安全专家服务

渗透测试

腾讯云

【版权声明】

【商标声明】

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

渗透测试
服务概述

最近更新时间：2024-01-25 17:35:02

基本概念

脆弱性

脆弱性也称为弱点，是安全风险中的重要内容。弱点是资产本身存在的，它可以被威胁利用，引起资产或商业目标的损害。弱点包括物理环境、组织、过程、人员、管理、配置、硬件、软件和信息等各种资产的脆弱性。
值得注意的是，弱点是资产本身固有的，但如果没有相应的威胁发生，单纯的弱点不会对资产造成损害。弱点只是一种可能被威胁利用导致资产损失的条件或环境。那些没有安全威胁的弱点可以不需要实施安全保护措施。

渗透测试

渗透测试是一种非常专业的安全服务，通过完全模拟黑客可能使用的漏洞发现技术和攻击技术，对目标系统的安全作深入的探测，发现系统最脆弱的环节。渗透测试能够让管理人员直观地知道自己网络所面临的问题。

客户收益

技术安全性的验证

渗透测试服务作为独立的安全技术服务，其主要目的是验证整个目标系统的技术安全性，亦可针对客户重点业务进行渗透测试，作为一种发现、验证系统风险的重要手段。通过渗透测试，可在技术层面定性地分析系统的安全性。

安全隐患点的发现

渗透测试是对传统安全弱点的串联并形成路径，最终通过路径式的利用达到模拟入侵的效果。在渗透测试的整个过程中，模拟黑客入侵事件可有效的验证每个安全隐患点的存在及其可利用程度,并从中找出企业最急需解决的安全问题，以非常明显直观的结果反映出系统的安全现状。

提供安全加固的依据

渗透测试和工具扫描的结果将一起为日后的安全规划和安全加固等提供重要数据。渗透测试的结果可作为内部安全意识的案例，在对相关的接口人员进行安全教育时使用。

安全技能的提升

渗透测试服务会给用户提供一份测试报告，一份专业的渗透测试报告不但可以为用户提供案例参考，更可作为常见安全原理的学习参考。

服务优势

优势点	优势说明
实施专业可控	腾讯云拥有技术实力一流和攻防经验丰富的专家团队，同时联合腾讯7大安全实验室攻防专家进行前瞻安全漏洞技术研究，洞察最新安全威胁。
安全研究能力	根据客户需求调整测试重点和渗透路径，漏洞统计层次清晰，帮助管理者了解系统风险点分布情况。
安全对抗能力	腾讯身为即时通讯软件平台，长期对抗黑色产业，积累了丰富的安全防护经验，具备先进的安全防护技术，能实时为您保驾护航。
安全实践能力	信息安全建设需要长期进行。腾讯云可提供具备长期履行承诺能力的、保障用户测试服务可长期落地执行的、系统化的解决方案。
规范与保密	腾讯云具备标准规范的流程和良好的风险控制策略，可确保客户私密信息不会外泄。
专业服务团队	全服务团队主要由 CISP、CISSP、CCSK、ISO27001 主任审核员、CCIE 等安全专家，联合腾讯7大安全实验室以及业内领先的安全攻防能力人员组成。
成熟的知识库	腾讯具有行业公认的信息系统全生命周期安全服务的知识库和方法论，同时具备先进的工具，以保障测试维度全面、完善、专业。
大数据风险联动	基于腾讯云海量用户的常见入侵、威胁等数据进行安全分析，将积累的防御对抗经验运用于客户安全建设，达到实践与理论相结合的目的。
精准防护策略	腾讯自身在行业已积累丰富的安全对抗经验，可协助用户输出可全面高效的精准防护策略，快速解决用户痛点问题。

服务内容

最近更新时间：2024-01-25 17:35:01

服务分类

- 腾讯云渗透测试服务的内容是可定制的，根据客户的不同需求，可调整渗透的重点方向，也可以对检测手段进行调整或裁减。
- 渗透测试服务按测试程度的不同，可分为常规渗透和业务逻辑渗透，按渗透目标的不同，可分为公有云与私有云。详见下表：

测试程度	测试目标		交付结果
	公有云	私有云	
常规渗透	远程模拟黑客入侵方式对公有云进行技术攻击测试	现场模拟黑客入侵方式对私有云进行技术攻击测试	输出事件处理报告并提出整改建议
业务逻辑渗透	远程模拟黑客入侵方式对公有云进行业务逻辑测试	现场模拟黑客入侵方式对私有云进行业务逻辑测试	输出事件分析报告并提出整改建议

服务范围

腾讯云安全服务团队提供的渗透测试服务覆盖主流的 IT 基础架构，保证漏洞发现的广泛覆盖。

IT 架构组件	覆盖范围
系统安全	Windows、Linux、Unix、 AIX、Solaris、FreeBSD 等主流操作系统
数据安全	Mysql、PostgreSQL、Microsoft SQL Server、Sybase、Oracle、Firebird、SQLite、DB2、Informix 等主流数据库系统
服务器	IIS、Tomcat、Apache、JBoss、Weblogic 等主流服务器
开发语言	PHP、JSP、ASP 等主流开发语言开发的 Web 应用

测试分类

白盒测试（White-Box Testing）

白盒测试渗透者可以通过正常渠道向被测用户获取各种资料,目的是模拟企业内部雇员的越权操作，通常包括从组织外部和组织内部两种方式进行渗透测试。

黑盒测试（Black-Box Testing）

黑盒测试是除测试目标已公开的信息外，用户不向渗透者提供任何其他信息，最初信息的获取来源为 DNS、Web、email 等对外公开的服务器。渗透者通常只从组织的外部进行渗透测试。

灰盒测试（Grey-Box Testing）

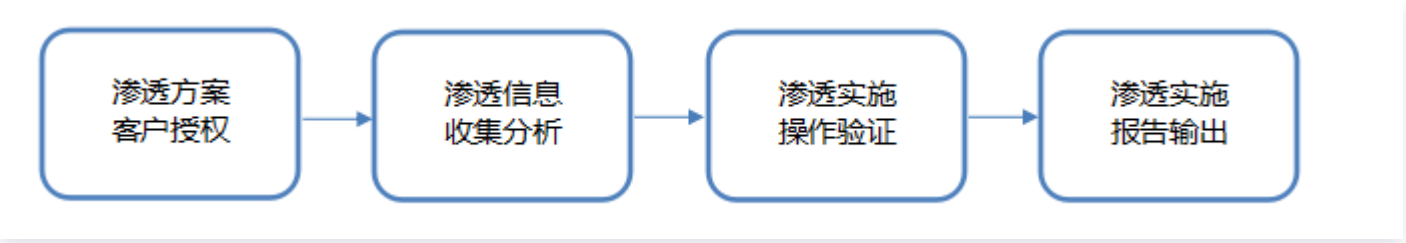
灰盒测试是介于白盒测试与黑盒测试之间的一种测试。灰盒测试被测单位中仅有极少数人知晓测试的存在，渗透测试的目的是检测用户单位中信息安全事件的监控、响应、恢复是否到位。

服务流程

1. 单击 立即申请 进入渗透测试服务申请页面，填写相关信息并提交申请。
2. 在线申请完成后，腾讯云安全专家和销售团队会与客户进行需求沟通，提供服务信息和报价信息。
3. 在确认客户安全需求后，双方签订合同，客户完成付款。
4. 腾讯云会与客户协商实施方式是由腾讯云实施或腾讯云推荐第三方实施（第三方实施过程腾讯云监督审计），实施过程包括渗透方案客户授权、渗透信息收集分析、渗透实施操作验证、渗透实施报告输出，实施完成后输出报告，最后由客户进行服务验收确认。

实施流程

腾讯云渗透测试总体实施流程图如下，实施步骤请详见表格：



渗透方案客户授权

阶段目标	客户知晓方案、流程实施细节，获取客户授权
阶段任务	制定渗透流程、交付实施方案、签署实施申请、客户授权许可
阶段步骤	方案提交、方案讲解、方案认同、方案采纳、实施申请、客户授权
交付成果文档	《渗透测试实施方案》《渗透实施申请报告》

渗透信息收集分析

阶段目标	提高模拟渗透攻击的成功率、有效降低渗透攻击测试的风险
阶段任务	完成目标系统信息采集分析、根据结果提交风险规避方案
阶段步骤	网络收集、端口扫描、系统判别、应用分析、账户扫描、漏洞扫描
交付成果文档	《风险规避措施方案》

渗透实施操作验证

阶段目标	渗透测试获取管理权限、完全控制目标信息系统主机
阶段任务	利用目标漏洞、提升渗透权限、控制目标系统、交付渗透记录
阶段步骤	验证漏洞、获得权限、提升权限、控制系统、渗透收尾、生成记录、问题讨论
交付成果文档	《渗透测试实施记录》

渗透实施报告输出

阶段目标	渗透成果汇报、安全隐患识别、安全意识提高、防护能力增强
阶段任务	交付实施报告、安全建议指导、服务产品验收
阶段步骤	记录整理、生成报告、报告交付、安全建议、服务验收
交付成果文档	《渗透测试实施报告》

购买指南

最近更新时间：2021-07-28 16:15:30

您可以根据 使用流程 提交服务申请，或直接 联系我们 进行购买咨询。

测试技术

最近更新时间：2024-08-07 10:36:41

自动测试

自动测试指借助系统和应用扫描工具对站点的系统层和应用层进行全面的安全扫描，来检测目标系统中是否包含已知的安全问题。

优点

- 借助自动化检测工具，检测速度更快
- 对已知漏洞的检测较为全面

缺点

- 自动化工具对于某些特殊的信息无法实现自动甄别
- 一些复杂的客户端脚本无法完全实现自动检测
- 一些具有较强逻辑性的业务无法通过自动化工具实现检测
- 自动化工具均无法避免误报

手动测试

手动测试作为自动测试的一种补充，会在深度与广度两方面弥补自动化测试的不足，是保障渗透测试质量的一个重要手段，也是渗透测试的精髓所在。手动测试由测试人员进行操作，测试人员的个人技能和经验会直接影响手动测试的结果。
手动测试主要涵盖以下几个方面：

对自动测试结果的验证

自动化检测工具难免存在误报，因而手动测试需要筛选出自动化检测中的误报结果，同时还要对正确告警的结果进行验证和再利用，以确认其危险程度与自动扫描的结果一致。

个性化页面信息的人工甄别

多数自动化测试工具，都是以返回页面中的关键字或 HTTP 的状态值作为判断条件，而某些经过精心构造的个性化页面，其返回内容可能无法完全由自动化工具进行判断，这样的站点就需进行手动测试。

JavaScript 测试

随着 Web2.0 的兴起，JavaScript 被广泛使用，而自动化扫描工具对 JavaScript 脚本的解析能力不强，在自动扫描过程中难免遗漏，因此，需要手动对自动化扫描工具无法解析的、含有 JavaScript 脚本的页面进行二次测试，以检测其安全性。

提交数据的精细化测试

自动化测试在对提交数据进行构造时，其构造方式均遵循一定的规律，而手动测试则可避免这样的问题出现。因此某些可从本地构造恶意数据并提交测试的页面，需手动进行深度测试。

业务逻辑的安全测试

业务逻辑相对来说与程序本身关系不大，无论使用什么样的自动化检测工具都无法检测业务逻辑的正确与否。由此就需要人工先对已有业务逻辑进行分析判断，再结合测试人员的经验对业务逻辑安全性进行必要的检测。

常规漏洞

最近更新时间：2021-07-28 16:27:56

信息泄露

- 常规信息泄露的自动化检测主要是针对某些已知的威胁类型进行的，例如，返回的页面中包含路径信息、某目录存在匿名浏览目录、某文件存在自动备份文件等等。
- 某些信息泄露漏洞往往需要人工介入进行判断，例如，返回信息中存在与目标系统业务具有极大相关性的数据，这些数据的泄露十分危险，但却无法被自动化扫描工具识别，需要人工对此类信息泄露进行挖掘和验证。

注入漏洞

- 注入漏洞有多种注入方式，例如 SQL 注入、XPath 注入、LDAP 注入等等。
- 不同类型的注入漏洞在利用方式和原理上是相似的，但后台存储的数据内容和用户权限决定了注入漏洞所能获得的收益大小。
- 测试人员手动测试注入漏洞时，除验证注入漏洞是否真实存在外，还需对该注入漏洞产生危害的深度与广度进行分析判断，并结合其影响为该注入漏洞设置合理的危险等级。

XSS 与 CSRF 深度利用

多数 Web 扫描器对 XSS 与 CSRF 的识别与测试方式单一，一般情况下，扫描器只能从理论层面验证这类漏洞的存在，但这类漏洞所带来的安全风险，需由人工辅助来完成鉴别与评估。

重定向检测与利用

重定向漏洞往往与其他漏洞一起被结合利用。在传统的自动化评估过程中，难以对重定向漏洞进行识别和深度测试，但通过人工检测的方式，可对重定向漏洞的利用方式及其影响进行重新评估与定义。

参数错误

参数错误分为多种类型，其中涉及到逻辑及权限的错误就难以通过扫描器实现自动识别，对这类错误，往往需要借助渗透工程师的丰富测试经验来进行识别和测试。

认证错误

认证错误包含多层含义，最简单的理解便是用户登录入口暴露（尤其是敏感用户的登录入口，例如管理登录入口），且存在弱口令或暴力破解的可能（例如无验证码的登录页面即可借助暴力破解的方式通过验证）。除此之外，还有某些认证错误是自动化程序无法识别的，例如，登录某系统之后，不再对用户身份进行校验，用户在系统内进行任意操作，或是当用户修改口令时候不对原始口令进行校验，这些漏洞都可能导致普通用户的越权行为。

常用工具

最近更新时间：2021-08-13 17:36:55

报文重放工具

Burp Suite

工具说明

Burp Suite 是用于攻击 Web 应用程序的集成平台，它包含了许多工具，并为这些工具设计了许多接口，以加快攻击应用程序的过程。

下载地址

Burp Suite 下载地址

Fiddler

工具说明

Fiddler 是一个 HTTP 协议调试代理工具，它能够记录并检查您的电脑和互联网之间所有的 HTTP 通讯，设置断点，查看所有“进出” Fiddler 的数据。

下载地址

Fiddler 下载地址

Web 漏洞利用工具

Metasploit

工具说明

Metasploit 是一款开源的安全漏洞检测工具，可以帮助 IT 和安全专业人士识别安全性问题，验证漏洞的缓解措施，并管理专家驱动的安全性评估，提供真正的安全风险情报。这些功能包括智能开发、代码审计、Web 应用程序扫描、社会工程。

下载地址

Metasploit 下载地址

KALI Linux

工具说明

Kali Linux 是基于 Debian 的 Linux 发行版，用于数字取证操作系统。Kali Linux 预装了许多渗透测试软件，包括 nmap 、Wireshark 、John the Ripper 以及 Aircrack-ng。用户可通过硬盘、Live CD 或 Live USB 运行 Kali Linux。Kali Linux 既有32位和64位的镜像，可用于 x86 指令集，同时还有基于 ARM 架构的镜像。

下载地址

KALI Linux 下载地址

其他参考资料

OWASP

相关说明

开放式 Web 应用程序安全项目（OWASP，Open Web Application Security Project）是一个组织，它提供有关计算机和互联网应用程序的公正、实际、有成本效益的信息，其目的是协助个人、企业和机构来发现和使用可信赖软件。

相关地址

OWASP 更多信息

CVE

相关说明

CVE（Common Vulnerabilities and Exposures）即通用漏洞披露，又称常见弱点与漏洞，是一个与资讯安全有关的数据库，收集各种资安弱点及漏洞并给予编号以便于公众查阅。此数据库现由美国非营利组织 MITRE 所属的 National Cybersecurity FFRDC 所营运维护。

相关地址

CVE 更多信息

安全服务承诺

最近更新时间：2020-08-17 10:56:17

为提高安全服务质量，保证安全服务规范，腾讯云计算（北京）有限责任公司特做如下服务承诺：

- 一切安全测试、评估类活动，均遵循国家法律以及双方所约定的合同及补充条款要求。
- 所有执行项目遵循双方约定的服务范围。
- 对于可能造成危害的测试行为需获得服务用户的同意与认可，并在双方约定的可控范围内进行测试。
- 服务人员在整个测试过程中，将遵循内部规范，避免可能存在的风险和隐患。
- 测试结果按双方约定形式，由服务人员撰写报告完整地提供给用户，并按用户要求对内容做出适当的说明。
- 在服务过程中，若因为人工失误造成系统运行异常，服务人员应第一时间通知用户并协助恢复。
- 服务团队遵循安全保密要求，在服务过程中和服务完成后，均不会以任何形式将服务过程中所获取的用户数据泄露给第三方。