

java代码审计 深度解析

第二课 文件下载修复方法及修复源码编写

文件下载

直接从request中获取文件名

```
16 public void doGet(HttpServletRequest request, HttpServletResponse response)
17     throws ServletException, IOException {
18     //得到要下载的文件名
19     String fileName = request.getParameter("filename"); //23239283-92489-阿凡达.avi
20     fileName = new String(fileName.getBytes("iso8859-1"), "UTF-8");
21     //上传的文件都是保存在/WEB-INF/upload目录下的子目录当中
22     String fileSaveRootPath=this.getServletContext().getRealPath("/WEB-INF/upload");
23     //通过文件名找出文件的所在目录
24     String path = findFileSavePathByFileName(fileName,fileSaveRootPath);
25     //得到要下载的文件
```



文件下载

直接利用路径+文件名进行下载

```
5 String realname = fileName.substring(fileName.indexOf("_")+1);
6 //设置响应头，控制浏览器下载该文件
7 response.setHeader("content-disposition", "attachment;filename=" + URLEncoder.encode(realname, "UTF-8"))
8 //读取要下载的文件，保存到文件输入流
9 FileInputStream in = new FileInputStream(fileSaveRootPath + "\\\" + fileName);
10 //创建输出流
11 OutputStream out = response.getOutputStream();
12 //创建缓冲区
13 byte buffer[] = new byte[1024];
14 int len = 0;
15 //循环将输入流中的内容读取到缓冲区当中
16 while((len=in.read(buffer))>0){
17     //输出缓冲区的内容到浏览器，实现文件下载
18     out.write(buffer, 0, len);
19 }
20 //关闭文件输入流
21 in.close();
22 //关闭输出流
23 out.close();
```



攻击效果

```
GET
/FileUploadAndDownLoad/servlet/DownLoadServlet?filename=../
web.xml HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0)
Gecko/20100101 Firefox/52.0
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
Referer:
http://localhost:8080/FileUploadAndDownLoad/servlet/ListFileServ
let
Cookie: JSESSIONID=F1F6217B9B407F4CF0A9C330D598C2F3;
Pycharm-a78b22bc=1f28a72c-29b1-4a91-ab73-d33de7a62882;
PJBlog3Setting=ViewType=normal
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
content-disposition: attachment;filename=..%2Fweb.xml
Content-Length: 1356
Date: Tue, 23 Apr 2019 07:13:51 GMT
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
<web-app version="3.0"
  xmlns="http://java.sun.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://java.sun.com/xml/ns/javaee
    http://java.sun.com/xml/ns/javaee/web-app_3_0.xsd">
  <display-name></display-name>
  <welcome-file-list>
    <welcome-file>/jsp/upload.jsp</welcome-file>
  </welcome-file-list>

  <servlet>
    <servlet-name>UploadHandleServlet</servlet-name>

    <servlet-class>me.qacl.web.controller.UploadHandleServlet</se
```



修复建议

- 1、过滤文件名不允许./ ../
- 2、下载文件白名单



修复建议

过滤文件名不允许./ ../

```
if(fileName.indexOf("./")!=-1 &&  
fileName.indexOf("../")!=-1){  
Xxx}else{  
}
```



修复建议

读取失败

```
GET
/FileUploadAndDownLoad/servlet/DownLoadServlet?filename=../
web.xml HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0)
Gecko/20100101 Firefox/52.0
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
Referer:
http://localhost:8080/FileUploadAndDownLoad/servlet/ListFileServ
let
Cookie: JSESSIONID=F1F6217B9B407F4CF0A9C330D598C2F3;
Pycharm-a78b22bc=1f28a72c-29b1-4a91-ab73-d33de7a62882;
PJBlog3Setting=ViewType=normal
Connection: close
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=3981012E01DC064BE232147A059B2F06;
Path=/FileUploadAndDownLoad
Content-Type: text/html;charset=UTF-8
Content-Length: 285
Date: Tue, 23 Apr 2019 07:54:06 GMT
Connection: close
```

```
<!DOCTYPE HTML>
<html>
<head>
<title>消息提示</title>
</head>

<body>
  您正在非法操作
  <br/>
  <a href="/FileUploadAndDownLoad/servlet/ListFileServlet">
    <input type="button" value="点我去下载"> </a>
</body>
```



修复建议

白名单

- 1、上传上后就在数据库中添加文件名
- 2、下载时拿着request获取到的文件名与数据库中文件名对比





谢谢观赏