## 学习目标

★了解安全测试的概念
★熟悉常见的安全漏洞
★了解渗透测试的流程及常见安全测试工具
★熟悉安全测试工具 AppScan 的使用

在 Internet 大众化、Web 技术飞速演变的今天，软件给我们带来便利的同时，也带来了很多安全隐患。例如，2018 年 3 月，美国功能性运动品牌 Under Armour（安德玛）公司的移动应用程序 MyFitnessPal 遭受黑客攻击，导致 1.5 亿账户信息泄露。

软件安全测试是软件测试的重要研究领域，它是保证软件能够安全使用的最主要手段，做好软件安全测试的必要条件有 2 个，一是充分了解软件安全漏洞，二是拥有高效的软件安全测试技术和测试工具。本章将针对安全测试的相关知识进行讲解。

# 5.1 安全测试概述

## 5.1.1 什么是安全测试

安全测试是在 IT 软件产品的生命周期中，特别是产品开发基本完成到发布阶段，对产品进行检验以验证产品符合安全需求定义和产品质量标准的过程，可以说，安全测试贯穿于软件的整个生命周期。下面通过一张图描述软件生命周期各个阶段的安全测试，如图 5-1 所示。

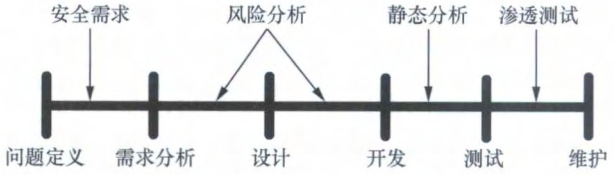


图 5-1 软件生命周期各个阶段的安全测试

图 5-1 中的风险分析、静态分析、渗透测试都属于安全测试的范畴，与前面介绍的普通测试相比，安全测试需要转换视角，改变测试中模拟的对象。下面从以下维度比较常规测试与安全测试的不同。

（1）测试目标不同

普通测试以发现 Bug 为目标；安全测试以发现安全隐患为目标。

（2）假设条件不同

普通测试假设导致问题的数据是用户不小心造成的，接口一般只考虑用户界面；安全测试假设导致问题的数据是攻击者处心积虑构造的，需要考虑所有可能的攻击途径。

（3）思考域不同

普通测试以系统所具有的功能为思考域；安全测试的思考域不但包括系统的功能，还有