

java代码审计 深度解析

第二课 文件上传漏洞修复

文件上传

```
filename = filename.substring(filename.lastIndexOf("\\")+1);  
//获取item中的上传文件的输入流  
InputStream in = item.getInputStream();  
//创建一个文件输出流  
FileOutputStream out = new FileOutputStream(savePath + "\\" + filename);  
//创建一个缓冲区  
byte buffer[] = new byte[1024];  
//判断输入流中的数据是否已经读完的标识  
int len = 0;  
//循环将输入流读入到缓冲区当中, (len=in.read(buffer))>0就表示in里面还有数据  
while((len=in.read(buffer))>0){  
    //使用FileOutputStream输出流将缓冲区的数据写入到指定的目录(savePath + "\\" + filename)当中  
    out.write(buffer, 0, len);  
}  
//关闭输入流  
in.close();  
//关闭输出流  
out.close();  
//删除处理文件上传时生成的临时文件  
item.delete();  
message = "文件上传成功!";
```



修复建议

白名单限制

获取文件后缀，判断是否在白名单内

```
filename.substring(filename.lastIndexOf(".")+1,filename.length())
```



修复建议

重命名后缀

```
String fileName2 = filename.substring(0,filename.lastIndexOf("."));  
filename = fileName2+".txt";
```





谢谢观赏