永恒无限，源代码审计，代码审计

产品名称	永恒无限，源代码审计，代码审计
公司名称	北京永恒无限科技有限公司
价格	1.00/件
规格参数	网络安全:源代码审计 网络安全:代码审计
公司地址	北京市海淀区万柳东路25号9层902号
联系电话	17778098090

产品详情

源代码审计：

顾名思义就是检查源代码中的安全缺陷，检查程序源代码是否存在安全隐患，或者有编码不规范的地方，通过自动化工具或者人工审查的方式，对程序源代码逐条进行检查和分析，发现这些源代码缺陷引发的安全漏洞，并提供代码修订措施和建议。

源代码审计是一种以发现程序错误，安全漏洞和违反程序规范为目标的源代码分析。软件代码审计是对编程项目中源代码的全面分析，旨在发现错误，安全漏洞或违反编程约定。它是防御性编程范例的一个组成部分，它试图在软件发布之前减少错误。 C和C++源代码是常见的审计代码，因为许多语言（如Python）具有较少的潜在易受攻击的功能（例如，不检查边界的函数）。

对象：

我们的代码审计对象包括并不限于对Windows和Linux系统环境下的以下语言进行审核：java、C、C#、ASP、PHP、JSP、NET。

内容包括

1.前后台分离的运行架构

2.W E B服务的目录权限分类

3.认证会话与应用平台的结合

4.数据库的配置规范

5.S Q L语句的编写规范

6W E B服务的权限配置

7.对抗爬虫引擎的处理措施

审核软件时，应对每个关键组件进行单审核，并与整个程序一起进行审核。 搜索高风险漏洞并解决低风险漏洞是个好主意。 高风险和低风险之间的漏洞通常存在，具体取决于具体情况以及所使用的源代码的使用方式。 应用程序渗透测试试图通过在可能的访问点上启动尽可能多的已知攻击技术来尝试降低软件中的漏洞，以试图关闭应用程序。这是一种常见的审计方法，可用于查明是否存在任何特定漏洞，而不是源代码中的漏洞。 一些人声称周期结束的审计方法往往会压倒开发人员，终会给团队留下一长串已知问题，但实际上并没有多少改进; 在这些情况下，建议采用在线审计方法作为替代方案。