HP Fortify Software Security Center产品介绍

北京晓通宏志科技有限公司

ENTERPRISE SECURITY

HP Fortify ——软件安全的领导者

- 领先的市场份额
  - 全世界最大的10大银行的9家、大型IT基建供应商、大型独立软体公司
  - 支持市场上最流行、最多样化的编程語言
- 领先解决方案
  - 获奖产品支持整个开发周期
  - 超过150项专利
  - 最庞大的安全编码规则库
- 专业的安装部署
  - 与Fortune100 企业及大型 ISVs 开发出來的最佳做法
  - 由世界顶尖安全专家鉴定

"Fortify is the clear winner for many reasons, including their superior analysis and reporting capabilities, and their understanding and support of how security fits into the software development lifecycle."

— Mary Ann Davidson
*CSO, **Oracle***

ORACLE

SD Times 2007 100 | SD Times 2008 100 | Software Development 16th annual product excellence award Jolt | InfoWorld 2006 Technology of the Year Award | Software Development 16th annual product excellence award Jolt | //CODiE// 2011 SIIA CODiE FINALIST | CODiE Finalist 2011

HP Fortify的主要客户

银行及金融

基础软件厂商

政府机构

医疗及保健

电信

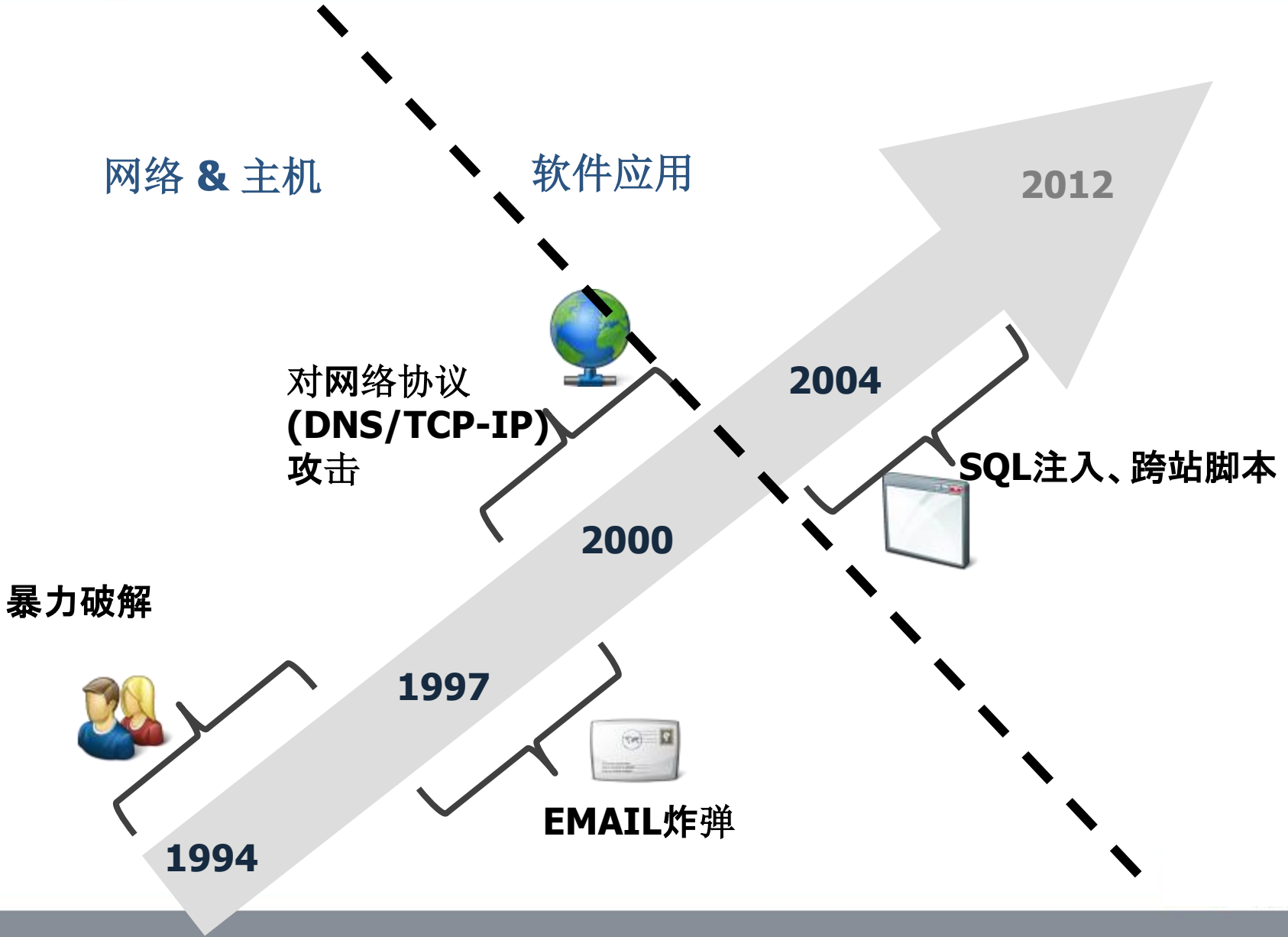
其它

电子商务

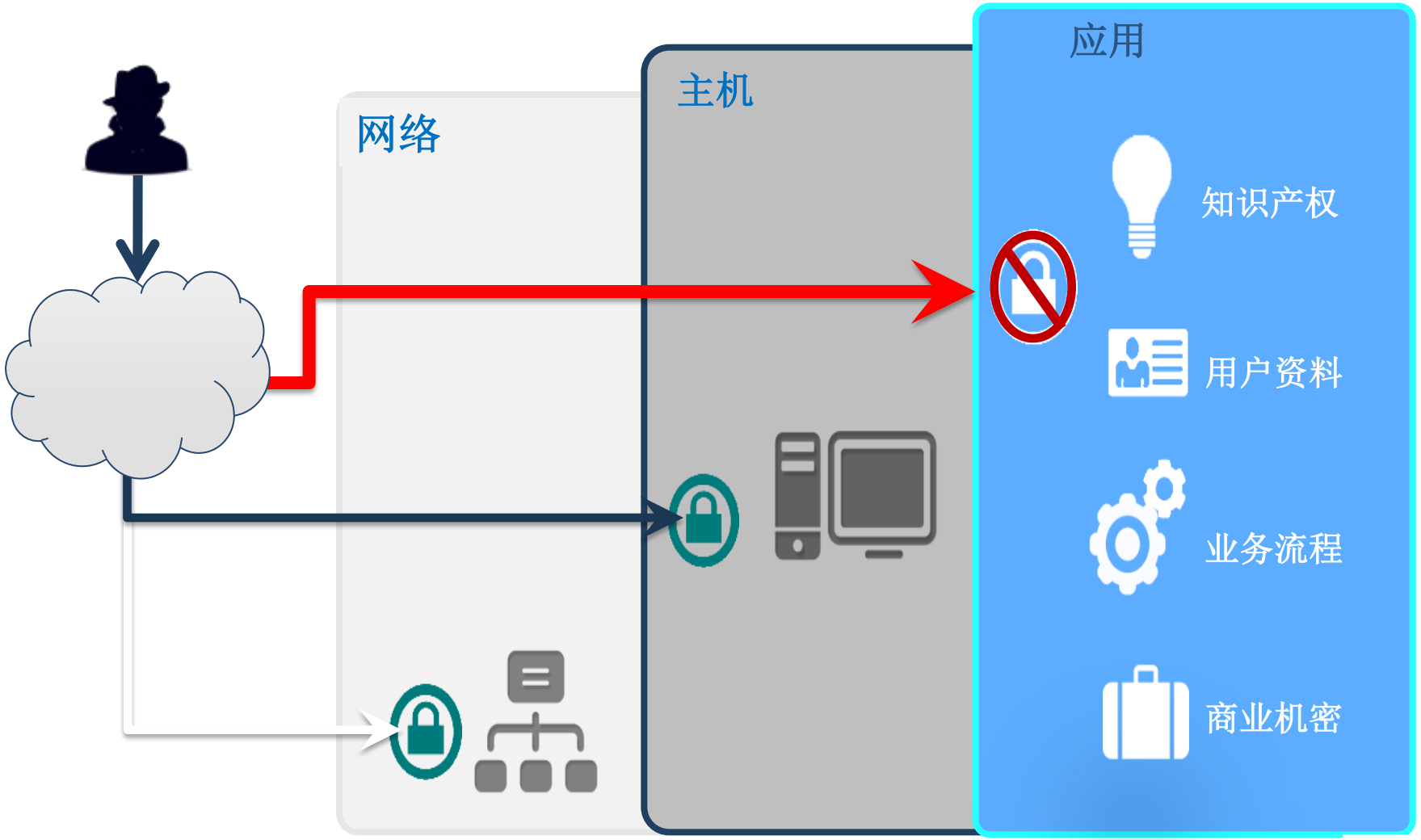
国内客户


REUTERS
广州农商银行
GUANGZHOU RURAL COMMERCIAL BANK
兴业银行
INDUSTRIAL BANK CO.,LTD.
浦发银行
SPD BANK
中国民生银行
CHINA MINSHENG BANKING CORP.,LTD.
中国人民银行
THE PEOPLE'S BANK OF CHINA
中国建设银行
China Construction Bank
上海银行
Bank of Shanghai
厦门银行
Xiamen Bank
中国银联
China UnionPay
北京银行
BANK OF BEIJING
中信银行
CHINA CITIC BANK
中国平安
PING AN OF CHINA
专业·价值
中国邮政储蓄银行
POSTAL SAVINGS BANK OF CHINA
中华英才网
ChinaHR.com
中国人寿
CHINA LIFE
中国太平
CHINA TAIPING
中国电信
CHINA TELECOM
海南航空
Hainan Airlines
CSTC 中国评测
中国移动
CHINA MOBILE
Amway 安利
SIPIS
China Customs
CEPREI
HUAWEI
ZTE中兴
NCI
CNAS
COSCO Network
COSCONET (Beijing)

黑客攻击的演化方式


网络 & 主机
软件应用
2012
2004
2000
1997
1994
对网络协议
(DNS/TCP-IP)
攻击
SQL注入、跨站脚本
暴力破解
EMAIL炸弹

新的软件架构——软件的应用因为业务和功能的需要必打破传统的保护层,直接与外面的系统交互



OWASP 2010 TOP 10 漏洞

- **A1.** 注入漏洞 **Injection Flaw**
- **A2.** 跨站脚本攻击 **Cross Site Scripting** 简称**XSS**
- **A3.** 错误的认证和会话管理 **Malicious File Execu Broken Authentication and Session Management tion**
- **A4.** 不安全的直接对象引用 **Insecure Direct Object Reference**
- **A5.** 跨网站请求伪造 **Cross-Site Request Forgery** 简称**CSRF**
- **A6.** 安全性误配置 **Security Misconfiguration**
- **A7.**不安全的加密存储 **Insecure Cryptographic Storage**
- **A8.** 限制远程访问失败**Failure to Restrict URL Access**
- **A9.** 不足的传输层保护 **Insufficient Transport Layer Protection**
- **A10.** 未验证的重定向和传递**Unvalidated Redirects and Forwards**

Fortify 软件安全漏洞研究

FORTIFY

http://www.hpenterprisesecurity.com/vulncat/zh_CN/vulncat/index.html

Expand All | Close All

- A Taxonomy of Coding Errors that Affect Security
- ColdFusion
- C/C++
- C#/VB.NET/ASP.NET
- HTML
- Java/JSP
  - API Abuse
  - Code Quality
  - Encapsulation
  - Environment
  - Errors
  - Input Validation and Representation
  - Security Features
  - Time and State
    - Code Correctness: Double-Checked Locking
    - J2EE Bad Practices: Non-Serializable Object Stor
    - J2EE Bad Practices: System.exit
    - J2EE Bad Practices: Threads
    - Race Condition: Singleton Member Field
    - Race Condition: Static Database Connection(dbc
    - Session Fixation
- Javascript
- PHP
- PLSQL/TSQL
- VisualBasic/VBScript/ASP
- XML

Cross-Site Scripting

ABSTRACT

向 Web 浏览器发送非法数据会导致浏览器执行恶意代码。

EXPLANATION

Cross-Site Scripting (XSS) 漏洞在以下情况下发生：

1. 数据通过一个不可信赖的资源进入 Web 应用程序，通常是一个网页请求或者数据库。

2. 在未检验包含数据的动态内容是否存在恶意代码的情况下，便将其传送给了 Web 用户。

传送到 Web 浏览器的恶意内容通常采用 JavaScript 代码片段的形式，但也可能会包含一些 HTML、Flash 或者其它任意一种可以被浏览器执行的代码。基于 XSS 的攻击手段花样百出，几乎是无穷无尽的，但通常它们都会包含传输给攻击者的私人数据（如 Cookie 或者其它会话信息）。在攻击者的控制下，指引受害者进入恶意的网络内容；或者利用易受攻击的站点，对用户的机器进行其它恶意操作。

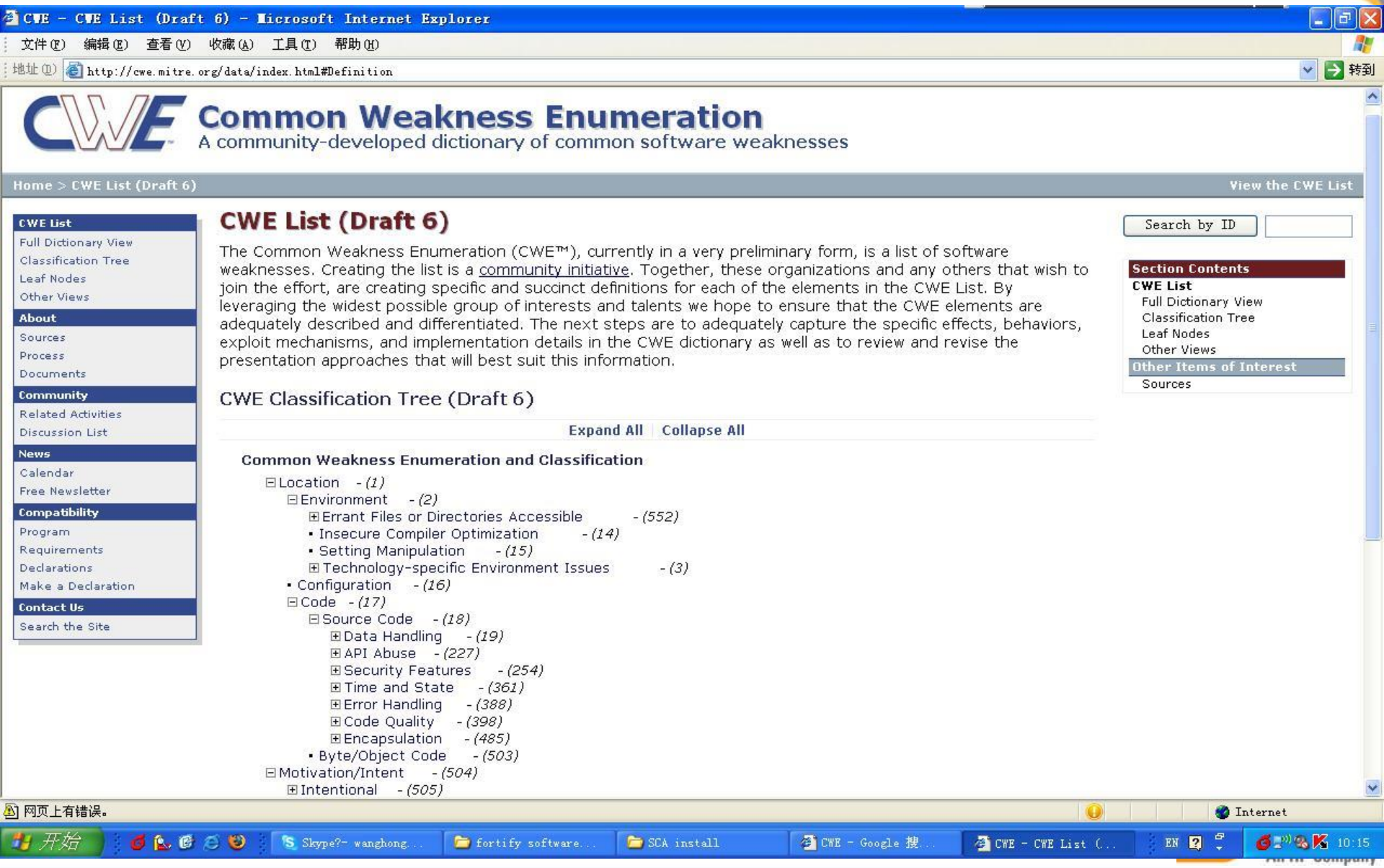
例 1： 下面的 JSP 代码片段可从 HTTP 请求中读取雇员的 ID，eid，并将其显示给用户。

```
<% String eid = request.getParameter("eid"); %>
...
Employee ID:<%= eid %>
```

如果 eid 只包含标准的字母或数字文本，这个例子中的代码就能正确运行。如果 eid 里有包含元字符或源代码中的值，那么 Web 浏览器就会像显示 HTTP 响应那样执行代码。

起初，这个例子似乎是不会轻易遭受攻击的。毕竟，有谁会输入导致恶意代码的 URL，并且还在自己的电脑上运行呢？真正的危险在于攻击者会创建恶意的 URL，然后采用电子邮件或者社会工程学的欺骗手段诱使受害者访问到此 URL 的链接。当受害者单击这个链接时，他们不知不觉地通过易受攻击的网络应用程序，将恶意内容带到了自己的电脑中。这种对易受攻击的 Web 应用程序进行盗取的机制通常被称为反射式 XSS。

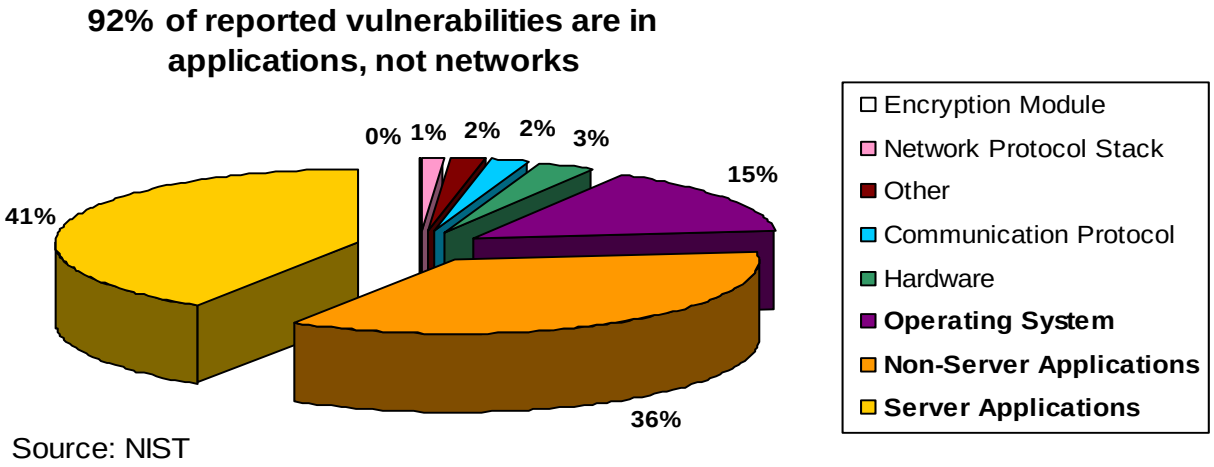
CWE：美国安全漏洞辞典采用Fortify漏洞分类



软件安全新的防御方式

- 软件安全问题的产生的根源：

  如今的黑客攻击主要利用软件本身的安全漏洞，这些漏洞是由不良的软件架构和不安全的编码产生的。

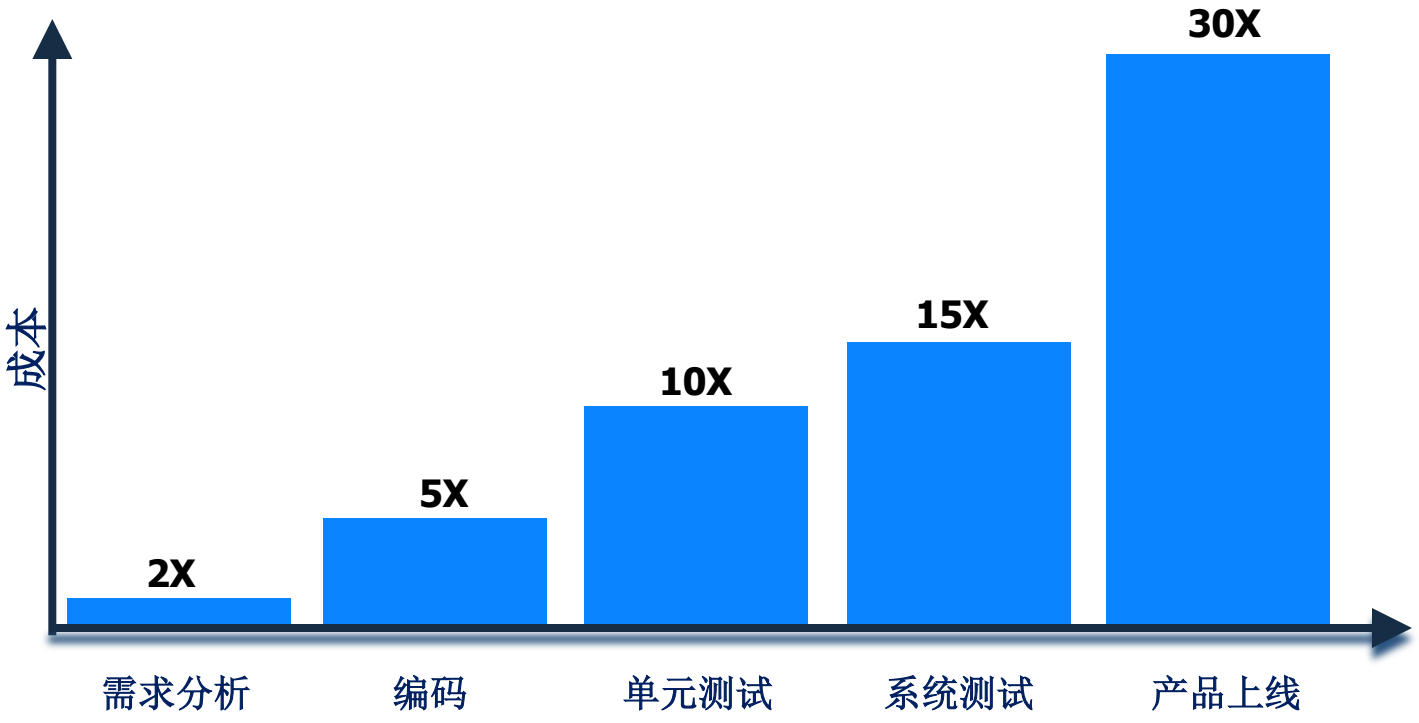


- 新的防御方案：

  Building Security In——构建安全的代码安全的软件

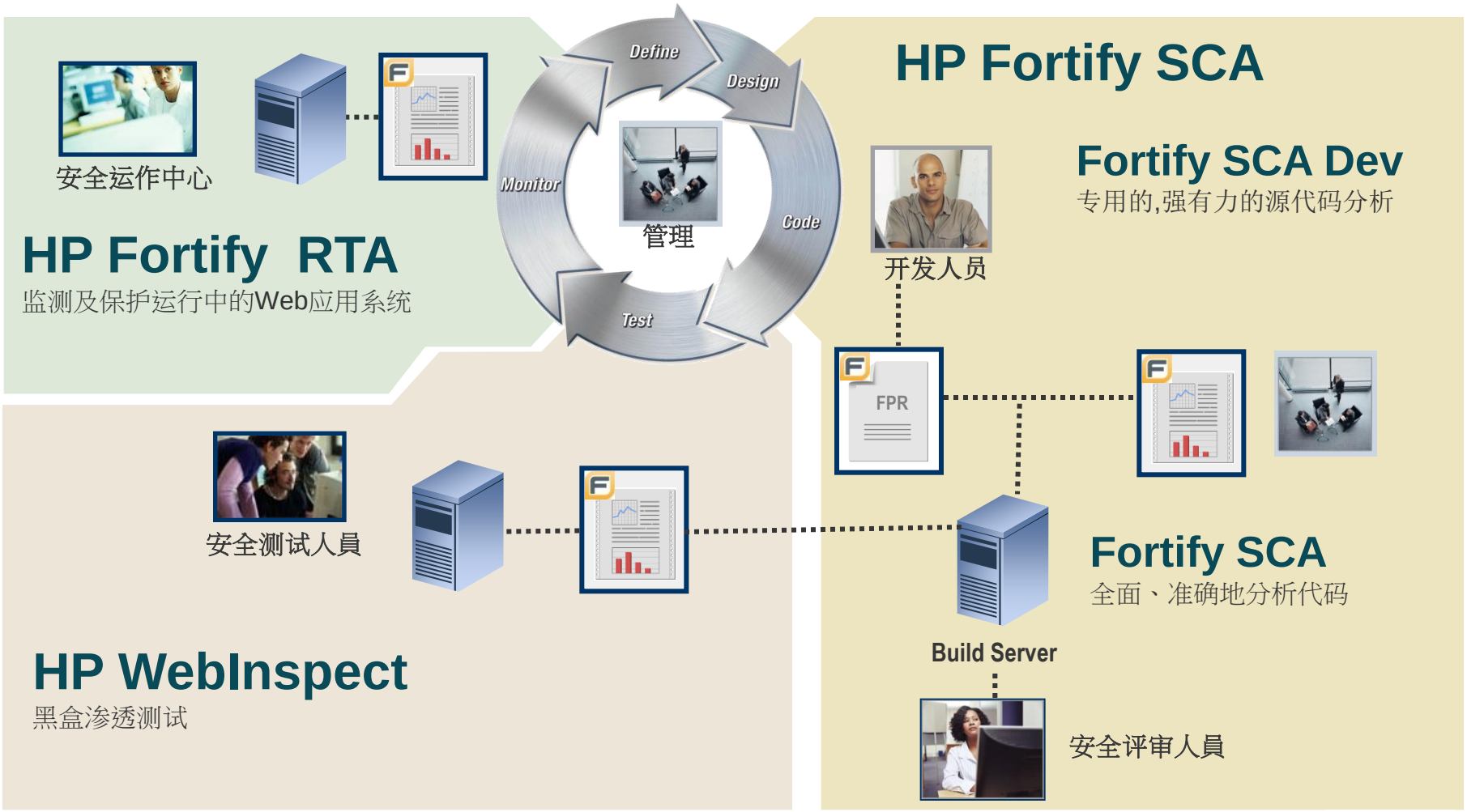
修复漏洞的成本

- 在产品上线阶段修复漏洞的成本多花费超过30倍

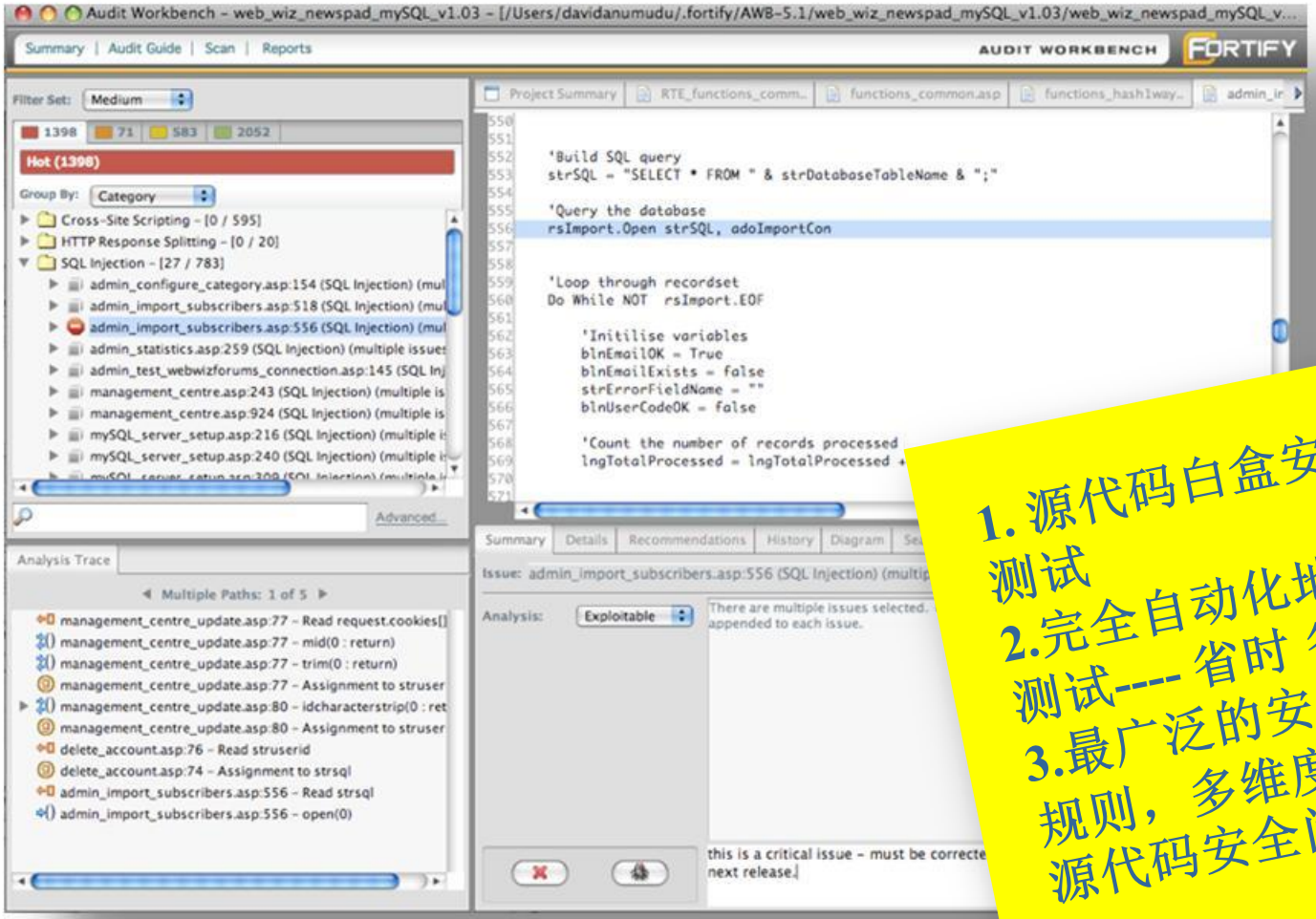


*来源：**NIST***

HP Fortify 的安全方案—HP Software Security Center



HP Fortify SCA –静态应用安全测试工具



1. 源代码白盒安全测试
2.完全自动化地完成测试---- 省时 省力
3.最广泛的安全漏洞规则，多维度分析源代码安全问题

Fortify SCA 产品组件及功能

- Source Code Analysis Engine（源代码分析引擎）
  - **数据流分析引擎**-----跟踪,记录并分析程序中的数据传递过程的安全问题
  - **语义分析引擎**-----分析程序中不安全的函数,方法的使用的安全问题
  - **结构分析引擎**-----分析程序上下文环境,结构中的安全问题
  - **控制流分析引擎**-----分析程序特定时间,状态下执行操作指令的安全问题
  - **配置分析引擎** -----分析项目配置文件中的敏感信息和配置缺失的安全问题
  - **特有的X-Tier™跟踪器**-----跨跃项目的上下层次,贯穿程序来综合分析问题
- Secure Coding Rulepacks ™（安全编码规则包）
- Audit Workbench（审查工作台）
- Custom Rule Editor & Custom Rule Wizard(规则自定义编辑器和向导)
- Developer Desktop (IDE 插件）

Fortify SCA的关键特点：

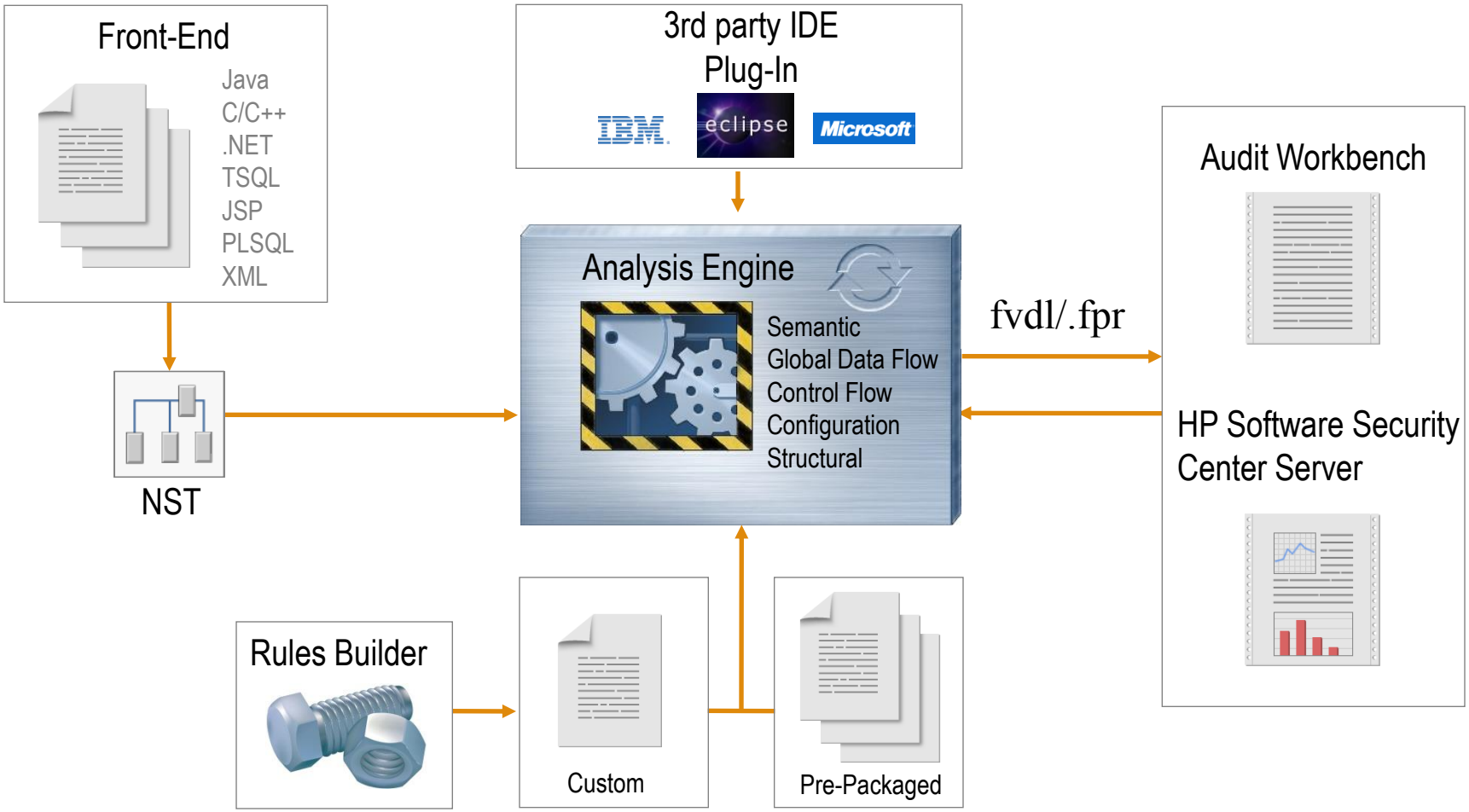
- 最庞大的安全编码规则包
- 跨层、跨语言地分析代码的漏洞的产生

  ABAP、ASP.NET、C,C++、C#、Classic ASP、COBOL、Cold Fusion、Flex/ActionScript、Java、JavaScript/AJAX、JSP、Objective C、PL/SQL、PHP、Python、T-SQL、VB.NET、VBScript、VB6、XML/HTML等语言
- 精确地定位漏洞的产生的全路径
- 支持不同的软件开发平台

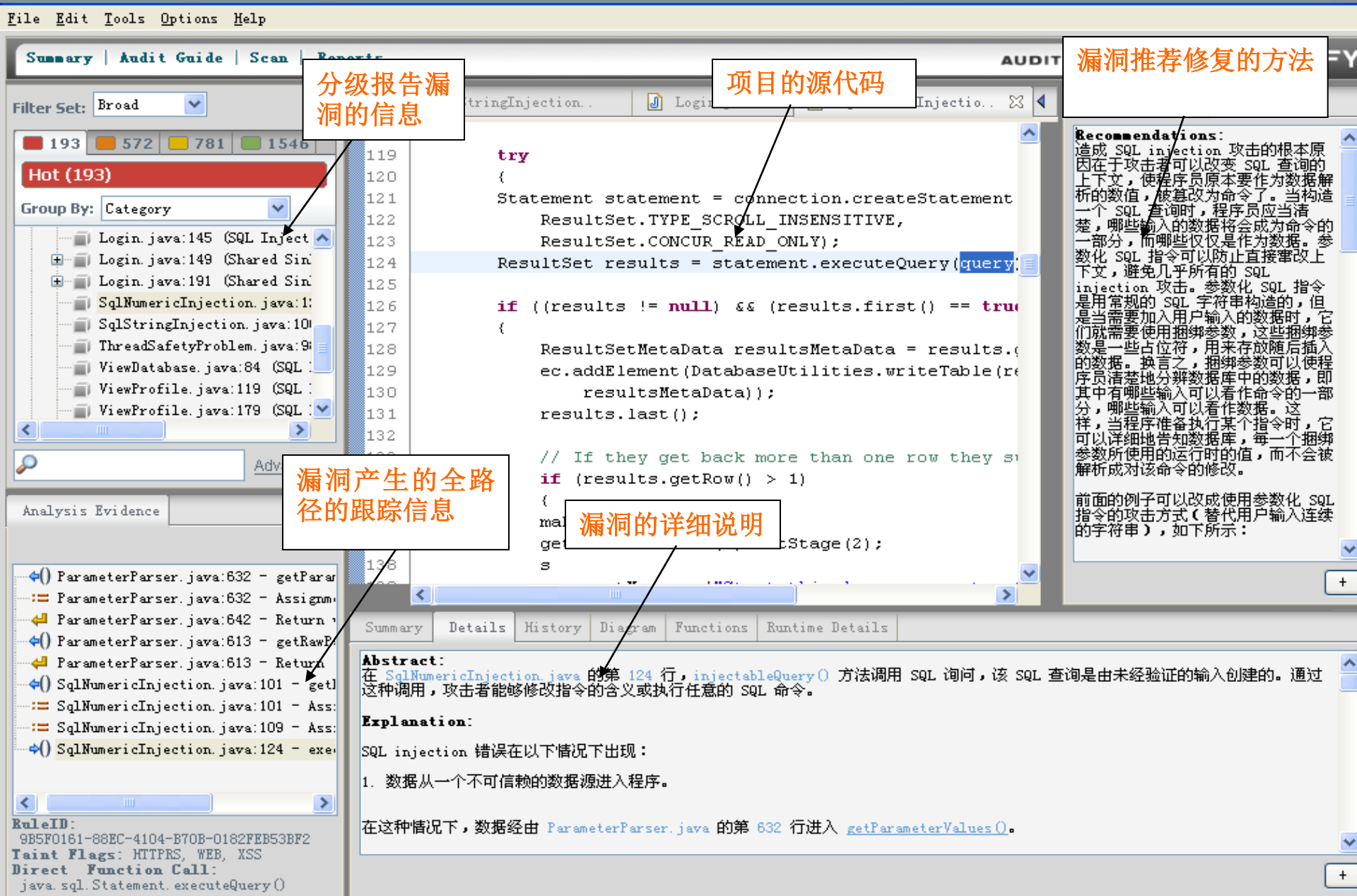
  Platform: Windows, Solaris, Red Hat Linux, Mac OS X, HP-UX, IBM AIX

  IDEs : Visual Studio, Eclipse, JDeveloper , JBuilder , RAD, RSA

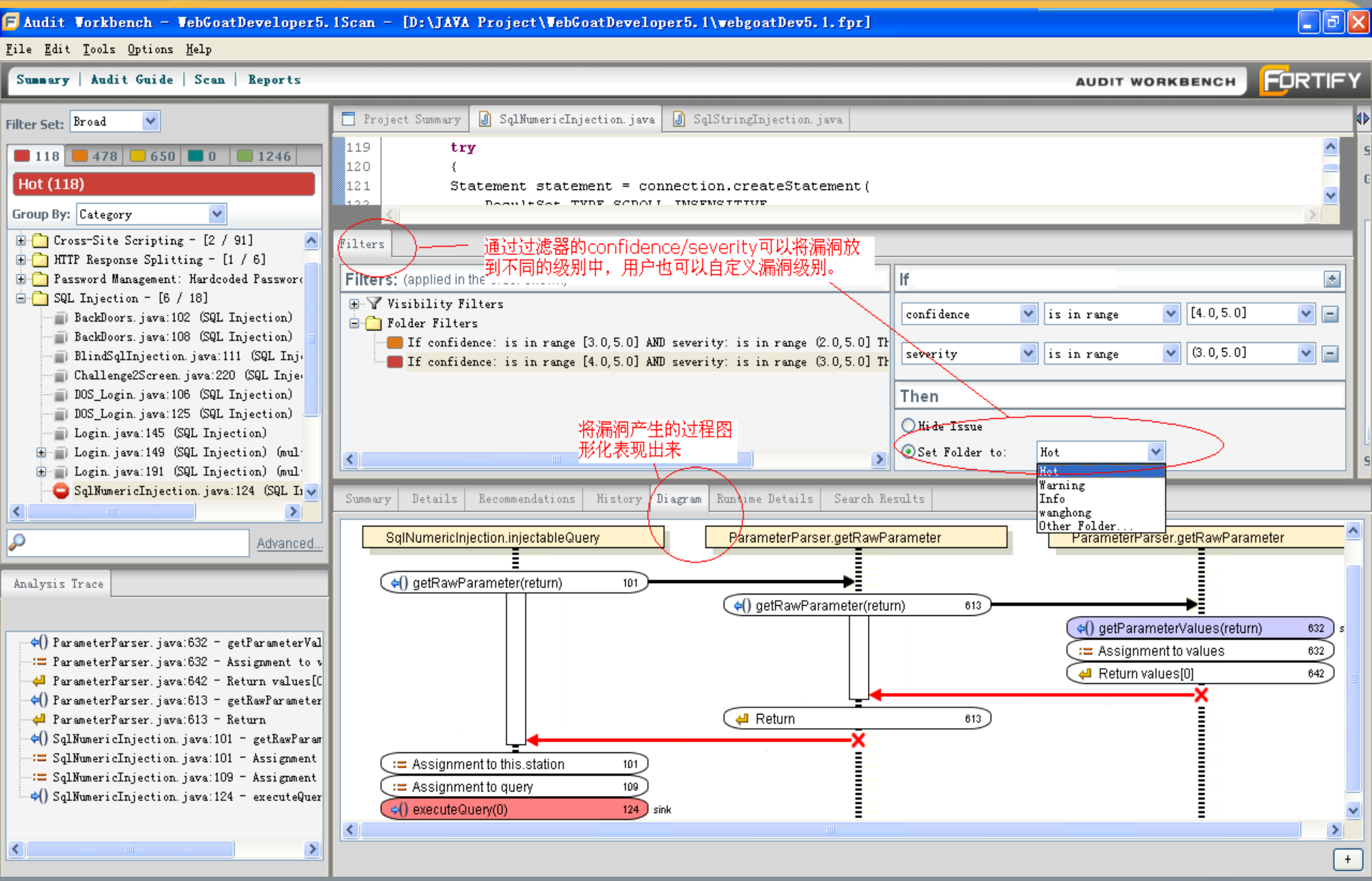
Fortify SCA 工作原理



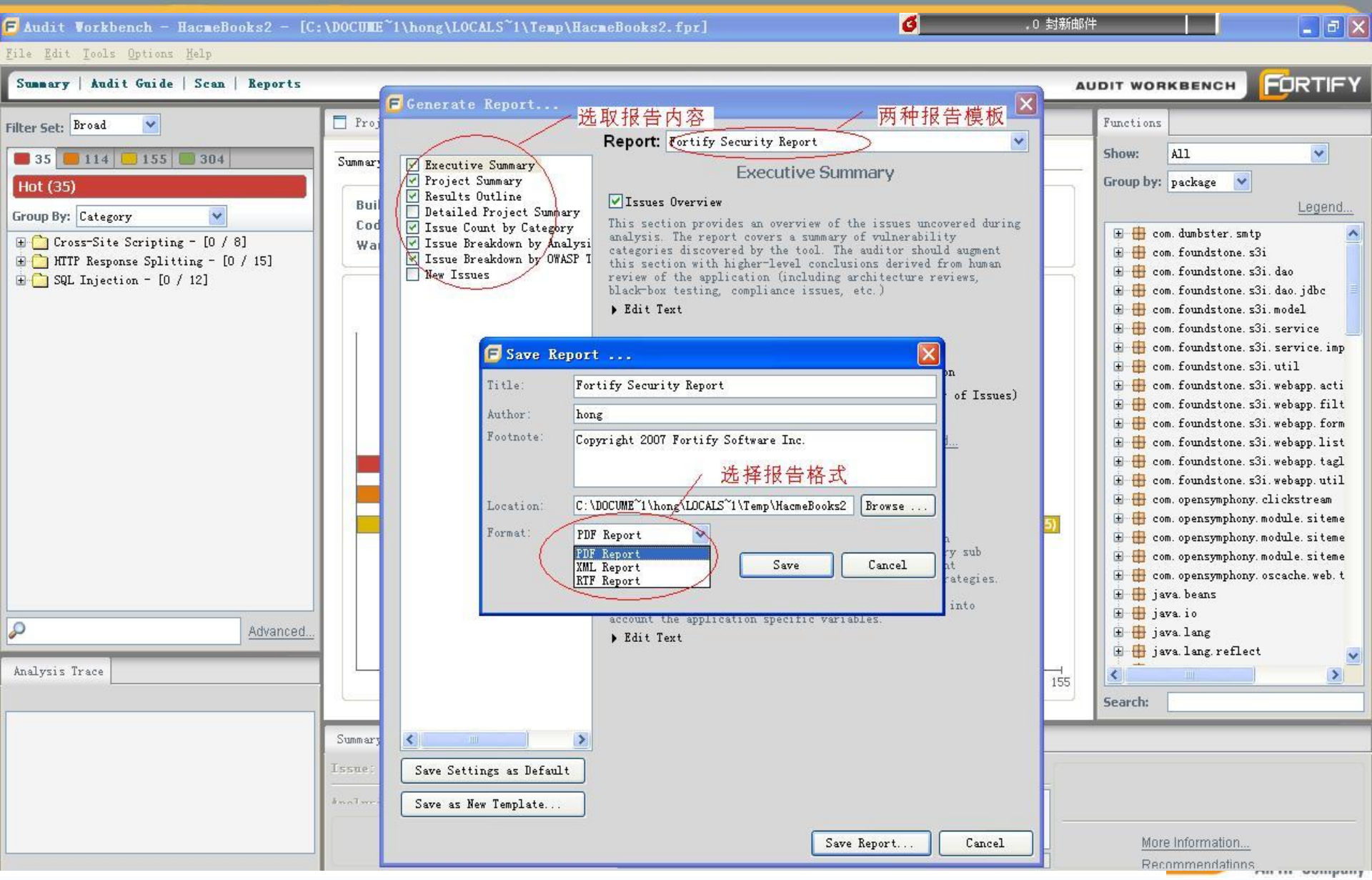
Fortify 漏洞审计---Audit Workbench



Audit Workbench---Audit



Audit Workbench---Report



HP Fortify SCA Remediation Process

Developer
Code & Remediate in IDE

Check In / Out

Source Code Control

Latest Code

Build Engineer / Monitor
Maintain build & SCA

Automated Build and HP Fortify SCA

Upload FPR

HP SW Security Centre

Reports

Triage, Audit & Assign Issues

Audit Workbench

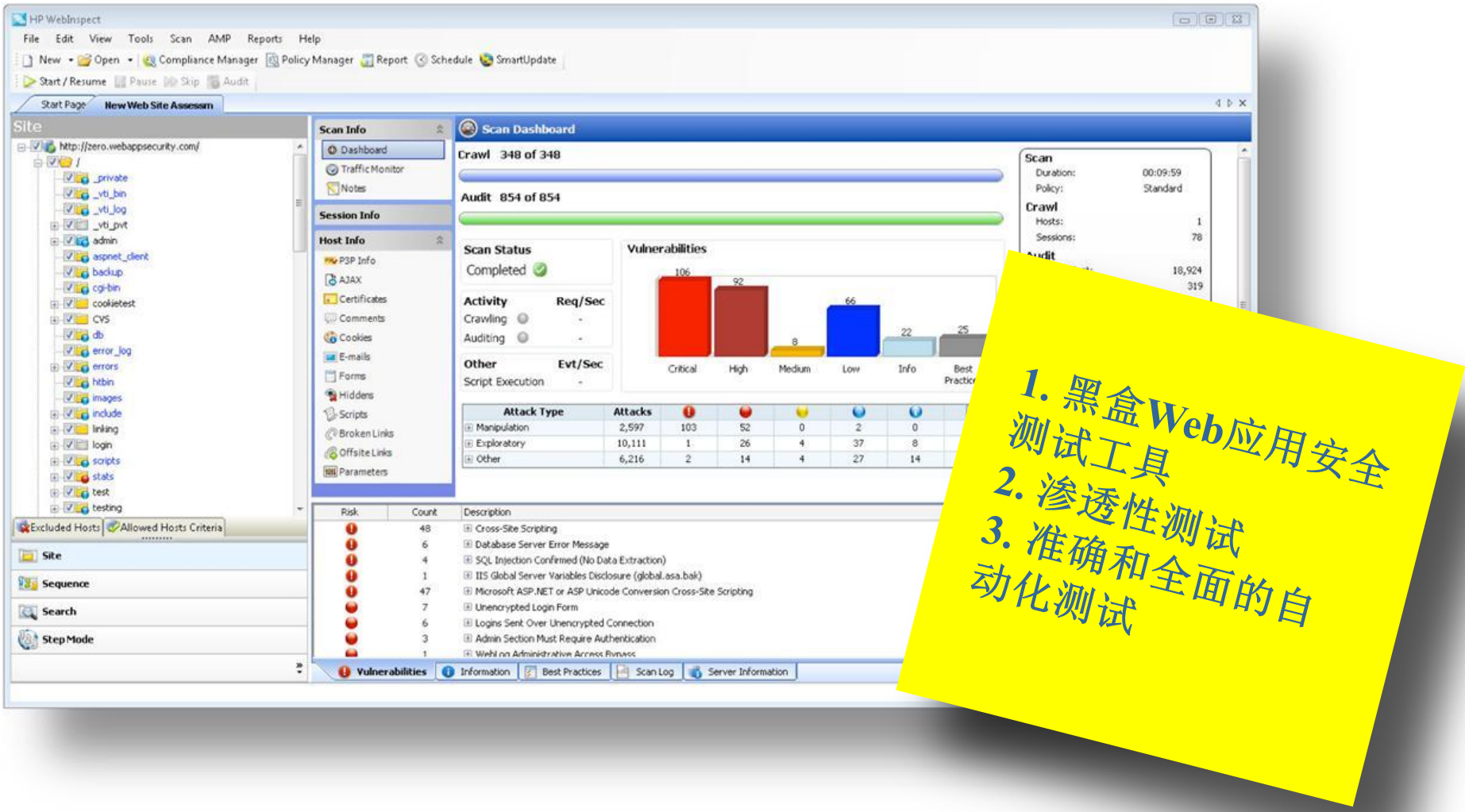
Open Collaborative Audit or Bug Tracker to resolve Assigned Issues

Security Specialist & Development Lead
Audit and Review Analysis Results

Project Manager
Monitor & Evaluate SSA Progress

Compliance Officer
Report & Audit Security Objectives

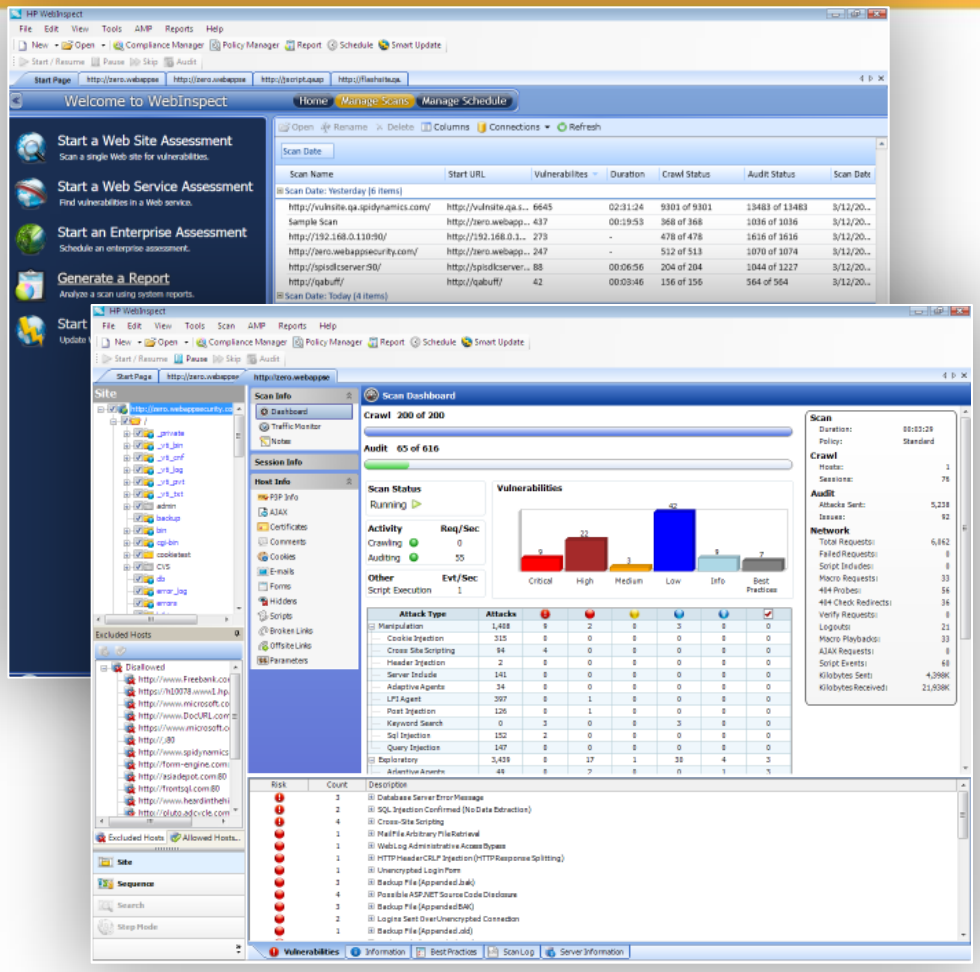
HP WebInspect –动态应用安全测试工具



1. 黑盒Web应用安全测试工具
2. 渗透性测试
3. 准确和全面的自动化测试

HP Web Inspect

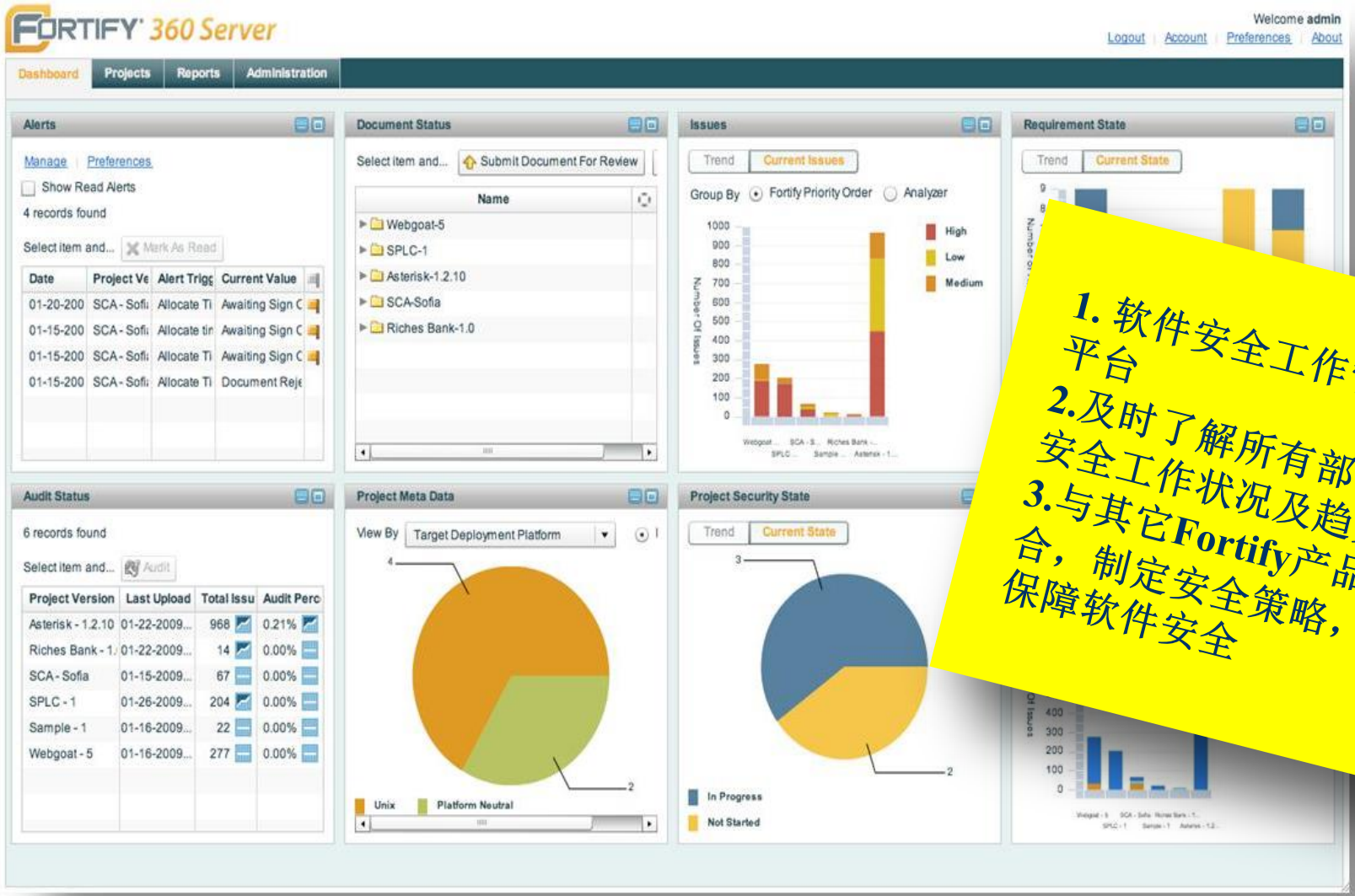
- 业界领先的自动化应用安全测试解决方案
- 对Web、WebServices应用进行安全检测
- 抓取（crawl）与审计（audit）
- 自动更新安全规则
- 自动产生缺陷报告和详细修复建议



HP Web Inspect

- 对**Web**应用技术的广泛支持
  - AJAX、JavaScript、Flash、Silverlight、Web Services等
- 创建宏以记录检测步骤，实现重复性检测的自动化
- 同步扫描与审计和智能引擎
- 同时启动和管理多个扫描进程，从而增加检测量
- 自带多种渗透检测工具，从而对所发现的应用安全漏洞进行再验证
- **WebInspect smart update**安全策略的支持力度与更新频率很高。
- 快速分析应用与**web** 服务
- **WebInspect**较其他产品，具备更全面的安全高级工具集成以及更深度的安全评估报告。以各种标准格式（**HTML**、**PDF**、**RTF**、**XML**、**TXT**以及**XLS**等格式）导出结果报告

HP Software Security Center Server



1. 软件安全工作管理平台
2. 及时了解所有部门的安全工作状况及趋势
3. 与其它**Fortify**产品结合，制定安全策略，保障软件安全

HP Software Security Center Server:软件安全管理平台

- **软件安全管理器是软件安全分析、管理的综合平台。**

  帮助软件开发的管理人员统计和分析软件安全的风险、趋势，跟踪和定位软件安全漏洞，提供足够多的软件安全质量方面的真实的状态信息以便于管理人员制定安全管理决策及编码规则。

- **其主要特点：**

  1.集中管理

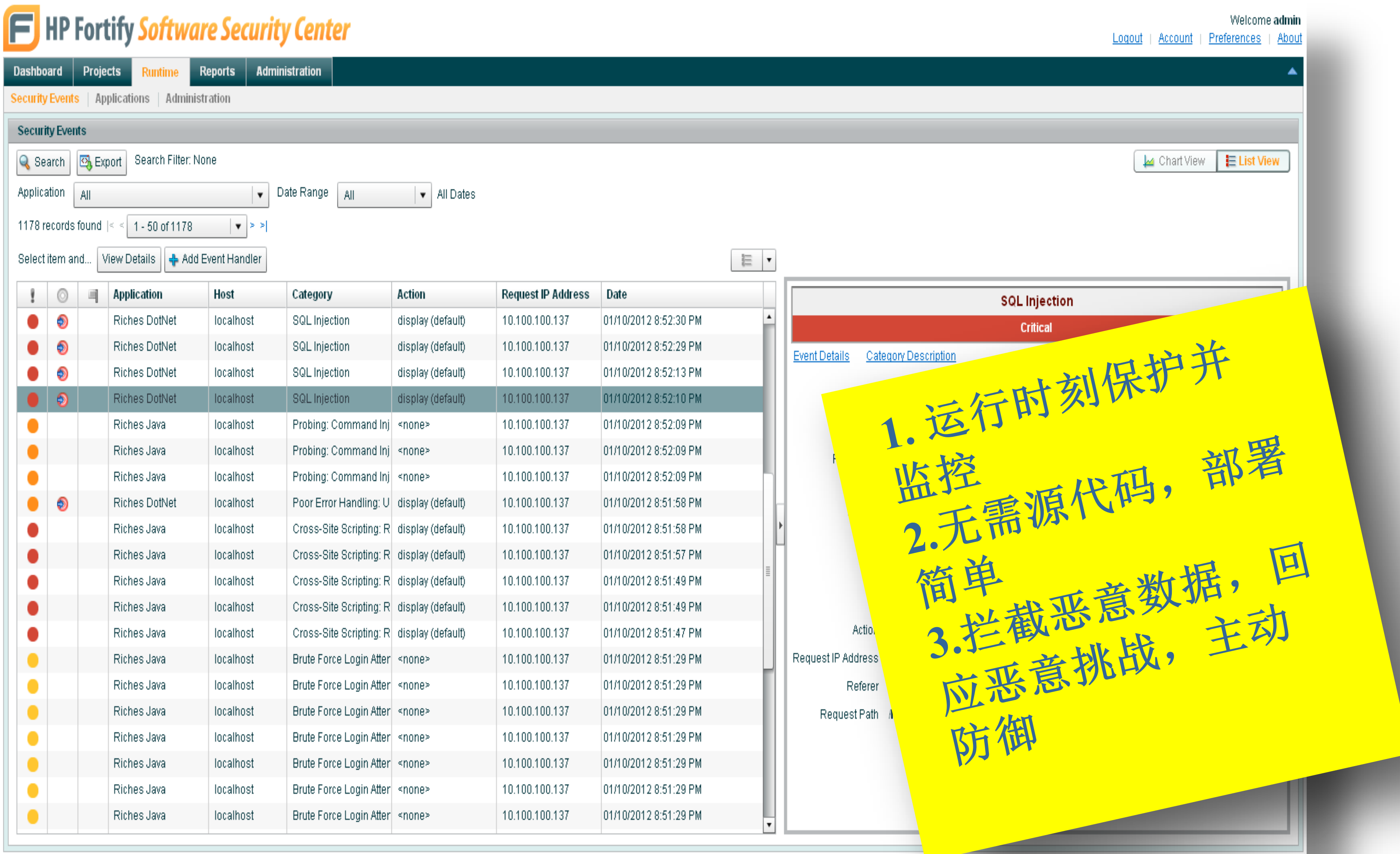
  2.化分优先级

  3.标记趋势

  4. 协同工作平台

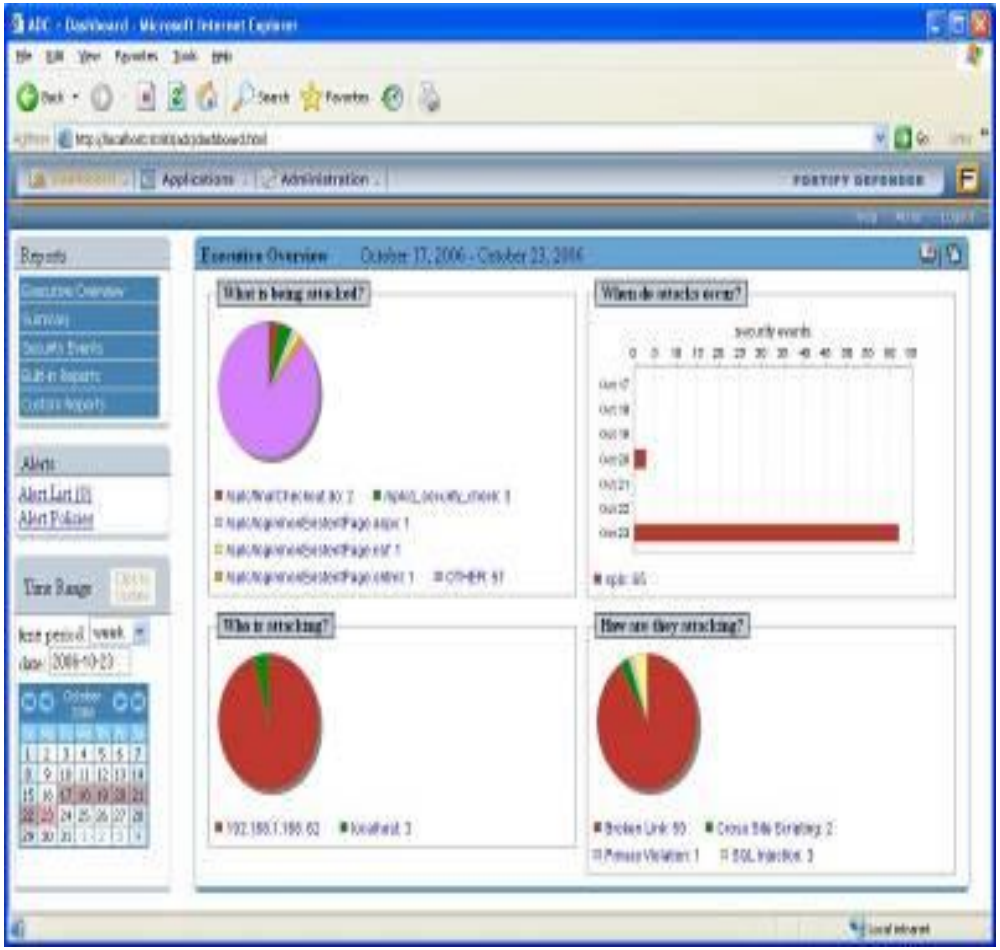
  5.产生多种报表

Fortify RTA – Application Deployment Protection



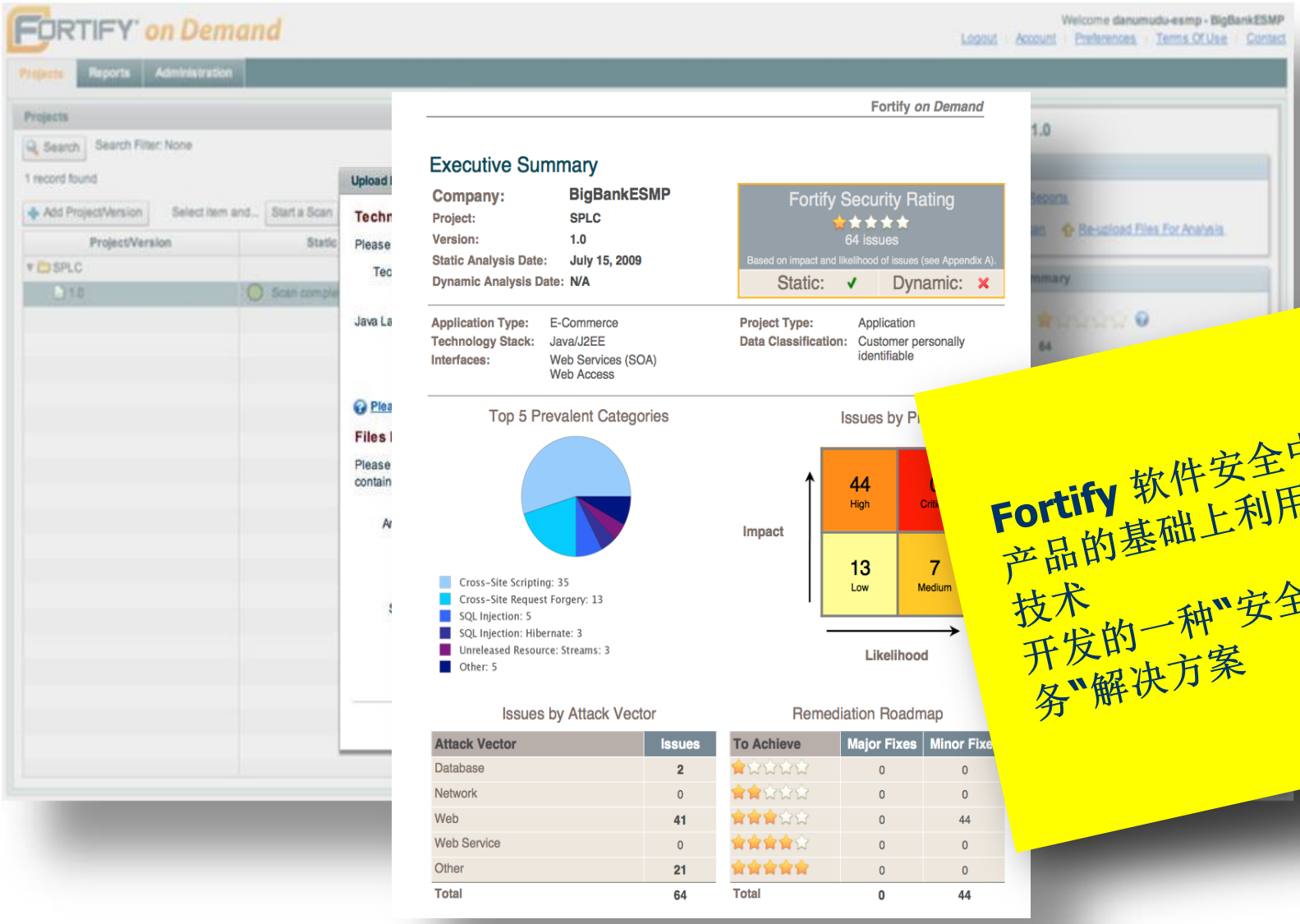
Fortify RTA – 保护运行时的 Web系统

- 在不可以修改源代码的情况下，实为最理想的解决办法
- 直接安装在应用系统二进制码上 —— 完全不需要源代码
- 快、易于安装及部署
- 为大部份已知的漏洞提供防御



FORTIFY
An HP Company

Fortify OnDemand – Security Testing Service



Fortify 软件安全中心产品的基础上利用云技术
开发的一种"安全即服务"解决方案

RTIFY
An HP Company

Thanks!