web系统安全测试

产品名称	web系统安全测试
公司名称	北京尚拓云测科技有限公司
价格	.00/件
规格参数	
公司地址	北京市朝阳区东三环中路39号建外SOHO11号楼1106
联系电话	010-87713983 15699806440

产品详情

第三方安全测试是在IT企业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。

软件安全测试服务详情

web信息系统安全测试是指有关验证应用程序的安全等级和识别潜在安全性缺陷的过程，主要是测试应用程序层的安全，包括两个层面：

一是应用程序本身的安全性

一般来说，应用程序的安全问题主要是由软件漏洞导致的，这些漏洞可以是设计上的缺陷或是编程上的问题，甚至是企业开发人员预留的后门；

二是应用程序的数据安全

包括数据存储安全和数据传输安全两个方面。

一般来说，对安全性要求不高的软件，其安全性测试可以混在单元测试、集成测试、系统测试里一起做。但对安全性有较高需求的软件，则必须做专门的安全测试，以便在破坏之前预防并识别软件的安全问题。主要目的是查找软件自身程序设计中存在的安全隐患，并检查应用程序对非法侵入的防范能力，根据安全指标不同测试策略也不同。

软件安全测试服务价值

web信息系统安全测试是用来验证集成在软件内的保护机制是否能够在实际中保护系统免受非法的侵入。通俗的说：软件系统的安全当然必须能够经受住正面的攻击——但是它也必须能够经受住侧面的和背后的攻击，才能保证企业的安全运行，CNAS安全检测报告规避企业的安全风险，保证企业立于不败之地。

白盒测试

对软件源代码进行扫描，检测软件源代码中存在的漏洞；提供全面的数据流分析，定位存在漏洞代码段及其路径，找出外部输入能影响到的易损函数。例如：SQL Injections、Cross-Site Scripting等漏洞。

黑盒测试

对正在运行的B/S架构的系统进行动态的渗透性测试，检测B/S架构系统的特定功能点是否存在漏洞，并收集系统泄露的各种信息。例如：HTTP Response Splitting、System Information Leak、Privacy Violation等漏洞。测试工具：Fortify Source Code Analysis Engine、Fortify Security Tester

代码审计（软件源代码安全审查）

（以发现程序错误，安全漏洞和违反程序规范为目标的源代码分析）。
1.密码管理（包括各种常用的加密方式的审查）。
2.跨站脚本（利用http协议的特点，跨站脚本的可能攻击漏洞）。
3.资源管理（数据权限，功能权限的审查）。 4.配置管理（session，错误页面）。
5.检测工具使用（使用Checkstyle进行缺陷模式匹配、FindBugs 缺陷模式匹配及数据流分析、使用PMD 缺陷模式匹配，FindSecurityBugs，fortify）。
6.代码质量的审查。

渗透测试

（选择不影响业务系统正常运行的模拟攻击方法，对主机操作系统、数据库系统、应用系统、网络设备进行渗透测试，评估计算机网络系统安全）。 1.权限管理测试（包括横向越权测试、纵向越权测试、使用kali社会工程学工具包实施测试等）。
2.文件、目录测试（包括目录列表测试、文件归档测试等）。
3.身份认证测试（包括：使用Burp Suite对网络认证服务的攻击、哈希密码破解、密码字典破解等内容）。 4.会话管理测试（包括：身份信息维护方式测试、Cookie存储方式测试、用户注销登录方式测试、注销时会话信息是否清除测试、会话超时测试等）。
5.文件上传、下载测试（包括文件上传测试、下载测试等内容）。
6.信息泄露测试（借助wireshark\fiddler等工具嗅探敏感数据是否泄露）。
7.SQL注入测试（包括：手动SQL注入和借助Sqlmap工具注入等内容）。 8.XSS攻击（包括：XSS漏洞扫描、存储型XSS、DOM型XSS、BeFF-XSS渗透测试框架、BeFF-XSS与Metasploit协同工作等内容）。
9.CSRF攻击（包括：CSRF漏洞扫描、利用条件、检测方法和对策等内容）。
10.WebShell（包括：WebShell检测方法及对策）。 11.无线安全渗透测试（包括无线网络嗅探、使用Aircrack-NG工具破解无线网络、使用Arpspoof实施arp攻击等）。 12.其他渗透测试（包括：逻辑测试，html5安全测试，日志审计，class文件反编译测试，Stru

ts2框架测试等）。

漏洞扫描

（提供包括网络设备、操作系统、数据库、常见应用服务器以及WEB应用等范围的扫描扫描）。 1.AppScan扫描扫描测试（首先利用AppScan对Web应用和服务器进行全面扫描扫描，发现部分漏洞和问题）。 2.使用Nessus/OpenVAS进行漏洞扫描（包括：扫描本地漏洞扫描、网络漏洞扫描、扫描指定Linux的系统漏洞扫描、扫描指定Windows的系统漏洞扫描等内容）。

移动APP安全检测

（包括对移动APP产品进行的代码审计、配置验证、人工验证）。 APP安全检测要点
1、Allowbackup漏洞扫描 2、WebView漏洞扫描 3、关键数据明文传输
4、任意账号注册 5、登录界面可被钓鱼劫持

软件安全测试工具

主要包括：包括：nmap、Sqlmap、Nessus、Appscan、Metasploit、Burp Suite、Aircrack-ng、wireshark\fiddler、Checkstyle，FindBugs，PMD，FindSecurityBugs，fortify等。 1.AppScan扫描测试（首先利用AppScan对Web应用和服务器进行全面扫描，发现部分漏洞和问题）。 2.代码审计（使用Checkstyle进行缺陷模式匹配、FindBugs缺陷模式匹配及数据流分析、使用PMD 缺陷模式匹配，FindSecurityBugs，fortify）。 3.信息收集（使用Nmap、Recon-NG等工具收集Web应用、服务器、网络的信息，包括：运行账号权限测试、服务端口扫描、HTTP方法测试、网络范围测试、服务器其他信息收集等）。 4.使用Nessus/OpenVAS进行漏洞扫描（包括：扫描本地漏洞、网络漏洞、扫描指定Linux的系统漏洞、扫描指定Windows的系统漏洞等内容）。 5.使用Metasploit发起渗透攻击（包括：对操作系统的攻击、对Web应用程序攻击、对mysql数据库的攻击等）。

安全测试过程说明保密性

应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问。
访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作。
应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限。 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。
在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证。
应对通信过程中的敏感信息字段进行加密。

完整性

应采用校验码技术保证通信过程中数据的完整性。 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。
在故障发生时，应用系统应能够继续提供一部分功能，确保能够实施必要的措施。

抗抵赖性

应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计。
应保证无法删除、修改或覆盖审计记录。

可核查性

审计记录的内容至少应包括事件日期、时间、发起者信息、类型、描述和结果等。

真实性

应提供专用的登录控制模块对登录用户进行身份标识和鉴别。 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。
应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

用户鉴别

软件应具备身份鉴别机制检测（用户使用软件过程中是否需要输入用户名和口令）
检测是否具备鉴别失败处理机制 检测是否存在口令或账户登录错误提示混淆

软件容错

检测软件应对异常输入操作进行有效处理

组件安全

软件调用Activity组件的过程中，应确保无法进行权限攻击或劫持 软件调用Broadcast Receiver组件的过程中，应确保无法进行监听或劫持 软件调用Content Provider组件的过程中，应确保无法进行权限攻击
软件调用Intent组件的过程中，应确保无法进行权限攻击

API安全

检测软件调用的API应不包含已知可被利用的漏洞

权限管理

检测软件软件应确保权限最小化

数据输入

检测隐私数据输入时是否明文显示

数据输出

检测软件软件的隐私数据显示应是安全的（隐私信息进行显示时（口令、身份证等），是否进行屏蔽）

数据存储

检测软件记录的隐私信息是否加密处理 检测数据存储位置是否安全

接口安全

软件与服务器通信时，隐私数据应加密

软件测试外包商务流程

1.业务受理：达成合作意向，确认需求，合同签订；
2.测试准备：需求分析，环境准备，资源调配；
3.测试设计：计划方案，用例设计，工具准备；
4.测试执行：环境核查，原始记录，回归测试；
5.报告发布：测评报告起草，报告评审，发布。