

上海图书馆全文OCR检索功能项目

安全检测报告



2019-10-31

上海双地信息系统有限公司

目 录

[1. 概述 2](#_Toc24015679)

[2. 项目背景 2](#_Toc24015680)

[3. 安全评估方式 3](#_Toc24015681)

[4. 安全评估的必要性 3](#_Toc24015682)

[5. 安全评估方法 4](#_Toc24015683)

[5.1.信息收集 4](#_Toc24015684)

[5.2.权限提升 4](#_Toc24015685)

[5.3.溢出测试 4](#_Toc24015686)

[5.4.SQL注入攻击 5](#_Toc24015687)

[5.5.检测页面隐藏字段 5](#_Toc24015688)

[5.6.跨站攻击 5](#_Toc24015689)

[5.7.第三方软件误配置 5](#_Toc24015690)

[5.8.Cookie利用 5](#_Toc24015691)

[5.9.后门程序检查 6](#_Toc24015692)

[5.10.其他测试 6](#_Toc24015693)

[6. 测试结果 6](#_Toc24015694)

# 概述

安全评估是可以帮助用户对目前自己的网络、系统、应用的缺陷有相对直观的认识和了解。以第三方角度对用户网络安全性进行检查，可以让用户了解从外部网络漏洞可以被利用的情况，安全顾问通过解释所用工具在探查过程中所得到的结果，并把得到的结果与已有的安全措施进行比对。

# 项目背景

《全国报刊索引》创立于1955年，是上海图书馆（上海科学技术情报研究所）主管主办并倾力打造的知名信息服务品牌。

上海图书馆的中文报刊文献馆藏在海内外具有举足轻重的地位。1955年，在国家文化部的委托下，上海图书馆创办了《全国报刊索引》杂志，旨在汇聚和揭示全国出版发行的所有报刊文献资源内容，它也成为国内最早出版发行的综合性中文报刊文献检索工具。

六十余年来，《全国报刊索引》已由最初的月刊，发展成为集印刷版与网络服务平台为一体的综合性知识服务体系，现可提供5万余种报刊、5000余万篇文献的一站式服务，年更新数据量超过500万条，相继挖掘出版了《晚清期刊全文数据库》（1833～1911）、《民国时期期刊全文数据库》（1911～1949）、《字林洋行中英文报全文纸数据库》（1850～1951）等珍稀数字资源。

为了给读者用户带来更好的使用体验，网络服务平台历经多次改版升级，逐步优化平台架构、扩充服务功能，努力实现知识服务的全面性、多样性与互动性，为读者用户提供更专业化、规范化、人性化的数字资源服务。凭借珍贵丰富的资源收藏、专业的二次文献组织和深度的知识挖掘，《全国报刊索引》以精致的服务获得了海内外用户的广泛认可，并致力于成为中国近代报刊数字文献资源的权威知识服务体系。

随着资源加工的逐步深入，以中国近代中文期刊全文数据库（简称全文OCR）为代表的精品资源不断加入到服务平台的资源序列中，而目前的服务平台在对这些精品资源的服务呈现上难以发挥精品资源的内在价值，亟需进行服务功能的升级，让这些资源得到充分揭示，满足广大用户的专业服务需求。

# 安全评估方式

安全评估主要依据安全工程师已经掌握的安全漏洞和安全检测工具，采用工具扫描 + 手工验证的方式。模拟黑客的攻击方法在客户的授权和监督下对客户的系统和网络进行非破坏性质的攻击性测试。

# 安全评估的必要性

安全评估利用网络安全扫描器、专用安全测试工具和富有经验的安全工程师的人工经验对授权测试环境中的核心服务器及重要的网络设备，包括服务器、防火墙等进行非破坏性质的模拟黑客攻击，目的是侵入系统并获取机密信息并将入侵的过程和细节产生报告给用户。

安全评估和工具扫描可以很好的互相补充。工具扫描具有很好的效率和速度，但是存在一定的误报率和漏报率，并且不能发现高层次、复杂、并且相互关联的安全问题；安全评估需要投入的人力资源较大、对测试者的专业技能要求很高（安全评估报告的价值直接依赖于测试者的专业技能），但是非常准确，可以发现逻辑性更强、更深层次的弱点。

# 安全评估方法

## 5.1.信息收集

信息收集分析几乎是所有入侵攻击的前提/前奏/基础。“知己知彼，百战不殆”，信息收集分析就是完成的这个任务。通过信息收集分析，攻击者（测试者）可以相应地、有针对性地制定入侵攻击的计划，提高入侵的成功率、减小暴露或被发现的几率。

本次评估主要是启用网络漏洞扫描工具，通过网络爬虫测试网站安全、检测流行的攻击 、如交叉站点脚本、SQL注入等。

## 5.2.权限提升

通过收集信息和分析，存在两种可能性，其一是目标系统存在重大弱点：测试者可以直接控制目标系统，这时测试者可以直接调查目标系统中的弱点分布、原因，形成最终的测试报告；其二是目标系统没有远程重大弱点，但是可以获得远程普通权限，这时测试者可以通过该普通权限进一步收集目标系统信息。接下来，尽最大努力获取本地权限，收集本地资料信息，寻求本地权限升级的机会。这些不停的信息收集分析、权限升级的结果构成了整个安全评估过程的输出。

## 5.3.溢出测试

当无法直接利用帐户口令登陆系统时，也会采用系统溢出的方法直接获得系统控制权限，此方法有时会导致系统死机或从新启动，但不会导致系统数据丢失，如出现死机等故障，只要将系统重新启动并开启原有服务即可。

## 5.4.SQL注入攻击

SQL注入常见于那些应用了SQL 数据库后端的网站服务器，黑客通过向提交某些特殊SQL语句，最终可能获取、篡改、控制网站 服务器端数据库中的内容。此类漏洞是黑客最常用的入侵方式之一。

## 5.5.检测页面隐藏字段

网站应用系统常采用隐藏字段存储信息。许多基于网站的电子商务应用程序用隐藏字段来存储商品价格、用户名、密码等敏感内容。心存恶意的用户，通过操作隐藏字段内容，达到恶意交易和窃取信息等行为，是一种非常危险的漏洞。

## 5.6.跨站攻击

攻击者可以借助网站来攻击访问此网站的终端用户，来获得用户口令或使用站点挂马来控制客户端。

## 5.7.第三方软件误配置

第三方软件的错误设置可能导致黑客利用该漏洞构造不同类型的入侵攻击。

## 5.8.Cookie利用

网站应用系统常使用cookies 机制在客户端主机上保存某些信息，例如用户ID、口令、时间戳等。黑客可能通过篡改cookies 内容，获取用户的账号，导致严重的后果。

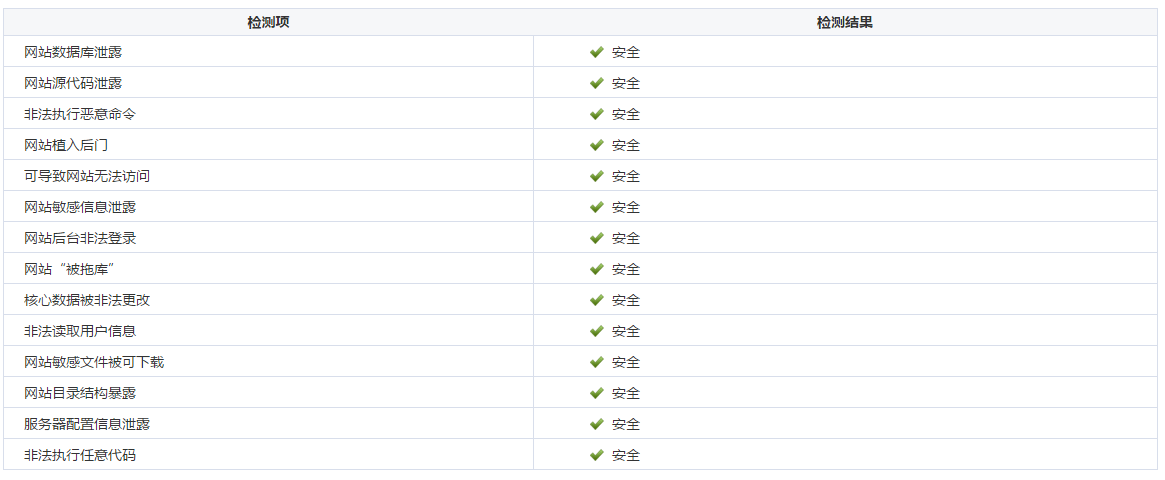
## 5.9.后门程序检查

系统开发过程中遗留的后门和调试选项可能被黑客所利用，导致黑客轻易地从捷径实施攻击。

## 5.10.其他测试

在安全评估中还需要借助暴力破解、网络嗅探等其他方法，目的也是为获取用户名及密码。

# 测试结果



从测试报告来看，系统无严重漏洞，可以提供较为安全的服务。