网络安全测试报告

系统名称：晨光科力普电商平台

委托单位：上海晨光科力普办公用品有限公司

****

**2019年05月**

**保密声明**

本报告涉及上海晨光科力普办公用品有限公司（以下简称“上海晨光科力普”）的敏感信息，仅限于上海晨光科力普和上海市网络技术综合应用研究所（以下简称“网综所”）所有，未经双方书面许可，请勿扩散到第三方，违者追究法律责任。

本报告内容泄密或将导致下述风险：

* 利用本报告披露的敏感信息发起对上海晨光科力普信息系统入侵攻击；
* 增加入侵成功的可能性。

**文档属性**

|  |  |  |  |
| --- | --- | --- | --- |
| **属性** | **内 容** | | |
| **被测单位名称** | 上海晨光科力普办公用品有限公司 | | |
| **项目名称** | 上海晨光科力普办公用品有限公司信息安全等级保护测评项目 | | |
| **文档主题** | 上海晨光科力普办公用品有限公司信息系统网络安全测试报告 | | |
| **保密级别** | 高 | | |
| **扩散范围** | * 上海晨光科力普办公用品有限公司 | | |
| * 上海市网络技术综合应用研究所管理层 | | |
| * 上海市网络技术综合应用研究所项目组 | | |
| **版本号** | 1.1 | | |
| **文档状态** | 发布 | | |
| **编制** | Xxx | **日 期** |  |
| **QA** | 祁雯华 | **日 期** |  |
| **审核** | 马威 | **日 期** |  |

**分发控制**

|  |  |  |  |
| --- | --- | --- | --- |
| **编号** | **读者** | **权限** | **与文档主要关系** |
| 1 | 上海市网络技术综合应用研究所项目组 | 创建、修改、读取 | 项目组成员负责编制、修改、  审核本文档 |
| 2 | 项目经理 | 批准 | 项目经理，负责本文档的批准  程序 |
| 3 | 上海晨光科力普办公用品有限公司 | 读取、建议 | 最终用户 |

目录

[报告摘要 1](#_Toc8657088)

[风险分布 1](#_Toc8657089)

[1. 概述 2](#_Toc8657090)

[1.1 测试目的 2](#_Toc8657091)

[1.2 测试范围 3](#_Toc8657092)

[1.3 测试依据和原则 3](#_Toc8657093)

[1.3.1 依据 3](#_Toc8657094)

[1.3.2 原则 3](#_Toc8657095)

[1.4 测试工具与方法 4](#_Toc8657096)

[1.5 测试时间 5](#_Toc8657097)

[2. 测试内容 5](#_Toc8657098)

[2.1 代码层测试 6](#_Toc8657099)

[2.2 应用层测试 8](#_Toc8657100)

[2.3 系统层测试 9](#_Toc8657101)

[3. 测试结果分析 10](#_Toc8657102)

[3.1 （http://cip.colipu.com/） 10](#_Toc8657103)

[3.1.1 越权访问 10](#_Toc8657104)

[3.1.2 暴力破解 11](#_Toc8657105)

[3.1.3 Web应用默认目录泄露 12](#_Toc8657106)

[3.1.4 明文传输 13](#_Toc8657107)

[3.1.5 访问控制 14](#_Toc8657108)

[3.1.6 js文件中内部IP泄露 15](#_Toc8657109)

[3.1.7 启用了OPTIONS方法 16](#_Toc8657110)

[4. 总结和建议 16](#_Toc8657111)

## 报告摘要

网综所评估团队通过对信息系统的综合评估，发现上海晨光科力普办公用品有限公司存在多个区域，存在众多子系统，系统的总体复杂度高。导致其中一部分系统导入了风险，存在安全突破口，形成了IT风险点。针对晨光科力普电商平台测试评估，发现的主要问题如下：

* 越权访问
* 暴力破解
* Web应用默认目录泄露
* 明文传输
* 访问控制
* js文件中内部IP泄露
* 启用了OPTIONS方法

通过综合评估，该套信息系统处于**较不安全**状态。

建议从下述几个方面进行改进：

* 在每个敏感页面判断用户登录状态和访问权限，避免越权访问；
* 正确配置验证码，限制用户登录失败次数；
* 对重要敏感数据进行加密后使用https传输；
* 增加每个页面的访问控制，返回到登录页；
* 验证登录逻辑的时候，强制让Session过期；
* 部署行为监控系统，针对入侵行为实时监控和对抗，增加IPS等设备；
* 加强各网段之间隔离措施，尤其是核心网段；
* 与外部安全团队加强合作，持续强化IT安全力量配备。

以下章节含有专业内容，建议供专业人士阅读。

## 风险分布

经委托单位授权，上海市网络技术综合应用研究所对被测系统（http://cip.colipu.com/）进行了网络安全测试。

安全风险分布图如下：

安全风险分布图

高危问题：2个

* 越权访问
* 暴力破解

中危问题：3个

* Web应用默认目录泄露
* 明文传输
* 访问控制

低危问题：2个

* js文件中内部IP泄露
* 启用了OPTIONS方法

# 概述

## 测试目的

通过网络安全测试，了解被测系统运行环境的安全风险，运用最新漏洞库全面检测被测系统的漏洞，清晰定位安全风险，给出修复建议和预防措施，并对风险控制策略进行有效审核，从而在全面评估的基础上实现自主掌控。

## 测试范围

本次安全评估测试对象为上海晨光科力普的晨光科力普电商平台

## 测试依据和原则

### 依据

在本次安全评估过程中，参考业界信息安全相关标准和监管规范对被测系统进行安全评估，主要参考的标准规范如下：

* 《信息技术 安全技术 信息技术安全性评估准则》GB/T 18336-2001
* 《信息系统安全保障评估框架》GB/T 20274-2006
* 《web安全危险分类标准》
* 《OWASP 十大web应用安全威胁》

### 原则

在本次安全评估中，主要遵循以下原则对被测系统进行安全评估：

* 标准性原则：评估方案的设计和具体实施都严格依据国内和国外的相关标准及理论模型来执行。
* 规范性原则：评估过程中的工作开展和文档编写，均具有很好的规范性，以便于评估工作的跟踪和控制；
* 可控性原则：评估工作所采用的工具均经过多次评估项目考验，并在WEB网络环境中经过严格测试，在专业工作人员的指导和监督下开展评估工作，具有很好的可控性。
* 整体性原则：评估工作从实际需求出发，从技术、管理和业务等各个角度进行评估，涵盖物理、网络、系统、应用、数据、安全、管理和业务等多个层面。
* 最小影响原则：评估工作做到充分的计划性，并做好系统备份和应急预案，不对现有网络系统的运行和业务的正常开展产生较大影响，尽可能将风险降低到最小程度。
* 保密性原则：签订保密协议，项目组成员不带出有关此次评估的现场数据，不泄露与此次评估有关的评估结果，不做出有损利益的任何行为，做到对评估数据严格保密。

## 测试工具与方法

在本次安全评估中，使用了系统漏洞扫描、应用漏洞扫描、网络通信检查等技术评估工具，主要工具如下表：

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **工具名称** | **版本号** | **工具用途** |
| 1 | Kali linux | 2018.3 | 渗透测试平台 |
| 2 | Nessus漏洞扫描系统 | 7.0.3 | 漏洞扫描 |
| 3 | APPSCAN | 9.0.3.6 | WEB安全检测 |
| 4 | AWVS | 11.0 | WEB安全检测 |
| 5 | BurpSuite | 2.05 | WEB安全检测 |
| 6 | SQLMAP | 1.2.4 | 注入检测 |
| 7 | Wireshark | 2.4.3.0 | 网络嗅探 |
| 8 | Nmap | 7.70 | 网络扫描探测工具 |

漏洞扫描：根据已有的安全漏洞知识库，利用漏洞扫描工具，扫描网络设备、防火墙、服务器、数据库等，发现被测系统的安全漏洞。

**配置测试流程：**

采用如下图所示检查列表：

**是**

**客户委托**

**信息收集、分析**

**控制系统**

**信息收集、分析**

**本地信息收集、分析**

**信息收集、分析**

**生成报告**

**是**

**否**

**是**

**是**

**否**

**否**

**否**

**是**

**客户委托**

**信息收集、分析**

**存在远程控制弱点**

**控制系统**

**存在远程普通弱点**

**信息收集、分析**

**获取本地普通权限**

**本地信息收集、分析**

**本地权限升级、控制系统**

**信息收集、分析**

**生成报告**

**是**

**否**

**是**

**是**

**否**

**否**

**否**

网络安全测试：在委托单位的授权下通过模拟入侵者攻击方式，对被测系统进行安全测试，以发现系统中存在的安全问题。本次测试包括信息泄露测试、配置管理测试、认证测试、授权测试、会话管理测试、数据检测测试、主程序、WEB站点、同步程序等几个方面。

## 测试时间

参照网络安全测试授权书约定的时间。

# 测试内容

网络安全测试对授权网站进行全面的安全检查，其中包括3个层面：

* 代码层
* 应用层
* 系统层

## 代码层测试

应用程序及代码在开发过程中，由于开发者缺乏安全意识，疏忽大意极为容易导致应用系统存在可利用的安全漏洞。一般包括SQL注入漏洞、跨站脚本漏洞、上传漏洞、CSRF跨站请求伪造漏洞等。

1. **SQL注入漏洞**

SQL注入漏洞的产生原因是网站程序在编写时，没有对用户输入数据的合法性进行判断，导致应用程序存在安全隐患。SQL注入漏洞攻击就是利用现有应用程序没有对用户输入数据的合法性进行判断，将恶意的SQL命令注入到后台数据库引擎执行的入侵者攻击手段。

1. **跨站脚本漏洞**

跨站脚本攻击简称为XSS又叫CSS (Cross Site Script Execution)，是指服务器端的CGI程序没有对用户提交的变量中的HTML代码进行有效的过滤或转换，允许攻击者往WEB页面里插入对终端用户造成影响或损失的HTML代码。

1. **会话管理漏洞**

会话管理主要是针对需授权的登录过程的一种管理方式，以用户密码验证为常见方式，通过对敏感用户登录区域的验证，可有效校验系统授权的安全性，测试包含以下部分：

* 用户口令易猜解

通过对表单认证、HTTP认证等方式的简单口令尝试，以验证存在用户身份校验的登录入口是否存在易猜解的用户名和密码。

* 是否存在验证码防护

验证码是有效防止暴力破解的一种安全机制，通过对各登录入口的检查，以确认是否存在该保护机制。

* 是否存在易暴露的管理登录地址

某些管理地址虽无外部链接可介入，但由于采用了容易猜解的地址（如：admin）而导致登录入口暴露，从而给外部恶意用户提供了可乘之机。

* 是否提供了不恰当的验证错误信息

某些验证程序返回错误信息过于友好，如：当用户名与密码均错误的时候，验证程序返回“用户名不存在”等类似的信息，通过对这一信息的判断，并结合HTTP Fuzzing工具便可轻易枚举系统中存在的用户名，从而为破解提供了机会。

会话管理主要是针对验证通过之后，服务端程序对已建立的、且经过验证的会话的处理方式是否安全，一般会从以下几个角度检测会话管理的安全性。

* Session是否随机

Session作为验证用户身份信息的一个重要字符串，其随机性是避免外部恶意用户构造Session的一个重要安全保护机制，通过抓包分析Session中随机字符串的长度及其形成规律，可对Session随机性进行验证，以此来确认其安全性。

* 校验前后Session是否变更

通过身份校验的用户所持有的Session应与其在经过身份验证之前所持有的Session不同。

* 会话储存是否安全

会话存储是存储于客户端本地（以cookie的形式存储）还是存储于服务端（以Session的形式存储），同时检测其存储内容是否经过必要的加密，以防止敏感信息泄露。

1. **不安全的对象引用**

不安全的对象引用是指程序在调用对象的时候未对该对象的有效性、安全性进行必要的校验，如：某些下载程序会以文件名作为下载程序的参数传递，而在传递后程序未对该参数的有效性和安全性进行检验，而直接按传递的文件名来下载文件，这就可能造成恶意用户通过构造敏感文件名而达成下载服务端敏感文件的目的。

1. **跨站请求伪造**

跨站请求伪造（Cross-site request forgery，缩写为CSRF），也被称成为“one click attack”或者session riding，通常缩写为CSRF或者XSRF，是一种对网站的恶意利用。尽管听起来像跨站脚本（XSS），但它与XSS非常不同，并且攻击方式几乎相左。XSS利用站点内的信任用户，而CSRF则通过伪装来自受信任用户的请求来利用受信任的网站。与XSS攻击相比，CSRF攻击往往不大流行（因此对其进行防范的资源也相当稀少）和难以防范，所以被认为比XSS更具危险性。

1. **越权漏洞**

越权访问(Broken Access Control，简称BAC)，是一种在web程序中常见的安全缺陷，其原理是对用户提交的参数不进行权限检查和跨越访问控制而造成的。

## 应用层测试

由于应用系统和数据库系统开发配置的具体过程中，可能由于管理员缺乏安全意识或疏忽大意导致应用层存在安全隐患。

1. **弱口令**

弱口令通常有以下几种情况：用户名和密码是系统默认、口令长度过短、口令选择与本身特征相关等。系统、应用程序、数据库存在弱口令可以导致入侵者直接得到系统权限、修改盗取数据库中敏感数据、任意篡改页面等。

1. **敏感信息泄露**

敏感信息泄露漏洞指泄露有关WEB应用系统的信息，例如，用户名、物理路径、目录列表和软件版本。尽管泄露的这些信息可能不重要，然而当这些信息联系到其他漏洞或错误设置时，可能产生严重的后果。例如：某源代码泄露了SQL服务器系统管理员帐号和密码，且SQL服务器端口能被攻击者访问，则密码可被攻击者用来登录SQL服务器，从而访问数据或运行系统命令。

1. **安全配置错误**

某些HTTP应用程序，或第三方插件，在使用过程中由于管理人员或开发人员的疏忽，可能未对这些程序或插件进行必要的安全配置和修改，这就很容易导致敏感信息的泄露。而对于某些第三方插件来说，如果存在安全隐患，更有可能对服务器获得部分控制权限。

1. **链接地址重定向**

重定向就是通过各种的方法将各种网络请求重新定个方向转到其它位置（如：网页重定向、域名的重定向、路由选择的变化也是对数据报文经由路径的一种重定向）。

而某些程序在重定向的跳转过程中，对重定向的地址未进行必要的有效性和安全性检查，且该重定向地址又很容易被恶意用户控制和修改，这就可能导致在重定向发生时，用户会被定向至恶意用户事先构造好的页面或其他URL，而导致用户信息受损。

## 系统层测试

由于服务器系统和网络设备研发生产过程中所固有的安全隐患及系统管理员或网络管理员的疏忽，一般网络层安全漏洞包括弱口令、敏感信息泄露，严重甚至存在系统远程溢出漏洞等安全漏洞。

1. **弱口令**

弱口令通常有以下几种情况：用户名和密码是系统默认、口令长度过短、口令选择与本身特征相关等。系统、应用程序、数据库存在弱口令可以导致入侵者直接得到系统权限、修改盗取数据库中敏感数据、任意篡改页面等。

1. **敏感信息泄露**

敏感信息泄露漏洞指泄露有关WEB应用系统的信息，例如，用户名、物理路径、目录列表和软件版本。尽管泄露的这些信息可能不重要，然而当这些信息联系到其他漏洞或错误设置时，可能产生严重的后果。例如：某源代码泄露了SQL服务器系统管理员帐号和密码，且SQL服务器端口能被攻击者访问，则密码可被攻击者用来登录SQL服务器，从而访问数据或运行系统命令。

1. **安全配置错误**

服务器系统、数据库系统及网络设备在使用过程中由于管理人员或开发人员的疏忽，可能未对这些默认配置进行必要的安全配置和修改，这就很容易引起越权操作，从而导致信息泄露或篡改。

1. **远程溢出漏洞**

溢出漏洞的产生是由于程序中的某个或某些输入函数（使用者输入参数）对所接收数据的边界验证不严密而造成。根据程序执行中堆栈调用原理，程序对超出边界的部分如果没有经过验证自动去掉，那么超出边界的部分就会覆盖后面的存放程序指针的数据，当执行完上面的代码，程序会自动调用指针所指向地址的命令。根据这个原理，恶意使用者就可以构造出溢出程序。

1. **恶意代码**

恶意代码泛指没有作用却带来危险的代码，其普遍的特征是具有恶意的目的；本身是一个独立的程序，通过执行发生作用。由于应用系统存在可被利用的安全漏洞，可能已被恶意人员植入恶意代码以获取相应权限或用以传播病毒。

# 测试结果分析

## （http://cip.colipu.com/）

### 越权访问

|  |  |
| --- | --- |
| **问题名称** | 越权访问 |
| **风险等级** | 高 |
| **问题描述** | 系统并没有判断用户的访问权限，导致越权访问，攻击者通过越权访问可能获得更多有利于入侵的条件，进而进一步的入侵系统。      2、直接访问登陆后的链接，无需登录直接可以访问 |
| **相关URL/IP** | http://cip.colipu.com/views/home/welcome.html#!/user/index |
| **修改建议** | 在每个敏感页面判断用户登录状态和访问权限，避免越权访问。 |

### 暴力破解

|  |  |
| --- | --- |
| **问题名称** | 暴力破解 |
| **风险等级** | 高 |
| **问题描述** | 登录页面没有验证码、限制登录失败次数等防爆破措施，恶意攻击者可以通过POST方式通过暴力破解获取正确的用户名及密码。如图： |
| **相关URL/IP** | 帐号：[chenfeilong@colipu.com](mailto:chenfeilong@colipu.com) 密码：123456  帐号：[yangying@colipu.com](mailto:yangying@colipu.com) 密码：7758521 |
| **修改建议** | 1、增加验证码。  2、限制用户登录失败次数（注:同一帐号登录3-5次失败，锁定10-30分钟)  3、用户密码需符合密码复杂度要求（超过8位，并包含大小写字母、数字及特殊符号）；  4、系统注意验证识别后销毁session中的验证码；  5、判断提交的验证码与服务器上存储的是否一致；  6、无论是否一致，都将服务器上存储的验证码清空；  7、页面跳转，产生登录错的时候就跳到另一个页面要求重新登录，做适当的延时，识别暴力破解行为，封锁多次暴力破解的IP。 |

### Web应用默认目录泄露

|  |  |
| --- | --- |
| **问题名称** | Web应用默认目录泄露 |
| **风险等级** | 中 |
| **问题描述** | Web应用架构中的目录都采用常见的目录名。如图片目录images，javascript目录js，不同的目录潜在的危险是不同的。攻击者一般利用常见目录中可能包含的敏感文件获取敏感信息。  本漏洞属于Web应用安全常见漏洞。 |
| **相关URL/IP** | 1、<http://cip.colipu.com/scripts/configcenter/com/status/>  2、http://cip.colipu.com/scripts/configcenter/com/ |
| **修改建议** | 如果不需要这些目录，可以删除此类目录；或者严格限制目录的访问权限。 |

### 明文传输

|  |  |
| --- | --- |
| **问题名称** | 明文传输 |
| **风险等级** | 中 |
| **问题描述** | 该风险是导致数据泄露、数据篡改、流量劫持、钓鱼攻击等安全问题的重要原因之一。HTTP协议无法加密数据，所有通信数据都在网络中明文“裸奔”。攻击者可以通过中间人攻击的手法，截获服务器与客户端的通信数据。并且用户密码未加密。 |
| **相关URL/IP** | http://cip.colipu.com/ |
| **修改建议** | 建议先对敏感关键数据进行加密后使用https进行传输。 |

### 访问控制

|  |  |
| --- | --- |
| **问题名称** | 访问控制 |
| **风险等级** | 中 |
| **问题描述** | 经测试，地理信息平台系统存在一些访问控制不足的情况，用户在未登录情况下可访问以下页面，并可看到相关数据，如图： |
| **相关URL/IP** | 1、http://cip.colipu.com:7024/#/property  2、<http://cip.colipu.com:7024/#/colipu>  3、http://cip.colipu.com:7024/#/PropertyGenerate  4、  http://cip.colipu.com/views/home/welcome.html#!/configcenter/com/index |
| **修改建议** | 1. 增加每个页面的访问控制，增加session认证； 2. 返回到自定义的默认错误页或返回登录页。 |

### js文件中内部IP泄露

|  |  |
| --- | --- |
| **问题名称** | js文件中内部IP泄露 |
| **风险等级** | 低 |
| **问题描述** | 内部IP定义为下列 IP 范围内的IP：  10.0.0.0 - 10.255.255.255  172.16.0.0 - 172.31.255.255  192.168.0.0 - 192.168.255.255  对攻击者而言，泄露内部 IP 非常有价值，因为它显示了内部网络的 IP 地址方案。知道内部网络的IP地址方案，可以辅助攻击者策划出对内部网络进一步的攻击。 |
| **相关URL/IP** | http://cip.colipu.com/scripts/configcenter/com/gateway.js |
| **修改建议** | 内部IP通常显现在Web应用程序/服务器所生成的错误消息中，或显现在HTML/JavaScript注释中。  [1] 关闭 Web 应用程序/服务器中有问题的详细错误消息。  [2] 确保已安装相关的补丁。  [3] 确保内部 IP 信息未留在 HTML/JavaScript 注释中。 |

### 启用了OPTIONS方法

|  |  |
| --- | --- |
| **问题名称** | 启用了OPTIONS方法 |
| **风险等级** | 低 |
| **问题描述** | OPTIONS方法是用于请求获得由Request-URI标识的资源在请求/响应的通信过程中可以使用的功能选项。通过这个方法，客户端可以在采取具体资源请求之前，决定对该资源采取何种必要措施，或者了解服务器的性能。OPTIONS方法可能会暴露一些敏感信息，这些信息将帮助攻击者准备更进一步的攻击。 |
| **相关URL/IP** | http://cip.colipu.com/ |
| **修改建议** | 1、限制这些文件的访问权限；  2、将这些文件放置在受保护的目录中。 |

# 总结和建议

经测试发现，目前被测系统存在一些缺陷，主要包括如下几点：

1. 越权访问，在每个敏感页面判断用户登录状态和访问权限，避免越权访问。
2. 暴力破解，建议正确配置验证码，限制用户登录失败次数。
3. Web应用默认目录泄露，建议如果不需要这些目录，可以删除此类目录；或者严格限制目录的访问权限。
4. 明文传输，建议对重要敏感数据进行加密后使用https传输。
5. 访问控制，建议增加每个页面的访问控制，返回到登录页。
6. js文件中内部IP泄露，建议关闭Web应用程序/服务器中有问题的详细错误消息。
7. 启用了OPTIONS方法，建议限制这些文件的访问权限或将这些文件放置在受保护的目录中。

信息系统的安全应当从“探虚实、练内功、勤体检”三方面来防范安全风险。系统上线之前一定要进行安全测试，排查安全漏洞，摸清系统防护水平，根据评估结果对系统进行整改加固，增强抗攻击能力；对于已经上线的系统，应定期进行漏洞扫描、渗透测试、挂马检测等“体检”，防范新的安全漏洞出现。另外，虽然技术上的问题可以通过各种措施加以解决，但重要的还是提升员工信息安全意识，安全管理必须引起足够重视。另外，在信息系统的开发、获取、运维等过程中，应充分考虑安全风险的因素，确保系统的先天健壮性。