# 白盒审计记录四

2018年5月2日 14:13

**51javacms**

恭喜您，系统已经安装成功！

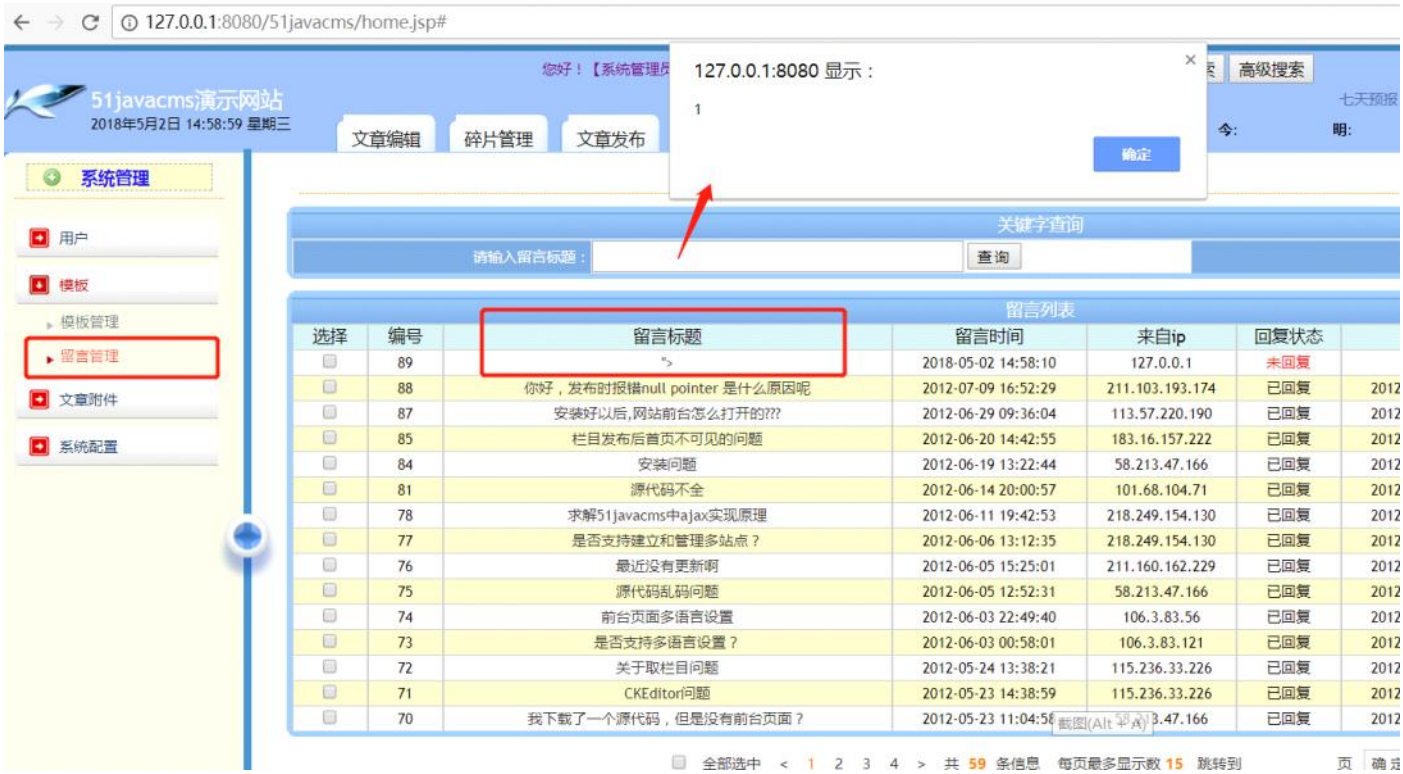
cms登录地址： “http://127.0.0.1:8080/51javacms/sign_in.jsp”

cms管理员：**admin**， 密码：**51javacms**。

主编：**chief_editor**， 密码：**51javacms**。

第一个xss

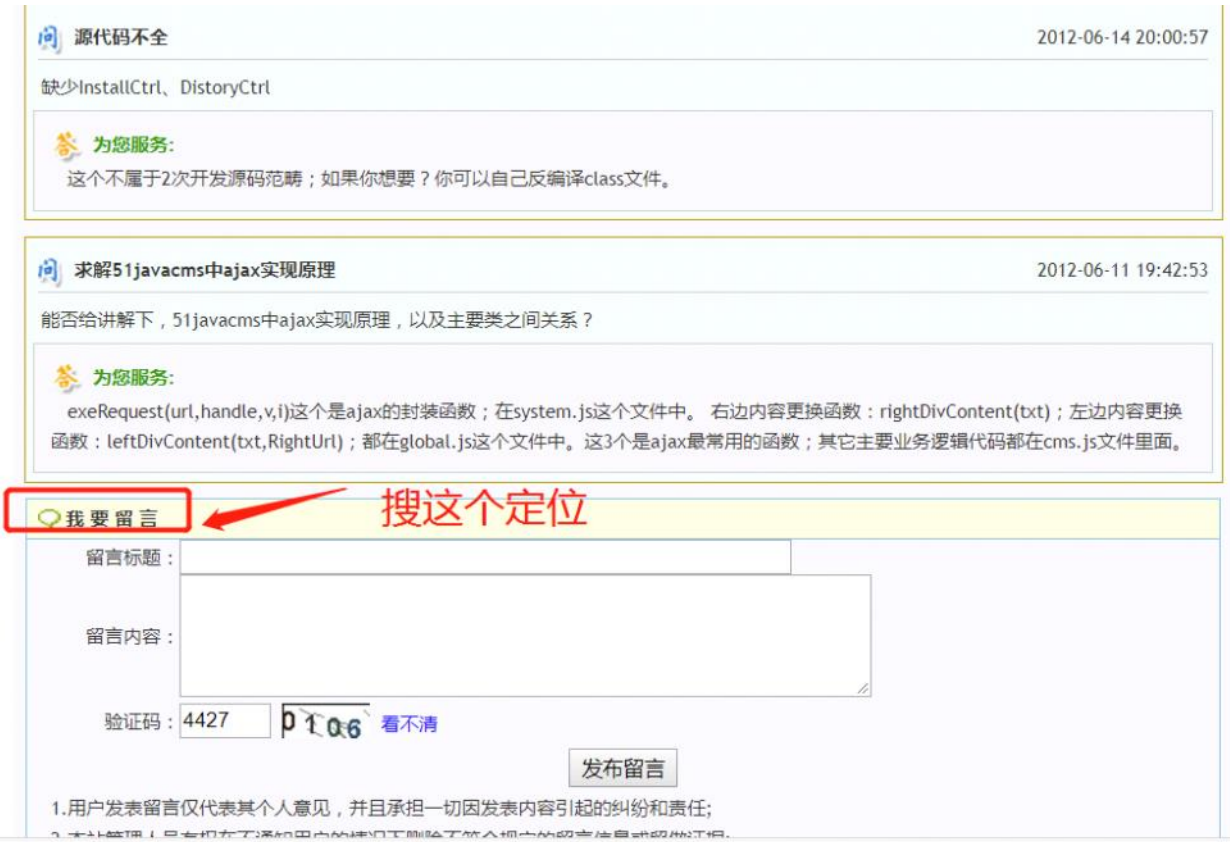
留言处xss，效果图




分析过程

先来看下这个留言页面：

全局搜一下：我 要 留 言



找到：

```
/img/plugin/answer.gif" border="0" align="absmiddle"/>
服务:</span><br />   <%=messages[i].getReply() %></div>

ng="0" width="98%" bgcolor="#7dbfdb" align="center" style="margin-top: 10px; margin-bottom: 10px">

gn="left">  <img border="0" alt="留言板" align="absMiddle" width="14" height="12" src="<%=request.getContextPath()%>/img/plugin/liuyan.gif" /> <strong>我 要 留 言</strong></td>

lign="top">
ellpadding="0" width="98%" align="center">
```

路径是：C:\Users\zheng\Desktop\install\51javacms\jsp\plugin\message\message.jsp

看下这个表单提交按钮的方法

```
59          <table border="0" cellspacing="0" cellpadding="0" width="98%" align="center">
60            <tbody>
61              <tr>
62                <td width="66" align="right">留言标题： </td>
63                <td width="478" align="left"><input id="title" class="required" maxlength="50" size="56" maxlength="30"  type="text" /></td>
64              </tr>
65              <tr>
66                <td height="25" align="right">留言内容： </td>
67                <td align="left"><textarea id="content" class="required" rows="5" cols="66" maxlength="255" ></textarea></td>
68              </tr>
69              <tr>
70                <td height="30" align="right">验证码： </td>
71                <td align="left"><input id="certify" class="required" title="请输入验证码" size="4"  type="text" />
72                 <img id="reg_random" src="<%=request.getContextPath()%>/RandomCodeCtrl" border="0"  />
73                 <a href="javascript:randomChangeReg('reg_random');"><font color="blue">看不清</font></a></td>
74              </tr>
75              <tr>
76                <td height="30" colspan="2" align="center"><input type="button" value="发布留言" onclick="submitMsg();" /></td>
77              </tr>
78            </tbody>
79          </table>
80        <table border="0" cellspacing="0" cellpadding="0" width="98%" align="center">
81          <tbody>
82            <tr>
83              <td align="left" style="line-height: 20px">  1.用户发表留言仅代表其个人意见，并且承担一切因发表内容引起的纠纷和责任;<br />
84                2.本站管理人员有权在不通知用户的情况下删除不符合规定的留言信息或留做证据;<br />
85                3.请客观的评价您所看到的资讯，提倡就事论事，杜绝漫骂和人身攻击等不文明行为.</td>
86            </tr>
87          </tbody>
```

全局搜submitMsg()这个方法，是个js方法。在

C:\Users\zheng\Desktop\install\51javacms\js\plugin\plugin.js

```
function submitMsg(){
 if($("title").value.trim()==''){
       alert("请输入留言标题。");
       $("title").focus();
 }else  if($("content").value.trim()==''){
            alert("请输入留言内容。");
            $("content").focus();
 }else if($("certify").value.length!=4){
            alert("留言验证码是4位数字。");
            $("certify").focus();
 }else if(!isNumCheck($("certify").value.trim())){
            alert("留言验证码是大于0的数字。");
            $("certify").focus();
       }else{
            exeRequest(rootUrl+"/PluginCtrl",returnMsg,
                       "page=PublishMessagePage&title="+encodeURIComponent($("title").
                       value.trim())+
                       "&content="+encodeURIComponent($("content").value.trim())+
                       "&certify="+$("certify").value.trim());
       }
}
```

```
1  function submitMsg(){
2    if($("title").value.trim()==''){
3      alert("请输入留言标题。");
4      $("title").focus();
5    }else  if($("content").value.trim()==''){
6      alert("请输入留言内容。");
7      $("content").focus();
8    }else if($("certify").value.length!=4){
9      alert("留言验证码是4位数字。");
10     $("certify").focus();
11   }else if(!isNumCheck($("certify").value.trim())){
12     alert("留言验证码是大于0的数字。");
13     $("certify").focus();
14   }else{
15     exeRequest(rootUrl+"/PluginCtrl",returnMsg,
16                "page=PublishMessagePage&title="+encodeURIComponent($("title").value.trim())+
17                "&content="+encodeURIComponent($("content").value.trim())+
18                "&certify="+$("certify").value.trim());
19   }
20 }
21 function returnMsg(txt){
22     alert(txt);
23     randomChangeReg('reg_random');
24     contiueAll();
25 }
26 function randomChangeReg(obj){
27     $(obj).src=rootUrl+'/RandomCodeCtrl?'+Math.random();
28 }
```

```
Find result - 2 hits
Search "submitMsg" (2 hits in 2 files)
  C:\Users\zheng\Desktop\install\51javacms\js\plugin\plugin.js (1 hit)
    Line 1: function submitMsg(){
  C:\Users\zheng\Desktop\install\51javacms\jsp\plugin\message\message.jsp (1 hit)
    Line 76:                <td height="30" colspan="2" align="center"><input type="button" value="发布留言" onclick="submitMsg();" /></td>
Search "submitMsg()" (0 hits in 0 files)
Search "我 要 留 言" (1 hit in 1 file)
Search "留言标题" (1 hit in 1 file)
Search "留言标题" (1 hit in 1 file)
```

这里只对提交的内容判断是否为空，并没有做任何的校验和过滤。

然后将留言标题，内容发送到后台留言管理

后台留言管理通过一下代码来接受这个message对象

MainCtrl.java | message_list.jsp | message.jsp | plugin.js

```jsp
<%@page contentType="text/html;charset=utf-8"%>
<%@page import="javabean.UserInfo"%>
<%@page import="javabean.Message" %>
<%@page import="util.Constant"%>
<%@page import="util.PubFun"%>
<%@page import="util.InitServlet"%>
<%/***************session fail****************************/
    UserInfo userInfo = (UserInfo)session.getAttribute("userInfo");
    Message[] messages = (Message[])request.getAttribute("messages");
    if (userInfo==null){
        response.sendRedirect(request.getContextPath() + Constant.ORGINAL_LOGIN_PAGE);
        return;
    }%>
<!--main div begin-->
<input type="hidden" id="page" value="MessageManagePage"></input>
<div id="maindiv" class="maindivelse">
    <span class="linktextbutton">
        <span>当前的位置：系统管理 \ 模板 \ 留言管理
    </span>
```

这个messages对象对应的类如下：

```
package javabean;

import java.util.Date;

//插件：留言板表plugin_Message
public class Message{
	private long id; //主键ID
	private String title; //留言标题
	private String message; //留言信息
	private String reply; //回复信息
	private Date creatime; //留言时间
	private String ip; //留言来自的ip
	private Date replytime; //回复时间
	private int replyer; //回复人
	private boolean replied; //回复状态

	/******* 计算字段 ********/
	private String replyName; // 回复人名字

	public String getReplyName() {
		return replyName;
	}
	public void setReplyName(String replyName) {
		this.replyName = replyName;
	}
	public long getId() {
		return id;
	}
	public void setId(long id) {
		this.id = id;
	}
	public String getTitle() {
		return title;
	}
	public void setTitle(String title) {
		this.title = title;
	}
	public String getMessage() {
		return message;
	}
	public void setMessage(String message) {
		this.message = message;
	}
	public String getReply() {
		return reply;
	}
	public void setReply(String reply) {
		this.reply = reply;
	}
	public Date getCreatime() {
		return creatime;
	}
	public void setCreatime(Date creatime) {
		this.creatime = creatime;
	}
	public String getIp() {
		return ip;
	}
	public void setIp(String ip) {
		this.ip = ip;
	}
	public Date getReplytime() {
		return replytime;
	}
	public void setReplytime(Date replytime) {
		this.replytime = replytime;
	}
	public int getReplyer() {
		return replyer;
	}
	public void setReplyer(int replyer) {
		this.replyer = replyer;
	}
	public boolean isReplied() {
		return replied;
	}
	}
```

```
    public void setReplied(boolean replied) {
        this.replied = replied;
    }
}
```

这个类对象定义了留言这个类流对象的数据结构

我们再看下这里的输出

```
                    }else{
                        className = "tablelisttext3rt";
                    }%>
                    <td class="<%=className%>"><input type="checkbox" name="checks_name" value="<%=messages[i].getId()%>"></td>
                    <td class="<%=className%>"><%=messages[i].getId()%></td>
                    <td class="<%=className%>"><a href="javascript:showReplyMessage(<%=messages[i].getId()%>,${pageNo})" ><%=messages[i].getTitle() %></a></td>
                    <td class="<%=className%>"><%=PubFun.getDateTime("yyyy-MM-dd HH:mm:ss",messages[i].getCreatime())%></td>
                    <td class="<%=className%>"><%=messages[i].getIp() %></td>
                    <td class="<%=className%>"><%=messages[i].isReplied()?"已回复":"<font color=\"red\">未回复</font>" %></td>
                    <td class="<%=className%>"><%=messages[i].getReplytime()==null?"":PubFun.getDateTime("yyyy-MM-dd HH:mm:ss",messages[i].getReplytime()) %></td>
                    <td class="<%=className%>"><%=messages[i].getReplyName()==null?"":messages[i].getReplyName()%></td>
                    <td class="<%=className%>"><a href="javascript:showReplyMessage(<%=messages[i].getId()%>,${pageNo});">回复</a>
                         <a href="javascript:delMessage(<%=messages[i].getId()%>,${pageNo});">删除</a>
                    </td>
                </tr><%}%>
            </table>
            <!-- table list end -->
```

这里是通过messages这个对象的getTitle方法来获取标题。

```
public String getTitle() {
    return title;
}
```

这里直接就返回了title，并没有对输出做实体编码

这里其实我们已经找到了所有的关键点，但是，有一个地方不看下，还是觉得有点不甘心，那

就是

```
    <!--menu_round-->
        <div class="RoundedCornertitle">
            <b class="rtop"><b class="r1"></b><b class="r2"></b><b class="r3"></b><b class="r4"></b></b>
        </div>
        <div class="topdiv">
            <font style="color:purple;">您好！【<%=userInfo.getAlias().equals("")?userInfo.getName():userInfo.getAlias()%>】</font>
             <a href="<%=InitServlet.WEB_SITE_URL%>" target="_blank">【站点首页】</a> 
            <a href="<%=request.getContextPath()%>/PluginCtrl?page=ShowMessagePage" target="_blank">【留言板】</a>
            <%if(userInfo.getName().equals(Constant.SUPER_USER) || userInfo.getName().equals(Constant.CHIEF_EDITOR)){%>
      文章标题：<input type="text" id="search_title" />
<input type="button" value="搜索" onclick="exeRequest(rootUrl+'/MainCtrl',rightDivContent,'page=SearchArticlePage&search_title='+encod
<input type="button" value="高级搜索" onclick="exeRequest(rootUrl+'/jsp/article/advanced_search.jsp',rightDivContent);"/><%}%></div>
    <div id="menulist">
        <span style="float:left;"><img src="img/logo.png"/></span>
```

按照这个说法这应该是一个servlet

```
Find result - 14 hits
  C:\Users\zheng\Desktop\install\51javacms\jsp\plugin\message\message.jsp (1 hit)
    Line 26:     <form action="<%=request.getContextPath()%>/PluginCtrl" method="post" name="page_form">
  C:\Users\zheng\Desktop\install\51javacms\template\51javacms\head.jsp (1 hit)
    Line 16:             <li><a href="http://${header["host"]}${pageContext.request.contextPath}/PluginCt
  C:\Users\zheng\Desktop\install\51javacms\template\51javacms\index.jsp (1 hit)
    Line 21:                     <a class="download_btn" href='http://${header["host"]}${pageContext.requ
  C:\Users\zheng\Desktop\install\51javacms\template\system\browse_cnt.jsp (1 hit)
  C:\Users\zheng\Desktop\install\51javacms\template\system\feeling.jsp (2 hits)
    Line 56:    exeRequest('http://${header["host"]}${pageContext.request.contextPath}/PluginCtrl',
    Line 59: exeRequest('http://${header["host"]}${pageContext.request.contextPath}/PluginCtrl',
  C:\Users\zheng\Desktop\install\51javacms\WEB-INF\classes\PluginCtrl.class (2 hits)
    Line 2: PluginCtrlBEL
    Line 20: SourceFileSOH
  C:\Users\zheng\Desktop\install\51javacms\WEB-INF\web.xml.bak (4 hits)
    Line 27:        <servlet-name>PluginCtrl</servlet-name>
    Line 28:        <servlet-class>PluginCtrl</servlet-class>
    Line 53:        <servlet-name>PluginCtrl</servlet-name>
    Line 54:        <url-pattern>/PluginCtrl</url-pattern>
```

然而这个servlet被编译成了.class文件，无法查看其中的源码。所以我们需要反编译下这个文件 PluginCtrl.class，这里我使用的是java decompiler来对这个.class文件进行反编译，获得

PluginCtrl源码

```
import java.io.IOException;
import java.io.PrintStream;
import java.util.Map;
import javax.servlet.RequestDispatcher;
import javax.servlet.ServletException;
import javax.servlet.http.*;
import page.inc.HtmlPage;
import util.PubFun;

public class PluginCtrl extends HttpServlet
{

  public PluginCtrl()
  {
  }

  protected void doPost(HttpServletRequest req, HttpServletResponse resp)
    throws ServletException, IOException
  {
    String jspStr = null;
    resp.setContentType("text/html; charset=utf-8");
    req.setCharacterEncoding("utf-8");
    HtmlPage page = initHtmlPage(req.getParameter("page"));
    if(page == null)
    {
      resp.sendRedirect("MainCtrl?page=LogoutPage");
      return;
    }
    try
    {
```

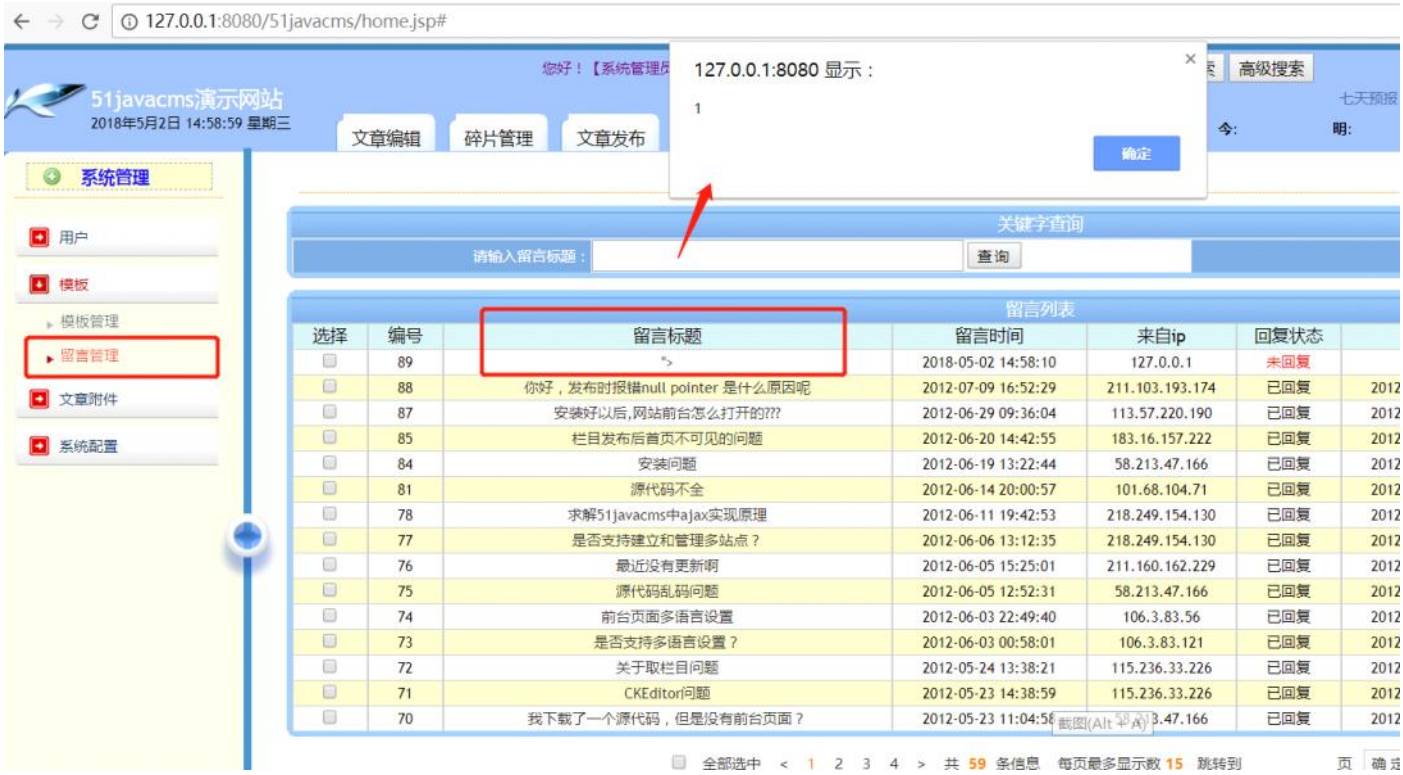
```
            jspStr = page.print(req, resp);
        }
        catch(Exception e)
        {
            if(jspStr == null)
            {
                PubFun.ajaxPrintC(e.getMessage(), resp);
            } else
            {
                req.setAttribute("inf", e.getMessage());
                jspStr = "/view_info.jsp";
            }
            System.out.println(e.getMessage());
        }
        if(jspStr != null)
            req.getRequestDispatcher(jspStr).forward(req, resp);
    }

    protected void doGet(HttpServletRequest req, HttpServletResponse resp)
        throws ServletException, IOException
    {
        doPost(req, resp);
    }

    private HtmlPage initHtmlPage(String page)
    {
        if(page == null || page.trim().length() == 0)
        {
            return null;
        } else
        {
            page = page.trim();
            return (HtmlPage)PubFun.getPluginPageMap().get(page);
        }
    }

    private static final long serialVersionUID = 1L;
}
```

这里是实现了post和get方法对应的操作，并没有做任何过滤校验的操作。

最后我们使用xss测试语句来测试一下漏洞是否存在

测试语句："><img src=l oneeror=alert(1)>

进入留言管理，果然触发了xss代码。




第二个xss（误报）

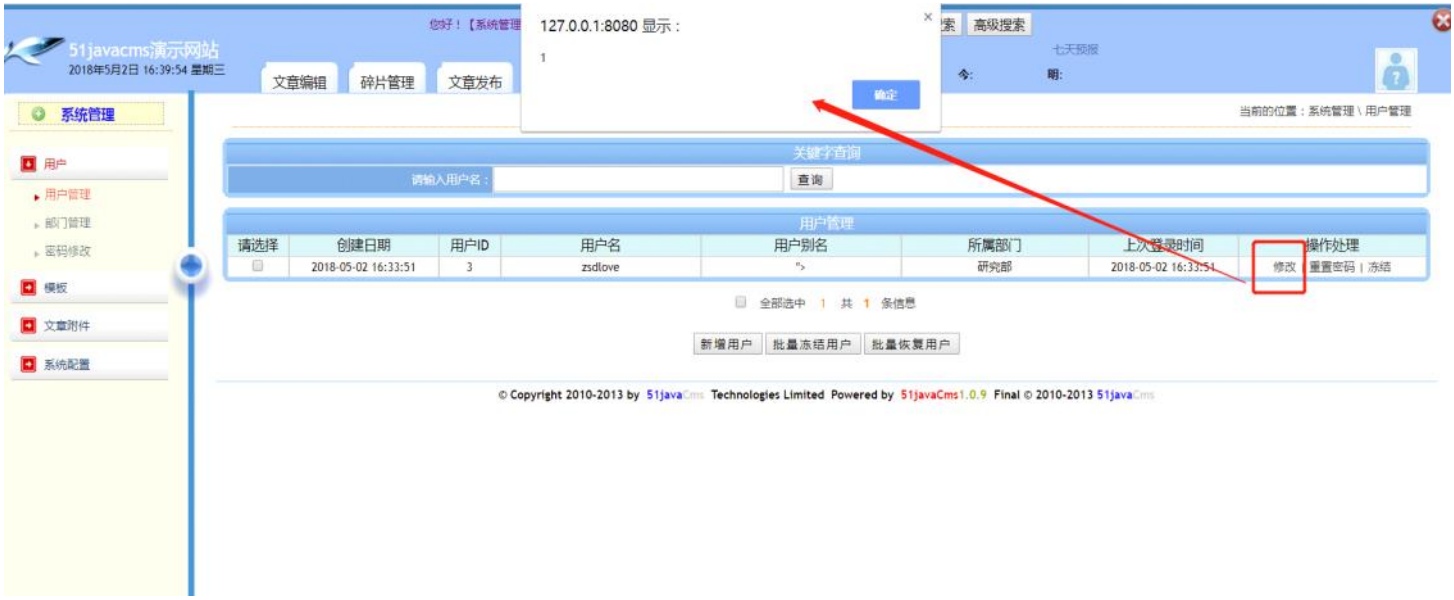
```java
import util.Constant;
import page.inc.HtmlPage;
import util.PubFun;

public class MainCtrl extends HttpServlet {

    private static final long serialVersionUID = 1L;

    protected void doPost(HttpServletRequest req, HttpServletResponse resp)
            throws ServletException, IOException {
        String jspStr = null;
        resp.setContentType("text/html; charset=utf-8");
        req.setCharacterEncoding("utf-8");
        HtmlPage page = initHtmlPage(req.getParameter("page"));
        if (page == null) {
            resp.sendRedirect(Constant.REDIRECT_LOGIN_PAGE);
            return;
        }
        try {
            jspStr = page.print(req, resp);
        } catch (Exception e) {
            String isPopup = req.getParameter("is_popup")==null?"false":req.getParameter("is_popup");
            if(isPopup.equals("true")){
                PubFun.ajaxPrint("alert('" + e.getMessage() + "');close();", resp);
                jspStr = null;
            }else if(page instanceof LoginPage){
                req.setAttribute("inf", e.getMessage());
```

这个xss是误报的。并没有将获取的获取到的参数打印到页面上。这个print方法是程序员自己
编写的类page中的一个方法。
我们跟进这个htmlPage类，这个print方法是用于打印异常输出的。

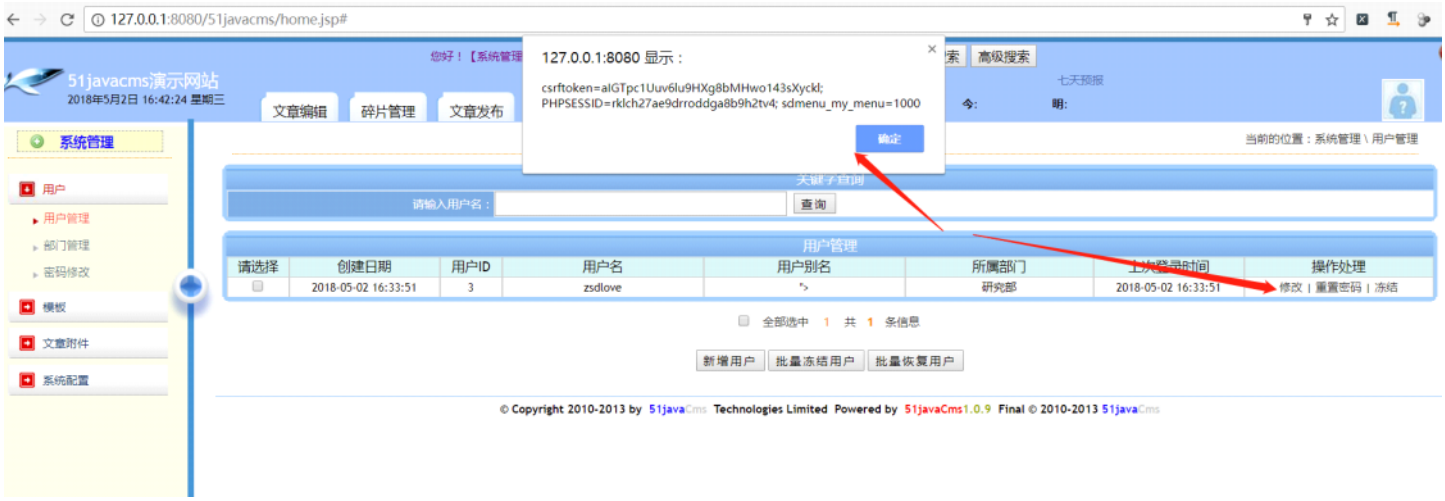
DownLoadFilePage.java | Message.java | HtmlPage.java

```java
package page.inc;

import java.io.BufferedWriter;

public abstract class HtmlPage {

    public abstract String print(HttpServletRequest req,
            HttpServletResponse resp) throws Exception;

    // 得到登录用户存在session的信息
    protected UserInfo getSessionUser(HttpServletRequest req) {
        HttpSession session = req.getSession(true);
        return (UserInfo) session.getAttribute("userInfo");
    }

    /****** 封装request值开始 *****/
    protected boolean getBooleanParameter(String key, boolean v,
            HttpServletRequest req) {
        String str = req.getParameter(key);
```

所以此处不存在xss。
第三处xss（存在）
存储型xss
在需改用户信息的地方
效果图




效果图二




分析过程

搜用户修改找到如下位置：

C:\Users\zheng\Desktop\install\51javacms\jsp\user\edit_user.jsp

MainCtrl.java | message_list.jsp | message.jsp | plugin.js | home.jsp | feeling.jsp | browse_cnt.jsp | index.jsp | head.jsp | edit_user.jsp

```
13      if(searchName == null) searchName = "";
14      String pageNo = request.getParameter("page_no");
15      if(pageNo == null) pageNo = "1";%>
16    <input id="search_name" type="hidden" value="<%=searchName%>"></input>
17    <input id="page_no" type="hidden" value="<%=pageNo%>"></input>
18
19    <!--main div begin-->
20    <div id="maindiv" class="maindivelse">
21        <span class="linktextbutton">
22            <span>当前的位置：用户管理 \ 修改用户</span>
23        </span>
24        <div class="viewfirst" onmouseout="ViewShowFirst(this);" onmouseover="ViewShowSecond(this);">
25            <!--keboardfirst begin-->
26            <b class="rtop"><b class="r1"></b><b class="r2"></b><b class="r3"></b><b class="r4"></b></b>
27                <div class="keyboardfirst" onmouseout="KeyboardShowFirst(this);" onmouseover="KeyboardShowSecond(this);">
28                    <span class="span_title">修改用户</span>
29                    <div>
30                        <span class="spanthree"></span>
31                        <!-- edit user begin -->
32                        <table border="0" cellpadding="0" cellspacing="0" width="100%">
33                            <tr class="userlist">
34                                <td class="userlisttext" width="20%">用户名：</td>
35                                <td class="userlistinput" width="40%"> <%=user.getName()%></td>
36                                <td class="userlistoutput" width="30%"> </td>
37                            </tr>
38                            <tr class="userlist">
39                                <td class="userlisttext">用户别名：</td>
40                                <td class="userlistinput"><input type="text" id="alias" value="<%=user.getAlias()%>"></input></td>
41                                <td class="userlistoutput">可以为空。</td>
42                            </tr>
43                            <tr class="userlist">
44                                <td class="userlisttext">所属部门：</td>
45                                <td class="userlistinput">
46                                    <select id="dep_id">
47                                    <%Department[] departmentList=(Department[])request.getAttribute("departmentList");
48                                    if(departmentList!=null){
```

看下提交表单的方法editUser

```
111             <b class="rbottom"><b class="r4"></b><b class="r3"></b><b class="r2"></b><b class="r1"></b></b>
112             <!--keboardfirst end-->
113         </div>
114         <!--submitbutton begin-->
115         <span><input class="submitbutton" type="button" onclick="editUser(<%=user.getId()%>);" value="修改"></input></span>
116         <span><input class="submitbutton" type="button" onclick="cancelEditUser(<%=userInfo.getId()%>);" value="取消"></input></span>
117         <!--submitbutton end-->
118     </div>
119     <!--maindiv end-->
120   <%String selTxt = (String)request.getAttribute("selTxt");
121       if(selTxt==null) selTxt="";%>
122   <div id="col_info_zone" class="infofloatzone">
```

方法如下

```
function editUser(userId){
  var checkboxs=$('makeSureItem').getElementsByTagName('input');
  var cols='';
  for(var i=0;i<checkboxs.length;i++){
   if(i==checkboxs.length-1){
          cols+=checkboxs[i].value;
   }else{
          cols+=checkboxs[i].value+',';
    }
  }
       exeRequest(rootUrl+"/MainCtrl",rightDivContent,
                    "page=EditUserInfoPage&user_id="+userId+'&search_name='
                    +encodeURIComponent($('search_name').value)
                    +'&page_no='+$('page_no').value
                    +'&alias='+$('alias').value+'&dep_id='+$('dep_id').value
                    +'&is_article='+$('is_article').value
                    +'&is_ad='+$('is_ad').value
                    +'&is_publish='+$('is_publish').value
                    +'&is_column='+$('is_column').value
                    +'&cols='+cols);
}
```

这里通过getElementsByTagName获取到所有的input标签，然后遍历input标签里的值，放入cols中，处理这个请求的servlet是MainCtrl，看下他的源码

```
import java.io.IOException;
```

```
import javax.servlet.ServletException;
import javax.servlet.http.HttpServlet;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;
import page.article.ArticleThumbnailsPage;
import page.user.LoginPage;
import util.Constant;
import page.inc.HtmlPage;
import util.PubFun;
public class MainCtrl extends HttpServlet {
	private static final long serialVersionUID = 1L;
	protected void doPost(HttpServletRequest req, HttpServletResponse resp)
			throws ServletException, IOException {
		String jspStr = null;
		resp.setContentType("text/html; charset=utf-8");
		req.setCharacterEncoding("utf-8");
		HtmlPage page = initHtmlPage(req.getParameter("page"));
		if (page == null) {
			resp.sendRedirect(Constant.REDIRECT_LOGIN_PAGE);
			return;
		}
		try {
			jspStr = page.print(req, resp);
		} catch (Exception e) {
			String isPopup =
			req.getParameter("is_popup")==null?"false":req.getParameter("is_popup");
			if(isPopup.equals("true")){
				PubFun.ajaxPrint("alert('" + e.getMessage() + "');close();", resp);
				jspStr = null;
			}else if(page instanceof LoginPage){
				req.setAttribute("inf", e.getMessage());
				jspStr = Constant.ORGINAL_LOGIN_PAGE;
			}else if(page instanceof ArticleThumbnailsPage){
				PubFun.ajaxPrintC("error", resp);
				jspStr = null;
			}else{
				PubFun.ajaxPrintStr(e.getMessage(), resp);
				jspStr = null;
			}
			System.out.println(e.getMessage());
		}
		if (jspStr != null) {
			req.getRequestDispatcher(jspStr).forward(req, resp);
		}
	}
	protected void doGet(HttpServletRequest req, HttpServletResponse resp)
			throws ServletException, IOException {
		doPost(req, resp);
	}
	private HtmlPage initHtmlPage(String page) {
		if ((page == null) || (page.trim().length() == 0))
			return null;
		else
			page = page.trim();
		return PubFun.getPageMap().get(page);
	}

}
```

这里也没有对参数进行任何的过滤或校验。

看下输出

```
56                      <td class="tablelistfirst3r" width="16%">用户别名</td>
57                      <td class="tablelistfirst3r" width="15%">所属部门</td>
58                      <td class="tablelistfirst3r" width="12%">上次登录时间</td>
59                      <td class="tablelistfirst3r" width="15%">操作处理</td>
60                  </tr>
61                  <%if(users != null){
62                      String className = "tablelisttext3ro";
63                      for (int i=0;i<users.length;i++){%>
64                      <tr class="tablelist" onmouseout="showThisLinkOut(this);" onmouseover="showThisLinkOver(this);">
65                          <%if((i%2)==0){
66                              className = "tablelisttext3ro";
67                          }else{
68                              className = "tablelisttext3rt";
69                          }%>
70                          <td class="<%=className%>"><input type="checkbox" name="checks_name" value="<%=users[i].getId()%>"></td>
71                          <td class="<%=className%>"><%=PubFun.getDateTime("yyyy-MM-dd HH:mm:ss",users[i].getCreateTime())%></td>
72                          <td class="<%=className%>"><%=users[i].getId()%></td>
73                          <td class="<%=className%>"><%=users[i].getName()%></td>
74                          <td class="<%=className%>"><%=users[i].getAlias()%></td>
75                          <td class="<%=className%>"><%=users[i].getDepartmentName()%></td>
76                          <td class="<%=className%>"><%=PubFun.getDateTime("yyyy-MM-dd HH:mm:ss",users[i].getLastLogin())%></td>
77                          <td class="<%=className%>"><%if(users[i].isDel()){ %>
78                              <a href="javascript:reUser(<%=users[i].getId()%>,'<%=users[i].getName()%>');"><font color="red">恢复用户</font></a>
79                          <%}else{ %>
80                              <a href="javascript:showEditUser(<%=users[i].getId()%>,${pageNo});">修改</a>
81                              | <a href="javascript:initUserPasswd(<%=users[i].getId()%>,'<%=users[i].getName()%>');">重置密码</a>
82                              | <a href="javascript:delUser('<%=users[i].getName()%>',<%=users[i].getId()%>,${pageNo});">冻结</a>
83                          <%}%>
84                          </td>
85                      </tr><%}%>
```

这里通过user类的getAlias()方法直接输出别名，并没有做实体编码。

```
public String getAlias() {
	return alias;
}
```

```
68                          }else{
69                              className = "tablelisttext3rt";
70                          }%>
71                          <td class="<%=className%>"><input type="checkbox" name="checks_name" value="<%=users[i].getId()%>"></td>
72                          <td class="<%=className%>"><%=PubFun.getDateTime("yyyy-MM-dd HH:mm:ss",users[i].getCreateTime())%></td>
73                          <td class="<%=className%>"><%=users[i].getId()%></td>
74                          <td class="<%=className%>"><%=users[i].getName()%></td>
75                          <td class="<%=className%>"><%=users[i].getAlias()%></td>
76                          <td class="<%=className%>"><%=users[i].getDepartmentName()%></td>
77                          <td class="<%=className%>"><%=PubFun.getDateTime("yyyy-MM-dd HH:mm:ss",users[i].getLastLogin())%></td>
78                          <td class="<%=className%>"><%if(users[i].isDel()){ %>
```