제공**(SecurityScope)**



[1]**Hybrid** 분석 기술 : 정적분석기법인 소스코드 분석**(Static code analysis)**과 런타임 분석 기법인 프로그램 실행분석**(SecurityScope)**, 동적분석기법인 웹 보안취약점 스캐너인 **WebInspect**를 상호 연동, 애플리케이션 보안취약점에 대해 통합분석함으로써, 동적분석의 한계인 분석 범위를 확장하고 정적분석결과를 실제 공격이 가능한 순으로 분류하여 분석결과를 제공하므로 위험도와 실행 가능성이 높은 보안취약점을 빠르게 식별 및 우선적으로 수정할 수 있도록하여 전체 개발비용과 소요시간을 급격히 절감 할 수 있는 新기술
Dynamic Application Security Testing (DAST), Static Application Security Testing (SAST), Interactive Application Security Testing (IAST)

WebInspect with 런타임 에이전트

***Interactive Application Security Testing** 기법 채용한 차세대 동적 분석기*



Fortify Software Security Center server

총체적인 보안 취약점 관리 센터

- 정적/동적/런타임 분석기에 의해 수집된 보안취약점 관리/연동분석/추적/제거 방안 제공 시스템
- 역할 기반 접근, 프로세스 기반의 보안취약점 관리
- 핵심개발환경과의 연동
  - **Build integration, Defect tracking, Source control, 3rd party analysis engines**
- 유연한 보안취약점 저장소 관리 및 리포팅 제공
  - **Normalized, correlated vulnerability repository**
  - **Aggregated risk metrics**

Mobile Application Security Testing

모바일 인프라 전반에 걸친 애플리케이션 스택 보안취약점 발견 및 조치

모바일 지원 플랫폼

- Apple iOS (**Objective C**)
- Android
- Windows Phone / Blackberry

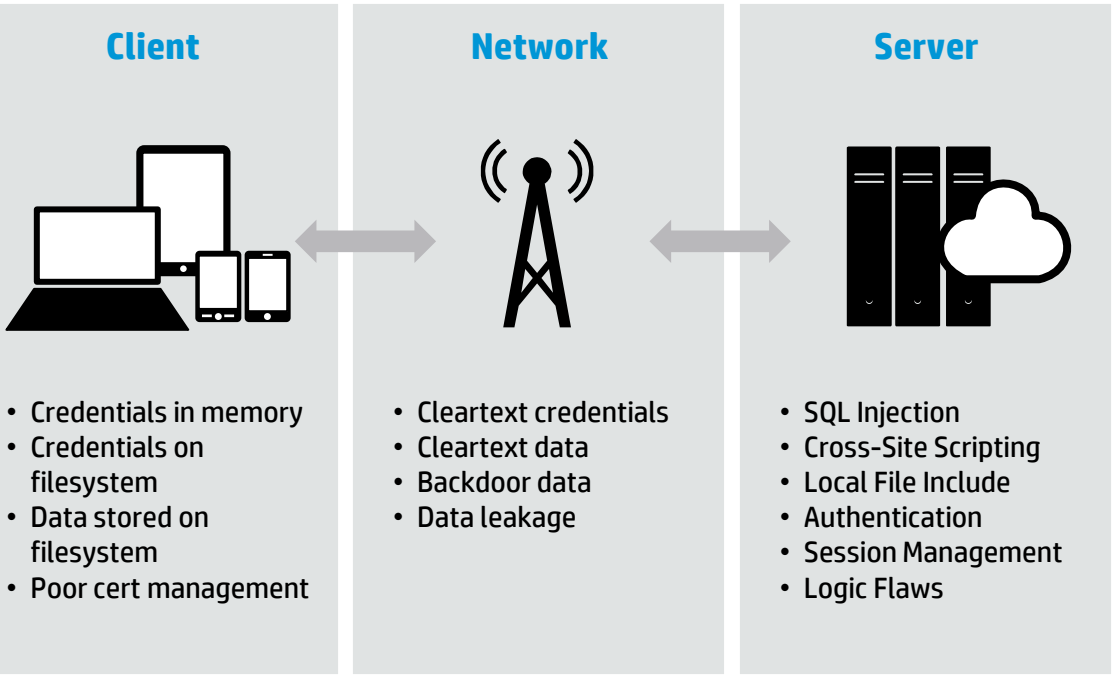
Hybrid 분석 기술 채용

- 소스코드 분석결과와

동적분석결과의 **Correlation**

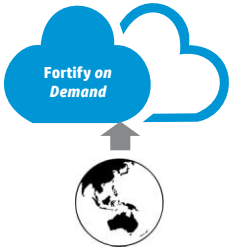
모바일 인프라 **3-Tier** 지원

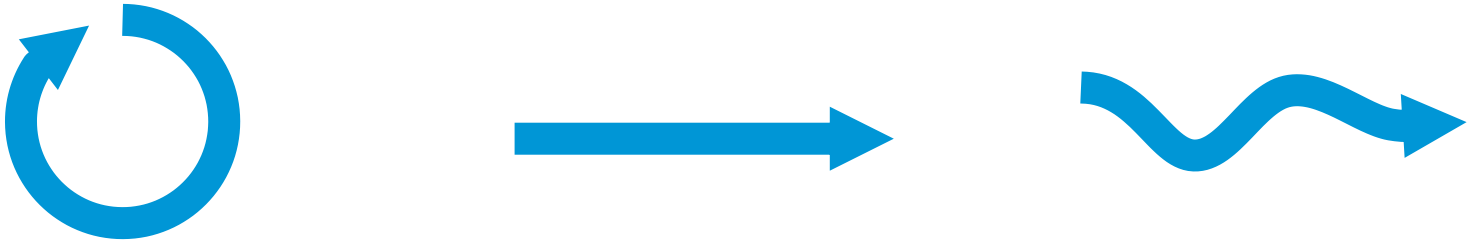
- 모바일 단말상의 애플리케이션
- 모바일 백엔드 서버상의 애플리케이션



HP Fortify On Demand

애플리케이션 보안, 적은 비용으로 간단하게 빠르게 유연하게!





Simple

Fast

Flexible

1일이내 Application 보안 시작

- 하드웨어, 소프트웨어 先투자 필요 – **No!**
- 보안 전문인력 필요 – **No!**

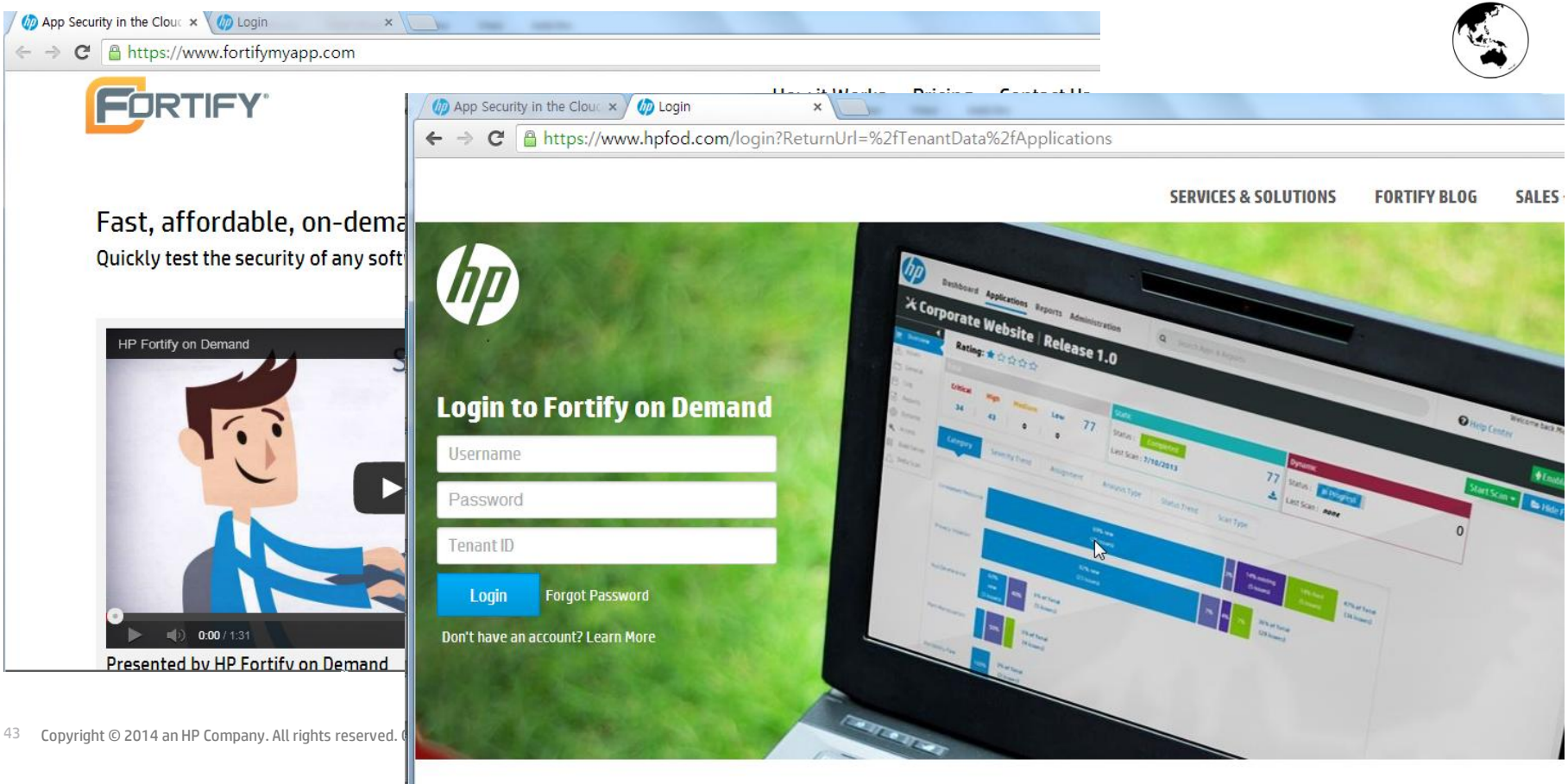
신속, 뛰어난 확장성 제공

- **Application** 보안 테스트 결과 – 최단기간 소요
- 데스크탑, 모바일 혹은 클라우드 상의 **1,000**여개 이상 **Application** 지원

유연한 테스팅

- 상용, 오픈소스, **3rd Party** 애플리케이션 보안 테스트 지원
- **On-Premise, On-Demand,** 혹은 **both** 지원

HP Fortify On Demand



HP Fortify Coverage

Static Analysis

Static analysis supports 21 languages and growing

- ABAP
- Android
- C#
- Classic ASP
- Cold Fusion
- HTML
- JavaScript/AJAX
- Objective C
- PL/SQL
- T-SQL
- VB6
- XML
- ASP.NET
- C/C++
- COBOL
- Flex
- Java
- JSP
- PHP
- Python
- Ruby
- VB.NET
- VBScript

Dynamic analysis covers all web environments

- QA or production environments
- Web services

Mobile application security solution covers

- Objective C
- Android
- Blackberry
- Microsoft

Gartner Magic Quadrant for Application Security Testing

- "HP offers comprehensive SAST capabilities with Fortify's strong brand name and breadth of languages tested.
- The company has innovative IAST capability with Fortify SecurityScope, which integrates with its WebInspect DAST.
- There is strong integration within HP's security portfolio, such as integration of AST knowledge into ArcSight and DAST knowledge into TippingPoint's IPS for WAF-like protection.
- HP uniquely offers runtime application self-protection (RASP) technology