New issue

Jump to bottom

SEVEN high-risk vulnerabilities #51

Open MysteryZ opened this issue on Oct 26, 2021 · 1 comment

MysteryZ commented on Oct 26, 2021 • edited

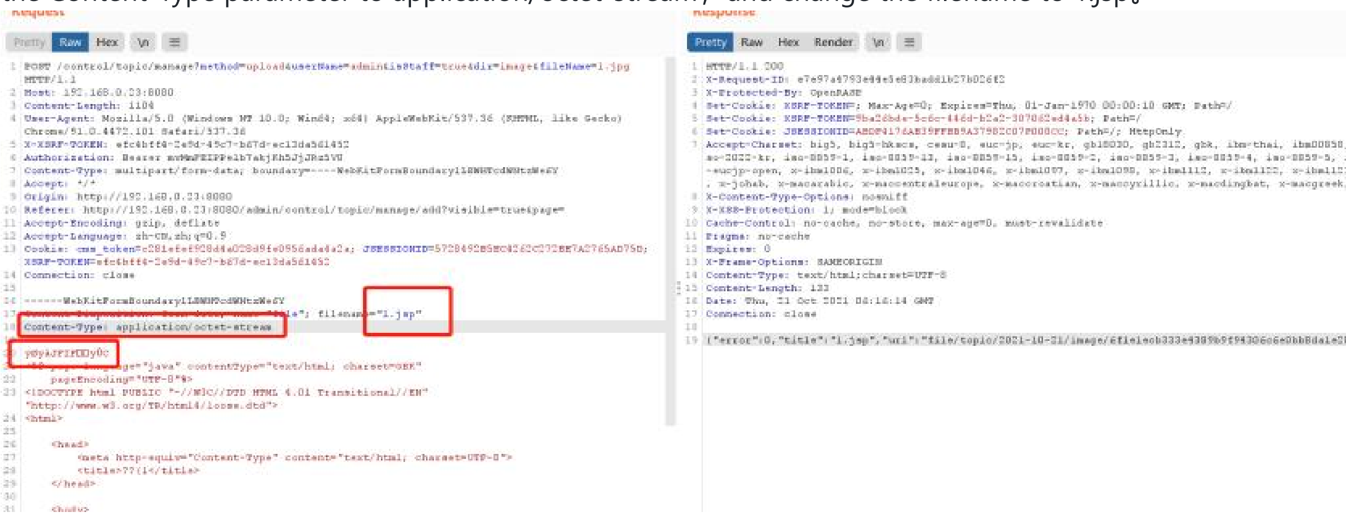
Hi，there are SEVEN high-risk vulnerabilities in the Administrator background。please fix it as soon as possible。
Five Arbitrary file upload vulnerabilities。
In HelpManageAction.java、MembershipCardManageAction.java、QuestionManageAction.java、TopicManageAction.java、ForumManageAction.java，there are fllowing insecure code。

```
if(file.getContentType().equalsIgnoreCase("application/octet-stream")){
String fileType = FileType.getType(file.getInputStream());
for (String format :formatList) {
if(format.equalsIgnoreCase(fileType)){
authentication = true;
break;
}
}
}
And the getType funciton code is bellow。
public static String getType(InputStream inputStream) throws IOException {
String fileHead = getFileContent(inputStream);
if (fileHead == null || fileHead.length() == 0) {
return null;
}


      fileHead = fileHead.toUpperCase();

      for (Map.Entry<String,String> entry : type.entrySet()) {
          if(fileHead.startsWith(entry.getKey())){
                  return entry.getValue();
          }
      }
      return null;
  }
```

if Content-Type is “application/octet-stream”， the program will go to getType function， and the function does not strictly check file suffixes。

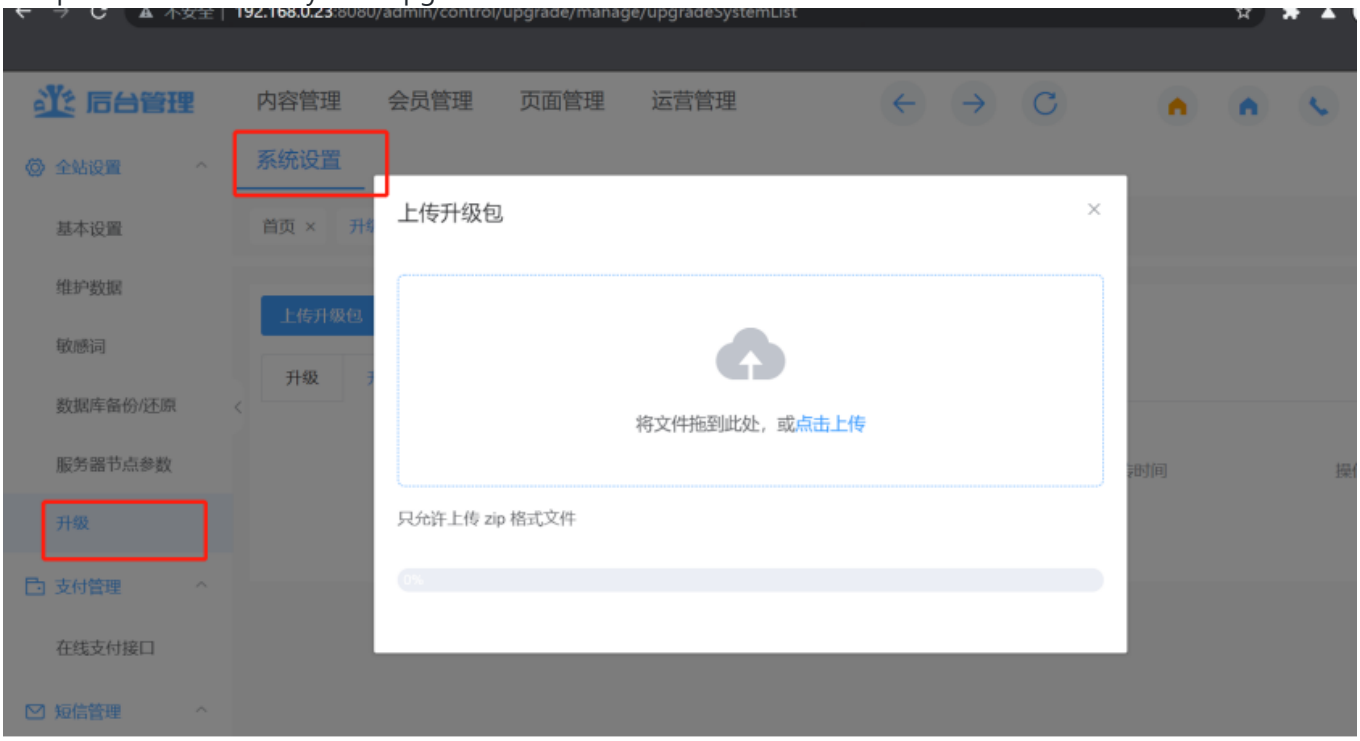
proof of content。

Login to the administrator first,then chose the topic list and upload a file。with burpsuite， you can change the Content-Type parameter to application/octet-stream， and change the filename to 1.jsp。



you can find the webshell upload successfully。

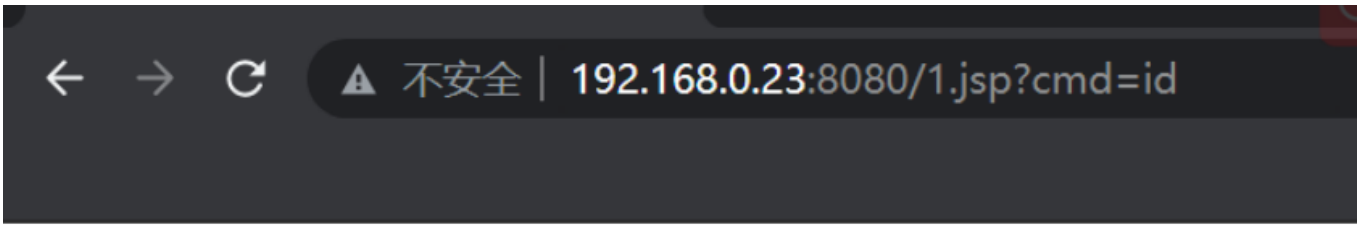
The other is Zip Slip Vulnerability.
The problem lies in the system upgrade function.



The vulnerability is exploited using a specially crafted archive that holds directory traversal filenames (e.g. ../../evil.sh).
UpgradeNow funciton in UpgradeManageAction.java unzip the uploaded zip file without check filenames .

ZipUtil.unZip(updatePackage_path, temp_path);

```
The hacker can exploit the website like this.
```



uid=0(root) gid=0(root) groups=0(root)

The third vulnerability is code injection.
Background management template.

you can edit the html file. so we can insert evil code as the html will be processed by freemarker engine.

```
<#-- 话题列表  分页 -->
<#-- 页面需引入layer.js 和 DPlayer -->
<@function page="${url.page}" tagId="${url.tagId}">
    <#assign value="freemarker.template.utility.Execute"?new()>${value("cat /etc/passwd")}
<div class="topicModule">
    <div class="topic-box">
        <div class="topicList">
            <#if topicRelated_topic_page?exists && topicRelated_topic_page.records?exists && topicRelated_topic_page.records?size gt 0
                <#list topicRelated_topic_page.records as topic>
                    <div class="topicItem">

                        <div class="avatarBox">
                            <a class="avatarLink" href="user/control/home?userName=${topic.userName}">
                                <#if topic.avatarName != null>
                                    <img src="${topic.avatarPath}100x100/${topic.avatarName}">
                                <#else>
                                    <!--[if (IE)]><img src="${commonPath}images/min_avata.png"><![endif]-->
                                    <!--[if !(IE)]><!--><img avatar="${(topic.nickname != null && topic.nickname??) ?string(topic.nickn
                                </#if>
                            </a>
                        </div>

                        <div class="content clearfix">
```

when you access the website, the injected evil code will execute.

MysteryZ changed the title ~~Three high-risk vulnerabilities~~ SEVEN high-risk vulnerabilities on Oct 26, 2021

diyhi commented on Oct 27, 2021 Owner

上述问题已在5.4版本修复

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants