渗透测试（Penetration Testing）是指在客户授权许可的情况下，由具备高技能和高素质的安全服务人员发起、在没有网站代码和服务器权限的情况下，模拟常见黑客所使用的攻击手段对目标系统进行模拟全方位渗透入侵测试，来评估企业业务平台和服务器系统的安全性。

渗透测试服务的目的在于充分挖掘和暴露系统的弱点，从而让管理人员了解其系统所面临的威胁。

渗透测试工作往往作为风险评估的一个重要环节，为风险评估提供重要的原始参考数据。

渗透服务内容

漏洞挖掘|修复建议|回归测试

1.安全性漏洞挖掘

找出应用中存在的安全漏洞。应用检测是对传统安全弱点的串联并形成路径，终通过路径式的利用而达到模拟入侵的效果。发掘应用中影响业务正常运行、导致敏感信息泄露、造成现金和信誉损失的等的漏洞。

2.漏洞修复方案

渗透测试目的是防御，故发现漏洞后，修复是关键。安全专家针对漏洞产生的原因进行分析，提出修复建议，以防御恶意攻击者的攻击。

3.复测

漏洞修复后，对修复方案和结果进行有效性评估，分析修复方案的有损打击和误打击风险，验证漏洞修复结果。汇总漏洞修复方案评估结果，标注漏洞修复结果，更新并发送测试报告。

服务对象

安卓应用 | iOS 应用 | 网页应用 | 微信服务号 | 微信小程序

1.安卓应用

对客户端、组件、本地数据、敏感信息、业务等 64 个检测项目进行安全检测

2.iOS 应用

对客户端、策略、通信、敏感信息、业务等 33 个检测项目进行安全检测

3.网页应用

对注入、跨站、越权、CSRF、中间件、规避交易、信息泄露、业务等 67 个检测项进行安全检测

4.微信服务号

对客户端、组件、本地数据、敏感信息、业务等 64 个检测项目进行安全检测

4.微信小程序

根据小程序的开发特性，在 SQL 注入、越权访问、文件上传、CSRF 以及个人信息泄露等漏洞进行检测，防护衍生的重大危害

服务流程

1.意向(1 个工作日)

填写表单：企业填写测试需求；商务沟通：确定测试意向，签订合作合同。

2.启动(1 个工作日)

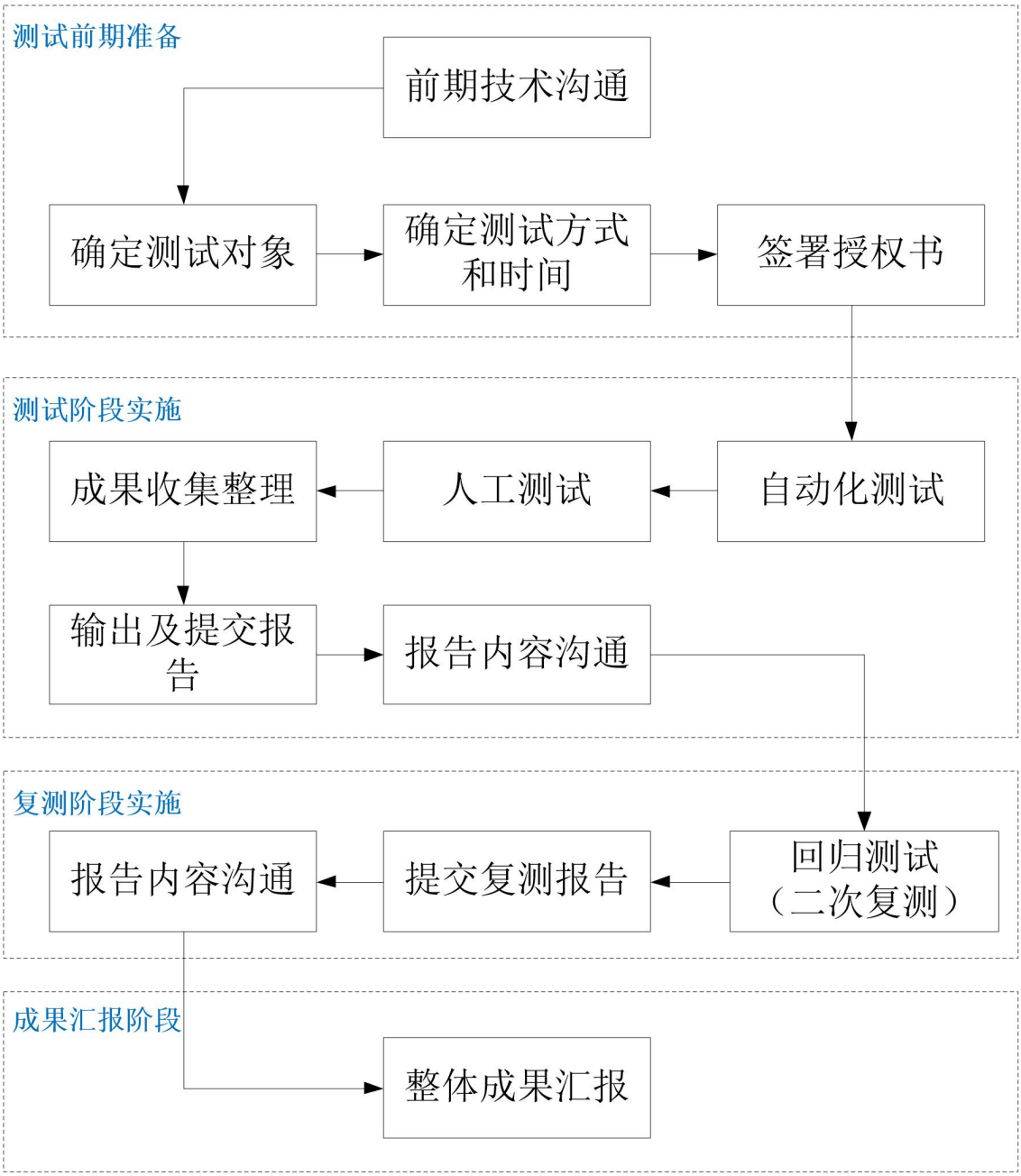
收集材料：系统账号、稳定的测试环境、业务流程等。

3.执行(5-8 个工作日)

风险分析：熟悉系统，进行风险分析，设计测试风险点；漏洞挖掘：安全测试专家分组进行安全渗透测试，提交漏洞；报告汇总：汇总系统风险评估结果和漏洞，发送测试报告。

4.完成(1-5 个工作日)

漏洞修复：企业按照测试报告进行修复；复测：对修复过的环境进行复测确认漏洞已修复。



渗透测试的优势

1. 精英安全专家团队

黑客视角：长期实战钻研于一线企业安全环境下的攻防专家，区别于传统测试，顶尖团队的精湛技术让渗透测试与众不同。

2.针对性更强

紧贴业务：服务会根据业务提供一套专属的攻防方案，深入用户业务，贴近用户需求，快速安全分析，全面深度检测。

3.完善的测试方案

覆盖全面：依据业界安全测试的最佳实践，参考国际标准制定专业的渗透测试检测用例，确保渗透测试过程全面有效。测试范围包括：系统、WEB 应用、移动 APP、网络/IoT/智能设备。

4.项目管理团队

高效执行：渗透测试服务团队由数十位安全专家组成，优秀的安全人才是提供高质量安全服务管理的基础保障。

客户收益

1.避免业务安全隐患

技术层面定性的分析系统的安全性，串联系统安全隐患点，有效验证其存在性及其可利用程度，避免因安全漏洞造成业务损失。

2.提供权威安全保障

出具网站安全认证证书、检测报告、官方标识等权威的正式材料，有效提升用户对业务站点的信任度，促进业务快速成交。

3.助力企业品牌形象

提升企业网站安全实力的同时，展现企业责任心等正面品牌形象，获取用户好感的同时提高业务竞争力，轻易脱颖而出。

4.明确安全隐患点

渗透测试是一个从空间到面再到点的过程，测试人员模拟黑客的入侵，从外部整体切入最终落至某个威胁点并加以利用，最终对整个网络产生威胁，以此明确整体系统中的安全隐患点。

5.提高安全意识

任何的隐患在渗透测试服务中都可能造成“千里之堤溃于蚁穴”的效果，因此渗透测试服务可有效督促管理人员杜绝任何一处小的缺陷，从而降低整体风险。

6.提高安全技能

在测试人员与用户的交互过程中，可提升用户的技能。另外，通过专业的渗透测试报告，也能为用户提供当前流行安全问题的参考。

成功案例

累积为 1872 个客户进行渗透测试。

常见问题

1.测试所取得的信息是否会外泄？

我们绝对不会把任何客户测试数据泄露给第三方。所有测试结果都只会通过报告形式发送给客户。

2.测试结束后是否可高枕无忧？

恶意攻击者的手法层出不穷，不能完全保证不会被新的攻击方式入侵。因此建议定期进行安全性测试。