ThoughtWorks®

致测试同仁们:
让我们做Web安全测试吧!

2016-11-19

SFDC SegmentFault Developer Conference

安全测试并不遥远

ThoughtWorks®

SFDC SegmentFault Developer Conference

安全测试并不陌生

ThoughtWorks®

SFDC SegmentFault Developer Conference

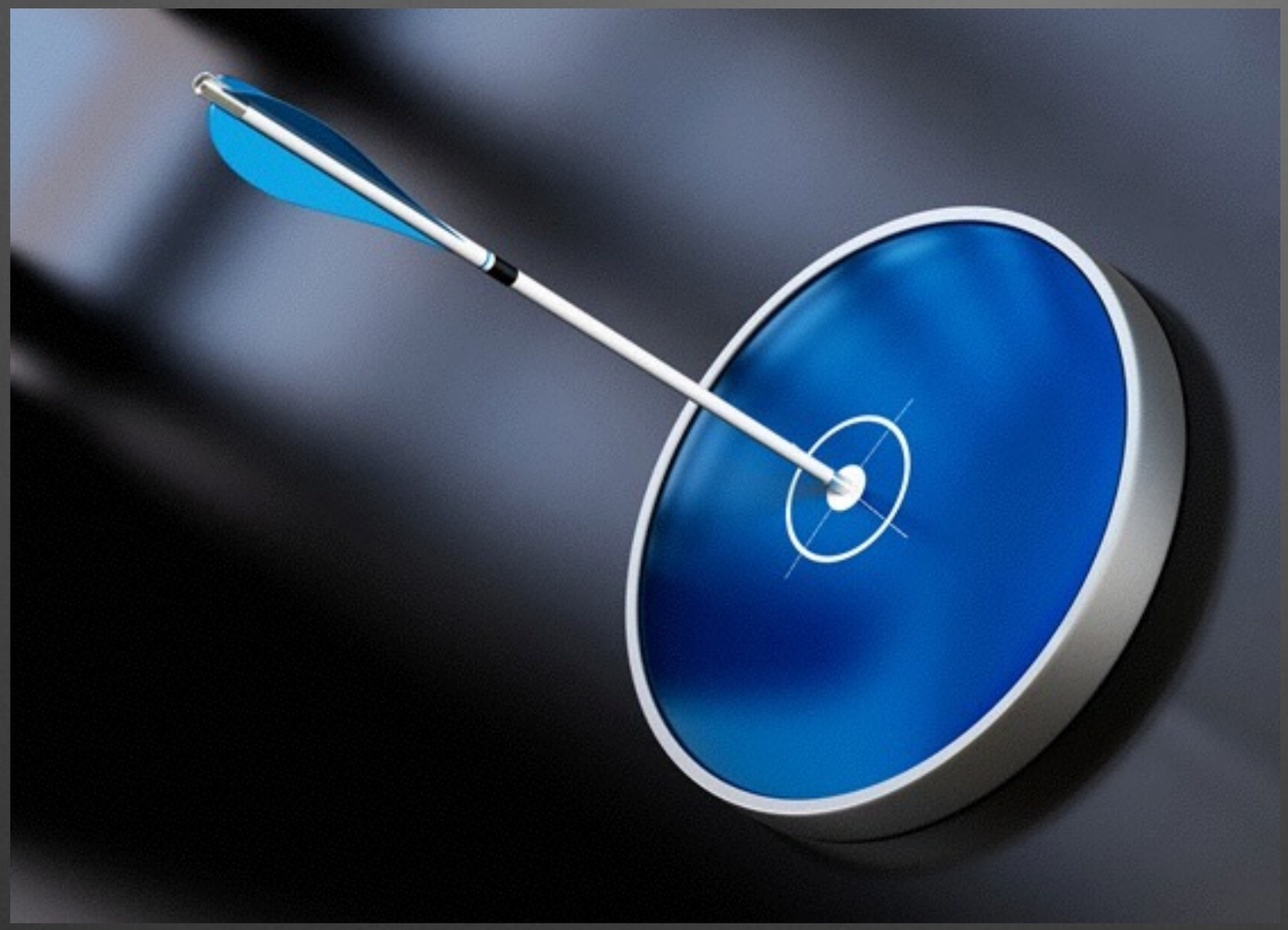
安全测试并不陌生

- 都是“测试”
- 关注软件质量

与“其他”测试的相似之处

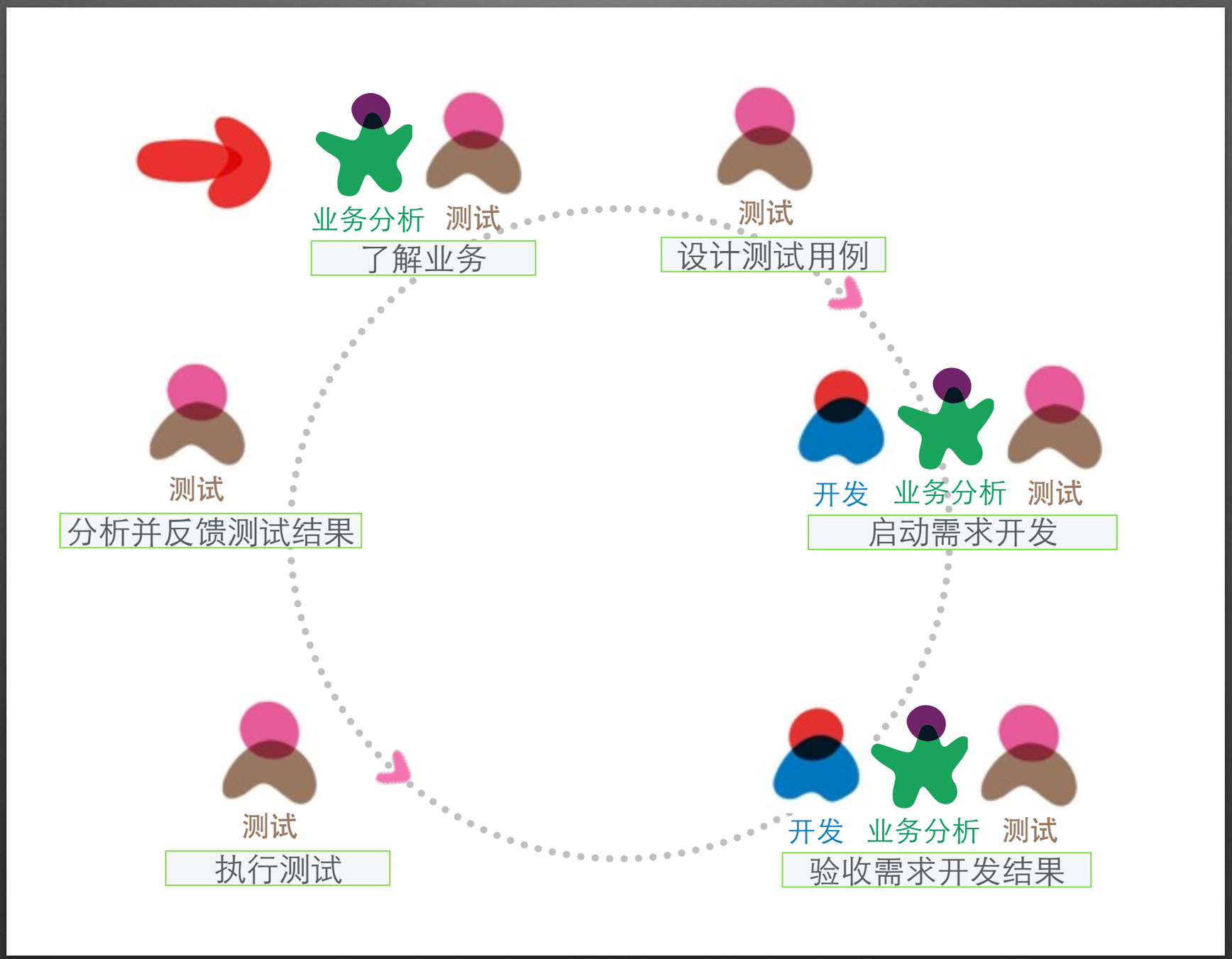
- 目标
- 过程
- 测试用例
- 探索
- 怀疑的态度

目标类似

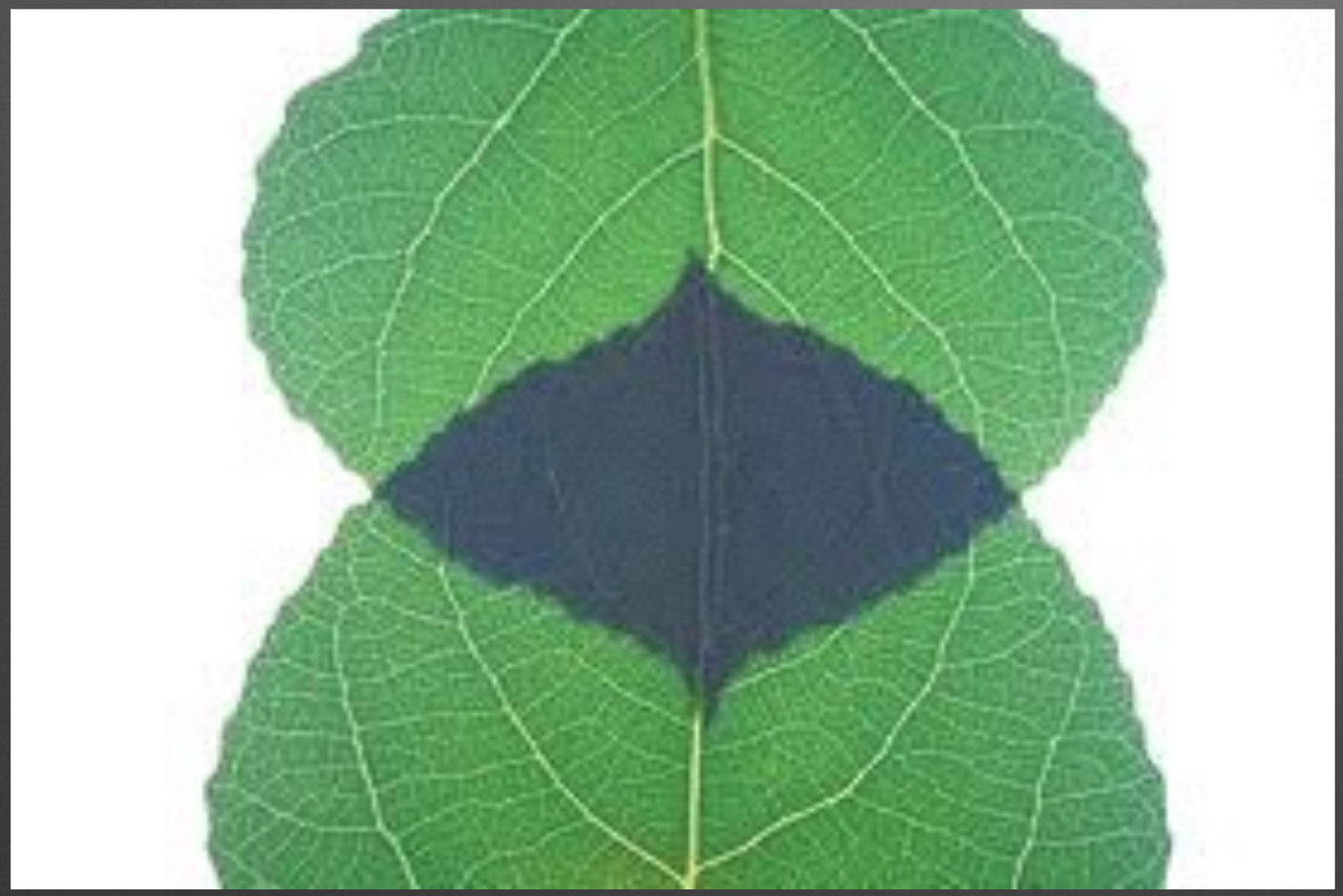


- 预防缺陷
- 发现缺陷

过程类似


业务分析 测试
了解业务
测试
设计测试用例
测试
分析并反馈测试结果
开发 业务分析 测试
启动需求开发
测试
执行测试
开发 业务分析 测试
验收需求开发结果

测试用例有重合



- “我要登陆系统”
- “我要下订单”
- “我要上传文件”
- …

探索

- 探索软件系统的“计划外”行为

怀疑的态度

- 注意！ 这个Dev说他只改了付款流程的一点点东西。影响范围真的只是一点点吗?

安全测试从何做起

ThoughtWorks®

SFDC SegmentFault Developer Conference

安全起步“三板斧”

- 转化视角
- 改变模拟对象
- 使用专用的测试工具

转换视角

改变模拟对象

- 合法用户
- 没有恶意

改变模拟对象

- 我想买一本书，我想有个简化的付款流程

改变模拟对象

- 非法用户
- 不怀好意

改变模拟对象

- 我想买一本书，但是我不想付钱

使用专用测试工具

- 恶意用户不总走“前门”，我们需要工具来走“后门”

使用专用测试工具

OWASP ZAP

Burp Suite

- https://portswigger.net/burp/
- https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

来个栗子吧！

ThoughtWorks®

SFDC SegmentFault Developer Conference

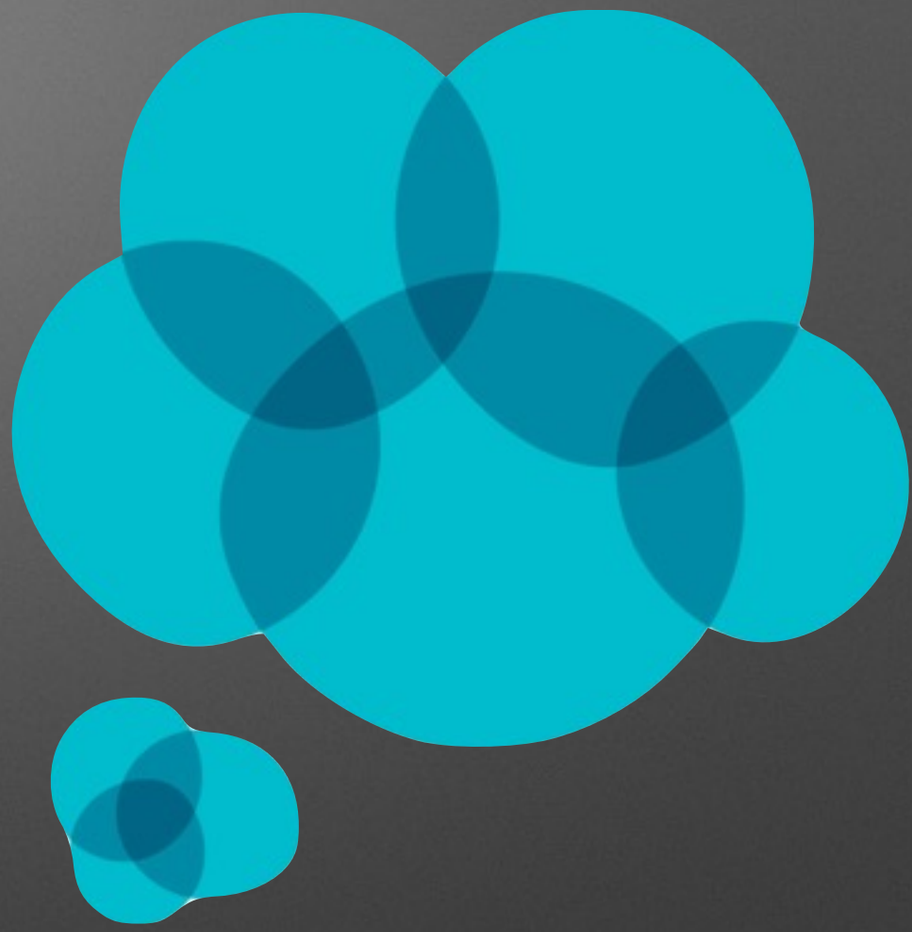
“栗子”的场景

- 网上商城的买家评价
- 作为一个商城买家
- 我想购买成功后能够分享我的购买心得

栗子：七步骤

“栗子”中测试用例

- 恶意用户想做什么?
  - 不买东西也评论
  - 冒充别人评论
  - 恶意评论内容
  - 等等



总结

- 转换视角
- 改变模拟对象
- 使用专用工具

增强
现有测试流程

谢谢！

www.thoughtworks.com

&

www.buildsecurityin.cn

ThoughtWorks®

SFDC SegmentFault Developer Conference