51testing

电子商务测试方法探讨

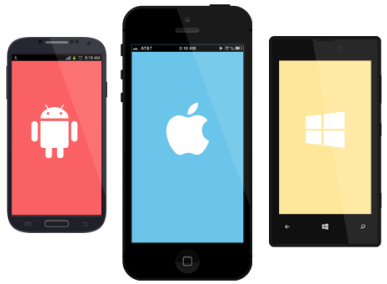
刘平

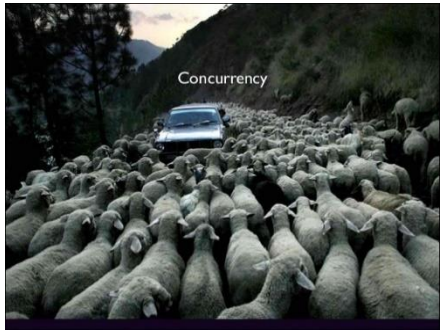
专业测试·卓越品质

上海博为峰软件技术股份有限公司

目录

电商系统软件特点





目录

性能测试 – 定义

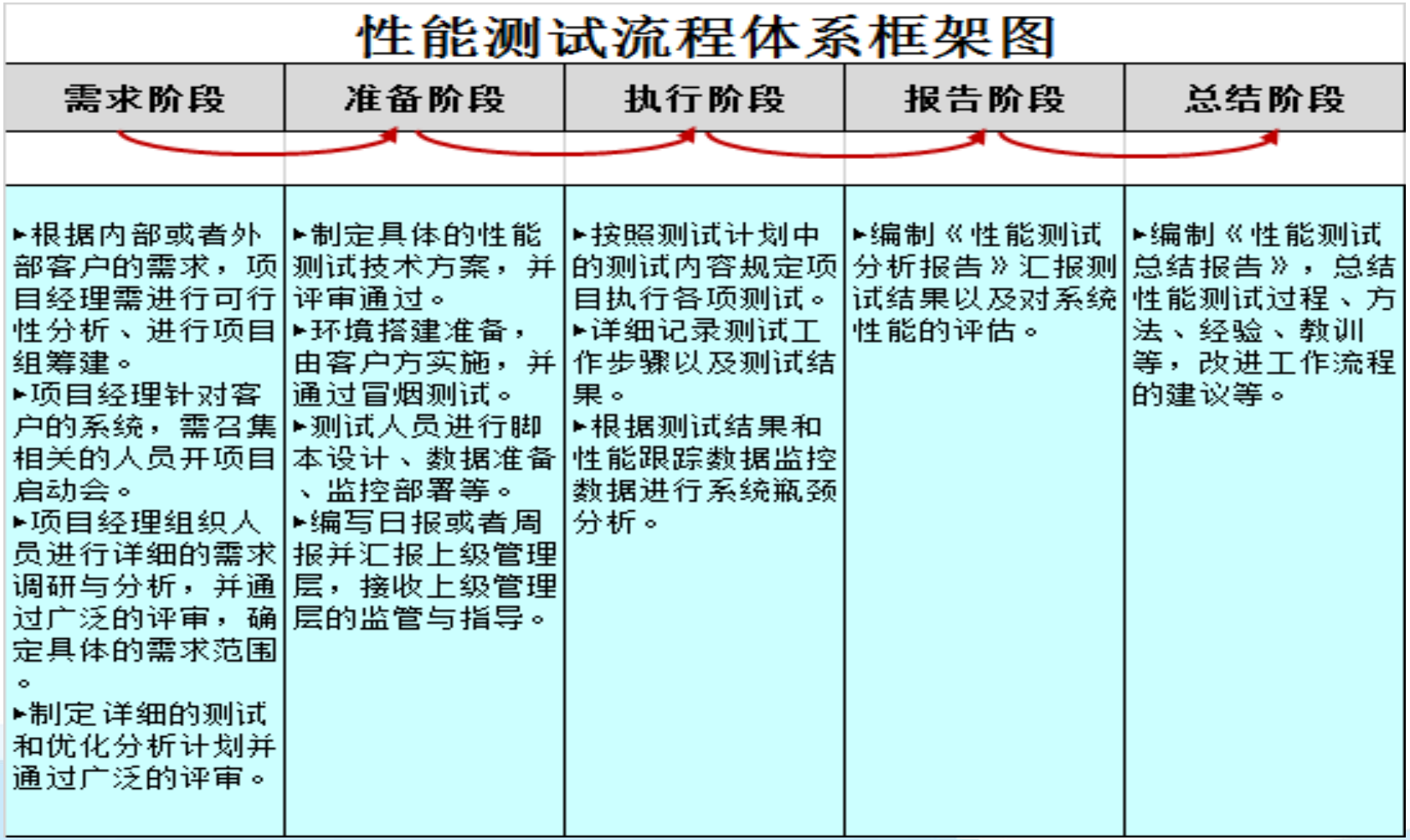
- 定义:

  In software engineering, performance testing is in general, a testing practice performed to determine how a system performs in terms of responsiveness and stability under a particular workload. It can also serve to investigate, measure, validate or verify other quality attributes of the system, such as scalability, reliability and resource usage. -- Wikipedia

- 目的:

  为了验证系统是否达到用户提出的性能指标，同时发现系统中存在的性能瓶颈，起到优化系统的目的。

性能测试 – 流程


性能测试流程体系框架图
需求阶段
准备阶段
执行阶段
报告阶段
总结阶段
▸根据内部或者外部客户的需求，项目经理需进行可行性分析、进行项目组筹建。
▸项目经理针对客户的系统，需召集相关的人员开项目启动会。
▸项目经理组织人员进行详细的需求调研与分析，并通过广泛的评审，确定具体的需求范围。
▸制定详细的测试和优化分析计划并通过广泛的评审。
▸制定具体的性能测试技术方案，并评审通过。
▸环境搭建准备，由客户方实施，并通过冒烟测试。
▸测试人员进行脚本设计、数据准备、监控部署等。
▸编写日报或者周报并汇报上级管理层，接收上级管理层的监管与指导。
▸按照测试计划中的测试内容规定项目执行各项测试。
▸详细记录测试工作步骤以及测试结果。
▸根据测试结果和性能跟踪数据监控数据进行系统瓶颈分析。
▸编制《性能测试分析报告》汇报测试结果以及对系统性能的评估。
▸编制《性能测试总结报告》，总结性能测试过程、方法、经验、教训等，改进工作流程的建议等。

性能测试 – 业务指标

指标	定义	标准
Response Time	响应时间指用户从客户端发起一个请求开始，到客户端接收到从服务器端返回的响应结束，整个过程所耗费的时间。	• 互联网企业：500毫秒以下。 • 金融企业：1秒以下为佳，部分复杂业务3秒以下。 • 保险企业：3秒以下为佳。 • 制造业：5秒以下为佳。
HPS	每秒点击次数，单位是次/秒	• 金融行业：1000TPS~9000TPS • 保险行业：100TPS~1000TPS • 制造行业：10TPS~50TPS • 互联网电子商务：10000TPS~100000TPS • 互联网中型网站：100TPS~500TPS • 互联网小型网站: 50TPS~100TPS
TPS	系统每秒处理交易数，单位是笔/秒	
QPS	系统每秒处理查询次数，单位是次/秒	
Virtual User（VU）	并发用户数指在同一时刻内，登录系统并进行业务操作的用户数量	一般情况下，性能测试是将系统处理能力容量测出来，而不是测试并发用户数，除了服务器长连接可能影响并发用户数外，系统处理能力不受并发用户数影响。
Failure Ratio	错误率指系统在负载情况下，失败交易的概率。错误率＝(失败交易数/交易总数)*100%。稳定性较好的系统，其错误率应该由超时引起，即为超时率。	不同系统对错误率的要求不同，但一般不超出千分之六，即成功率不低于99.4%

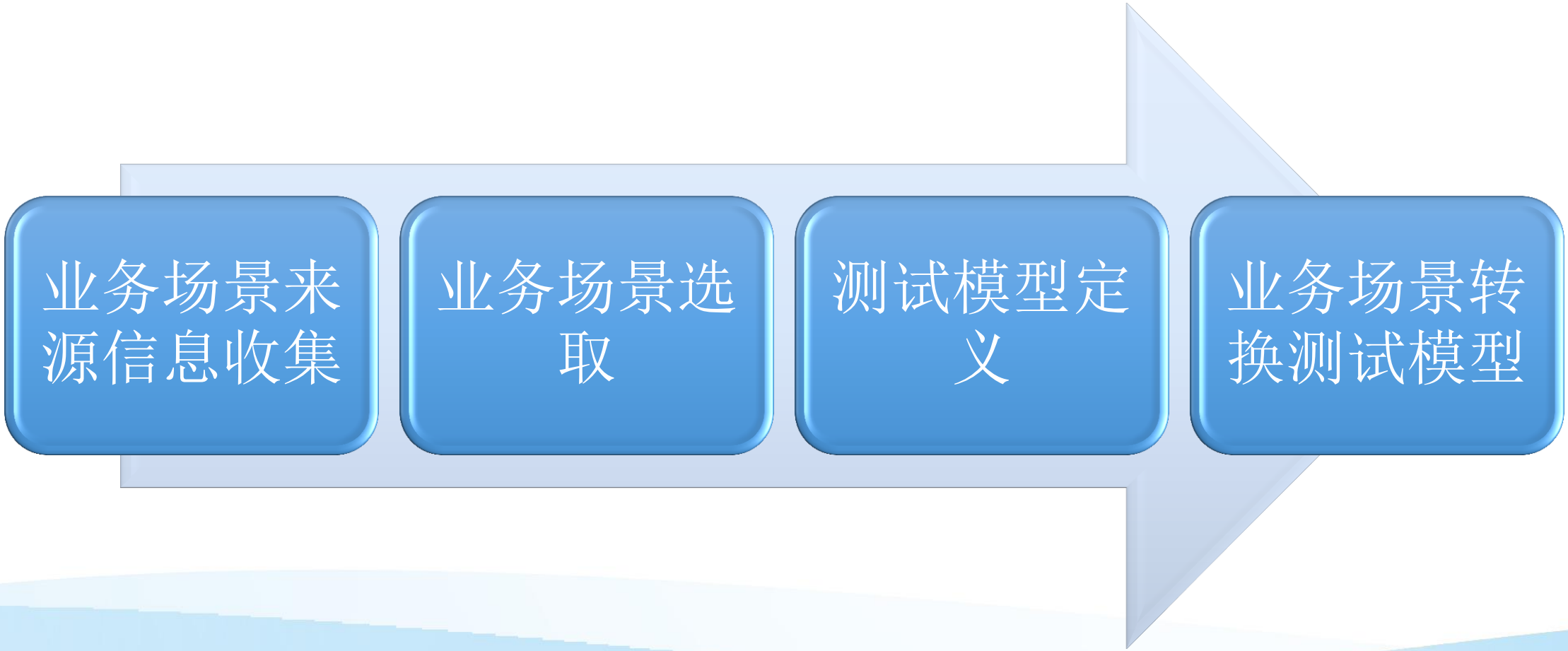
性能测试 – 资源指标

指标	定义	标准
CPU	CPU即中央处理器 CPU Load: 系统正在干活的多少的度量，队列长度。系统平均负载。	• CPU 利用率要低于业界警戒值范围之内，即小于或者等于75% • CPU Load要小于CPU 核数
Memory	Memory就是内存的简称	现代的操作系统为了最大利用内存，在内存中存放了缓存，因此内存利用率100%并不代表内存有瓶颈，衡量系统内存有瓶颈主要靠SWAP（与虚拟内存交换）交换空间利用率，一般情况下，SWAP交换空间利用率要低于70%,太多的交换将会引起系统性能低下
Disk Throughput	磁盘吞吐量是指在无磁盘故障的情况下单位时间内通过磁盘的数据量	磁盘指标主要有每秒读写多少兆，磁盘繁忙率，磁盘队列数，平均服务时间，平均等待时间，空间利用率。 其中磁盘繁忙率是直接反映磁盘是否有瓶颈的的重要依据，一般情况下，磁盘繁忙率要低于70%。
Network Throughput	网络吞吐量是指在无网络故障的情况下单位时间内通过的网络的数据数量。单位为Byte/s	网络吞吐量指标主要有每秒有多少兆流量进出，一般情况下不能超过设备或链路最大传输能力的70%

性能测试 – 中间件和数据库指标

指标	定义	标准
GC频率	java虚拟机垃圾部分回收频率	GC频率不能频繁，特别是FULL GC更不能频繁，一般情况下系统性能较好的情况下，JVM最小堆大小和最大堆大小分别设置1024M比较合适。
ThreadPool	线程池	当前正在运行的线程数不能超过设定的最大值。一般情况下系统性能较好的情况下，线程数最小值设置50和最大值设置200比较合适
JDBC Active Connection	JDBC活动连接数	当前运行的JDBC连接数不能超过设定的最大值。一般情况下系统性能较好的情况下，JDBC最小值设置50和最大值设置200比较合适
SQL 耗时	执行SQL耗时	SQL耗时越小越好，一般情况下微秒级别
SQL QPS	每秒查询次数	
SQL TPS	每秒事务次数	
Key Buffer命中率	索引缓冲区命中率	命中率越高越好，一般情况下不能低于95%
InnoDB Buffer命中率	InnoDB缓冲区命中率	
Query Cache命中率	查询缓存命中率	
Table Cache命中率	表缓存命中率	
Thread Cache命中率	线程缓存命中率	
等待次数	锁等待次数	锁等待次数越低越好，等待时间越短越好
等待时间	锁等待时间	

性能测试 – 测试模型构建



性能测试 – 业务场景来源信息收集

业务场景的来源可以通过以下信息获取:

1. 交易日的日均交易量
2. 历史峰值交易日的交易量
3. 特殊日的交易量
4. 不同交易渠道的交易量
5. 一般交易日的交易配比
6. 历史峰值交易日的交易配比
7. 特殊日的交易配比
8. 不同交易渠道的交易配比
9. 批量处理的流程
10. 批量处理的时间窗口要求
11. 系统历史数据量

性能测试 – 业务场景选取

选取典型业务交易的标准：

1. 根据业务量大小选取典型交易，一般通过统计生产系统TOP10 、TOP20确定；
2. 选取生产系统中消耗资源最多，或者耗时最长的业务交易；
3. 选取生产系统中交易路径最长的业务交易；
4. 选取生产系统容易发生故障的业务交易；
5. 为满足其他特殊测试目标需要选取的业务交易；

性能测试 – 测试模型定义

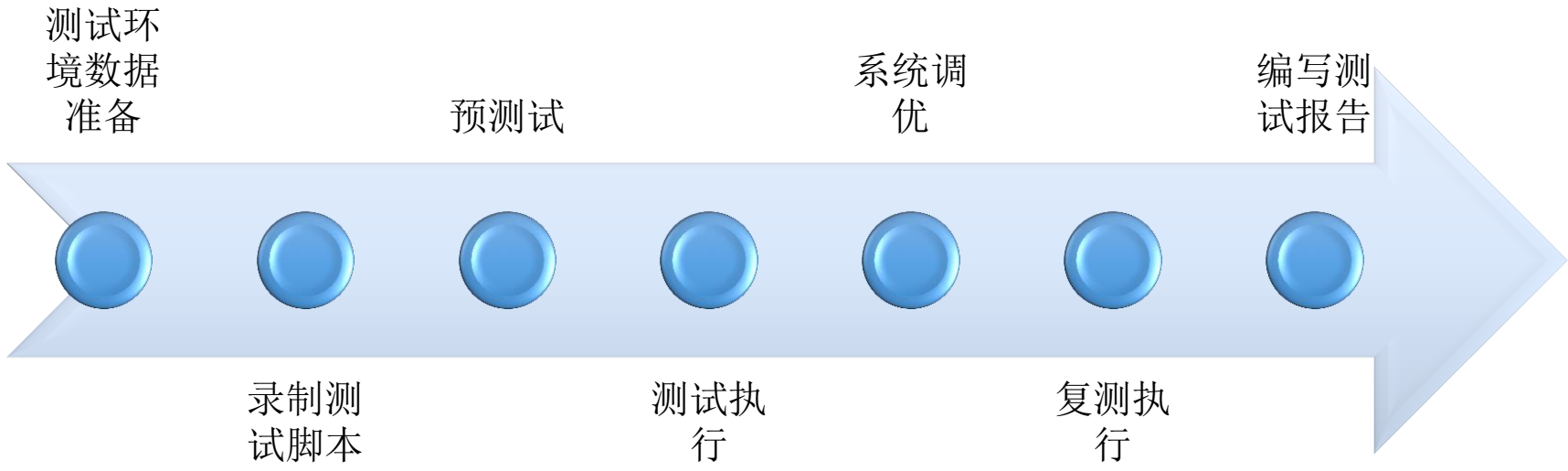
根据测试目标的需要，可能存在的测试模型有以下几种：

1. 单交易基准测试模型
2. 单交易负载测试模型
3. 日间混合负载测试模型
4. 稳定性测试模型
5. 可靠性测试模型
6. 批量处理测试模型

性能测试 – 业务场景转换测试模型

测试模型	测试目标	对应的业务场景	压力场景
单交易基准测试模型	通过测试，检查该交易是否存在性能缺陷，同时为性能测试提供参考数据	所有典型交易	单支交易在系统无压力情况下重复执行多次
单交易负载测试模型	通过逐步增加并发量进行负载测试，获取单交易业务处理性能峰值，并验证交易是否存在并发性问题	所有典型交易	逐渐增加并发量
混合负载测试模型	混合负载测试是按照业务模型的约定在一定量的并发情况下进行测试。通过测试，获取模拟实际生产环境中被测系统性能表现数据	该测试模型可能与正常业务日交易场景、特殊日交易场景、高峰交易场景、交易线与数据线混合场景等多个业务场景对应	逐渐增加并发量
稳定性测试模型	检查在持续的压力情况下，系统长期运行时的业务处理能力及系统可能存在的缺陷	正常业务日交易场景	稳定压力
可靠性测试模型	通过模拟系统可能遇到的各种异常情况，如带宽受限、网络连通不好、网络延时、超时、各系统主机宕机、应用异常终止、资源死锁、大并发用户集中爆发访问等情况，检查系统的异常处理能力	正常业务日交易场景,高峰交易场景	稳定压力＋突增压力
日终处理测试模型	验证日终设计操作正确性以及是否满足日终操作时间窗要求	日终批处理场景文件/数据处理场景	按照日终操作要求执行

性能测试 – 后续工作



目录

Web安全测试 – 流程

Web安全测试 – 信息收集

需要收集的信息包括:

1. 网站结构
2. 网站的目录
3. Whois信息
4. WEB容器信息
5. 所有的子域名
6. 网站旁站信息
7. 主机开放端口
8. 服务器操作系统信息

Web安全测试 – 漏洞扫描

漏洞扫描工具:

1. WebInspect
2. AppScan
3. Burpsuite
4. OWASP Zen Attack Proxy
5. Nikto

Active Scan

Passive Scan

Web安全测试 – 漏洞验证

OWASP top 10 vulnerabilities - 2015:

1. 注入
2. 失效的身份认证和会话管理
3. 跨站
4. 不安全的直接对象引用
5. 安全配置错误
6. 敏感信息泄漏
7. 功能级访问控制缺失
8. 跨站请求
9. 使用含有已知漏洞的组件
10. 未验证的重定向和转发

Web安全测试 – SQL注入

- 原理：注入往往是应用程序缺少对输入进行安全性检查所引起的，攻击者把一些包含指令的数据发送给解释器，解释器会把收到的数据转换成指令执行，其中SQL注入最为常见。
- 影响：SQL注入攻击容易对系统产生很严重的后果，导致整个数据库可被读写与修改，很可能得到数据库访问权限或系统账户的访问权限，甚至得到操作系统管理员的权限

例如：("SELECT COUNT(*) FROM Login WHERE UserName='{0}' AND Password='{1}'", userName, password)

输入注入数据：用户名：admin’—，密码可随便输入

SELECT COUNT(*) FROM Login WHERE UserName='admin'-- Password='123'

Payload: ‘

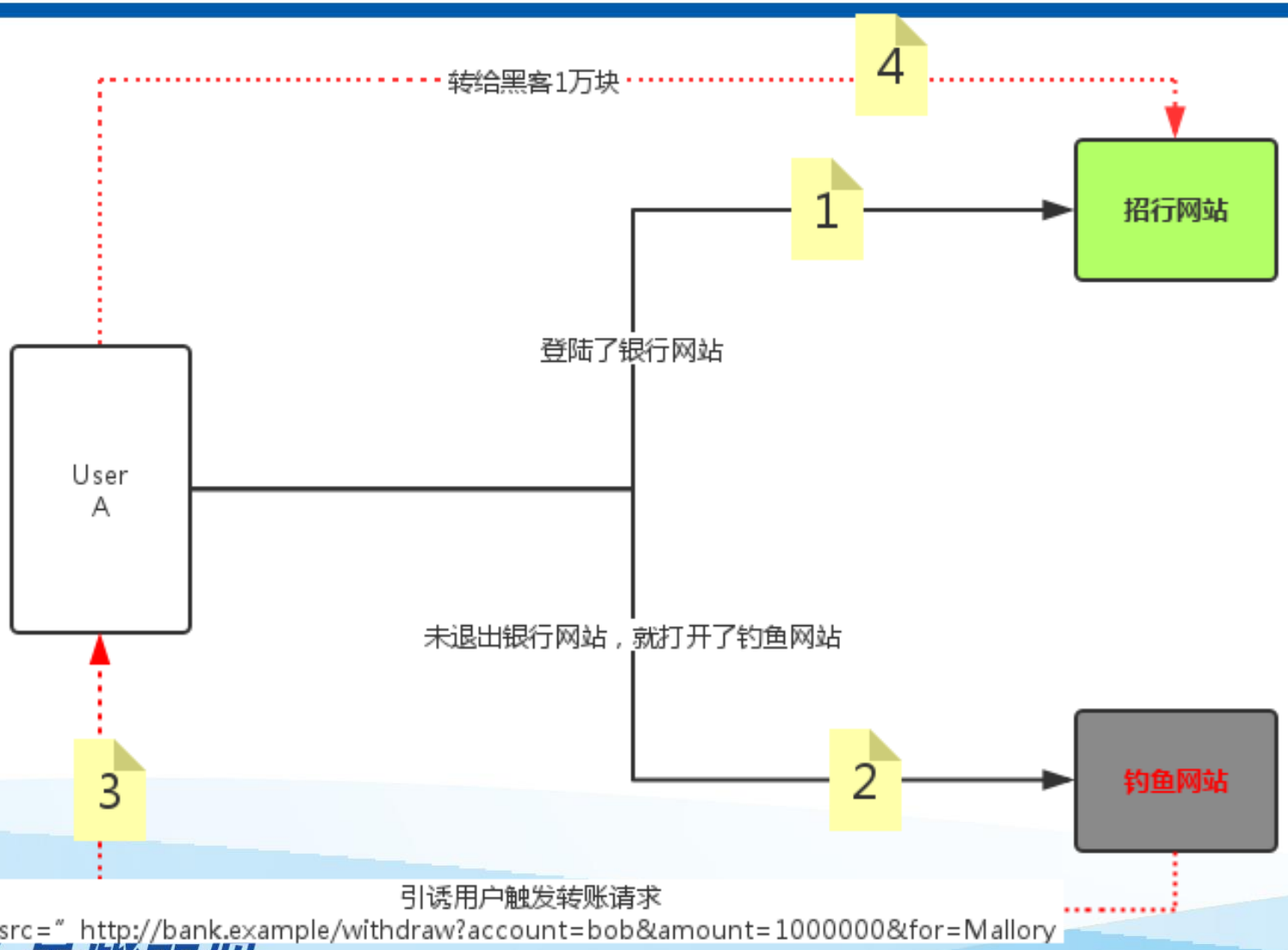
Web安全测试 – 失效的身份认证和会话管理

- 定义：与身份认证和会话管理相关的应用程序功能往往得不到正确的实现，这就导致了攻击者破坏密码、密匙、会话令牌或攻击其他的漏洞去冒充其他用户的身份。

1. 可预测Session ID
   - 用户ID或邮箱
   - 远程IP地址
   - 日期与时间
   - 随机数
2. 固定Session ID

   例如：诱使受害者通过http://www.xxx.com?PHPSESSID=test登录系统

Web安全测试 – CSRF



Web安全测试 – 其它安全漏洞

- 目录遍历漏洞

  例如：www.xxx.com/html/../../../etc/passwd

- 文件上传漏洞

  例如：上传文件hack.php%00.jpg，hack.php.rar.rar.rar

- 业务处理漏洞
- 输入检查漏洞

- 数据安全

  该项测试主要检查移动应用是否将用户的敏感信息以明文的方式保存在文件或数据库中。从而造成用户的数据容易被其它应用窃取和使用的安全隐患。

  例如移动应用保存明文密码信息（已过滤掉包名）：

  [高危]：data/data/com.***.v7/shared_prefs/rem_password.xml: 行 3: 发现明文敏感信息：passwd123 !!!

- 网络安全

  该项测试主要检查移动应用是否将用户的敏感信息以明文的方式在网络中进行传输。从而造成用户信息泄露。

移动APP安全测试（续）

- 组件安全

  在Android中存在多种组件，比如Content Provider、Broadcast Receiver等等，这些组件可能因权限设置不当导致信息泄露或者钓鱼欺骗等攻击。

  由于程序对Provider的权限设置不当，导致第三方软件可读取Content Provider提供的信息，其危害程度取决于Content Provider提供的信息内容，比如联系人、电话、短信等隐私信息就可能包含其中，比较容易被被第三方恶意软件利用。

- 代码安全

  是否可以被反编译

  是否经过代码混淆

  是否有签名信息

  是否能够被调试跟踪

目录

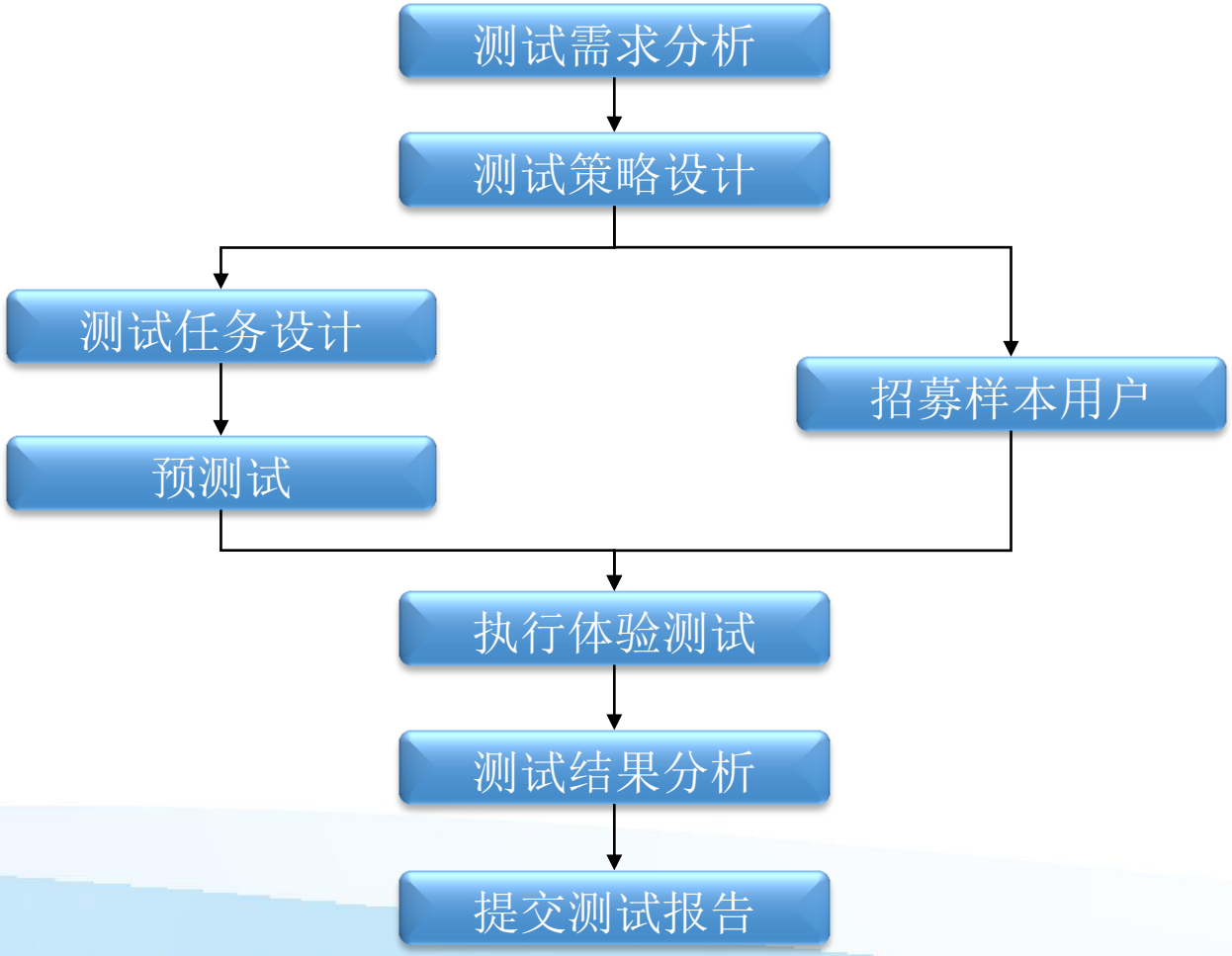
用户体验测试

感官角度	• 颜色 • 布局 • 风格
使用角度	• 易认知 • 易学习 • 易操作 • 容错

用户体验测试 – 指标

目标	有效性	效率	满意度
易认知性	目标达成百分比	完成一个任务所需的时间	满意程度
易操作性	主要功能被使用的数目	与专家级用户相比，完成一个任务的差距	对主要功能的满意度
易学习性	用户学习的功能占总数的百分比	用户学习时间	用户对易学习性的满意度
容错性	误操作被成功改正的百分比	改正误操作所需的时间	用户对错误处理的满意度

用户体验测试 – 流程



用户体验测试 – 工具

录屏工具：

- psr – Windows自带软件，Win7以上
- Microsoft Snip – 免费，可以通过摄像头录制视频
- Game Bar – 免费，Win10自带软件
- Camtasia Studio – 收费，可以录制屏幕/摄像头，并且能够扑捉鼠标轨迹

专业测试·卓越品质

上海博为峰软件技术股份有限公司

沙龙观看地址 www.atstudy.com