Web 系统测试

4.15 Web系统测试—内容总结

河北师范大学软件学院
Software College of Hebei Normal University

目 录

基础知识专项训练

- 测试计划
- 测试用例
- 测试缺陷书写
- 测试总结报告

探索式软件测试

- 探索式测试基础知识
  - 什么是探索式测试
  - 需要遵循哪些章程
- 每种探索测试方法是什么
- 每种探索方法怎样使用
- 哪几种方法有相似之处
- 哪些方法常用在哪些方面

敏捷软件测试

➢敏捷测试的基础理论

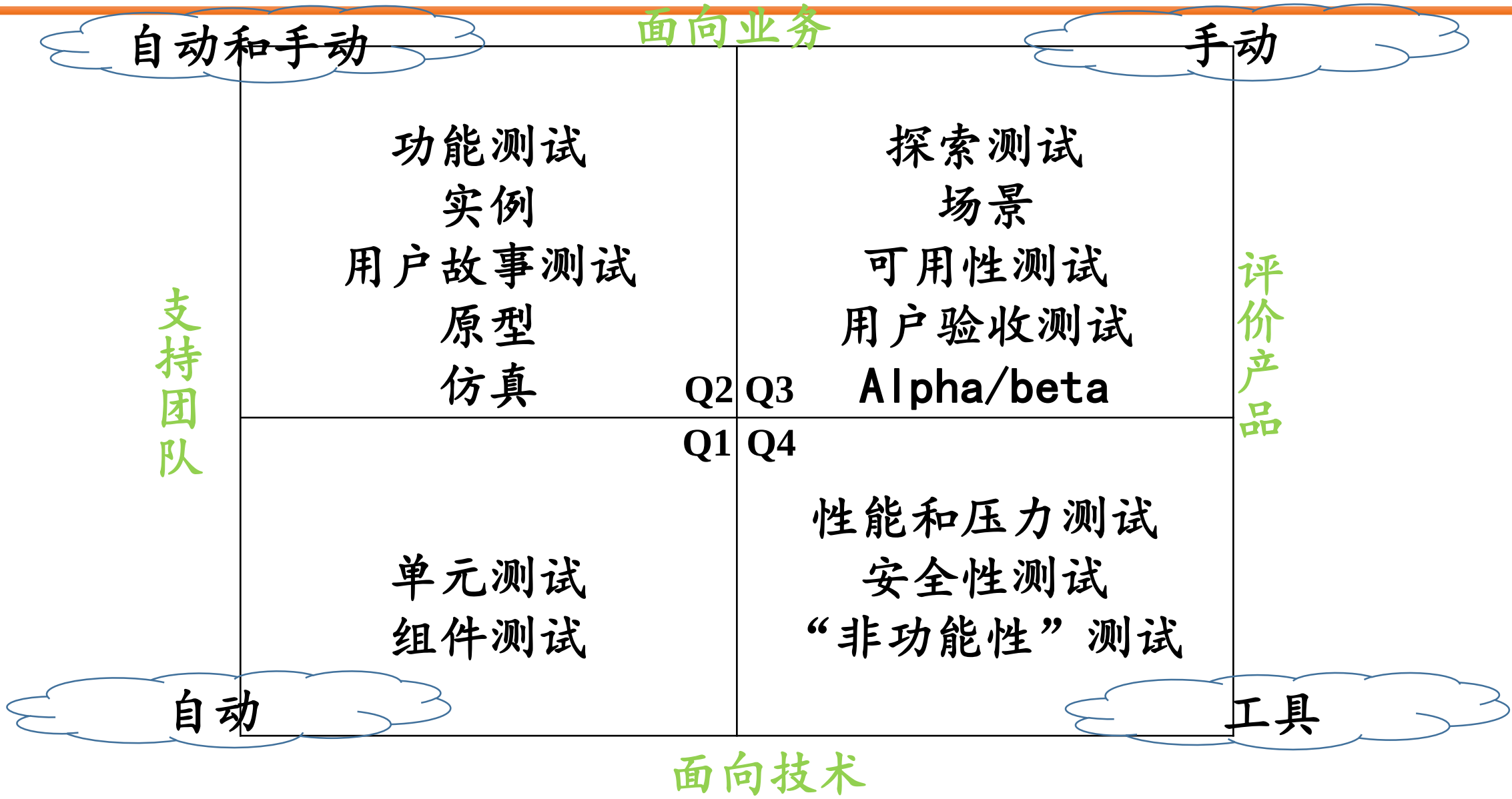
- ●敏捷宣言
- ●敏捷宣言核心价值
- ●什么是敏捷开发
- ●顺序模型与敏捷模型的比较
- ●用户故事

敏捷软件测试

➢敏捷测试基础

- ●测试驱动开发
- ●验收测试驱动开发
- ●行为驱动开发

敏捷测试—敏捷测试象限


面向业务
自动和手动
手动
功能测试
实例
用户故事测试
原型
仿真
探索测试
场景
可用性测试
用户验收测试
Alpha/beta
Q2
Q3
Q1
Q4
性能和压力测试
安全性测试
“非功能性”测试
单元测试
组件测试
支持团队
评价产品
自动
工具
面向技术

渗透测试

- 渗透测试基础知识
  - 什么是渗透测试
  - Web服务器端可能存在的漏洞
  - 怎样做渗透测试
  - 渗透测试的流程

渗透测试—HTTP请求流程

➢HTTP请求流程

- ●HTTP协议
- ●Cookie Session
- ●HTTP请求和响应内容
- ●响应状态码

渗透测试—信息收集

- 信息收集
  - 域名信息
  - 敏感目录
  - 端口扫描
  - 旁站C段
  - 整站分析

渗透测试—漏洞扫描

➢漏洞扫描

●什么是漏洞扫描

- 通过扫描等手段对指定的远程或者本地计算机系统的安全性进行检测，发现可利用漏洞的一种安全检测（渗透攻击）行为

●为什么进行漏洞扫描

●怎样进行漏洞扫描

- 可以借助的工具

渗透测试—文件上传漏洞

➢文件上传漏洞

●什么是文件上传漏洞

- 文件上传漏洞是指由于程序员在对用户文件上传部分的控制不足或者处理缺陷，而导致的用户可以越过其本身权限向服务器上上传可执行的动态脚本文件

●服务器端解析漏洞

- **IIS**
- **Apache**

渗透测试—文件上传漏洞

➢文件上传漏洞

●防止上传漏洞两种策略

- 客户端检测
  - 前端后缀名检测
- 服务器端检测
  - 白名单与黑名单过滤
  - 目录验证
  - MIME验证

渗透测试—文件上传漏洞

➢文件上传漏洞防御方式

- ●绕过前台脚本检测扩展名
- ●禁用JS脚本检测
- ●检查扩展名
  - 黑名单策略
  - 白名单策略

渗透测试—XSS漏洞

➢XSS漏洞

- ●即跨站脚本攻击，指攻击者在网页中嵌入客户端脚本，通常是JavaScript编写的恶意代码，当用户使用浏览器被嵌入恶意代码的网页时，恶意代码将会在用户的浏览器上执行
- ●XSS的危害
- ●XSS的分类
  - 反射型
  - 存储型
  - DOM型

渗透测试—XSS漏洞

- 反射型
  - 一般使用将构造好的URL发给受害者，使受害者点击触发，而且只执行一次，非持久化
  - 或者将恶意脚本附加到带参数的输出函数中
- 存储型
  - 当用户提交一段XSS代码后，被服务器端接收并存储，当攻击者再次访问某个页面时，这段XSS代码被程序读出来响应给浏览器，造成XSS跨站攻击

渗透测试—XSS漏洞

- 检测XSS
  - 手工检测
  - 自动检测

渗透测试—XSS漏洞

➢XSS漏洞防范

- ●增加过滤规则
- ●检验输入字符并进行转义

渗透测试—SQL注入漏洞

➢SQL注入漏洞基础知识

●什么是SQL注入漏洞

- 通过把SQL命令插入到Web表单提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

➢SQL注入原理

●攻击者通过Web应用程序利用SQL语句或字符串将非法的数据插入到服务器端数据库中，获取数据库的管理用户权限，获取重要信息及机密文件

渗透测试—SQL注入漏洞

- SQL注入方法
  - 通过字符串注入
  - 猜测：猜表名，猜列名，猜数据库名等等
  - 后台身份验证绕过漏洞
- 怎样测试SQL注入漏洞
  - 判断是否存在 Sql 注入漏洞
    - 单引号判断法
    - 数字型判断
    - 字符型判断

渗透测试—SQL注入漏洞

- 怎样防御SQL注入漏洞
  - 使用参数化的过滤性语句
  - 输入验证
  - 错误消息处理
  - 加密处理
  - 存储过程来执行所有的查询
  - 使用专业的漏洞扫描工具
  - 确保数据库安全

渗透测试—浏览器安全

- 同源策略
- 浏览器沙箱
- 恶意网址拦截
- 浏览器安全其他方面

渗透测试—浏览器安全

- 同源策略
  - 同源的概念
  - 同源策略
- 沙箱策略
  - 概念：泛指“资源隔离类模块”的代名词
  - 设计沙箱的目的
    - 让不可信任的代码运行在一定的环境中，限制不可信任的代码访问隔离去之外的资源

渗透测试—浏览器安全

- 恶意网址拦截
  - 服务器端读取黑名单
  - 安全证书

渗透测试—浏览器安全

➢浏览器其他安全策略

- IE8中推出了XSS Filter功能，用以对抗反射型XSS
- Firfox4 推出了Content Security Policy（内容安全政策）

渗透测试—点击劫持

- 点击劫持基础知识
- Flash点击劫持
- 图片覆盖攻击
- 拖拽劫持与数据窃取
- 触屏劫持

渗透测试—跨站点请求伪造

- CSRF（跨站点请求伪造）基础知识
  - 攻击者通过盗用身份，并用盗用来的身份发送恶意请求
  - CSRF的原理
- CSRF攻击过程
- CSRF的防御
  - 在表单里增加Hash值
  - 验证码
  - One-Time Tokens

渗透测试—HTML5安全

➢HTML5基础知识

- ●新标签的使用
- ●新标签的安全策略
- ●跨源资源共享
- ●跨窗口传递消息

渗透测试工具——Burp Suite的使用

- 基本安装和配置
- Target的使用
- Spider
- Intruder

渗透测试工具——Burp Suite的使用

- **Repeater——是一个靠手动操作来补发单独的HTTP 请求，并分析应用程序响应的工具**
- **Sequencer——是一个用来分析那些不可预知的应用程序会话令牌和重要数据项的随机性的工具**
- **Decoder——是一个进行手动执行或对应用程序数据者智能解码编码的工具**
- **Comparer——是一个实用的工具，通常是通过一些相关的请求和响应得到两项数据的一个可视化的“差异”**

Question