爱开发 重创新 更智慧

Innovate2011

IBM Rational 软件创新论坛

Software. Everyware.

IBM

IBM Rational
客户交流会

Software. Everyware.

Innovate2011

Appscan 助力构建安全智能电网

王甜
广东电网信息中心

Innovate2011

内容

- 广东电网信息化评测实验室介绍
- 实验室安全评测业务介绍--AppScan应用成效

广东电网信息化实验室介绍

- 实验室成立背景
- 实验室规模
- 评测成效

背景

- 贯彻落实GD248体系，建设质量保障体系、安全防护体系。
- 软件系统建设速度快，质量管控力度不够，需要有专业的测评技术团队，保障软件全生命周期的质量。
- 南方电网公司十二五规划中对信息化评测实验室进行了详细描述,下一步还将扩大建设规模。

总体介绍

- 评测实验室成立于2009年，受到上级主管部门的高度重视。
- 定位：

  信息化评价中心、

  检测中心。

人才队伍

专业资格认证

国际ISTQB测评

国内CISP信息安

研究生和本科为主、一专多能、阶梯式的团队，测试人员23人.

2010/12 2011/12 2012

评测专区

- 测试专区三个，专用机房一个，总面积约350m2

系统测试区

硬件设备评测区

安全攻防区

软硬件设施

- 专用测试工具约**10台套**，其中自主研发工具一套；覆盖信息安全测试、性能测试、实用化评价等领域，如AppScan等

基础类测试工具约**40台套**，包括pc server，小型机、网络设备等；完整模拟出信息系统的生产环境。

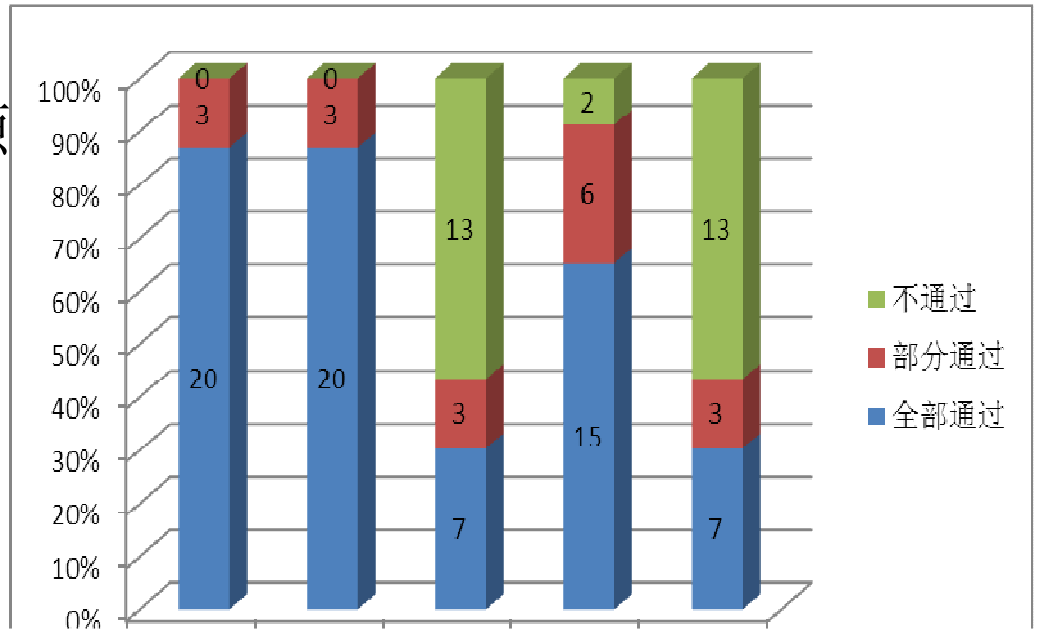
评测业务、成果

- 系统测评
  - 开展80余个系统检测
  - 积累了一套测评指标库
  - 覆盖核心业务系统：如营配一体化系统等。
  - 范围覆盖南方电网下属分子公司：如物资一体化系统
  - 常态化

评测业务、成果

- 选型测试
  - 集采项目选型测试，坚持公平、公正、诚信的原则。
  - 建立选型测试指标库，开展典型系统选型测试。
  - 典型案例：

南方电网数据资源管理平台选型测试。



评测业务、成果

- 等级保护测评
  - 自2008年以来，持续开展，常态化。
- 风险评估
  - 连续三年开展风险评估。
- 入网安评
  - 将生产设备入网检测的概念引入信息安全；
  - 信息系统上线前实施入网安评。
  - 常态化

质量管理体系


质量手册
程序文件
作业指导书
（测试规程，操作指南）
记录表格
纲领性文件
支持性文件
操作性文件
见证性文件
根据规定的质量方针、质量目标，描述与之相适应管理体系的基本文件，提出了对过程和活动的管理要求
描述质量管理体系所涉及到的各个部门的职能活动，为其提供了方法和指导，并分配具体的职责和权限，包括管理、执行、验证活动
检测活动的技术作业指导文件，由具体操作执行人员使用
贯穿于产品质量形成的全过程，完整地反映管理体系的运行状况和产品质量状况

学术论文

自2009年以来,发表13篇信息化领域论文	
论文题目	作者
《广东电网公司应用软件生命周期管理方案探讨》	魏理豪、徐晖、王甜
《广东电网公司物资管理信息系统实用化评价体系研究》	陈飞、朱奕
《县级供电局安全生产MIS实用化评价研究》	李小惠
《基于ISO27001的电力信息安全风险评估模型》	王甜、徐晖、魏理豪、崔磊

获奖及专利

- 荣获省部级奖两项,公司级奖项4项.
- 软件著作权一项.
- 正在申请的发明专利4项.

中华人民共和国国家版权局

计算机软件著作权登记证书

软件名称：广东电网公司信息系统实用化评价研究系统[简称：广东电网信息系统实用化评价系统] V1.0

著作权人：广东电网公司信息中心

开发完成日期：2011年02月28日

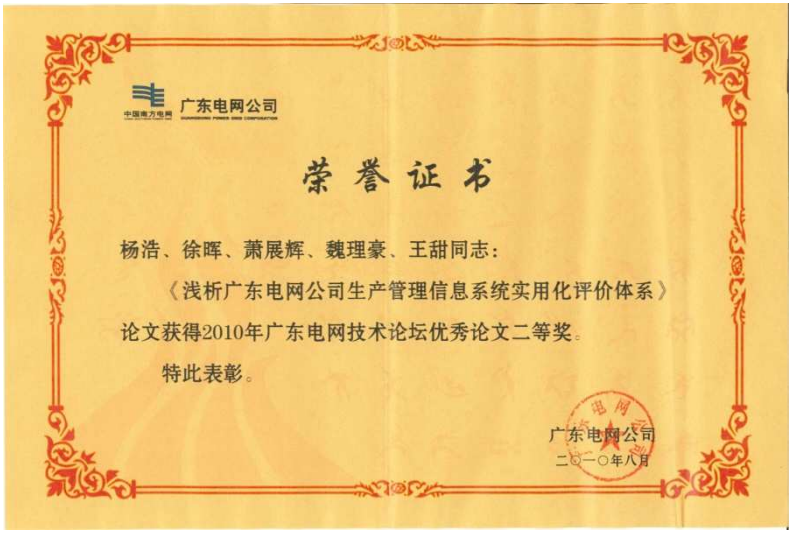
首次发表日期：2011年02月28日

权利取得方式：原始取得

权利范围：全部权利

登记号：2011SR012496

根据《计算机软件保护条例》和《计算机软件著作权登记办法》的规定，经中国版权保护中心审核，对以上事项予以登记。



广东电网公司

荣誉证书

杨浩、徐晖、萧展辉、魏理豪、王甜同志：

《浅析广东电网公司生产管理信息系统实用化评价体系》论文获得2010年广东电网技术论坛优秀论文二等奖。

特此表彰。

广东电网公司

二〇一〇年八月

实验室安全评测业务介绍

--AppScan应用成效

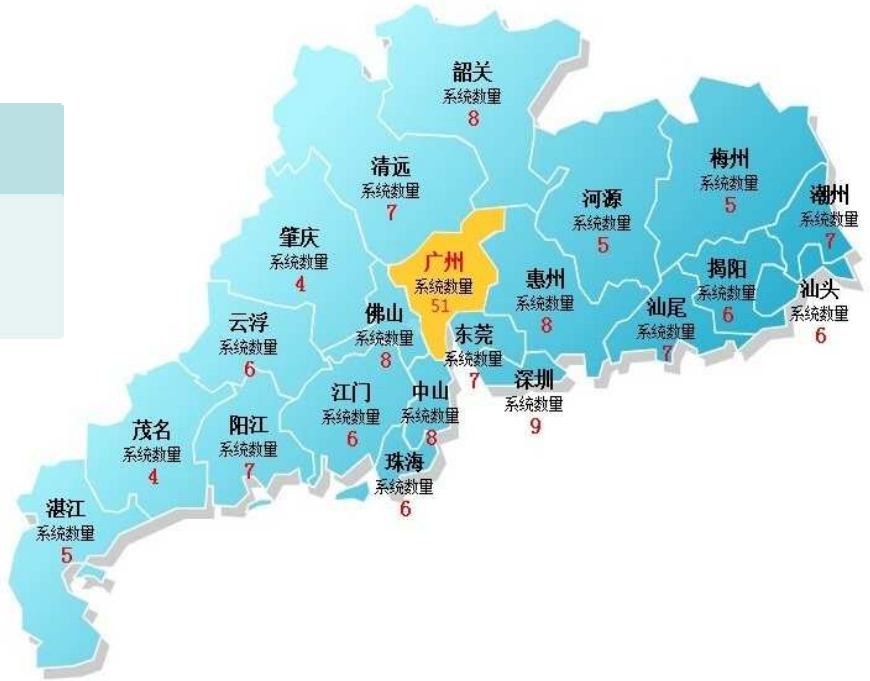
入网安评

在电网企业的信息化安全评测领域，首次引入了“入网安评”概念，建立一套“入网安全准入机制”。

等级保护、风险评估

连续3年开展公司信息安全等级保护测评工作，测评工作覆盖南方电网公司本部、广东电网公司及其下属共计 39家单位。

系统数目	二级	三级
• 303个	• 299个	• 4个



网络安全工作

信息安全等级保护工作专刊(11)

广东省公安厅网络警察总队　　2011 年 1 月 19 日

广东电网公司管理信息系统等级测评工作顺利通过专家验收

2010 年 10 月 15 日，广东电网公司组织召开了 2010 年广东电网公司管理信息系统等级测评工作验收会。广东省公安厅网络警察总队郭宏伟副总队长，南方电网公司信息部陈曦副处长及有关专家共 20 人出席了会议。会议成立了临时验收专家组，由 9 位专家组成，郭宏伟同志任组长。

会上，广东电网公司信息中心总结了公司及下属单位开展信息安全等级保护工作情况，介绍了测评工作报告和技术总体报告。郭宏伟同志对广东电网公司积极等级保护工作表示肯定。他指出，广东电网公司是广东省第一家通过第三方测评验收的单位，为全省各行各业做了很好的探索，为以后其他行业、单位开展等级保

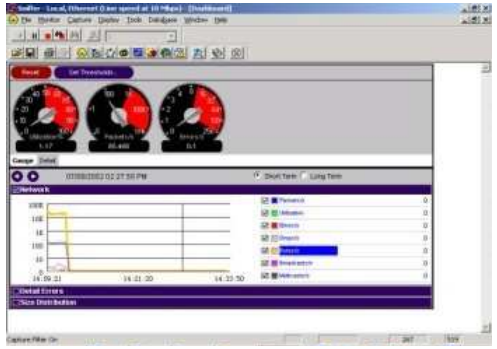
— 1 —

测评工作实践了差距评估、整改、验收测评等信息安全管理的三个环节，初步实现了信息安全PDCA循环机制，得到上级主管部门的高度认可。

等级保护、风险评估测试工具

Rational Appscan Enterprise Edition

网络嗅探工具



主机扫描工具

数据库扫描工具

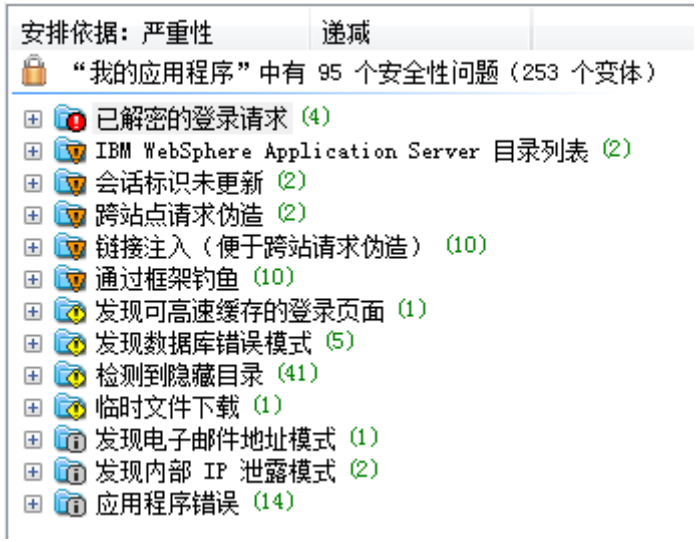
AppScan发现的问题

通过AppScan应用扫描工具发现的典型高风险问题

1、SQL注入漏洞

2、跨站点脚本编制漏洞

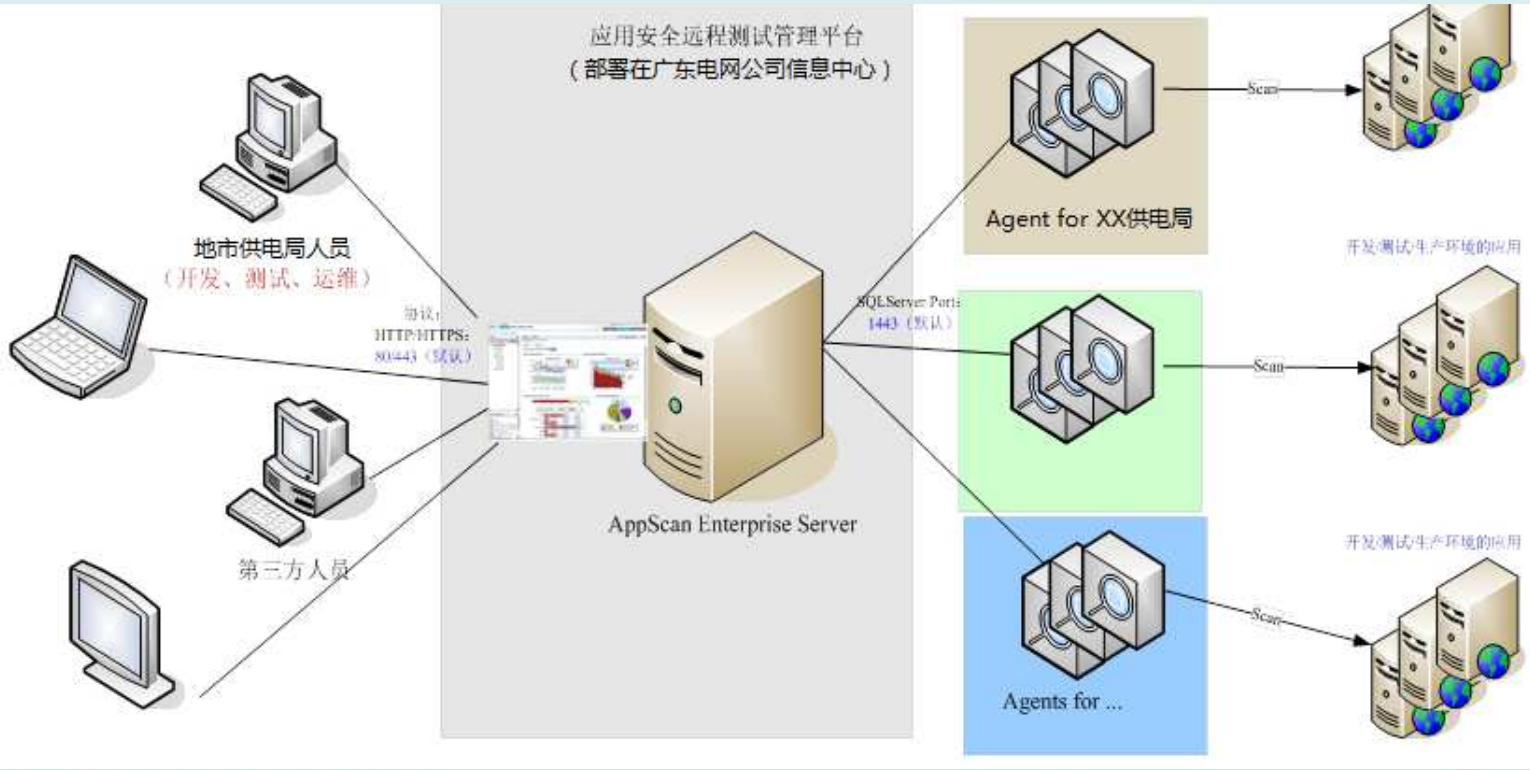
3、会话标识未更新



高风险修改率100%，中风险修改率超过95%

AppScan部署方式

采用分布式部署方式，在广东电网公司信息中心部署AppScan Enterprise和Source的服务器。给不同的地市供电局分配不同的Agent，并在指定的网段、服务器上进行web漏洞扫描，能够实现整个开发过程中web应用安全的“分布式测试、集中管理”。



AppScan 应用成效

- 通过给地市供电局部署Agent代理扫描程序，协助其制定扫描计划，对开发、测试和已上线的系统进行安全测试，形成报告，及时发现应用安全隐患。
- 方便测试人员全面了解Web应用系统的安全状况，提出有针对性的修复建议
- 提高了公司网络与信息系统的安全保障与运维能力

谢　谢

Thank you