一、安全性测试

定义：安全性测试是指有关验证应用程序的安全等级和识别潜在安全性缺陷的过程。应用程序级安全测试的主要目的是查找软件自身程序设计中存在的安全隐患，并检查应用程序对非法侵入的防范能力，根据安全指标不同测试策略也不同。

二、测试范围

正式环境：

1.发布前需要对发布包进行一次杀毒。

2.服务器需要安装杀毒软件并且定期更新和杀毒。

3.服务器和数据库等密码需要满足一定的复杂度。

功能类：

1.认证模块必须采用防暴力破解机制。例如：验证码或者多次连续尝试登录失败后锁定帐号或IP，账号冻结后，管理员可以手动解冻。

2.对于每一个需要授权访问的页面或servlet的请求都必须核实用户的会话标识是否合法、用户是否被授权执行这个操作，以防止URL越权。

3.登录过程中，往服务器端传递用户名和口令时，必须采用HTTPS安全协议（也就是带服务器端证书的SSL）。

4.用户产生的数据必须在服务端进行校验。

5.所有非查询的操作必须有日志记录。

6.密码需要满足一定的长度和复杂度，并且以高级的加密方法保存在数据库。

7.口令在传输的过程中以密文的形式传输。

8.输入密码时密码不能明文回显。输入密码不接受拷贝功能。

9.修改密码时需要验证旧密码。

10.日志中的密码不能以明文显示。

11.超时验证。

攻击类：

**SQL注入：**

通过把SQL命令插入到Web[表单](http://baike.baidu.com/view/296684.htm)递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令。

测试方法：

a验证绕过漏洞就是'or'='or'[后台](http://baike.baidu.com/view/179243.htm)绕过漏洞，利用的就是AND和OR的运算规则，从而造成后台[脚本](http://baike.baidu.com/view/54.htm" \t "_blank)逻辑性错误。

例如[管理员](http://baike.baidu.com/view/315045.htm" \t "_blank)的账号密码都是admin，那么再比如[后台](http://baike.baidu.com/view/179243.htm" \t "_blank)的数据库查询语句是

user=request("user")

passwd=request("passwd")

sql='select admin from adminbate where user='&'''&user&'''&' and passwd='&'''&passwd&'''

那么我使用'or 'a'='a来做用户名密码的话，那么查询就变成了

select admin from adminbate where user=''or 'a'='a' and passwd=''or 'a'='a'

根据运算规则，这里一共有4个查询语句，那么查询结果就是：假or真and假or真，先算and 再算or，最终结果为真，这样就可以进到[后台](http://baike.baidu.com/view/179243.htm" \t "_blank)了

b猜数据库的表名、列名

猜表名

And (Select count(\*) from 表名)<>0

猜列名

And (Select count（列名） from 表名）<>0

或者也可以这样

and exists (select \* from 表名）

and exists (select 列名 from 表名）

**Xss攻击**

跨站[脚本](http://baike.baidu.com/view/54.htm" \t "_blank)攻击(Cross Site Scripting简称XSS)

测试方法：

1、在文本输入地方输入Script代码，如：<script>alert("XSS")</script>。测试是否进行转义

2、在图片上传的地方上传gif格式的图片，图片使用记事本编辑插入一下内容：GIF89a<script>alert("XSS")</script>。测试是否会校验

根据目前现有的资料认为以上的情况有遭受XSS攻击的风险。

**DOS攻击**

DoS是Denial of Service的简称，即拒绝服务

1、死亡之ping，使用大量裸机一直去ping服务器。

测试方法：在运行中输入ping命令，如：ping 目标地址 -l 55000 -t

2、DDos攻击

分布式拒绝[服务](http://baike.baidu.com/view/133203.htm)(DDoS:Distributed Denial of Service)攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DoS攻击，从而成倍地提高拒绝服务攻击的威力。没有第三次握手。

根据目前掌握的资料认为，DDos攻击是利用了TCP/IP协议的漏洞，除非不用TCP/IP，才有可能完全抵御住DDoS攻击。同时测试模拟DDos攻击也存在着风险，所以对于该类型的攻击，建议以防御为主。网上看到的一些防御方法如下：

a、关闭不必要的服务

b、限制同时打开的Syn半连接数目

c、缩短Syn半连接的time out 时间

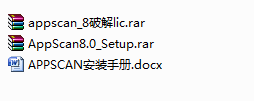
d、及时更新系统补丁

测试工具

网络上的安全性测试工具较多，但是模拟攻击的同时也有着风险，所以选择和使用工具的时候需要格外的小心。主流的安全性测试工具有：Cal9000、WebScarab、appscan等。

下面简单讲一下appscan工具的使用：

安装文件



根据安装手册中说明进行解压安装和破解。

Appscan的测试流程

1.在计划阶段：明确目的，进行策略性的选择和任务分解。

明确目的：选择合适的扫描策略

了解对象：首先进行探索，了解网站结构和规模

确定策略：进行对应的配置

按照目录进行扫描任务的分解

按照扫描策略进行扫描任务的分解

2.执行阶段：一边扫描一遍观察

进行扫描

先爬后扫（继续仅测试）

3.检查阶段（Check）

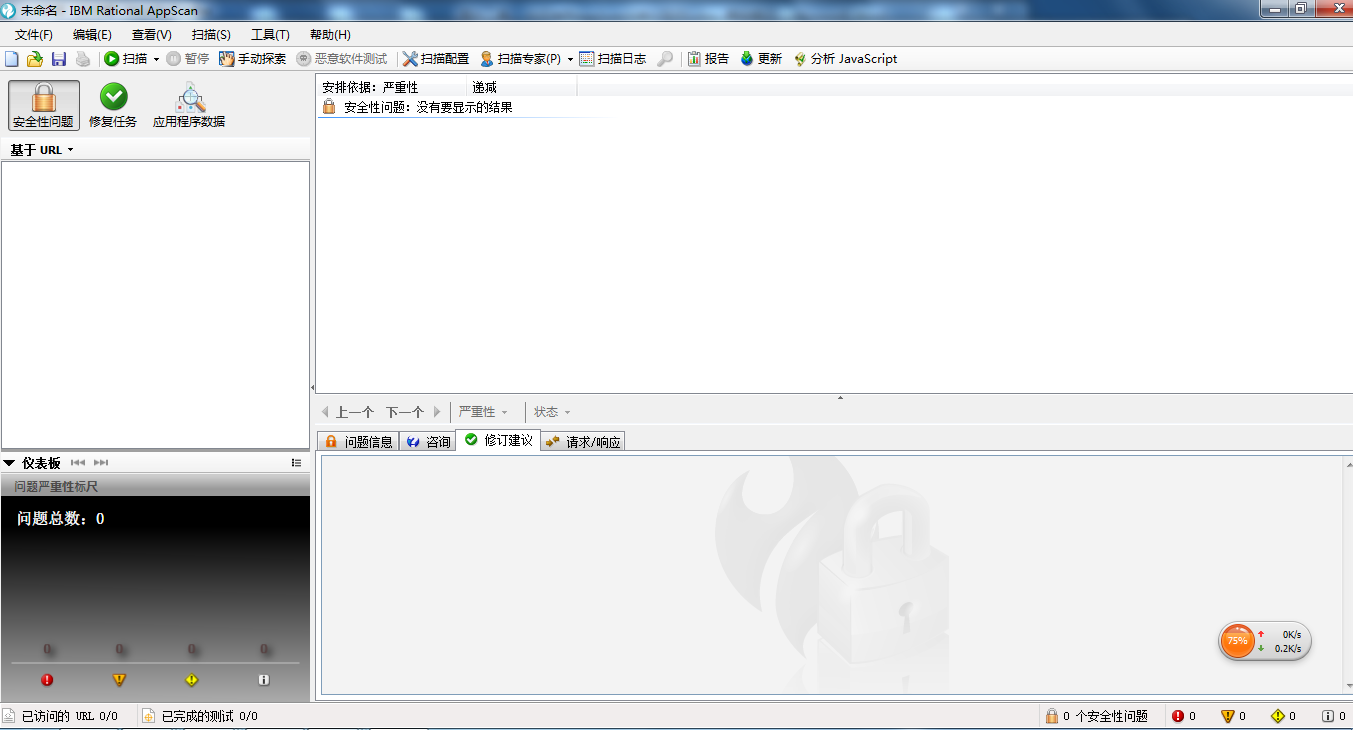
检查和调整配置

4.结果分析（Analysis）

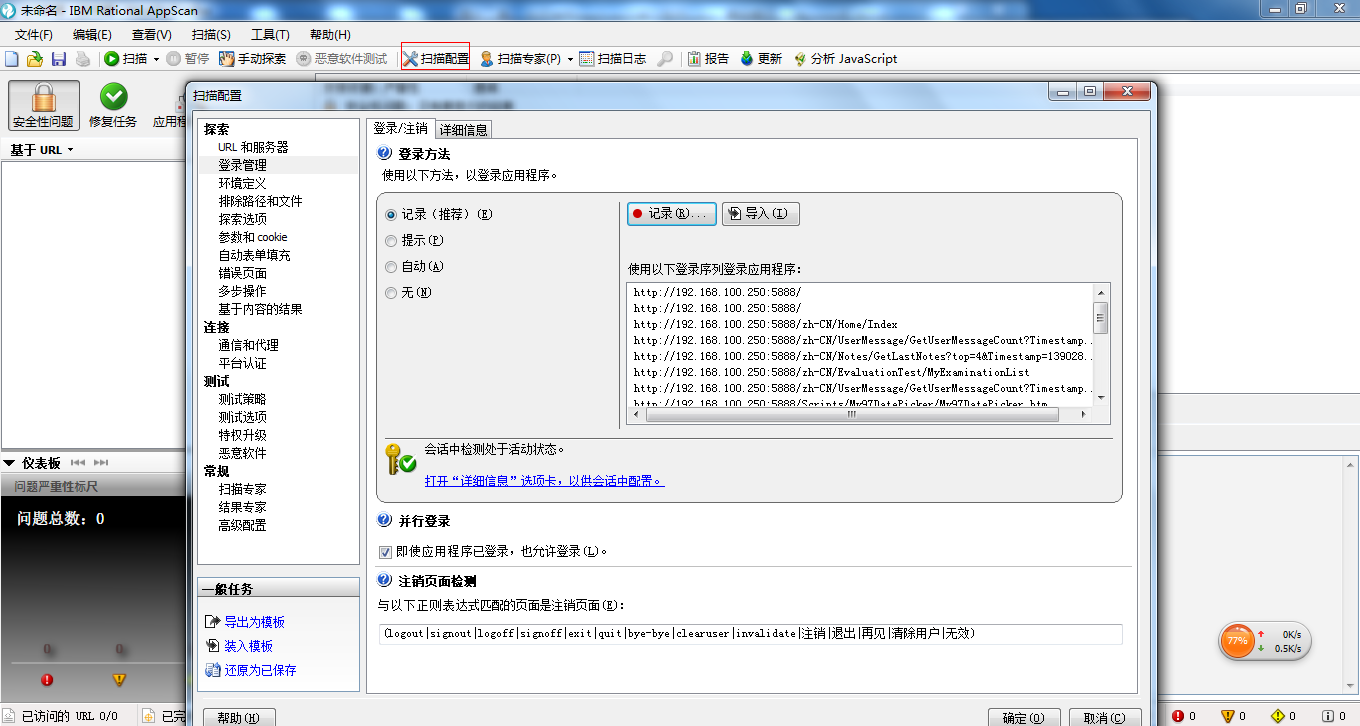
对比结果

汇总结果（整合和过滤）

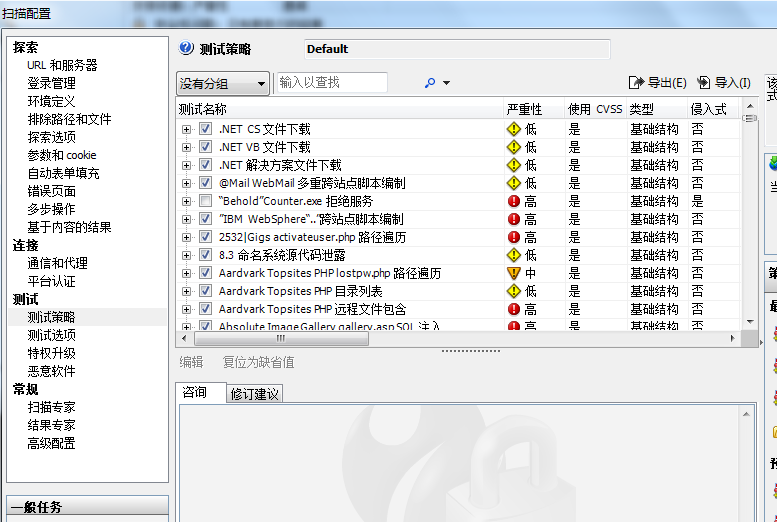
打开后appscan的主页面为：



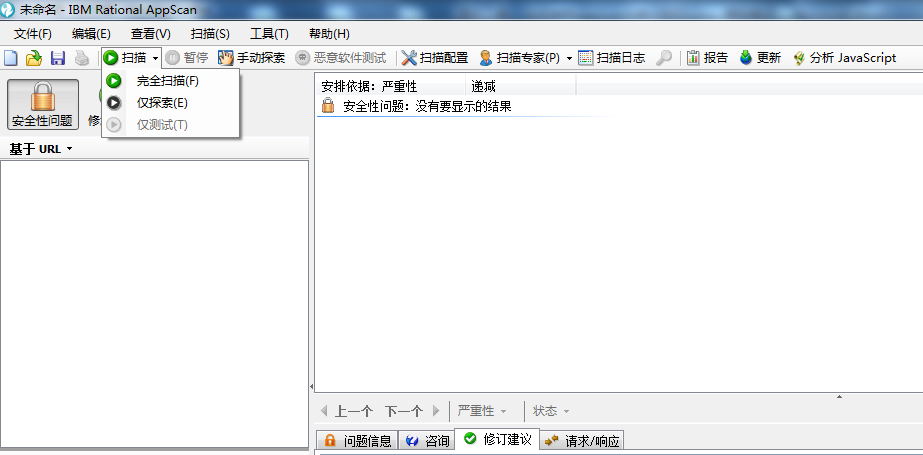
制定扫描配置：



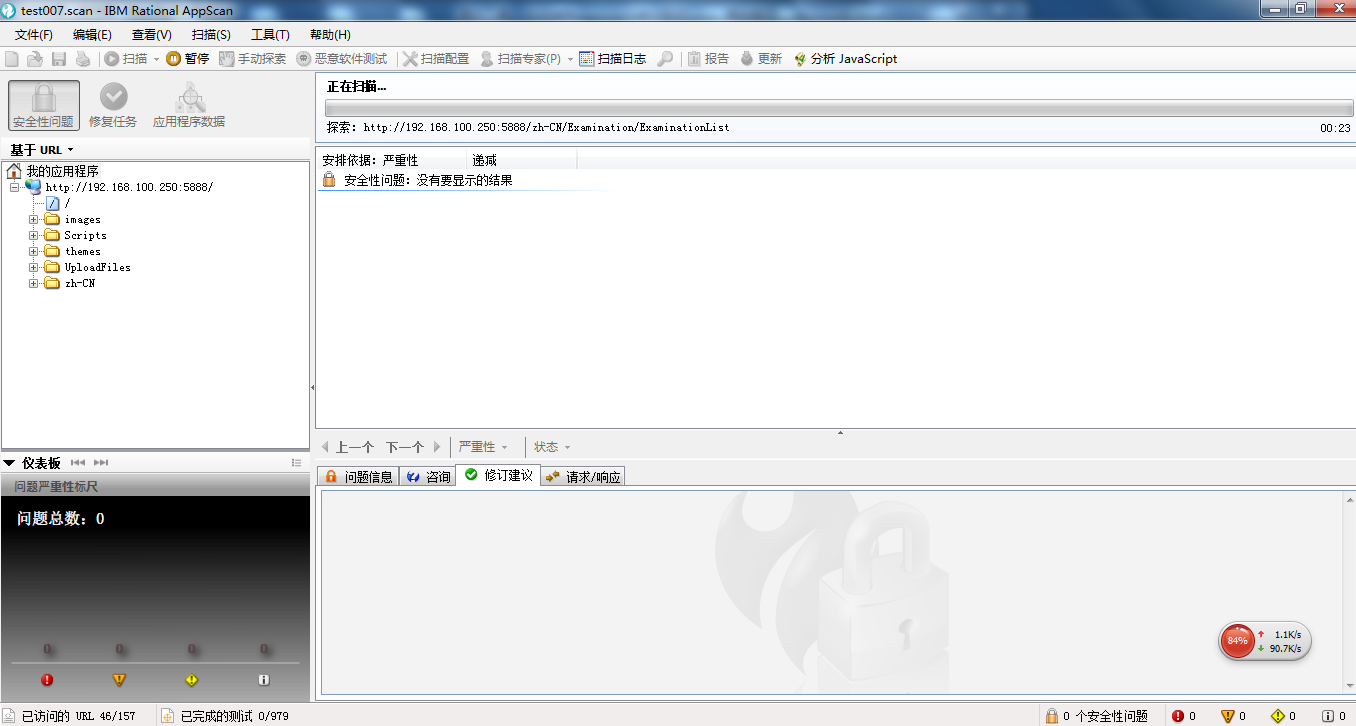
(重点制定测试策略)



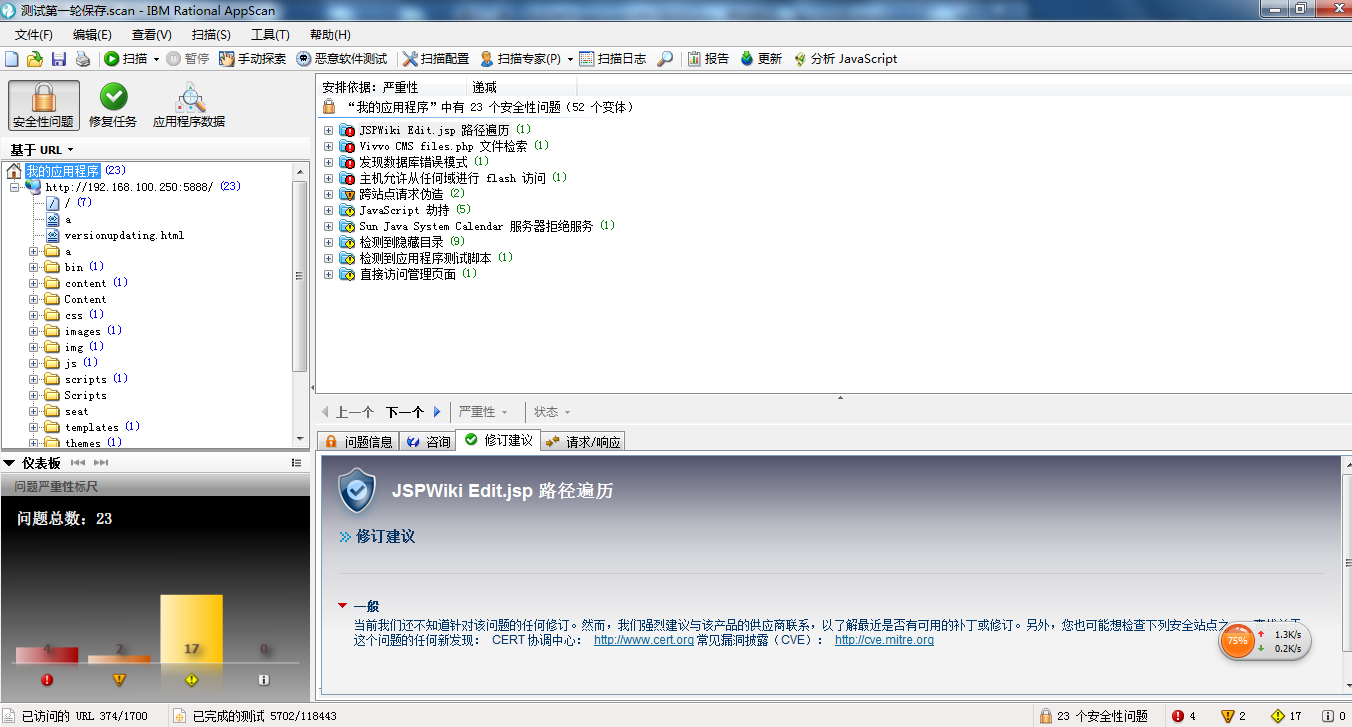
开始扫描（扫描分为探索和测试两步骤）



执行测试中：



测试结果：



测试报告

