上海久科信息技术有限公司

2016年9月30日

作者：久科产品研发部

上海久科有限公司

安全扫描设计说明书

**保 密**

本文件及其内容为上海久科信息技术有限公司保密资料。本文件及其内容永远属于上海久科信息技术有限公司拥有财产，在无上海久科信息技术有限公司采用书面形式表示同意外，本文件

1. 不可以用于其他非原指定用途；
2. 不可以向第三方披露；
3. 不可采用任何形式进行复制和传播，包括但不限于传真、纸张邮件和电子邮件。

**文档修改历史**

|  |  |  |  |
| --- | --- | --- | --- |
| **版 本** | **修改人** | **日 期** | **描 述** |
| V1.0 | mike | 20160930 | 版本创建 |
|  |  |  |  |
|  |  |  |  |

目录

[1 概述 5](#_Toc460518229)

[1.1 本文目的 5](#_Toc460518230)

[1.2 适用范围 5](#_Toc460518231)

[1.3 术语与缩略词 5](#_Toc460518232)

[1.4 运行环境 5](#_Toc460518233)

[1.5 参考文档 6](#_Toc460518234)

[2 总体说明 6](#_Toc460518235)

[2.1 系统密码（PC） 6](#_Toc460518236)

[2.2 在线客服系统XSS 9](#_Toc460518237)

[2.3 图形验证码规则 10](#_Toc460518238)

[2.4 内部IP泄露 10](#_Toc460518239)

[2.5 应用程序错误泄露 10](#_Toc460518240)

[2.6 访客端文件上传 11](#_Toc460518241)

[2.7 访客留言信息提交 15](#_Toc460518242)

[2.8 反射性跨站脚本漏洞 18](#_Toc460518243)

# 需求分析摘要

## 系统密码流程修改

创建公司使用的公司ID为Root的root账号的密码要改为any800!。手动创建公司默认账号any800，默认密码any800。系统初始密码默认为any800。修改密码时，要求复杂度包括字母、数字、特殊符号（任选2种）且长度介于6-16位之间。输入新密码登陆后，可在坐席端-个人设置中修改或在后台的客服管理中进行修改。密码修改满足密码修改规则，不满足时的提示语为：“请输入6-16位的英文、数字、字符（空格除外）”。

客服坐席账号密码需求如下：允许尝试失败的次数: 最低=5（管理员账号除外，其他账号登录5次失败后，该账号处于锁定状态，不能登录了。对于已经锁定的账号24小时后，自动解锁或由管理员解锁对于锁定的账号，在后台将该账号的状态置为禁用，需要管理员登录后台将该客服的状态重新设置为正常。对应的界面如下图所示。

## 在线客服系统XSS,访客留言信息提交,反射性跨站脚本漏洞

服务器端接收消息增加javascript语言判断,对用户输入的数据进行全面安全检查或过滤,过滤的内容主要为标签定义

## 访客端文件上传

访客端,服务器端对上传文件的类型进行判断，从服务器端校验禁止上传非允许类型的文件。仅允许上传图片（png、jpg、jpeg、bmp、gif为后缀的图片）、Word（.doc、.docx）、Excel（.xls、.xlsx）、PDF（.pdf）。

## 应用程序错误泄露

页面错误信息可能泄露敏感信息，如web服务器版本、数据库信息等，使攻击者掌握更多系统信息以发动进一步的攻击，使用同一的错误页面，对用户屏蔽服务器数据库的信息。

# 整体设计

## 系统技术架构

//用来描述系统整体软件模块结构图，包括用到的第三方软件。

## 系统部署拓扑图

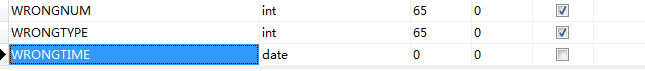
//描述项目、产品实际服务器部署结构图，其中包括部署的mysql、mongodb、cassandra、redis等软件。

# 详细设计

## 系统密码流程修改

### 算法流程

### 数据库表变更



alter table ecoperator add WRONGNUM int(65) not NUll;//记录失败次数

alter table ecoperator add WRONGTYPE int(65) not NUll;//记录失败类型是密码输入错误

alter table ecoperator add WRONGTIME date;//记录失败时间

### 接口设计

/\*\*

\* 激活失败的访客

\*

\* @param companyPk 公司名

\* @param name 访客编号

\* @return

\*/

public void enableOperatorWrong(String name,String companyPk);

/\*\*

\* 访客失败禁止登陆

\*

\* @param companyPk 公司名

\* @param name 访客编号

\* @return

\*/

public void disableOperatorWrong(String name,String companyPk);

/\*\*

\* 增加失败次数

\*

\* @param companyPk 公司名

\* @param name 访客编号

\* @return

\*/

public void increaseOperatorWrong(String name,String companyPk);

### 程序设计

/\*\*HomeController.java

\* 做用户登录操作 跳转到主页

\*

\* **@author** 王彬

\* **@2012**-04-12

\* **@param** request

\* **@param** response

\* **@return**

\* **@throws** Exception

\*/

@Override

**protected** ModelAndView defaultHandler(HttpServletRequest request, HttpServletResponse response) **throws** Exception {

/\*\*\*\*\*\*\*\*\*以上省略\*\*\*\*\*\*\*\*\*/

EcoperatorDTO ecdto = TalkHessianHelper.*getRemoteService*().getOperatorByName(name,company);

// 判断用户名是否存在或者是否被禁用

**if** (dto == **null**) {

msg = "账号输入错误,请重新输入";

model.addObject("msg", msg);

**return** model;

}

//出现5次并且不超过24小时非主动关闭,ACTIVE==0

**if**( ecdto.getWrongType() == 1 && ecdto.getActive()==0 && ecdto.getWrongNum()>=5){

**if**(**new** Date().getTime()-ecdto.getWrongTime().getTime()<24\*60\*60\*1000){

msg = "密码输入错误5次,账号被锁定";

model.addObject("msg", msg);

**return** model;

}**else**{

//超过24小时,修改表

TalkHessianHelper.*getRemoteService*().enableOperatorWrong(name,company);

}

}

**if** (dto.getActive() == 0) {

msg = "用户账号被禁用,无法登陆";

model.addObject("msg", msg);

**return** model;

}

// 判断密码是否正确

**if** (opdto == **null**) {

**if** (password == **null** || password.equals("")) {

msg = "请输入密码";

model.addObject("msg", msg);

**return** model;

}

// boolean isAdmin = false;

// if (loginName.equals("admin")) {

// isAdmin = true;

// }

String dtoPassword = "";

**if** (loginType.equals("client")) {

dtoPassword = TalkHessianHelper.*getRemoteService*().getEncryptedPassword(name,company);

}**else**{

dtoPassword = TalkHessianHelper.*getRemoteService*().getPassword(name,company);

}

**if** (!password.equals(dtoPassword)) {

EcroleDTO role = TalkHessianHelper.*getRemoteService*().getRoleById(dto.getRolePk());

**if**(!role.getName().equals("超级管理员")){

TalkHessianHelper.*getRemoteService*().increaseOperatorWrong(name,company);

**if**(ecdto.getWrongNum()>=4){

TalkHessianHelper.*getRemoteService*().disableOperatorWrong(name,company);

}

}

msg = "密码输入错误,请重新输入";

model.addObject("msg", msg);

**return** model;

}

}

**if**(!loginType.equals("client")){

**if**(!vercode.equalsIgnoreCase(\_vercode)){

msg = "验证码错误";

model.addObject("msg", msg);

**return** model;

}

}

TalkHessianHelper.*getRemoteService*().enableOperatorWrong(name,company);

/\*\*\*\*\*\*\*以下省略\*\*\*\*\*\*\*\*/

}

### 出错处理设计

## 在线客服系统XSS,访客留言信息提交,反射性跨站脚本漏洞

### 算法流程

### 数据库表变更

### 接口设计

*//提示：重点描述模块间的调用接口，包括函数名、输入、输出参数、返回值含义。*

### 程序设计

/\*\*

\*StringEscapeEditor.java

\*\*/

package com.nineclient.filter;

import java.beans.PropertyEditorSupport;

import org.springframework.web.util.HtmlUtils;

import org.springframework.web.util.JavaScriptUtils;

public class StringEscapeEditor extends PropertyEditorSupport {

private boolean escapeHTML;// 编码HTML

private boolean escapeJavaScript;// 编码JavaScript

public StringEscapeEditor() {

super();

}

public StringEscapeEditor(boolean escapeHTML, boolean escapeJavaScript) {

super();

this.escapeHTML = escapeHTML;

this.escapeJavaScript = escapeJavaScript;

}

@Override

public String getAsText() {

Object value = getValue();

return value != null ? value.toString() : "";

}

@Override

public void setAsText(String text) throws IllegalArgumentException {

if (text == null) {

setValue(null);

} else {

String value = text;

if (escapeHTML) {

value = HtmlUtils.htmlEscape(value);

}

if (escapeJavaScript) {

value = JavaScriptUtils.javaScriptEscape(value);

}

setValue(value);

}

}

}

/\*\*

\*HomeController.java

\*\*/

**public** **abstract** **class** BaseController **extends** MultiActionController {

@InitBinder

**public** **void** initBinder(ServletRequestDataBinder binder) {

binder.registerCustomEditor(Date.**class**, **new** CustomDateEditor(**new** SimpleDateFormat("yyyy-MM-dd HH:mm:ss"), **true**));

binder.registerCustomEditor(String.**class**, **new** StringEscapeEditor(**true**, **false**));

}

}

### 出错处理设计

## 访客端文件上传

### 算法流程

### 数据库表变更

### 接口设计

*//提示：重点描述模块间的调用接口，包括函数名、输入、输出参数、返回值含义。*

### 程序设计

/\*\*

\*ucc.js

\*\*/

**var** settings = {

flash\_url : "flashChart/swfupload.swf",

upload\_url: baseUrl+'/echatManager.do?method=uploadFile',

file\_size\_limit : "10 MB",

file\_types : "\*.png;\*.jpg;\*.jpeg;\*.bmp;\*.gif;\*.doc;\*.docx;\*.xls;\*.xlsx;\*.pdf",

file\_types\_description : "Web Files",

file\_upload\_limit : 10, // 配置上传个数

file\_queue\_limit : 0,

custom\_settings : {

progressTarget : "fsUploadProgress",cancelButtonId : "btnCancel"

},

debug: **false**,

button\_image\_url:"style/images/echat2.0/sbbg2.png",

button\_width: "60",

button\_height: "25",

button\_text\_top\_padding:"4",

button\_text\_left\_padding:"12",

button\_placeholder\_id: "s\_b",

button\_text: '<span class="theFont">浏览</span>',

button\_text\_style: ".theFont { font-size:12;color:#FFFFFF;}",

file\_queued\_handler : **function**(f){

$('.p\_r').css("width",0);

**if**(f.name.length >=20){

f.name = f.name.substring(0,20)+"...";

}

$('.fname').html(f.name);

},

file\_queue\_error\_handler : **function**(f,e,m){

**if**(e == -110){

$('.fname').html("文件大于10MB，请重新选择文件");

}

},

file\_dialog\_complete\_handler : **function**(numFilesSelected,numFilesQueued){

// this.startUpload();

},

upload\_start\_handler : **function**(file){},

upload\_progress\_handler : **function**(file, bytesLoaded, bytesTotal){

**var** percent = Math.ceil((bytesLoaded / bytesTotal) \* 100);

$('.p\_r').css("width",percent+"%");

},

upload\_error\_handler : **function**(file, errorCode, message){},

upload\_success\_handler : **function**(file, serverData){

**var** url = serverData.split("|");

**if**(url[0] == "t"){

**var** fileUrl = url[1];

**var** txt = '访客发送了一个文件：<a class = "download" target="\_blank" href="'+fileUrl+ '">下载</a>';

**var** imags = ["jpg","jpeg","bmp","gif","png"];

**for**(i **in** imags){

**if**(fileUrl.indexOf(imags[i]) != -1){

// --方式的文件包含文件.

txt+="<br><img id='img' src='"+fileUrl+"'>";

}

}

chatManager.sendMessage(txt,"send\_file");

chatManager.showMessage("v",txt);

pEventM.doRefreshTime();//计算超时提醒

}

},

upload\_complete\_handler : **function**(file){

$('.fname').append("<br>上传文件成功！");

setTimeout(**function**(){

$('#uploader').hide();

$('.p\_r').css("width",0);

$('.fname').html("");

},2000);

},

queue\_complete\_handler : **function**(numFilesUploaded){}

};

### 出错处理设计

## 应用程序错误泄露

### 算法流程

### 数据库表变更

### 接口设计

*//提示：重点描述模块间的调用接口，包括函数名、输入、输出参数、返回值含义。*

### 程序设计

/\*\*

\*web.xml

\*\*/

<error-page>

<error-code>403</error-code>

<location>/error.jsp</location>

</error-page>

<error-page>

<error-code>404</error-code>

<location>/error.jsp</location>

</error-page>

<error-page>

<error-code>500</error-code>

<location>/error.jsp</location>

</error-page>

### 出错处理设计

# 系统环境配置

## 开发环境配置

*//提示：说明本系统应当在什么样的环境下运行，有什么强制要求和建议？*

|  |  |  |
| --- | --- | --- |
| 类别 | 标准配置 | 最低配置 |
| 计算机硬件 |  |  |
| 软件 |  |  |
| 网络通信 |  |  |
| 其它 |  |  |

## 运行环境配置

*//提示：说明本系统应当在什么样的环境下运行，有什么强制要求和建议？*

|  |  |  |
| --- | --- | --- |
| 类别 | 标准配置 | 最低配置 |
| 计算机硬件 |  |  |
| 软件 |  |  |
| 网络通信 |  |  |
| 其它 |  |  |

## 测试环境配置

*//提示：说明本系统应当在什么样的环境下测试，有什么强制要求和建议？*

*（1）一般地，单元测试、集成测试环境与开发环境相同。*

*（2）一般地，系统测试、验收测试环境与运行环境相同或相似（更加严格）。*