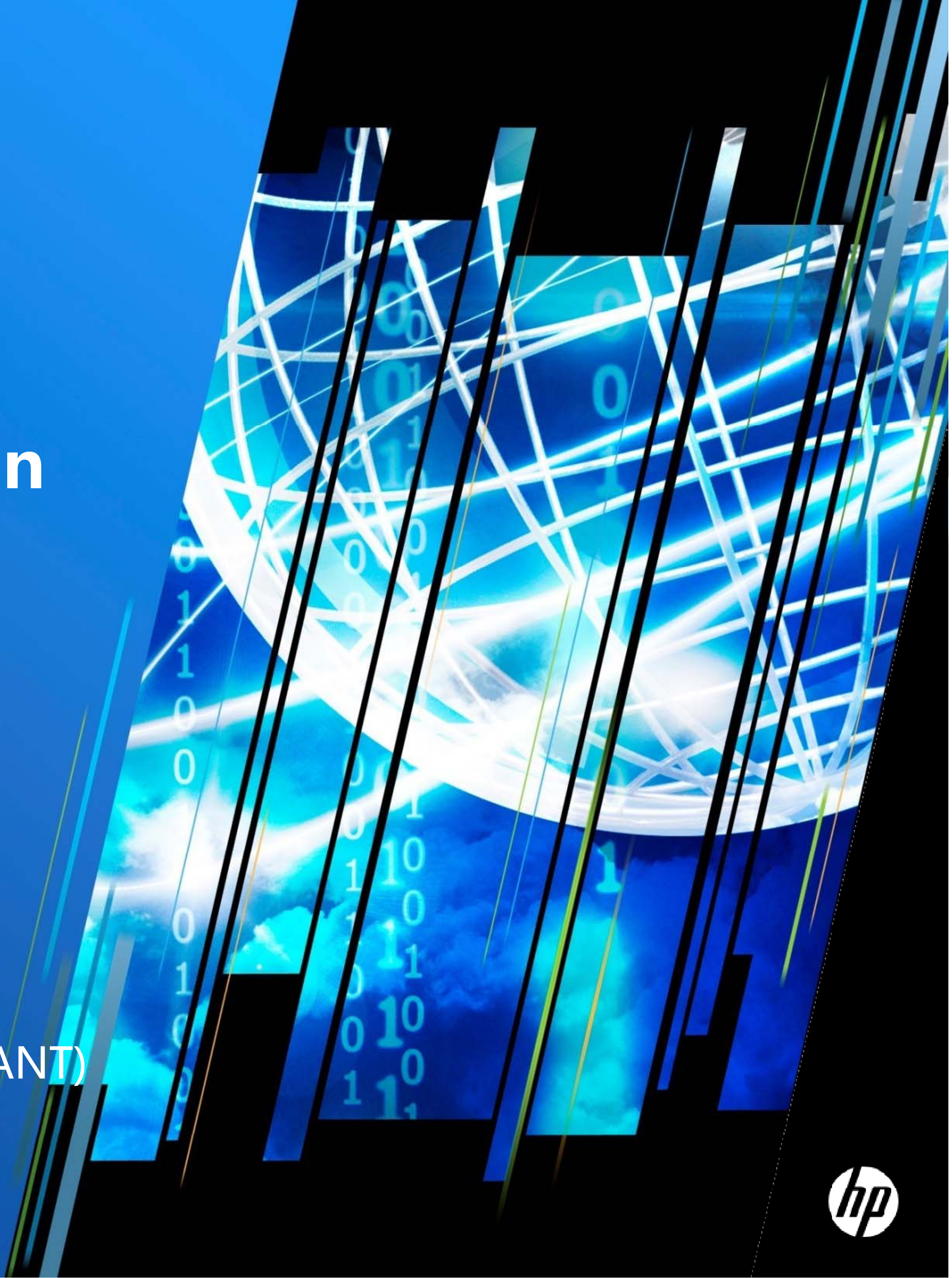
HP Mobile Application Security Solution

惠普移动应用安全解决方案



WILLY LIN
(HP FORTIFY PRODUCT CONSULTANT)

大綱

- 移动应用的趋势与威胁
- 移动应用 – Three Layers
- 移动应用安全設計思維
- 惠普移动应用安全解决方案
- HP Fortify SCA
- HP Fortify SSC Server
- 惠普移动应用安全解决方案視頻
- Q & A

移动应用的趋势与威胁

- 惠普趋势分析
- 2015年（约6亿个移动台设备, 将有近一个人均移动台设备）
- 2014年移动支付将超过的900亿美元
- 2010年和2015年间,全球移动台数据流量将增加26倍
- 2015年,全球移动台数据流量的三分之二将会什么视频(个人移动 TV , Movie)

2011 GARTNER REPORT
十大移动应用未來趋势

1、地理位置服务

2、社交网络

3、移动搜索

4、移动商务

5、移动支付

6、移动电邮

7、移动视频

8、情境感知(context-aware)服务

9、移动即时通讯（MIM）

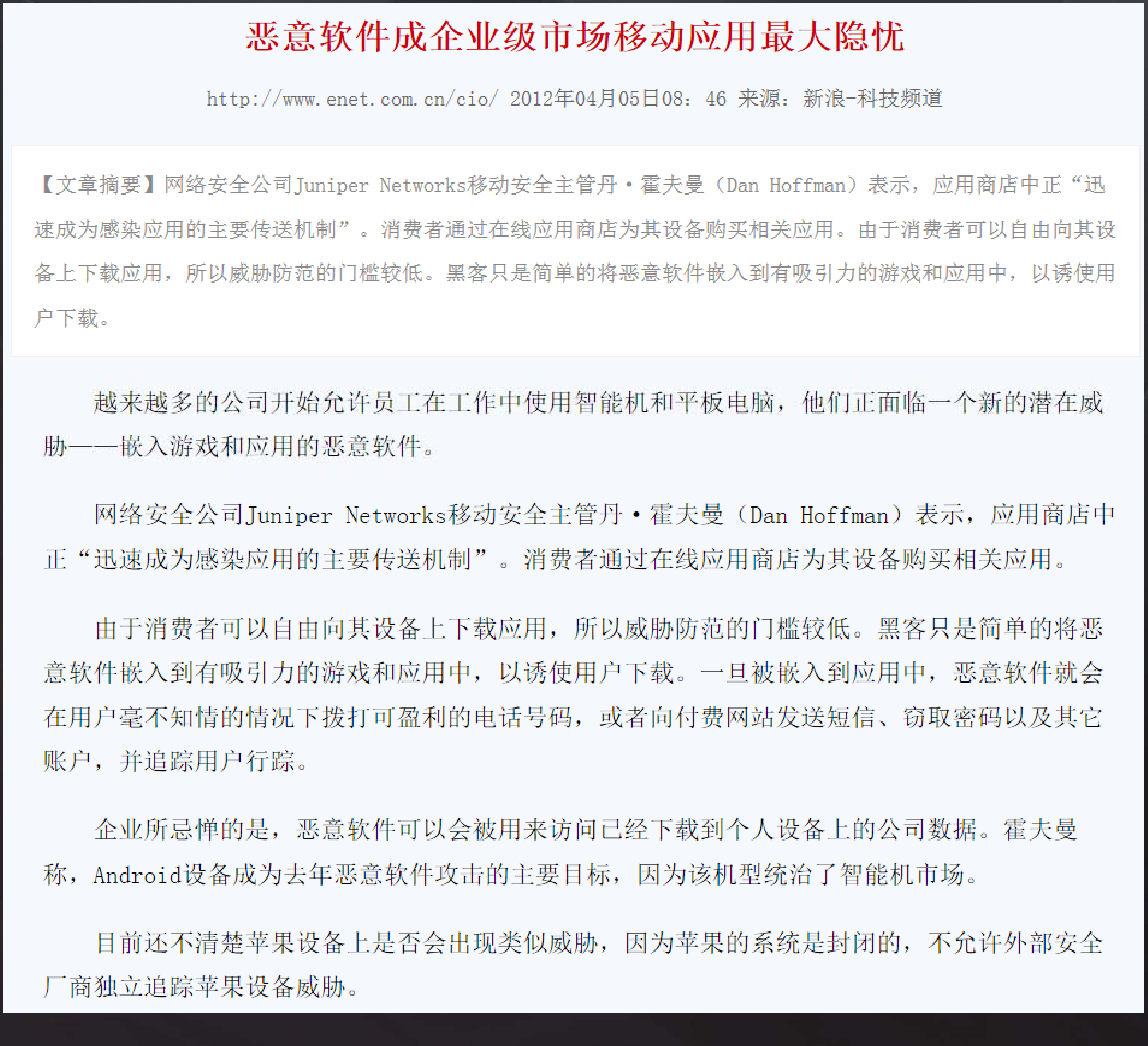
10、目标识别(object recognition)服务

- 这些移动应用趋势的背后意味着，需要有更多相关移动应用程序的支撑。

移動應用的趨勢與威脅

One in Four Adults Now Use Mobile Apps

恶意软件成企业级市场移动应用最大隐忧



恶意软件成企业级市场移动应用最大隐忧

http://www.enet.com.cn/cio/ 2012年04月05日08：46 来源：新浪-科技频道

【文章摘要】网络安全公司Juniper Networks移动安全主管丹·霍夫曼（Dan Hoffman）表示，应用商店中正“迅速成为感染应用的主要传送机制”。消费者通过在线应用商店为其设备购买相关应用。由于消费者可以自由向其设备上下载应用，所以威胁防范的门槛较低。黑客只是简单的将恶意软件嵌入到有吸引力的游戏和应用中，以诱使用户下载。

越来越多的公司开始允许员工在工作中使用智能机和平板电脑，他们正面临一个新的潜在威胁——嵌入游戏和应用的恶意软件。

网络安全公司Juniper Networks移动安全主管丹·霍夫曼（Dan Hoffman）表示，应用商店中正“迅速成为感染应用的主要传送机制”。消费者通过在线应用商店为其设备购买相关应用。

由于消费者可以自由向其设备上下载应用，所以威胁防范的门槛较低。黑客只是简单的将恶意软件嵌入到有吸引力的游戏和应用中，以诱使用户下载。一旦被嵌入到应用中，恶意软件就会在用户毫不知情的情况下拨打可盈利的电话号码，或者向付费网站发送短信、窃取密码以及其它账户，并追踪用户行踪。

企业所忌惮的是，恶意软件可以会被用来访问已经下载到个人设备上的公司数据。霍夫曼称，Android设备成为去年恶意软件攻击的主要目标，因为该机型统治了智能机市场。

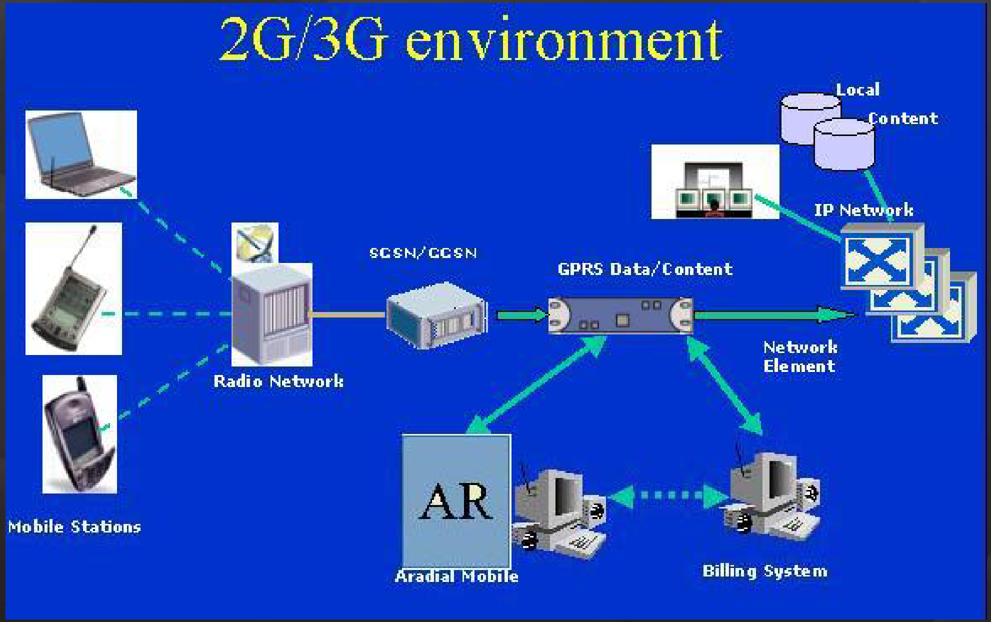
目前还不清楚苹果设备上是否会出现类似威胁，因为苹果的系统是封闭的，不允许外部安全厂商独立追踪苹果设备威胁。

移动应用 – THREE LAYERS

1. Server

Web Server
Web
Services

移动应用 – THREE LAYERS



2. Network

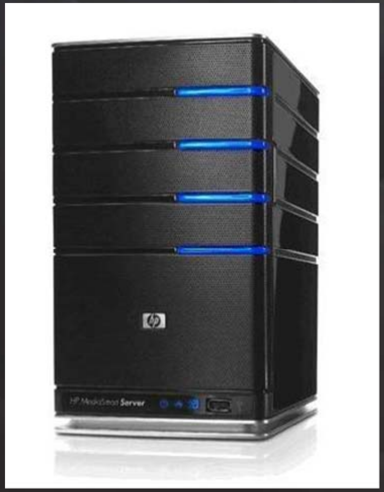
Data Type
Sensitivity
Transport Protection

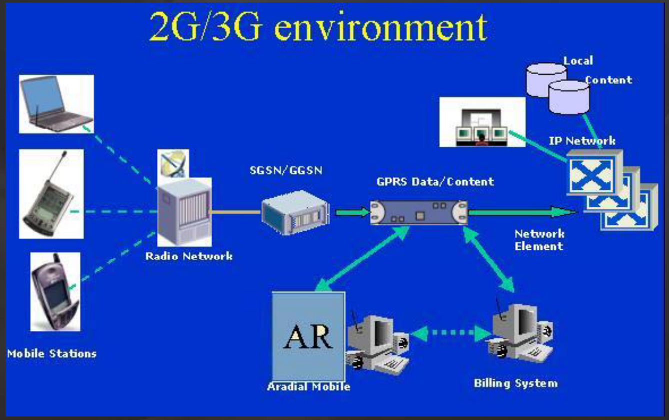
移动应用 – THREE LAYERS

3. Client

Storage of Credentials
Configuration Files
Insecure Development
Platform Issues

移动应用 – THREE LAYERS





1. Server

Web Server
Web Services

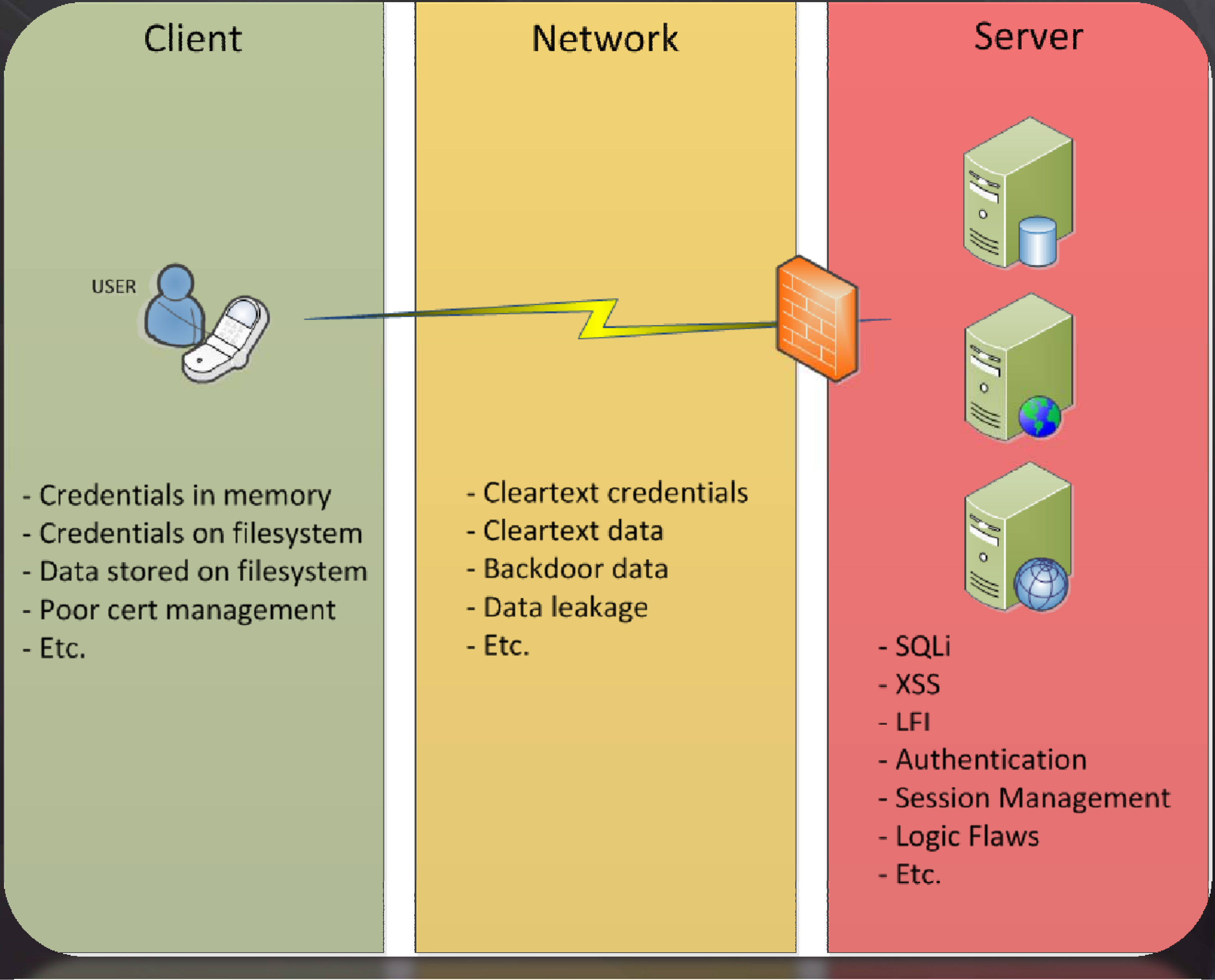
2. Network

Data Type
Sensitivity
Transport Protection

3. Client

Storage of Credentials
Configuration Files
Insecure Development
Platform Issues

移动应用安全設計 - Security Thinking



Client

- Credentials in memory
- Credentials on filesystem
- Data stored on filesystem
- Poor cert management
- Etc.

Network

- Cleartext credentials
- Cleartext data
- Backdoor data
- Data leakage
- Etc.

Server

- SQLi
- XSS
- LFI
- Authentication
- Session Management
- Logic Flaws
- Etc.

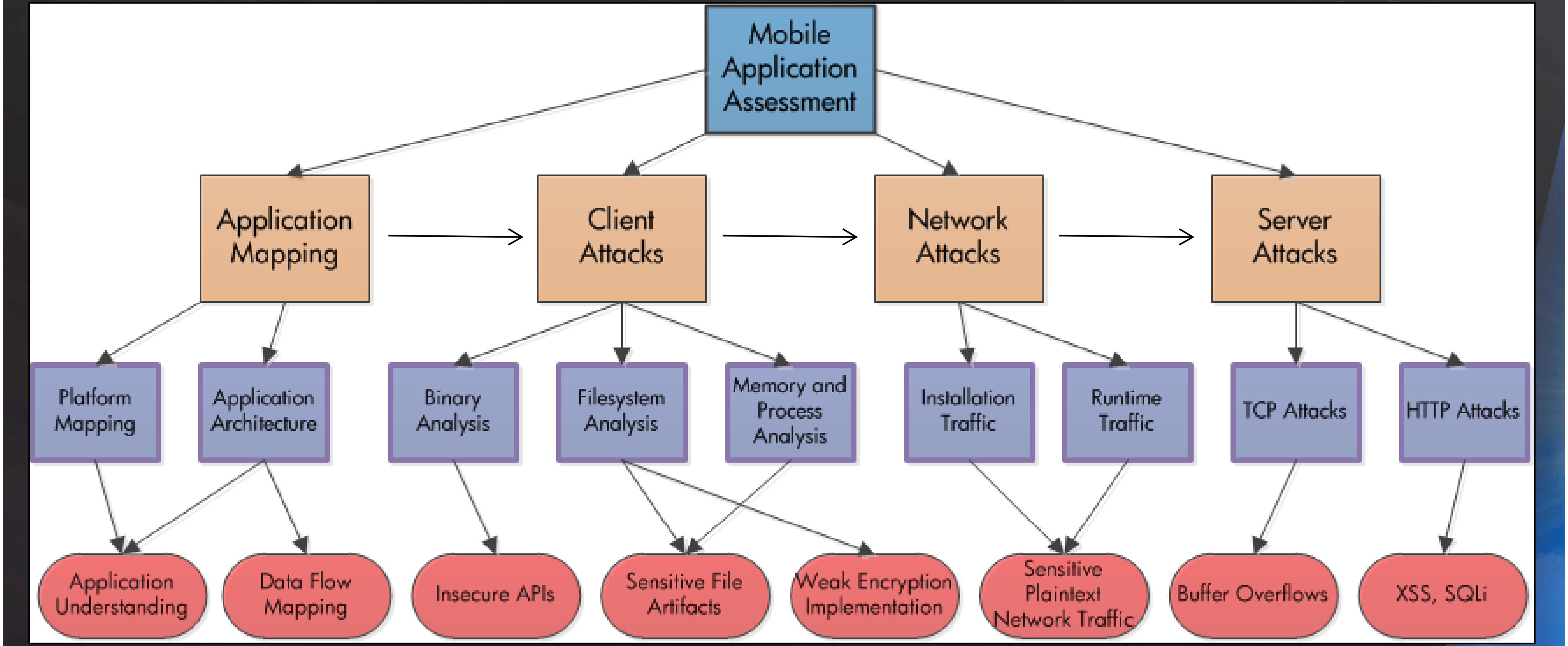
移动应用安全設計 – 基本检查表

Methodology Section	Check / Vulnerability Examples
Client (Static and Dynamic)	• Dropped files on the filesystem • Poor use of APIs • Certificate issues • Credentials stored on device • Data stored on device
Network (Dynamic)	• Insecure transmission of credentials • Improper transmission of application data • Reliance on the client for security • Checks for sensitive obfuscated data
Server (Static and Dynamic)	• SQL Injection vulnerabilities • XSS vulnerabilities • Authentication and Session management issues • All standard web assessment vulnerabilities

清晰的思维（Clear Thinking）

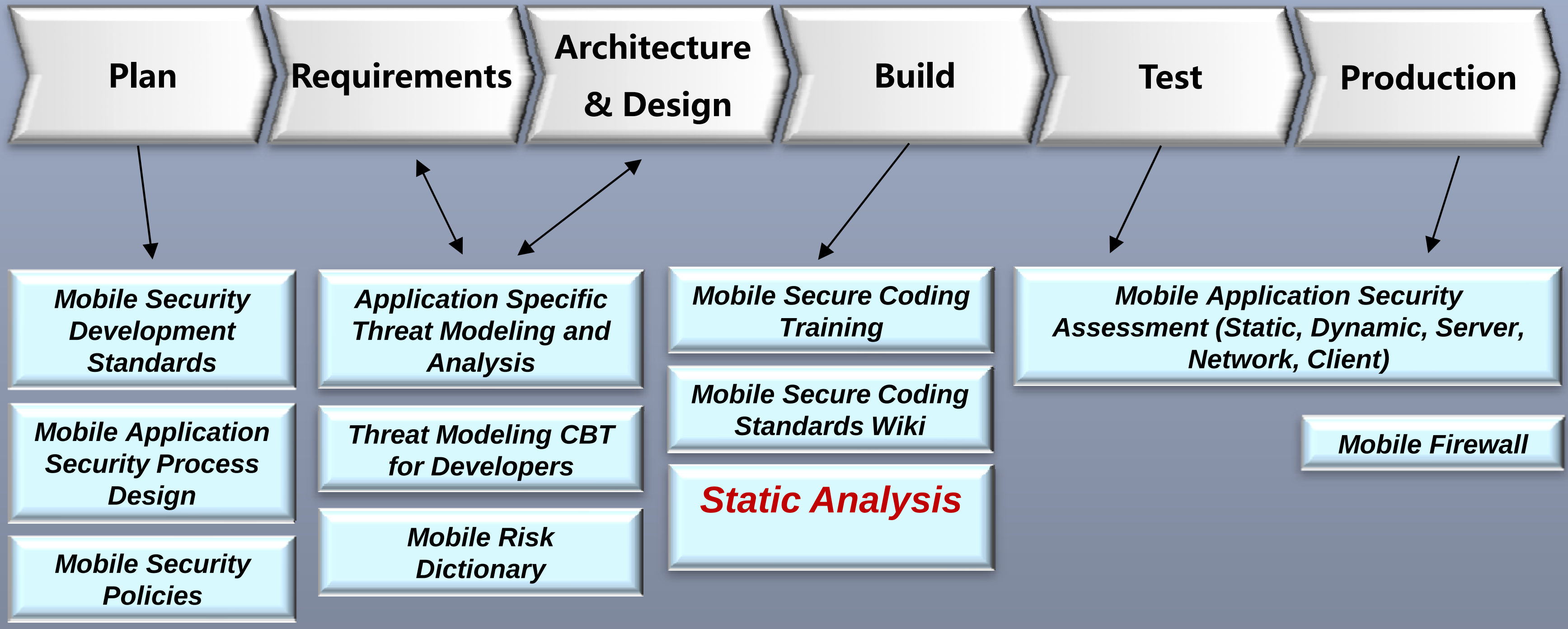
- **Know** where you are using credentials
- **Know** what sensitive data is in play
- **Track** these through the device, network, and backend
- **Test** those all components and their running paths

移动应用安全設計 - Security Thinking



移动应用安全开发流程整合 – SECURITY JOBS

Security Foundations – Mobile Applications



Plan

Requirements

Architecture & Design

Build

Test

Production

Mobile Security Development Standards

Mobile Application Security Process Design

Mobile Security Policies

Application Specific Threat Modeling and Analysis

Threat Modeling CBT for Developers

Mobile Risk Dictionary

Mobile Secure Coding Training

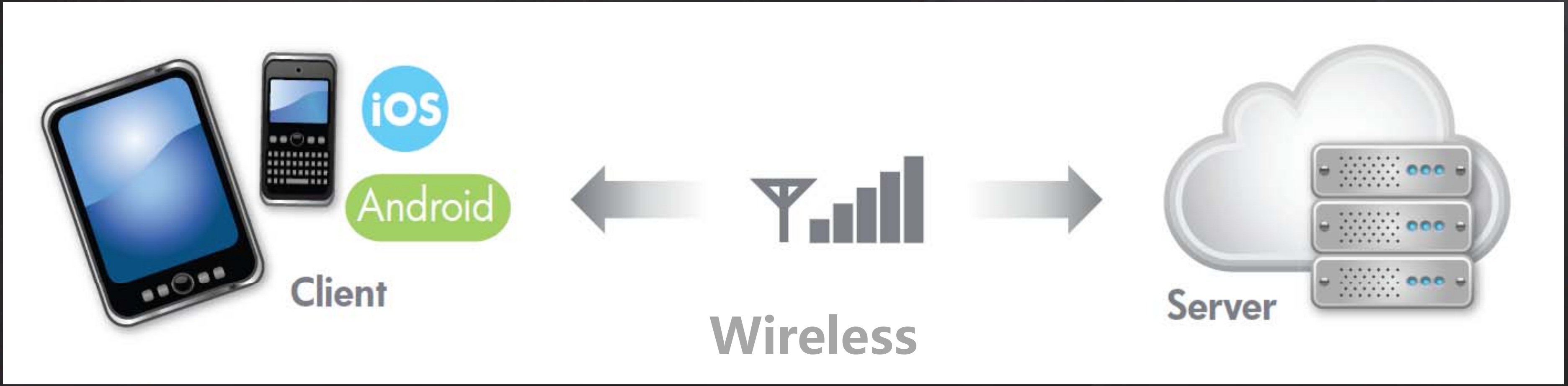
Mobile Secure Coding Standards Wiki

Static Analysis

Mobile Application Security Assessment (Static, Dynamic, Server, Network, Client)

Mobile Firewall

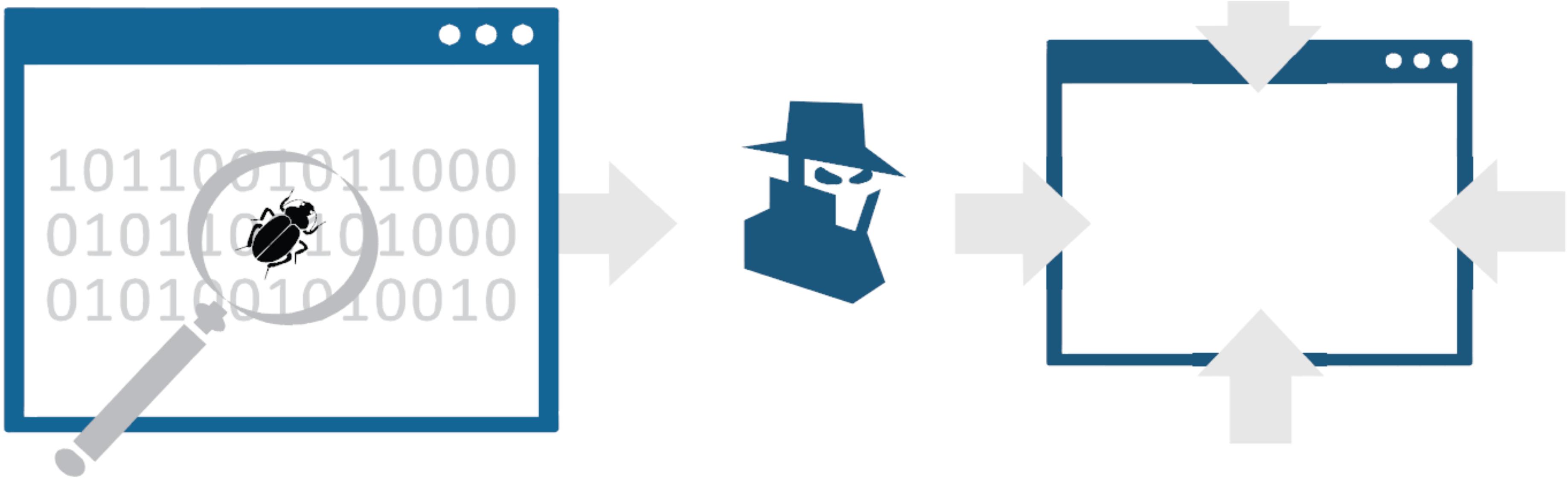
惠普移动应用安全解决方案
Securing the client, the server and the network communications.



惠普移动应用安全解决方案
静态测试 & 动态测试

HP Fortify SCA Tool

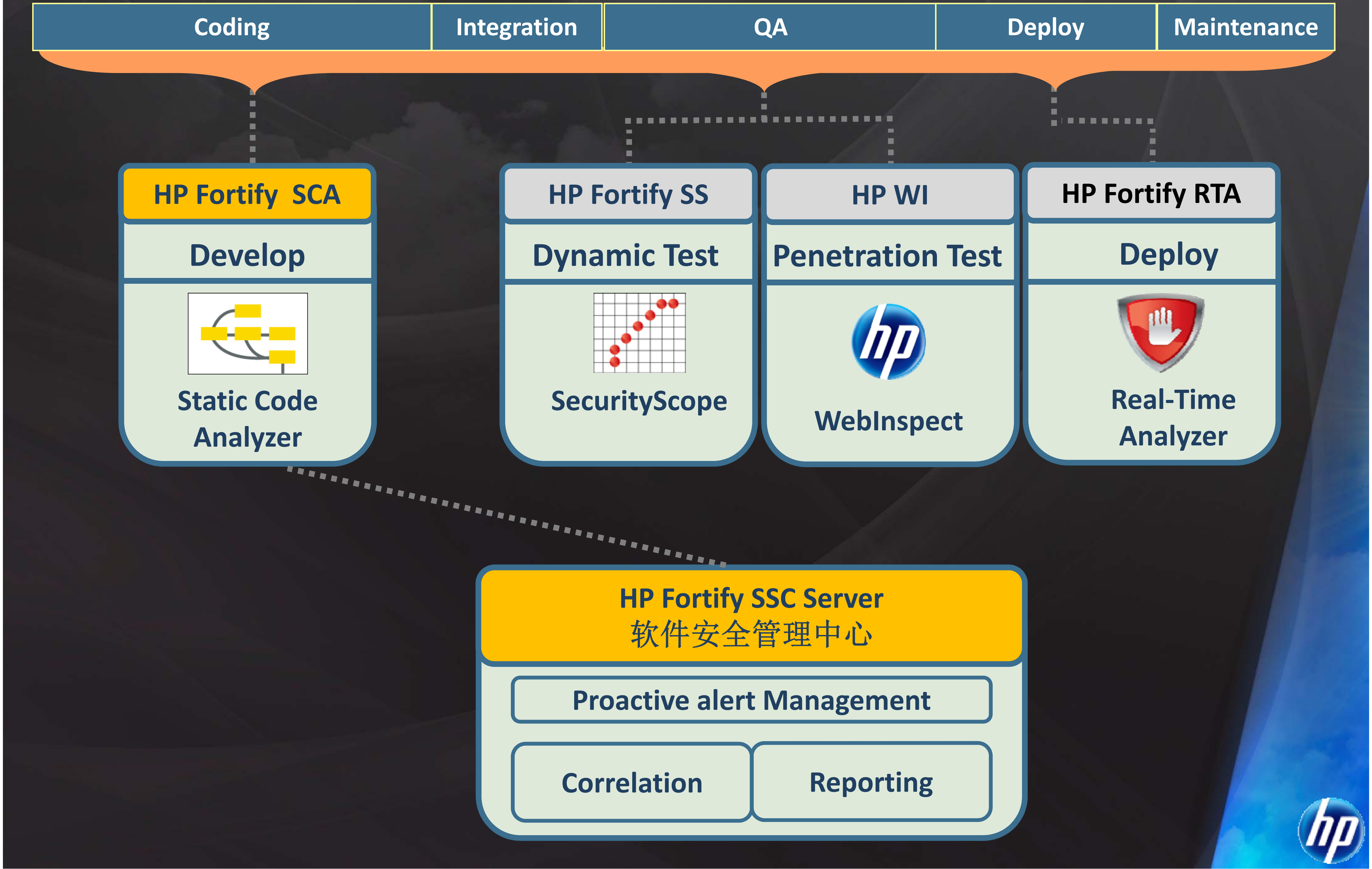
HP Fortify Experts



Static testing analyzes the source code for vulnerabilities

Dynamic testing simulates an attack against a running application

惠普移动应用安全解决方案
静态测试（HP FORTIFY SCA）



Coding | Integration | QA | Deploy | Maintenance

HP Fortify SCA

Develop

Static Code Analyzer

HP Fortify SS

Dynamic Test

SecurityScope

HP WI

Penetration Test

WebInspect

HP Fortify RTA

Deploy

Real-Time Analyzer

HP Fortify SSC Server
软件安全管理中心

Proactive alert Management

Correlation

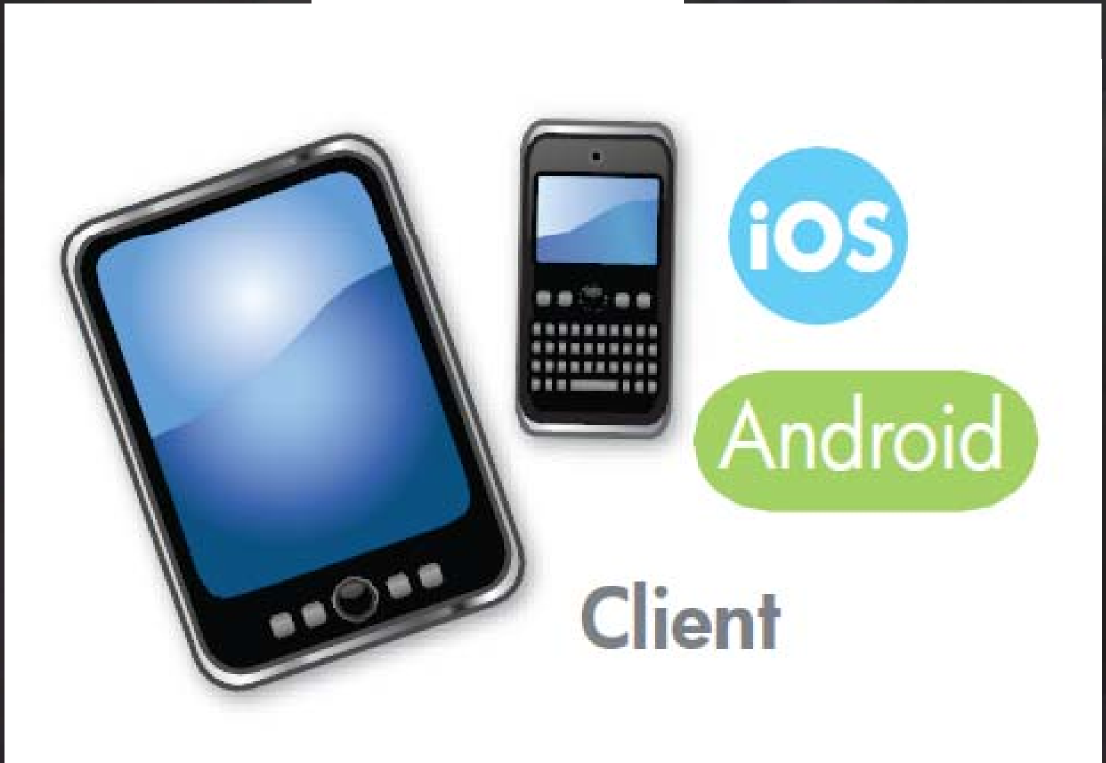
Reporting

HP FORTIFY SCA
支持21种程式源码安全漏洞检测

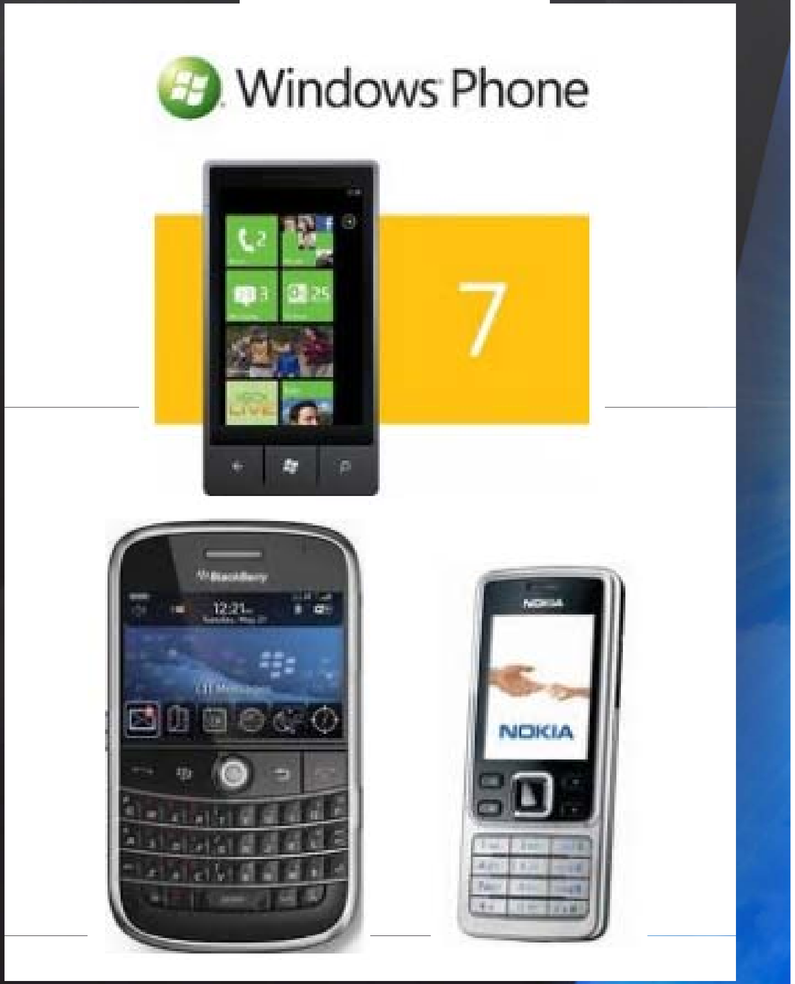
1. ASP.Net
2. VB.Net
3. C#.Net
4. ASP
5. VBScript
6. VB6
7. Java (Android – 2011/6)
8. JSP
9. JavaScript
10. HTML
11. XML
12. C/C++
13. PHP
14. T-SQL (MSSQL DB)
15. PL/SQL (Oracle DB)
16. Action Script
17. Object-C (iPhone-2012/5)
18. ColdFusion 5.0 – 选购
19. Python - 选购
20. COBOL - 选购
21. SAP-ABAP - 选购

惠普移动应用安全解决方案
支持移動手機平台

Yes!



No!



HP FORTIFY SCA
Support Android Java Packages

Android

1. android.app
2. android.content
3. android.database
4. android.database.sqlite
5. android.location
6. android.net
7. android.os
8. android.telephony
9. android.telephony.cdma
10. android.telephony.gsm
11. android.text
12. android.util
13. android.webkit
14. android.widget

HP FORTIFY SCA
支持 Android 源码安全漏洞检测类别 (1/2)

1. Access Control: Android Provider
2. Access Control: Database
3. Android Bad Practices: Missing Broadcaster Permission
4. Android Bad Practices: Missing Receiver Permission
5. Android Bad Practices: Sticky Broadcast
6. Cross Site Scripting: Persistent
7. Cross Site Scripting: Poor Validation
8. Cross Site Scripting: Reflected
9. Header Manipulation: Cookies
10. Insecure Storage: Android External Storage
11. Log Forging
12. Password Management
13. Password Management: Empty Password
14. Password Management: Hardcoded Password
15. Password Management: Null Password
16. Password Management: Weak Cryptography

HP FORTIFY SCA
支持 Android 源码安全漏洞检测类别 (2/2)

17. Path Manipulation
18. Privacy Violation
19. Privilege Management: Android Location
20. Privilege Management: Android Messaging
21. Privilege Management: Android Telephony
22. Privilege Management: Missing API Permission
23. Privilege Management: Missing Intent Permission
24. Query String Injection: Android Provider
25. Resource Injection
26. SQL Injection
27. System Information Leak

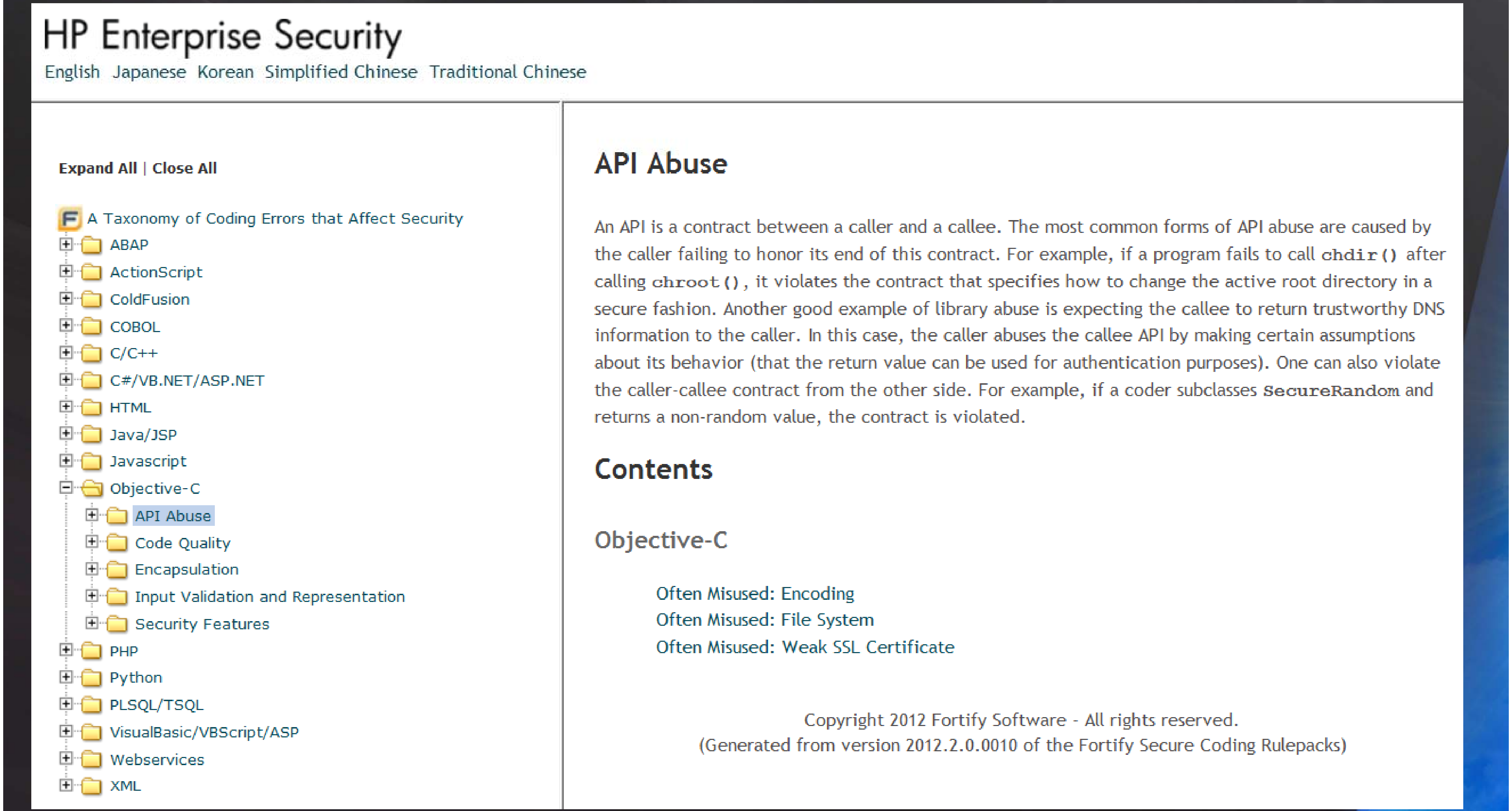
HP FORTIFY SCA
支持 iPhone 源码安全漏洞检测类别 (1/2)

1. Access Control: Database
2. Code Correctness: Regular Expressions Denial of Service
3. Format String
4. Key Management: Hardcoded Encryption Key
5. Log Forging
6. Memory Leak
7. Often Misused: Encoding
8. Often Misused: File System
9. Often Misused: SMS
10. Often Misused: Weak SSL Certificate
11. Password Management: Empty Password
12. Password Management: Hardcoded Password
13. Password Management: Null Password
14. Path Manipulation

HP FORTIFY SCA
支持 iPhone 源码安全漏洞检测类别 (2/2)

15. Privacy Violation
16. Privacy Violation: Keyboard Caching
17. Privacy Violation: Screen Caching
18. Resource Injection
19. SQL Injection
20. Unreleased Resource: Streams
21. Unsafe Mobile Code: Insecure Transport
22. Unsafe Reflection
23. Weak Cryptographic Hash
24. Weak Encryption
25. Weak Encryption: Insufficient Key Size

HP FORTIFY SCA
支持源码安全漏洞检测类别 – 互聯網
http://www.hpenterprisesecurity.com/vulncat/en/vulncat/



HP Enterprise Security

English Japanese Korean Simplified Chinese Traditional Chinese

Expand All | **Close All**

- A Taxonomy of Coding Errors that Affect Security
  - ABAP
  - ActionScript
  - ColdFusion
  - COBOL
  - C/C++
  - C#/VB.NET/ASP.NET
  - HTML
  - Java/JSP
  - Javascript
  - Objective-C
    - API Abuse
    - Code Quality
    - Encapsulation
    - Input Validation and Representation
    - Security Features
  - PHP
  - Python
  - PLSQL/TSQL
  - VisualBasic/VBScript/ASP
  - Webservices
  - XML

API Abuse

An API is a contract between a caller and a callee. The most common forms of API abuse are caused by the caller failing to honor its end of this contract. For example, if a program fails to call `chdir()` after calling `chroot()`, it violates the contract that specifies how to change the active root directory in a secure fashion. Another good example of library abuse is expecting the callee to return trustworthy DNS information to the caller. In this case, the caller abuses the callee API by making certain assumptions about its behavior (that the return value can be used for authentication purposes). One can also violate the caller-callee contract from the other side. For example, if a coder subclasses `SecureRandom` and returns a non-random value, the contract is violated.

Contents

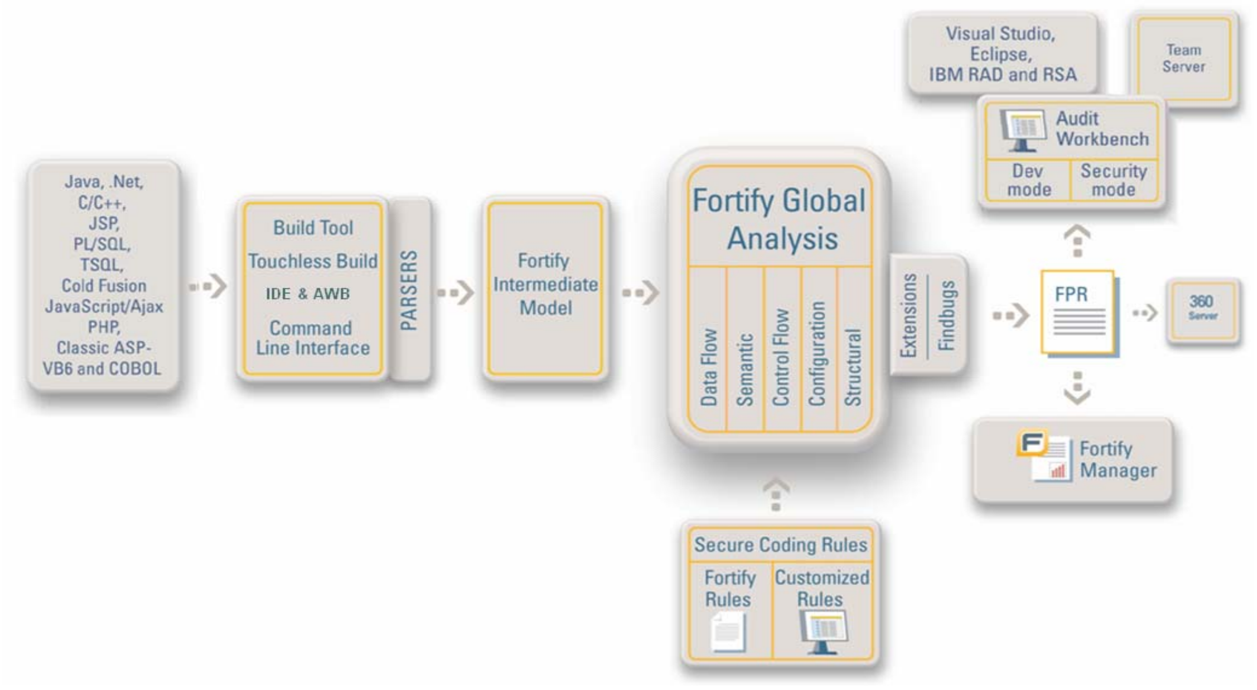
Objective-C

Often Misused: Encoding
Often Misused: File System
Often Misused: Weak SSL Certificate

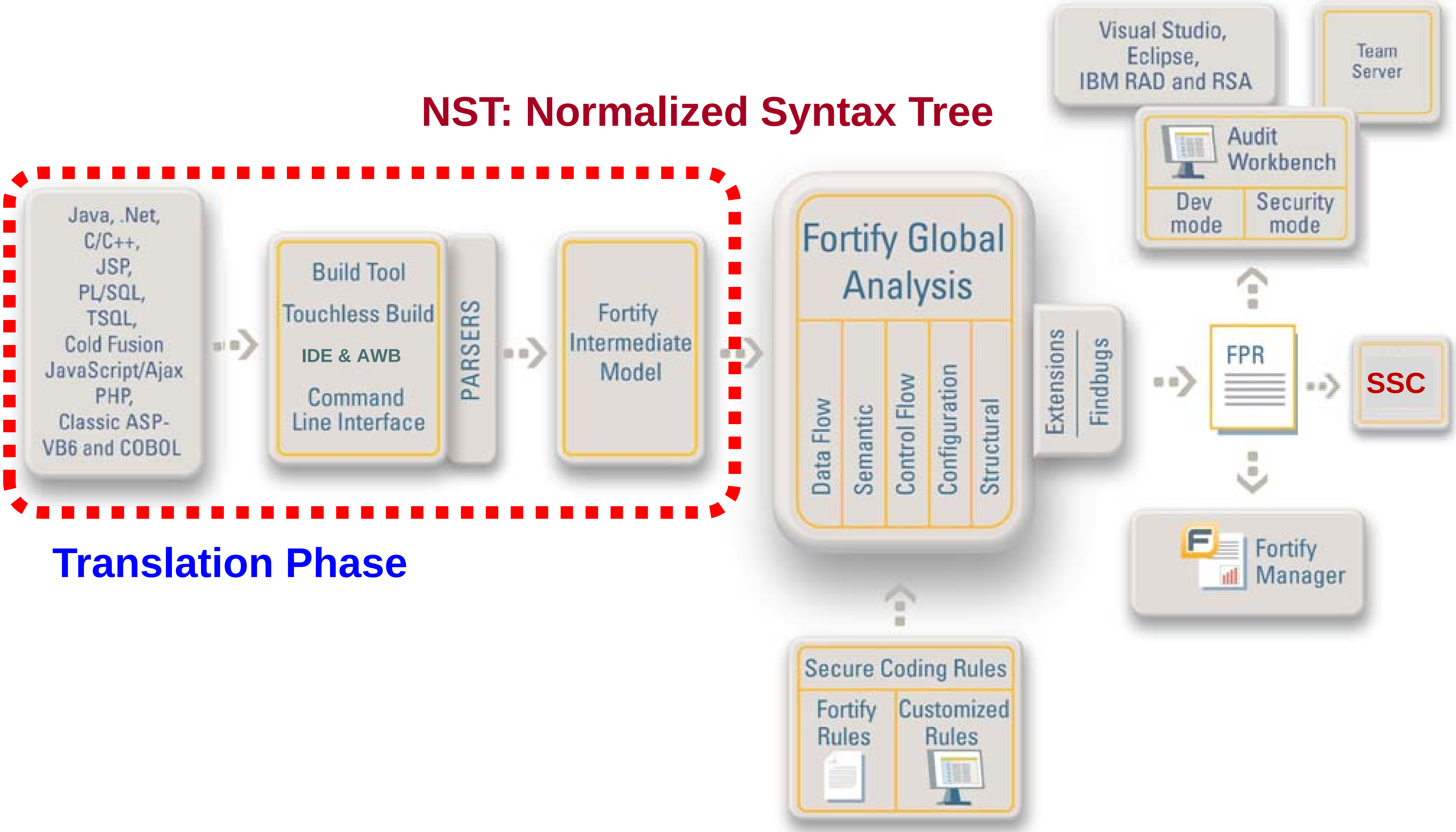
(Generated from version 2012.2.0.0010 of the Fortify Secure Coding Rulepacks)

HP FORTIFY SCA检测程序代码安全漏洞的程序

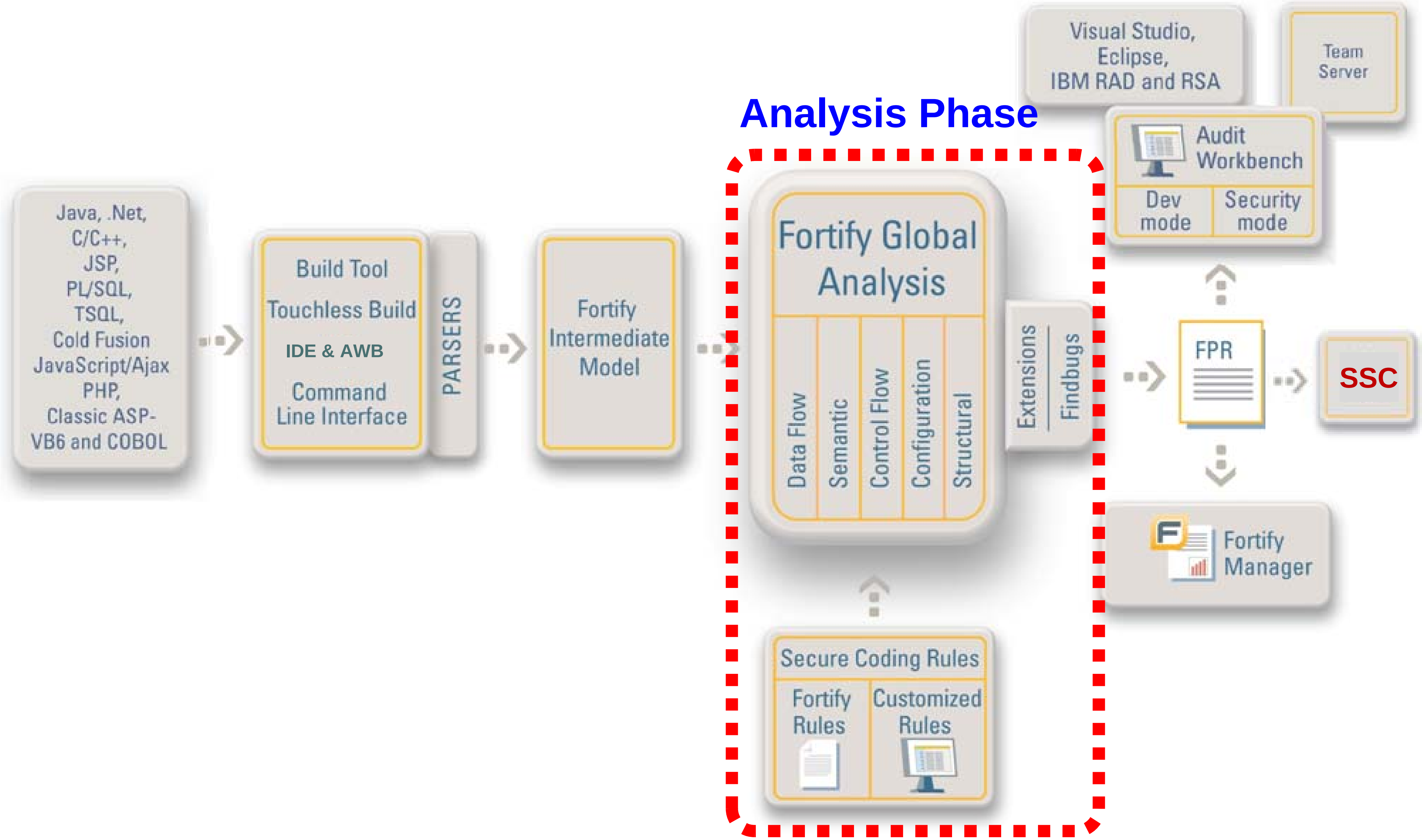
- 转译阶段Translation Phase[1]
- 分析阶段Analysis Phase[2]
- 稽核阶段Audit Phase[3]



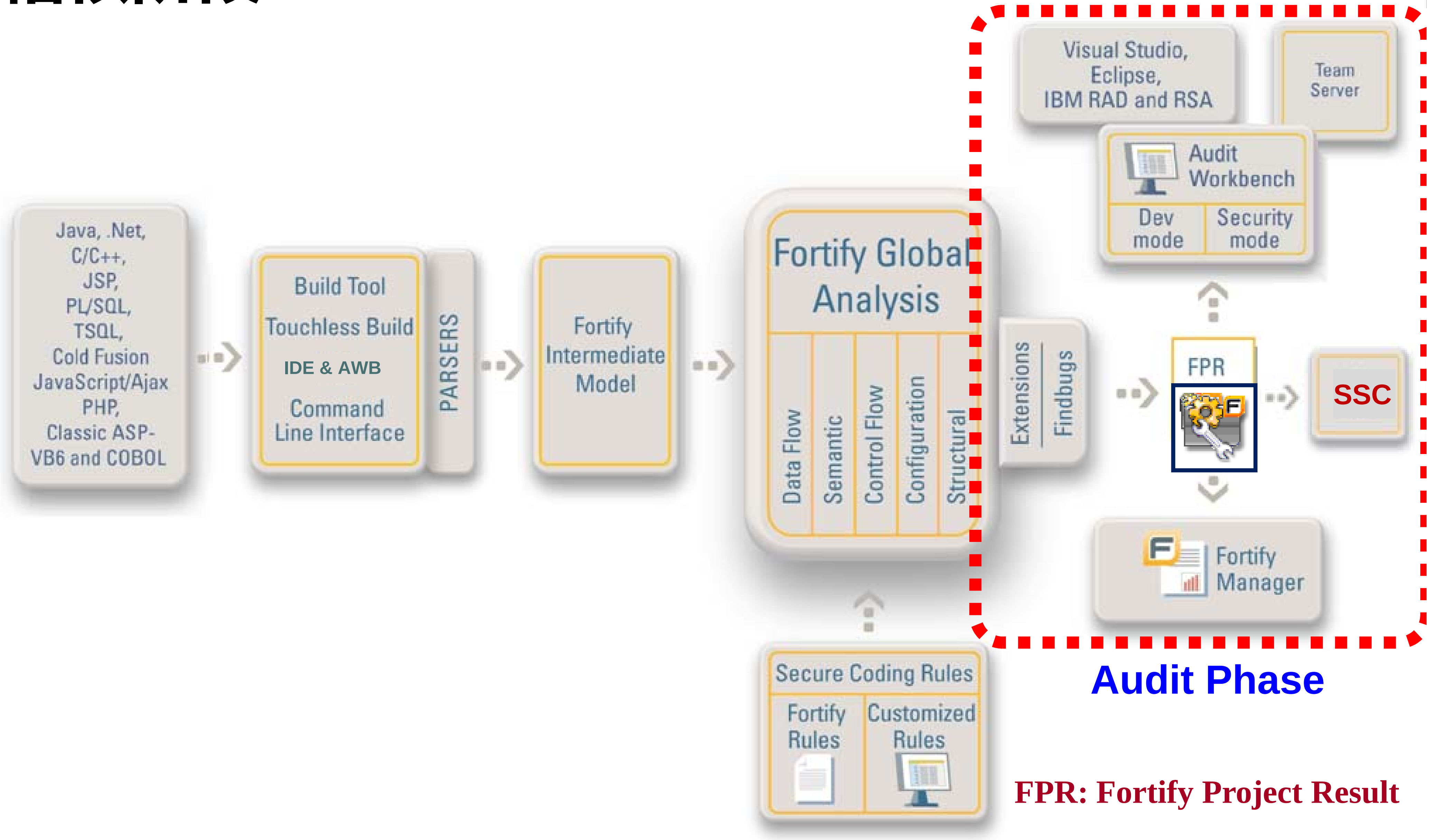
HP FORTIFY SCA (1)
转译阶段TRANSLATION PHASE



HP FORTIFY SCA（2）
分析阶段ANALYSIS PHASE



HP FORTIFY SCA (3) 稽核阶段AUDIT PHASE



Audit Phase

FPR: Fortify Project Result

HP FORTIFY SCA 检测问题等级的区分方法

检测问题等级的归类方式

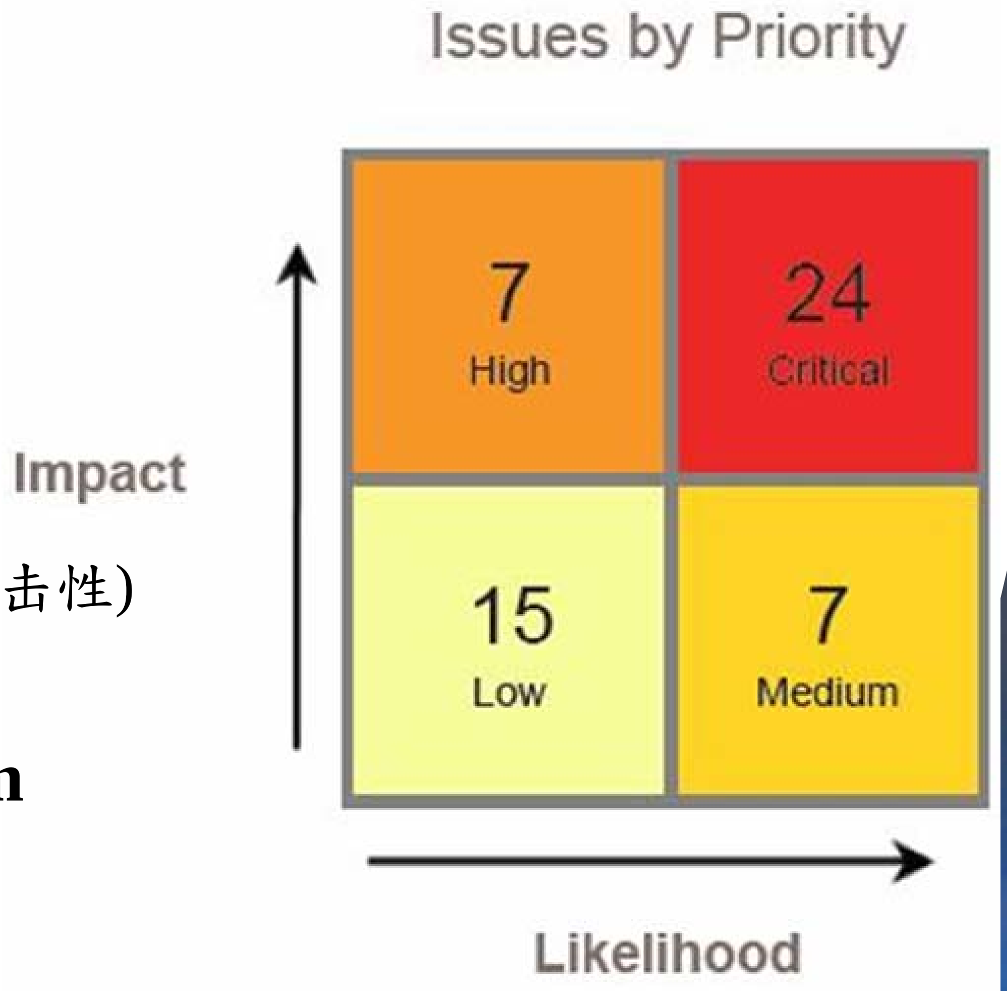
是以两个坐标值做为量化区分依据

(1) Likelihood

(问题准确度的可能性)

(2) Impact

(一旦发生对部门或企业的影响冲击性)



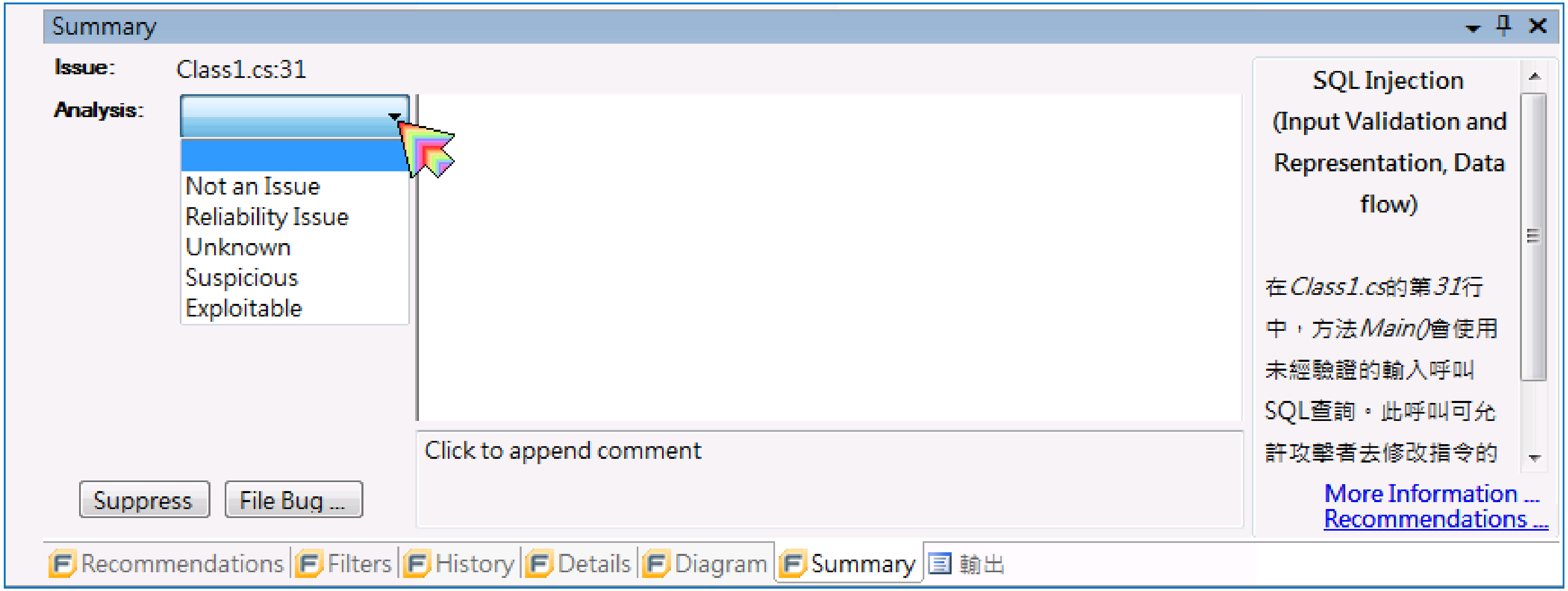
高准确度区: Critical / Medium

凡有嫌疑迹象区: High/ Low

凡有安全漏洞或质量问题的嫌疑迹象就列出的部分

资安人员再人工复核是否有问题

凡有嫌疑迹象区: HIGH/ LOW - AUDIT



Issue: Class1.cs:31

Analysis:

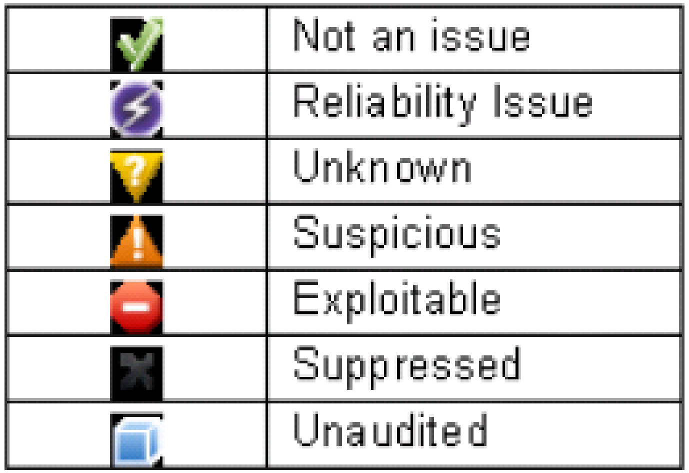
Click to append comment

SQL Injection (Input Validation and Representation, Data flow)

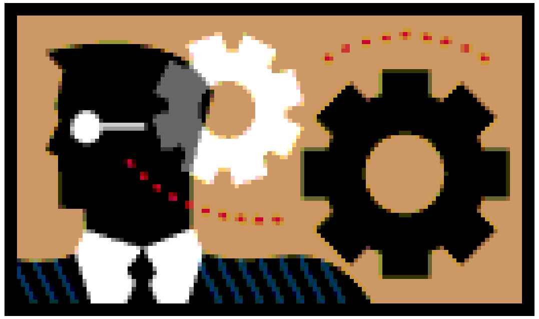
在*Class1.cs*的第*31*行中，方法*Main()*會使用未經驗證的輸入呼叫SQL查詢。此呼叫可允許攻擊者去修改指令的

More Information ...
Recommendations ...

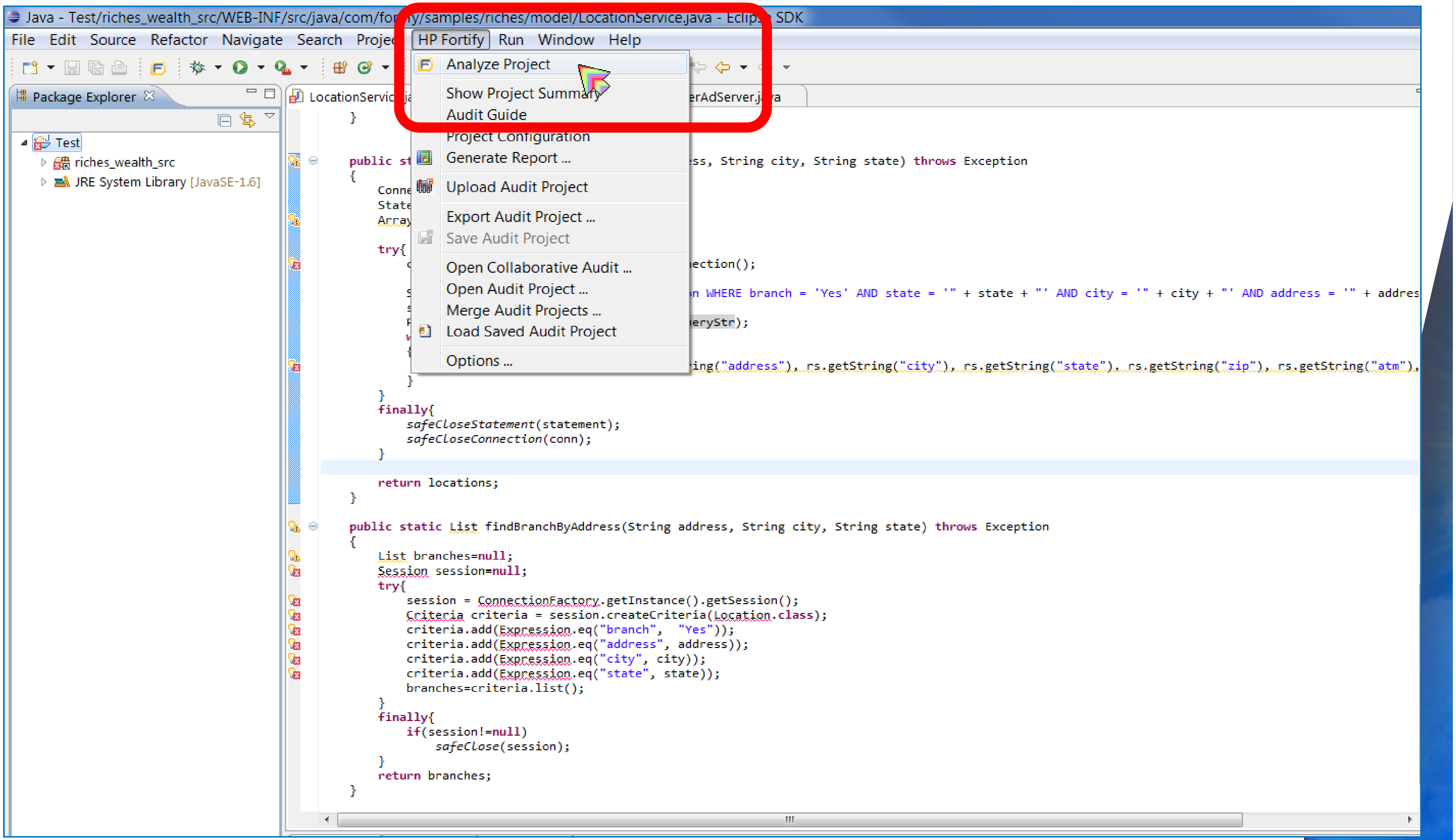
Figure 5: Audit Status Icons



✓	Not an issue
⚡	Reliability Issue
?	Unknown
!	Suspicious
⛔	Exploitable
✗	Suppressed
▢	Unaudited

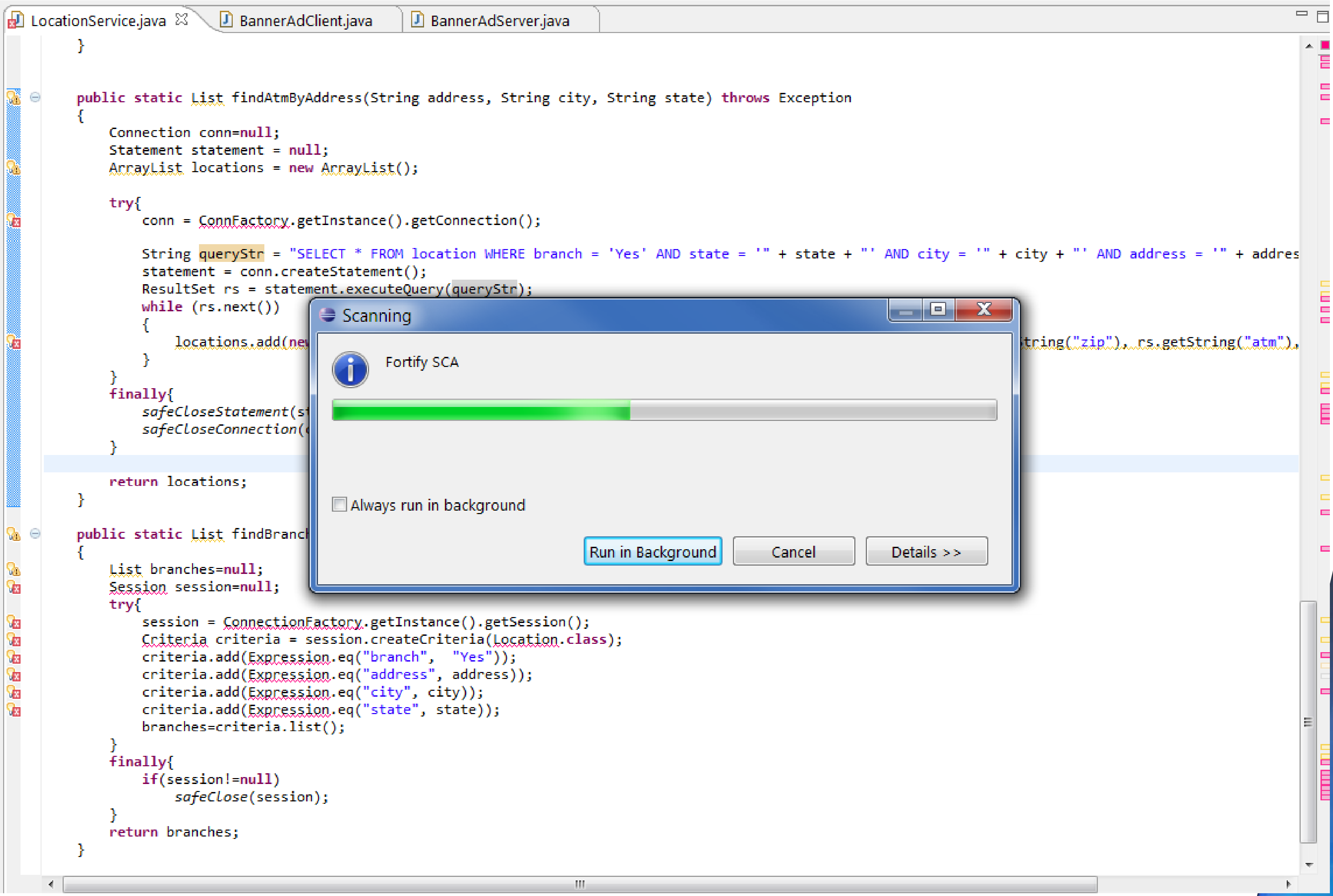


HP FORTIFY SCA 搭配 ECLIPSE 检测 ANDROID



```
    }

    public st                         ss, String city, String state) throws Exception
    {
        Conne
        State
        Array

        try{
            c                         ection();

            s                         n WHERE branch = 'Yes' AND state = '" + state + "' AND city = '" + city + "' AND address = '" + addres
            s
            F                         eryStr);
            w
            {                         ing("address"), rs.getString("city"), rs.getString("state"), rs.getString("zip"), rs.getString("atm"),
            }
        }
        finally{
            safeCloseStatement(statement);
            safeCloseConnection(conn);
        }

        return locations;
    }

    public static List findBranchByAddress(String address, String city, String state) throws Exception
    {
        List branches=null;
        Session session=null;
        try{
            session = ConnectionFactory.getInstance().getSession();
            Criteria criteria = session.createCriteria(Location.class);
            criteria.add(Expression.eq("branch",  "Yes"));
            criteria.add(Expression.eq("address", address));
            criteria.add(Expression.eq("city", city));
            criteria.add(Expression.eq("state", state));
            branches=criteria.list();
        }
        finally{
            if(session!=null)
                safeClose(session);
        }
        return branches;
    }
```

HP FORTIFY SCA搭配 ECLIPSE 检测 ANDROID



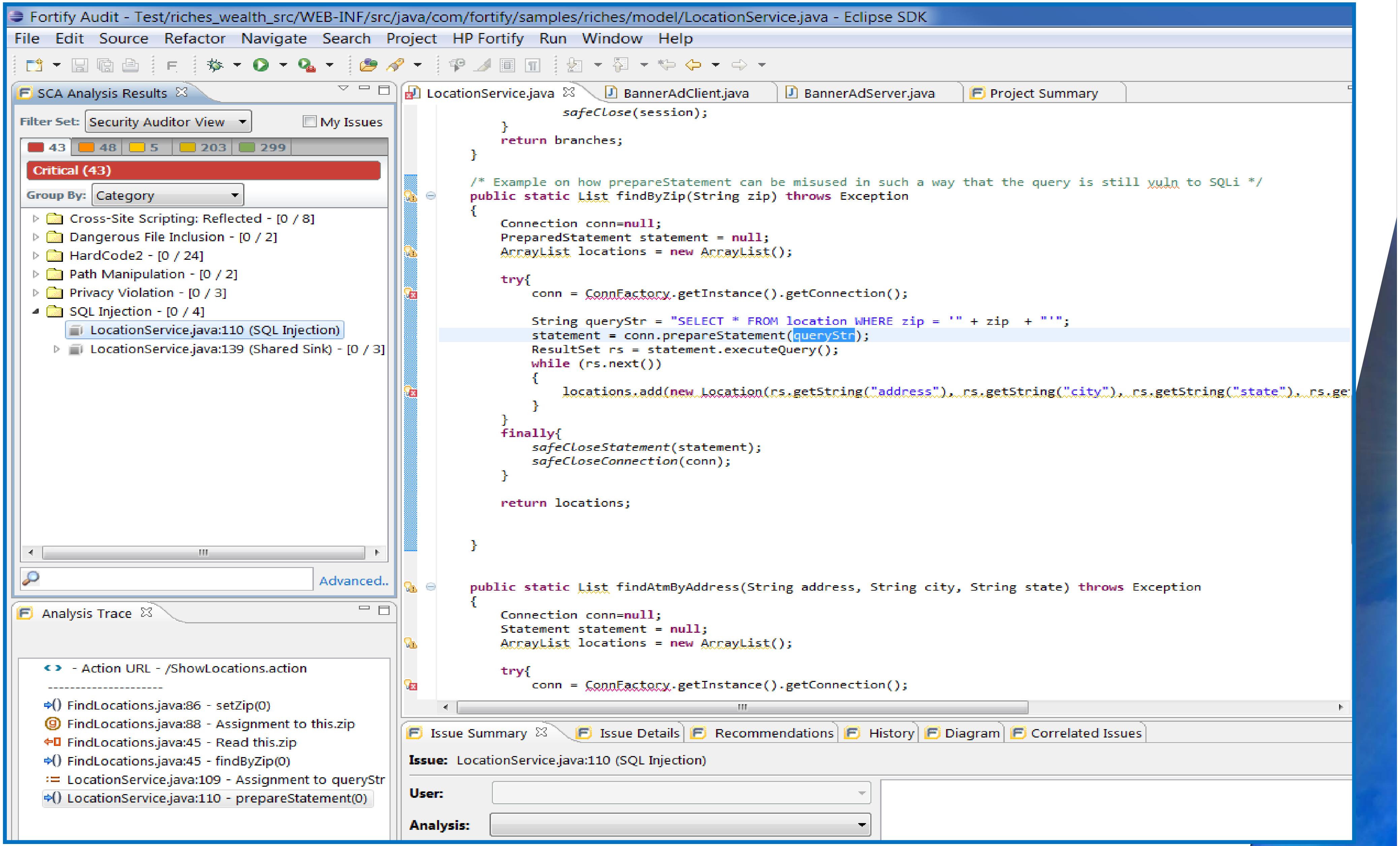
```
    }

    public static List findAtmByAddress(String address, String city, String state) throws Exception
    {
        Connection conn=null;
        Statement statement = null;
        ArrayList locations = new ArrayList();

        try{
            conn = ConnFactory.getInstance().getConnection();

            String queryStr = "SELECT * FROM location WHERE branch = 'Yes' AND state = '" + state + "' AND city = '" + city + "' AND address = '" + addres
            statement = conn.createStatement();
            ResultSet rs = statement.executeQuery(queryStr);
            while (rs.next())
            {
                locations.add(new                                             tring("zip"), rs.getString("atm"),
            }
        }
        finally{
            safeCloseStatement(st
            safeCloseConnection(
        }

        return locations;
    }

    public static List findBranch
    {
        List branches=null;
        Session session=null;
        try{
            session = ConnectionFactory.getInstance().getSession();
            Criteria criteria = session.createCriteria(Location.class);
            criteria.add(Expression.eq("branch",  "Yes"));
            criteria.add(Expression.eq("address", address));
            criteria.add(Expression.eq("city", city));
            criteria.add(Expression.eq("state", state));
            branches=criteria.list();
        }
        finally{
            if(session!=null)
                safeClose(session);
        }
        return branches;
    }
```

Scanning

Fortify SCA

□ Always run in background

HP FORTIFY SCA搭配 ECLIPSE 检测 ANDROID



- Cross-Site Scripting: Reflected - [0 / 8]
- Dangerous File Inclusion - [0 / 2]
- HardCode2 - [0 / 24]
- Path Manipulation - [0 / 2]
- Privacy Violation - [0 / 3]
- SQL Injection - [0 / 4]
  - LocationService.java:110 (SQL Injection)
  - LocationService.java:139 (Shared Sink) - [0 / 3]

```
            safeClose(session);
    }
    return branches;
}

/* Example on how prepareStatement can be misused in such a way that the query is still vuln to SQLi */
public static List findByZip(String zip) throws Exception
{
    Connection conn=null;
    PreparedStatement statement = null;
    ArrayList locations = new ArrayList();

    try{
        conn = ConnFactory.getInstance().getConnection();

        String queryStr = "SELECT * FROM location WHERE zip = '" + zip  + "'";
        statement = conn.prepareStatement(queryStr);
        ResultSet rs = statement.executeQuery();
        while (rs.next())
        {
            locations.add(new Location(rs.getString("address"), rs.getString("city"), rs.getString("state"), rs.ge
        }
    }
    finally{
        safeCloseStatement(statement);
        safeCloseConnection(conn);
    }

    return locations;


}


public static List findAtmByAddress(String address, String city, String state) throws Exception
{
    Connection conn=null;
    Statement statement = null;
    ArrayList locations = new ArrayList();

    try{
        conn = ConnFactory.getInstance().getConnection();
```

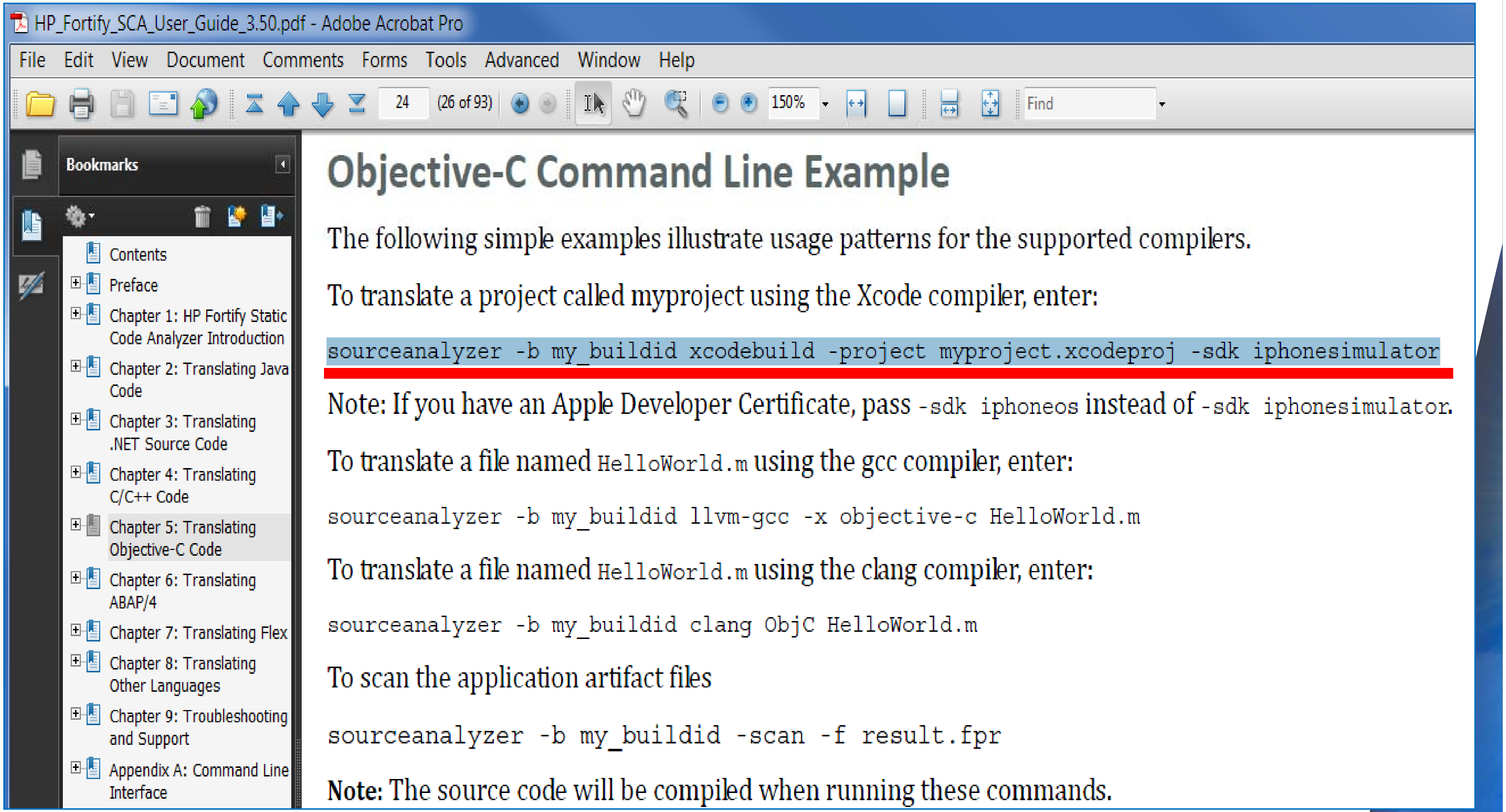
```
< > - Action URL - /ShowLocations.action
--------------------
FindLocations.java:86 - setZip(0)
FindLocations.java:88 - Assignment to this.zip
FindLocations.java:45 - Read this.zip
FindLocations.java:45 - findByZip(0)
LocationService.java:109 - Assignment to queryStr
LocationService.java:110 - prepareStatement(0)
```

Issue: LocationService.java:110 (SQL Injection)

User:

Analysis:

HP FORTIFY SCA 检测 OBJECT-C（iPhone）



HP_Fortify_SCA_User_Guide_3.50.pdf - Adobe Acrobat Pro
File Edit View Document Comments Forms Tools Advanced Window Help
24
(26 of 93)
150%
Find
Bookmarks

Objective-C Command Line Example

The following simple examples illustrate usage patterns for the supported compilers.

To translate a project called myproject using the Xcode compiler, enter:

```
sourceanalyzer -b my_buildid xcodebuild -project myproject.xcodeproj -sdk iphonesimulator
```

Note: If you have an Apple Developer Certificate, pass `-sdk iphoneos` instead of `-sdk iphonesimulator`.

To translate a file named `HelloWorld.m` using the gcc compiler, enter:

```
sourceanalyzer -b my_buildid llvm-gcc -x objective-c HelloWorld.m
```

To translate a file named `HelloWorld.m` using the clang compiler, enter:

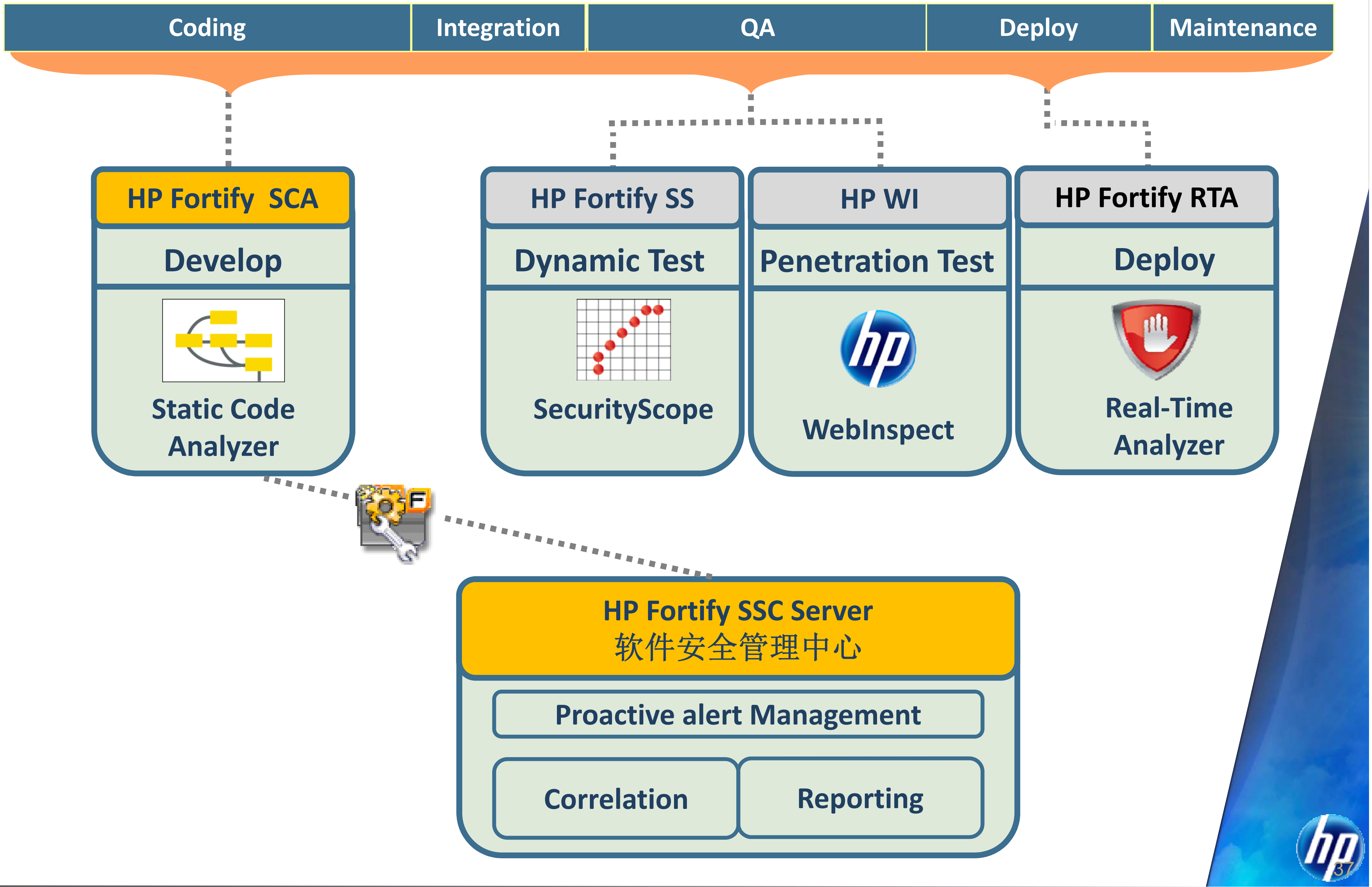
```
sourceanalyzer -b my_buildid clang ObjC HelloWorld.m
```

To scan the application artifact files

```
sourceanalyzer -b my_buildid -scan -f result.fpr
```

Note: The source code will be compiled when running these commands.

惠普移动应用安全解决方案
软件安全管理中心（SSC SERVER）



Coding | Integration | QA | Deploy | Maintenance

HP Fortify SCA
Develop
Static Code Analyzer

HP Fortify SS
Dynamic Test
SecurityScope

HP WI
Penetration Test
WebInspect

HP Fortify RTA
Deploy
Real-Time Analyzer

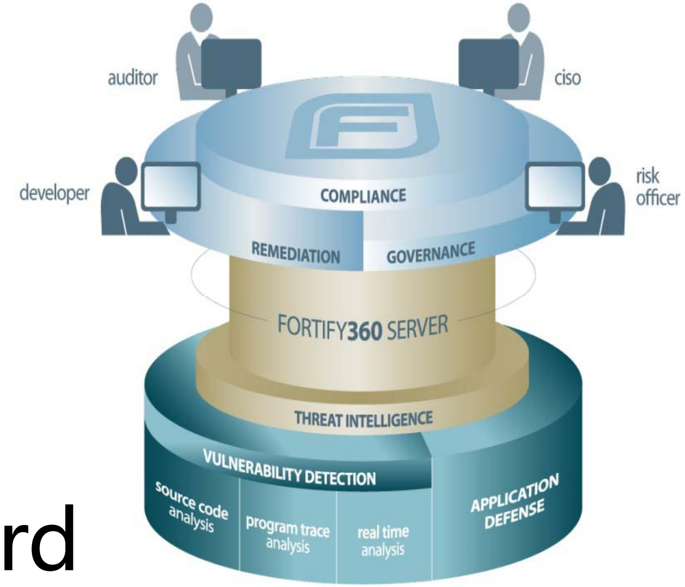
HP Fortify SSC Server
软件安全管理中心

Proactive alert Management

Correlation

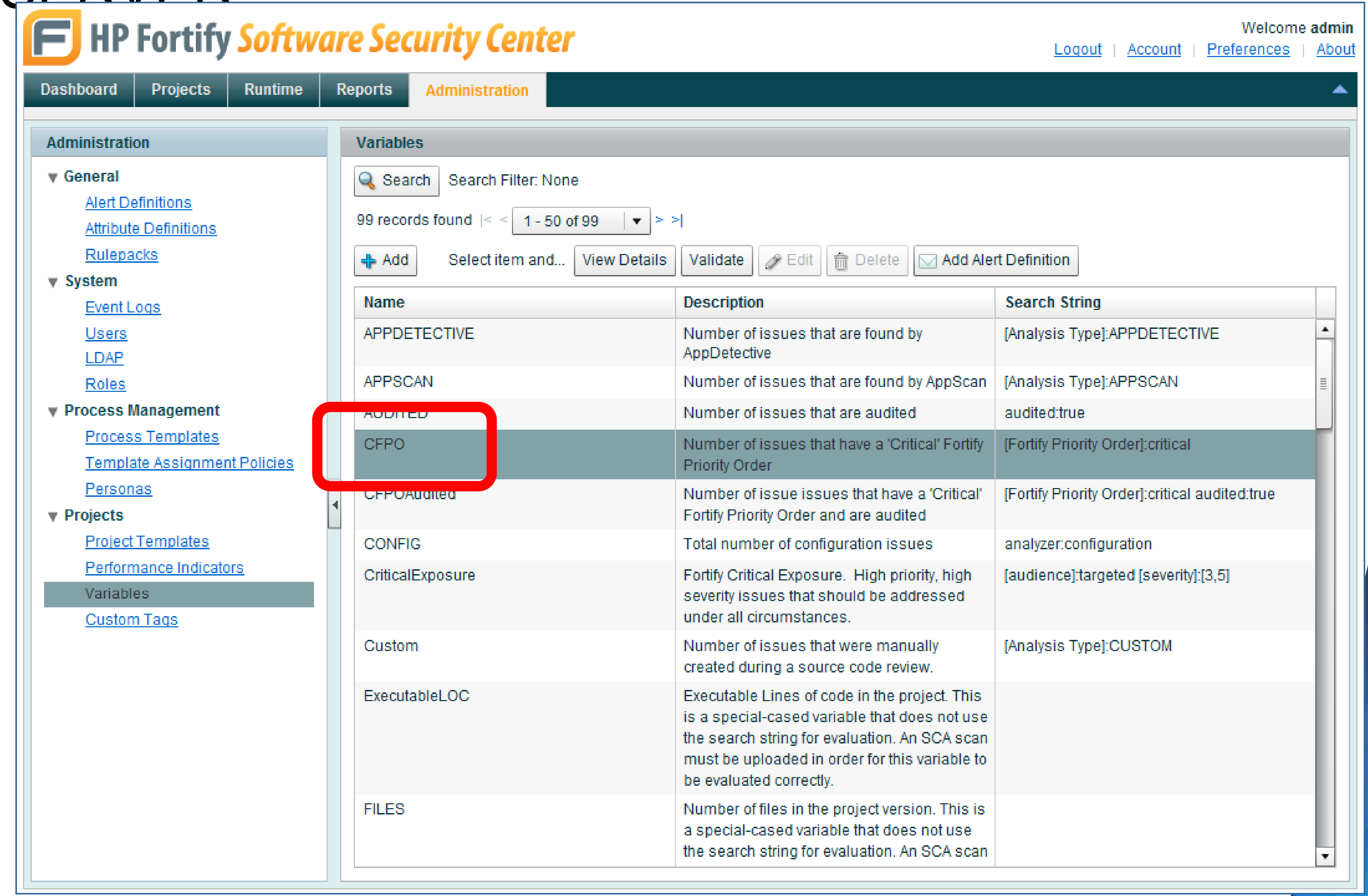
Reporting

主动式减少软件风险的平台



- **Security Policy Alert System Module**
  - Event Alert
  - Security Issues Status Dashboard
  - Remediating Vulnerabilities Collaboratively

DEFINE SOFTWARE SECURITY VARIABLES ON SSC SERVER

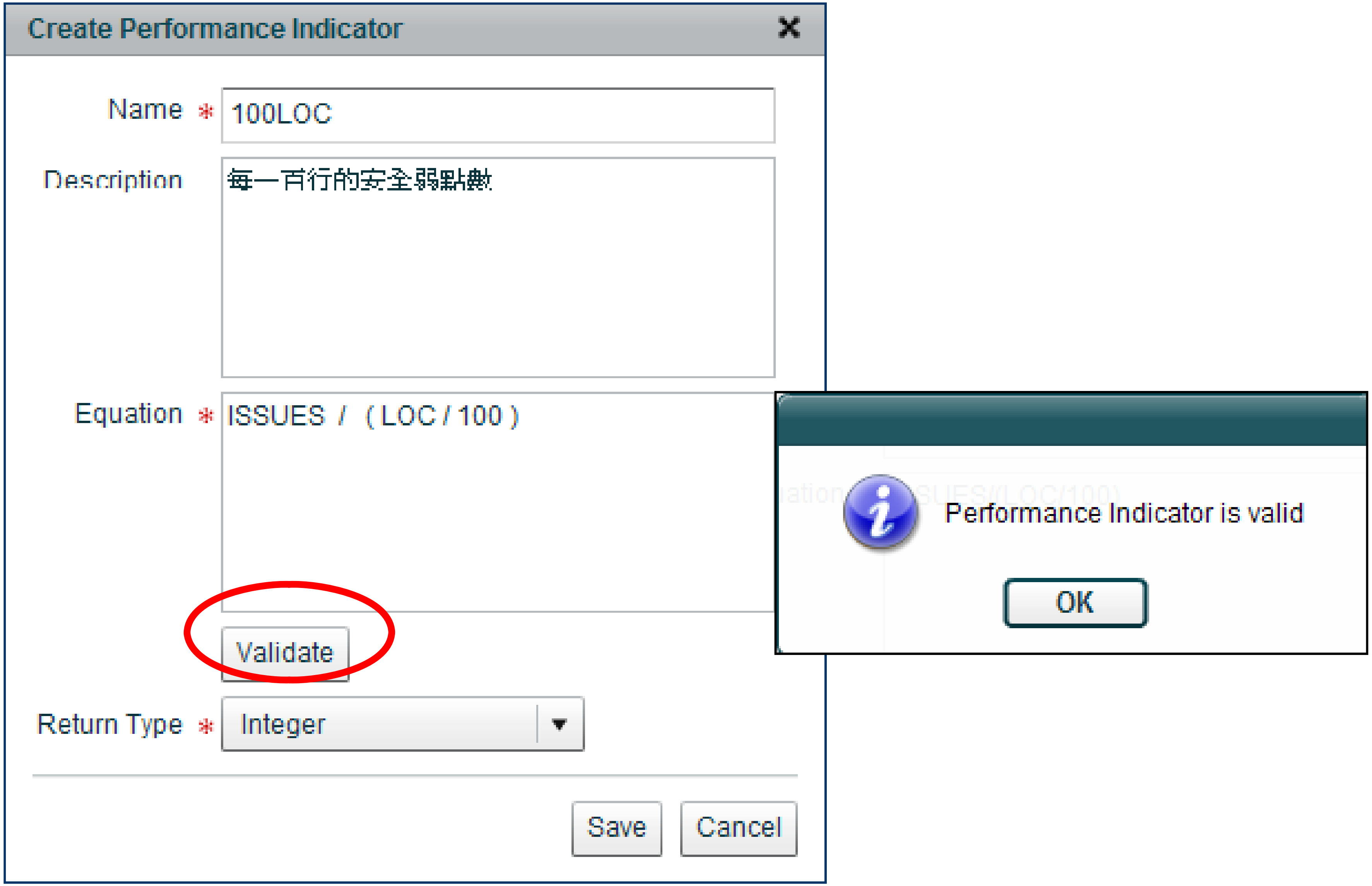


Search Filter: None

99 records found |< < 1 - 50 of 99 > >|

Name	Description	Search String
APPDETECTIVE	Number of issues that are found by AppDetective	[Analysis Type]:APPDETECTIVE
APPSCAN	Number of issues that are found by AppScan	[Analysis Type]:APPSCAN
AUDITED	Number of issues that are audited	audited:true
CFPO	Number of issues that have a 'Critical' Fortify Priority Order	[Fortify Priority Order]:critical
CFPOAudited	Number of issue issues that have a 'Critical' Fortify Priority Order and are audited	[Fortify Priority Order]:critical audited:true
CONFIG	Total number of configuration issues	analyzer:configuration
CriticalExposure	Fortify Critical Exposure. High priority, high severity issues that should be addressed under all circumstances.	[audience]:targeted [severity]:[3,5]
Custom	Number of issues that were manually created during a source code review.	[Analysis Type]:CUSTOM
ExecutableLOC	Executable Lines of code in the project. This is a special-cased variable that does not use the search string for evaluation. An SCA scan must be uploaded in order for this variable to be evaluated correctly.	
FILES	Number of files in the project version. This is a special-cased variable that does not use the search string for evaluation. An SCA scan	

SECURITY POLICY ALERT SYSTEM CUSTOM DEFINE 100LOC



Create Performance Indicator

Name * 100LOC

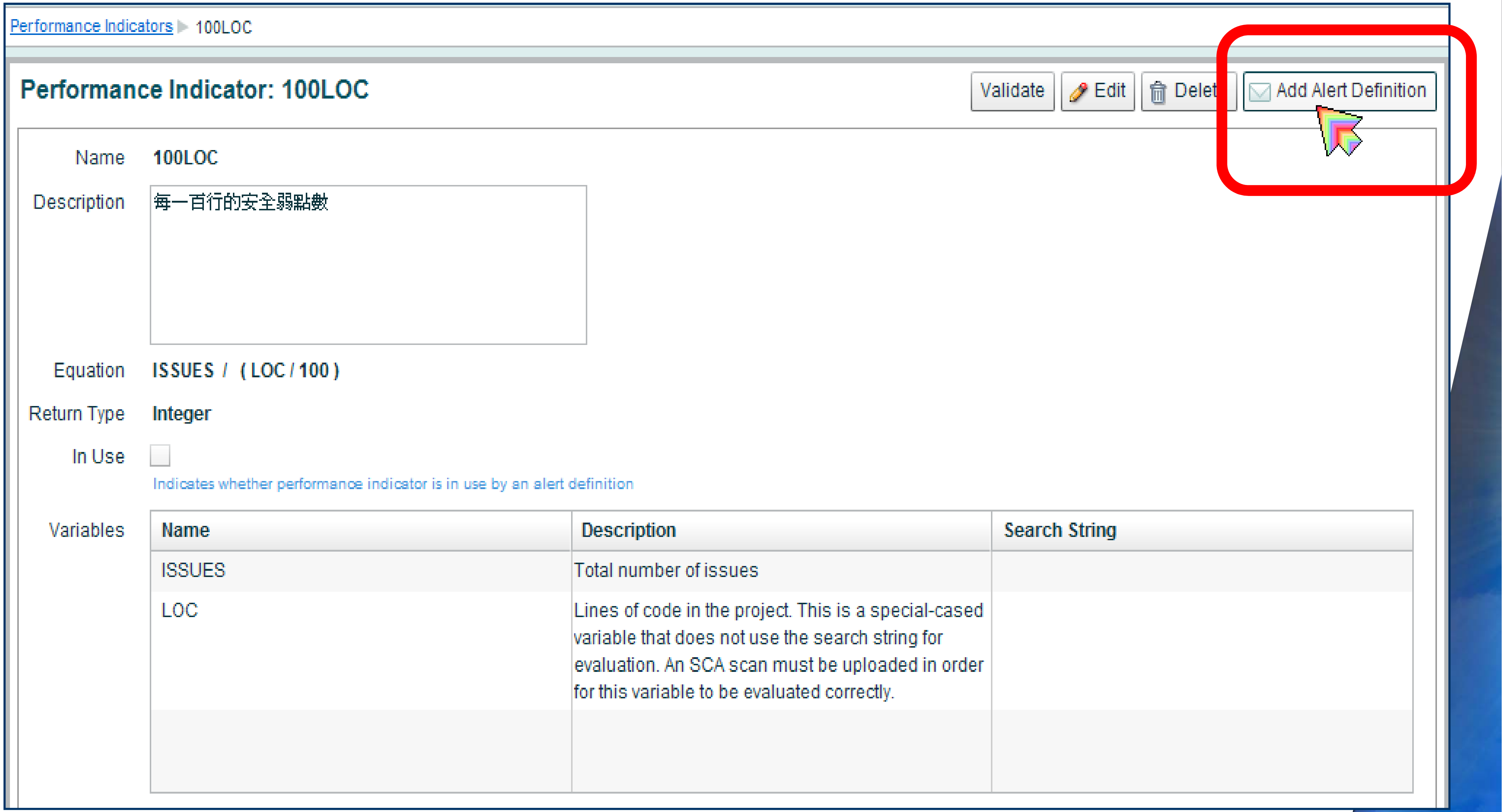
Description 每一百行的安全弱點數

Equation * ISSUES / (LOC / 100)

Return Type * Integer

Performance Indicator is valid

SECURITY POLICY ALERT SYSTEM
ADD ALERT FOR 100LOC



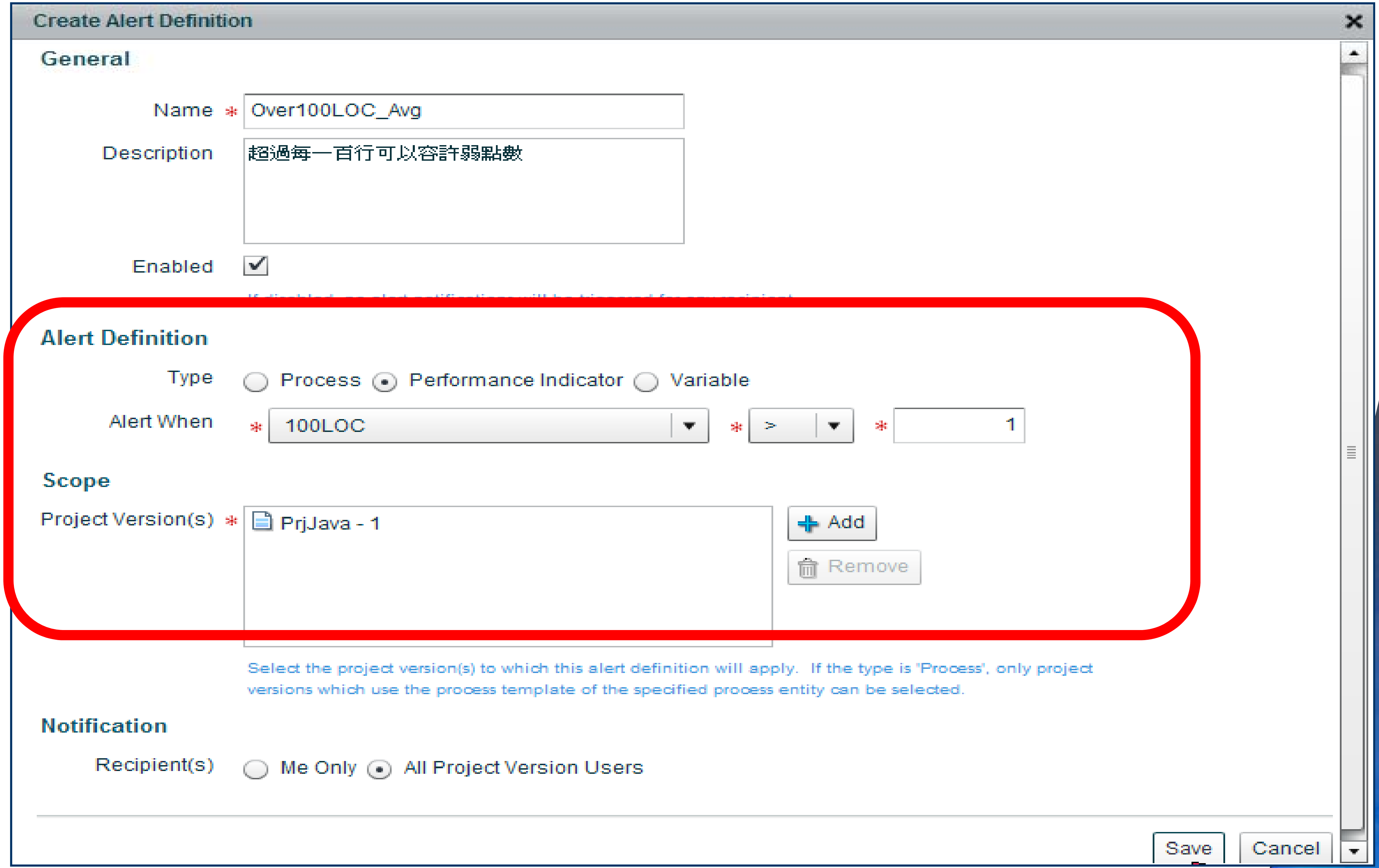
Performance Indicator: 100LOC

Name	100LOC
Description	每一百行的安全弱點數
Equation	ISSUES / (LOC / 100)
Return Type	Integer
In Use	□ Indicates whether performance indicator is in use by an alert definition

Variables

Name	Description	Search String
ISSUES	Total number of issues	
LOC	Lines of code in the project. This is a special-cased variable that does not use the search string for evaluation. An SCA scan must be uploaded in order for this variable to be evaluated correctly.	

SECURITY POLICY ALERT SYSTEM
ADD ALERT FOR 100LOC



Create Alert Definition

General

Name * Over100LOC_Avg

Description 超過每一百行可以容許弱點數

Enabled ☑

Alert Definition

Type ○ Process ● Performance Indicator ○ Variable

Alert When * 100LOC * > * 1

Scope

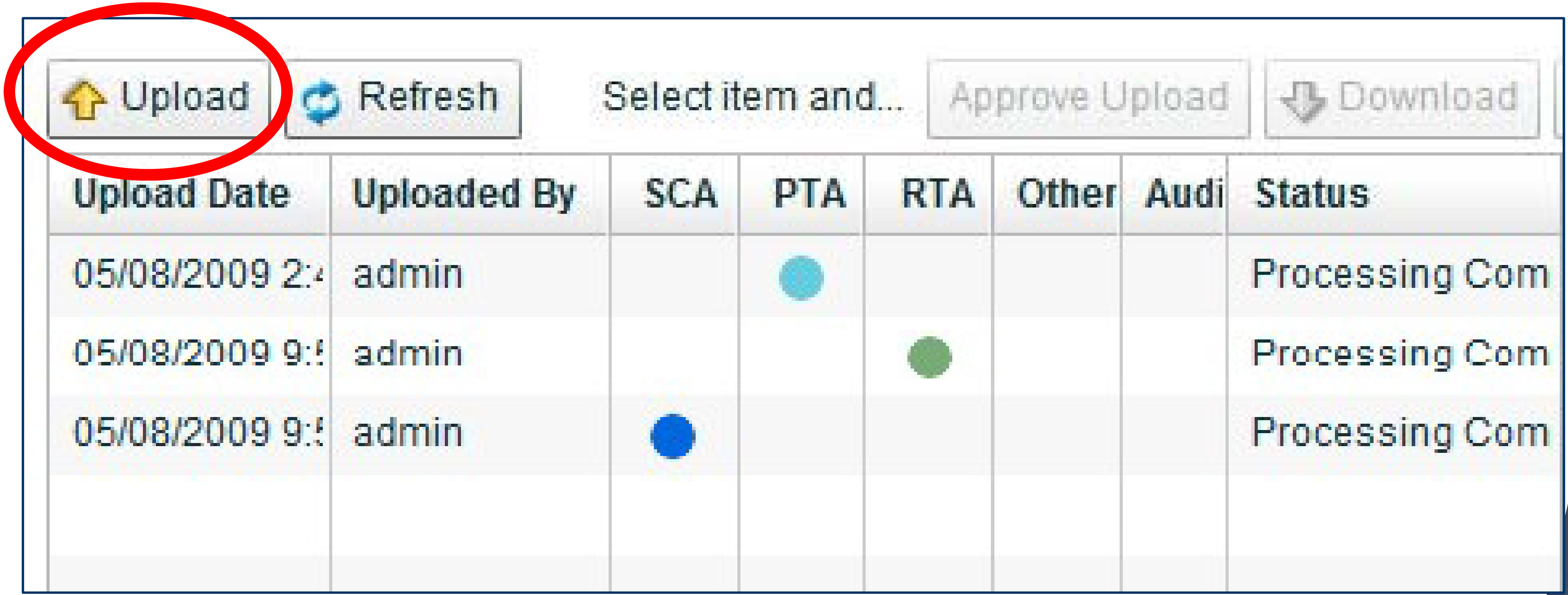
Project Version(s) * PrjJava - 1

Select the project version(s) to which this alert definition will apply. If the type is 'Process', only project versions which use the process template of the specified process entity can be selected.

Notification

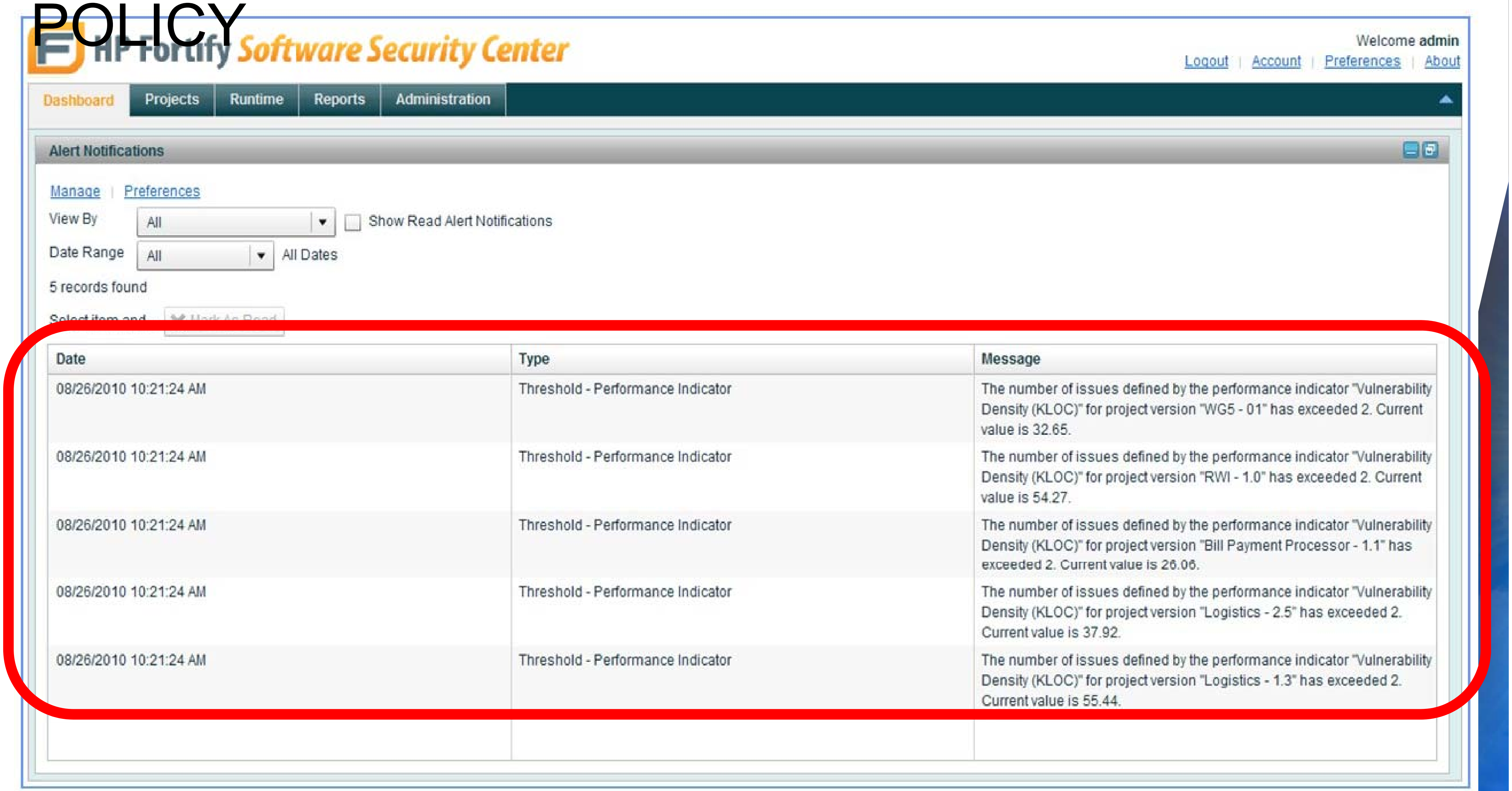
Recipient(s) ○ Me Only ● All Project Version Users

UPLOAD PROJECT SCAN RESULT (FPR) BY WEEKLY



Upload Date	Uploaded By	SCA	PTA	RTA	Other	Audi	Status
05/08/2009 2:4	admin		●				Processing Com
05/08/2009 9:5	admin			●			Processing Com
05/08/2009 9:5	admin	●					Processing Com

SEND PROACTIVE ALERT MESSAGE WHEN SCAN RESULT OVER ENTERPRISE SECURITY POLICY


HP Fortify Software Security Center
Welcome admin
Logout | Account | Preferences | About
Dashboard
Projects
Runtime
Reports
Administration

Alert Notifications

Manage | Preferences

View By: All ☐ Show Read Alert Notifications

Date Range: All — All Dates

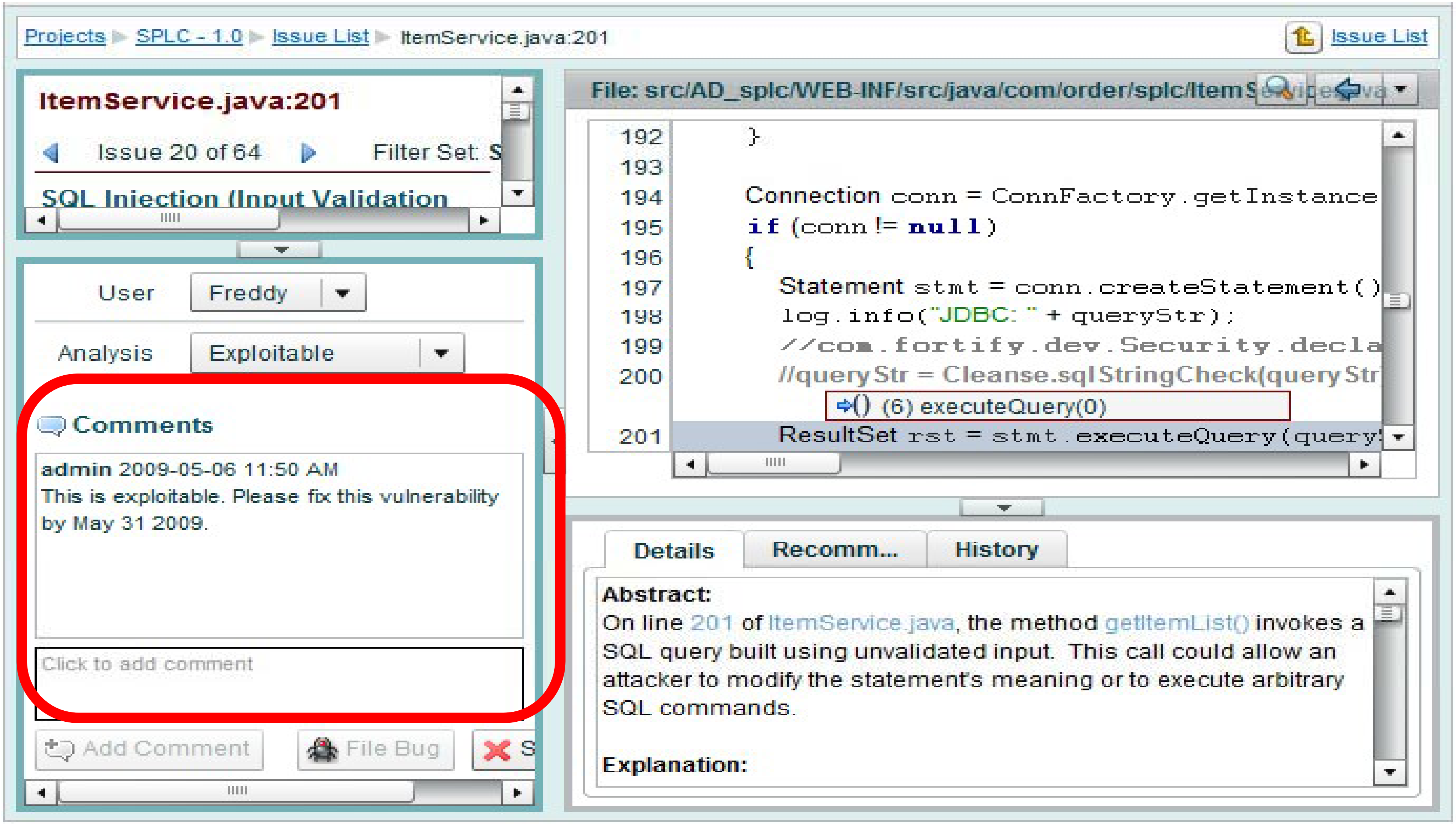
5 records found

Select item and … Mark As Read

Date	Type	Message
08/26/2010 10:21:24 AM	Threshold - Performance Indicator	The number of issues defined by the performance indicator "Vulnerability Density (KLOC)" for project version "WG5 - 01" has exceeded 2. Current value is 32.65.
08/26/2010 10:21:24 AM	Threshold - Performance Indicator	The number of issues defined by the performance indicator "Vulnerability Density (KLOC)" for project version "RWI - 1.0" has exceeded 2. Current value is 54.27.
08/26/2010 10:21:24 AM	Threshold - Performance Indicator	The number of issues defined by the performance indicator "Vulnerability Density (KLOC)" for project version "Bill Payment Processor - 1.1" has exceeded 2. Current value is 26.06.
08/26/2010 10:21:24 AM	Threshold - Performance Indicator	The number of issues defined by the performance indicator "Vulnerability Density (KLOC)" for project version "Logistics - 2.5" has exceeded 2. Current value is 37.92.
08/26/2010 10:21:24 AM	Threshold - Performance Indicator	The number of issues defined by the performance indicator "Vulnerability Density (KLOC)" for project version "Logistics - 1.3" has exceeded 2. Current value is 55.44.

REMEDIATING VULNERABILITIES COLLABORATIVELY

– Interactive Communication How to Fix Issues



Projects ▶ SPLC - 1.0 ▶ Issue List ▶ ItemService.java:201

Issue List

ItemService.java:201

◀ Issue 20 of 64 ▶ Filter Set: S

SQL Injection (Input Validation

User Freddy

Analysis Exploitable

Comments

admin 2009-05-06 11:50 AM
This is exploitable. Please fix this vulnerability by May 31 2009.

Click to add comment

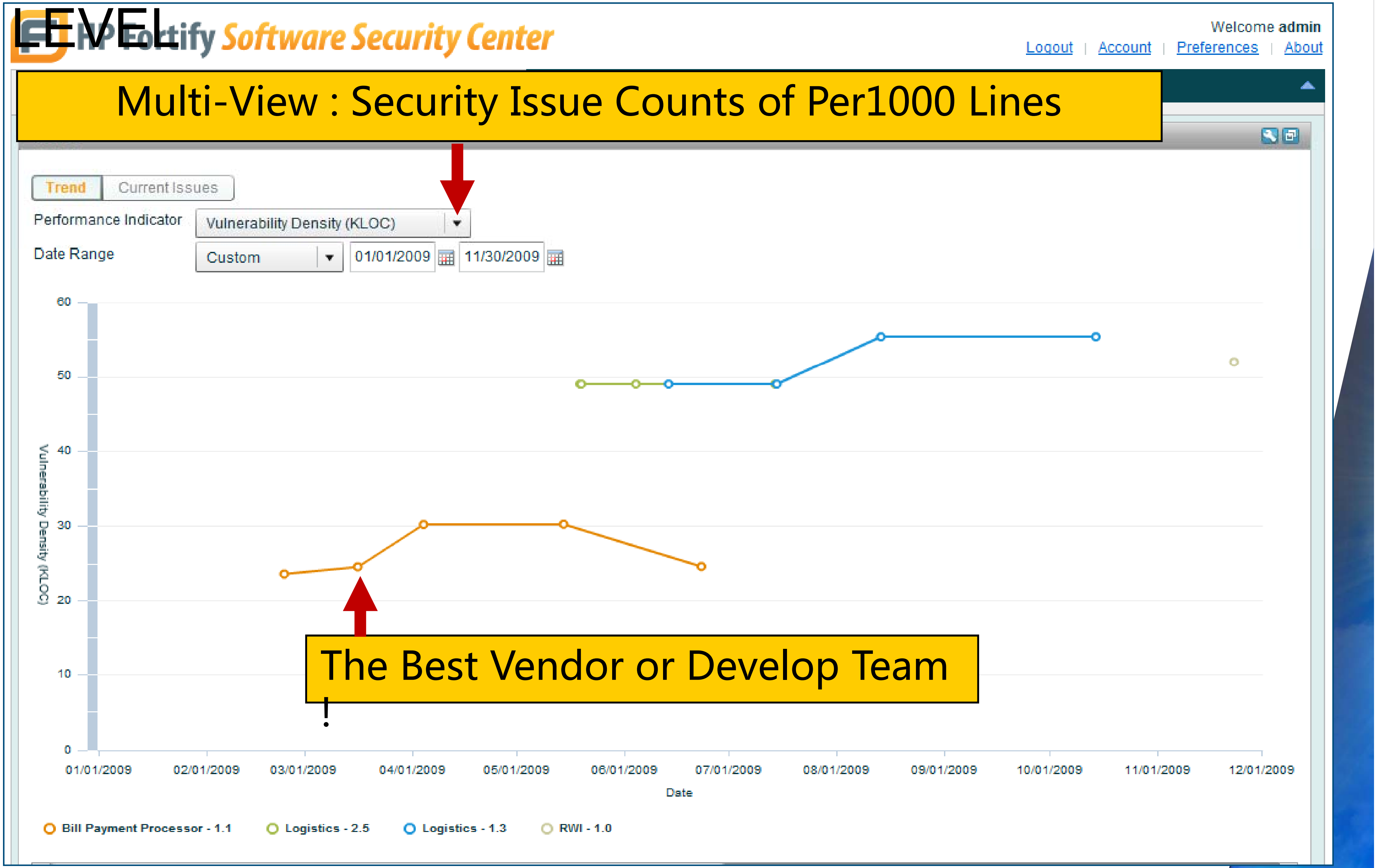
File: src/AD_splc/WEB-INF/src/java/com/order/splc/ItemServic...java

```
192        }
193
194        Connection conn = ConnFactory.getInstance
195        if (conn != null)
196        {
197            Statement stmt = conn.createStatement()
198            log.info("JDBC: " + queryStr);
199            //com.fortify.dev.Security.decla
200            //queryStr = Cleanse.sqlStringCheck(queryStr
                   ➪() (6) executeQuery(0)
201            ResultSet rst = stmt.executeQuery(query
```

Abstract:
On line 201 of ItemService.java, the method getItemList() invokes a SQL query built using unvalidated input. This call could allow an attacker to modify the statement's meaning or to execute arbitrary SQL commands.

Explanation:

EASILY COMPARED DEVELOP TEAMS SECURITY LEVEL



HP Fortify Software Security Center
Welcome admin
Logout | Account | Preferences | About
Trend
Current Issues

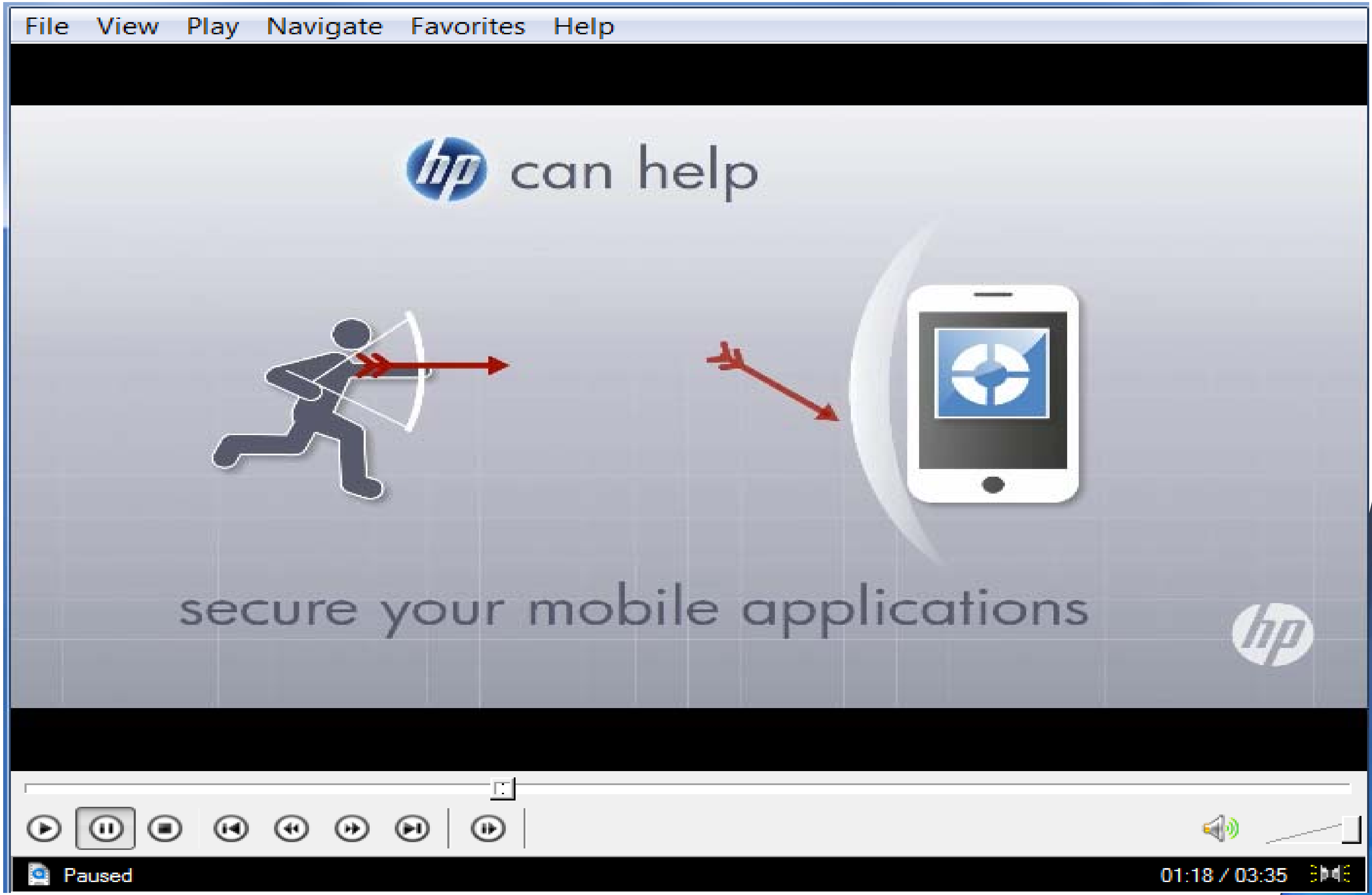
Performance Indicator: Vulnerability Density (KLOC)

Date Range: Custom 01/01/2009 11/30/2009

Multi-View : Security Issue Counts of Per1000 Lines

The Best Vendor or Develop Team !

惠普移动应用安全解决方案視頻


File View Play Navigate Favorites Help
can help
secure your mobile applications
Paused
01:18 / 03:35

Q & A