

## 0x00 前言

青云客网站管理系统（QYKCMS）是青云客开发的一款基于PHP+MySql的轻量级智能建站系统。在T00ls看到两篇QYKCMS的代码审计文章，也下载了一套回来测试，发现了两个后台漏洞，并没有跟前面的漏洞重复，分享一下思路。

## 0x01 环境搭建

QYKCMS官网：<http://www.qykcms.com/>

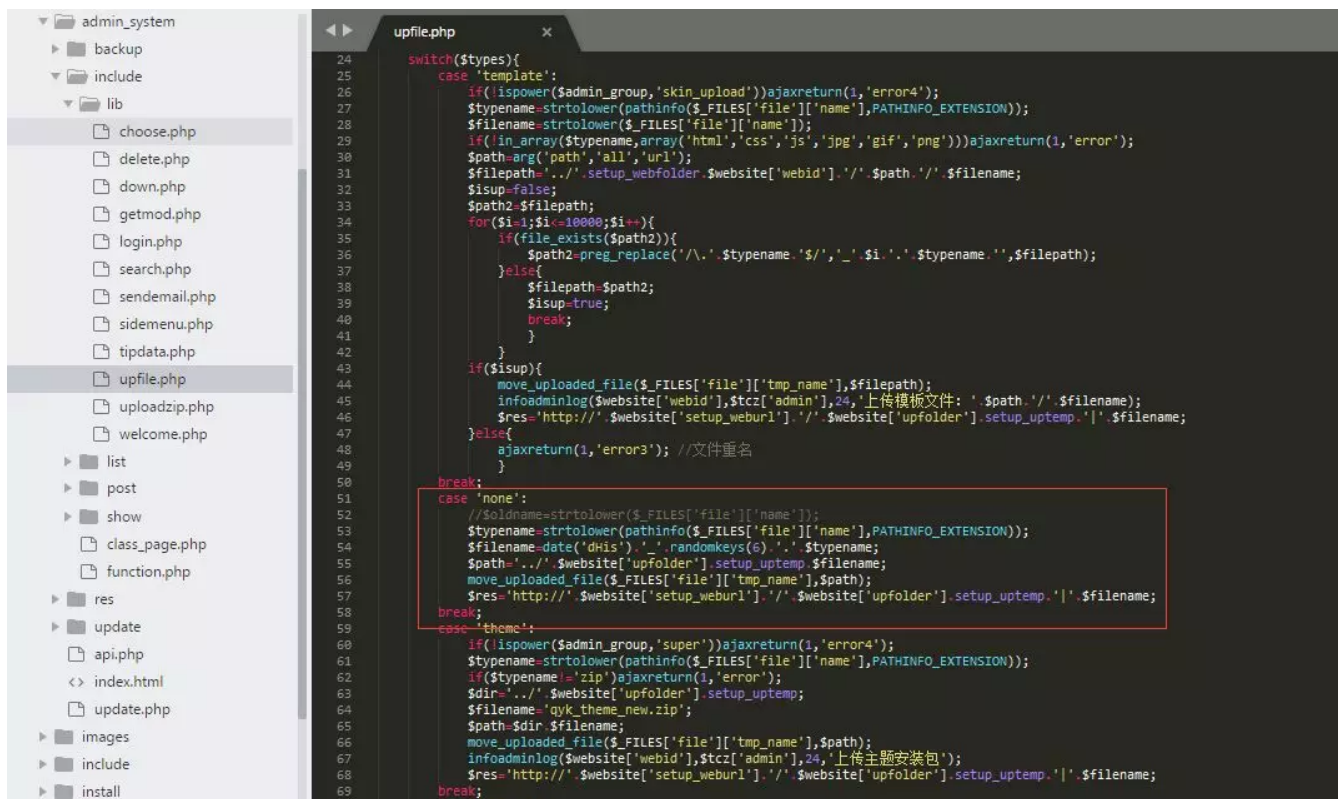
网站源码版本：QYKCMS\_v4.3.2（企业站主题）

程序源码下载：<http://bbs.gingyunke.com/thread-13.htm>

## 0x02 任意文件上传

代码分析：

1、漏洞文件位置：`/admin_system/include/lib/upfile.php` 第24-69行：



这段代码根据types的值进行操作，可以发现当\$types=None的时候（注意看红色代码部分），获取文件名后缀，拼接成完整路径，然后将文件上传到服务器。

并没有对文件类型进行过滤，导致程序在实现上存在任意文件上传漏洞，攻击者可以通过上传脚本木马，控制服务器权限。

漏洞利用：

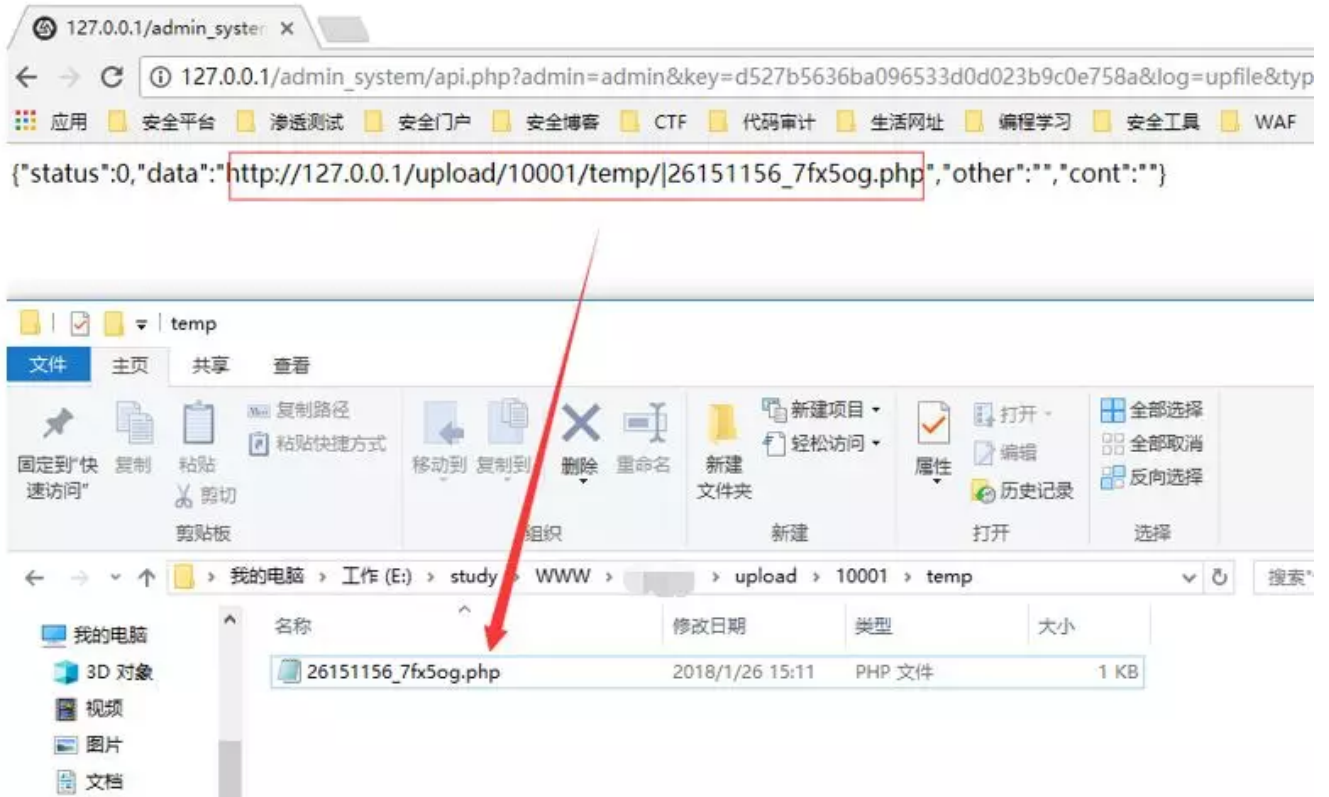
1、构造Form表单，key可通过XSS获取管理员COOKIE得到：

Upload a **new** file:

选择文件 未选择任何文件

Upload

## 2、成功上传脚本木马，并回显上传路径



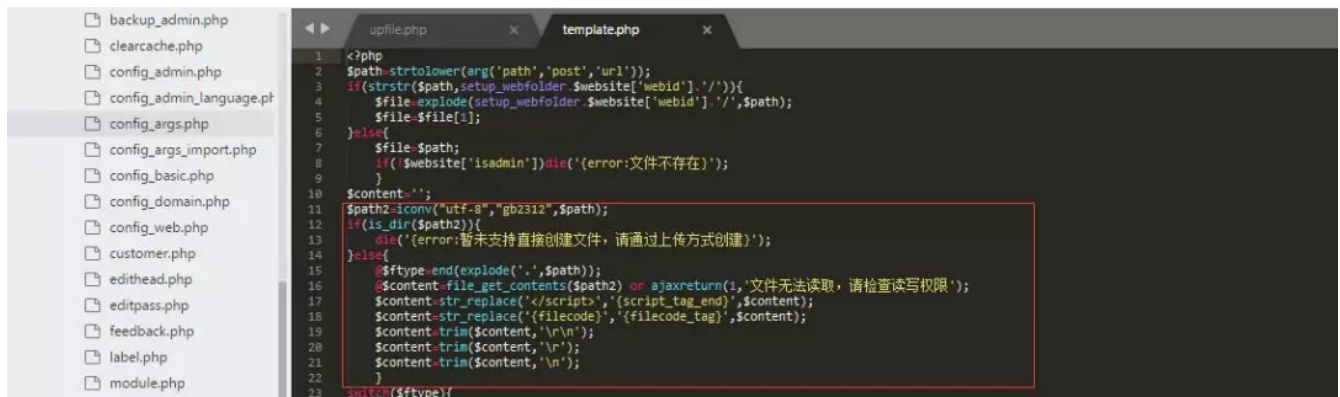
3、去掉文件名称的第一个“|”符，然后访问脚本木马地址



## 0x03 任意文件读取

代码分析：

1、漏洞文件位置：/admin\_system/include/show/template.php 第1-22行：



```
1 <?php
2 $path=strtolower(arg('path','post','url'));
3 if(strpos($path,setup_webfolder.$website['webid'].'/')){
4     $file=explode(setup_webfolder.$website['webid'].'/',$path);
5     $file=$file[1];
6 }else{
7     $file=$path;
8     if(!$website['isadmin'])die('error:文件不存在');
9 }
10 $content='';
11 $path2=iconv("utf-8","gb2312",$path);
12 if(is_dir($path2)){
13     die('error:暂未支持直接创建文件,请通过上传方式创建');
14 }else{
15     $ftype=end(explode('.', $path));
16     $content=file_get_contents($path2) or ajaxreturn(1,'文件无法读取,请检查读写权限');
17     $content=str_replace('</script>','</script_end>',$content);
18     $content=str_replace('{filecode}','{filecode_tag}', $content);
19     $content=trim($content, "\r\n");
20     $content=trim($content, "\r");
21     $content=trim($content, "\n");
22 }
23 switch($ftype){
```

这段代码中接收path参数，然后进行转码处理，注意看红色代码部分，接着判断是否是一个目录，然后带入file\_get\_contents函数中执行，可以看到path参数并未进行任何过滤或处理，导致程序在实现上存在任意文件读取漏洞，可以读取网站任意文件，攻击者可利用该漏洞获取敏感信息。

漏洞利用：

QYKCMS默认数据库配置文件存放在\include\config\_db.php中，我们构造一个路径去读取数据库敏感信息,成功读取配置文件信息。

[http://127.0.0.1/admin\\_system/api.php](http://127.0.0.1/admin_system/api.php)

POST:

admin=admin&key=682b82f8dc3b753d6eb9ceafd5a64301&log=show&desc=template&path=../include/config\_db.php



## 0x04 END

说一下感悟，小CMS后台中，涉及文件操作的参数基本没怎么过滤，可以黑盒结合白盒挖到很多任意文件删除、任意文件读取、任意文件下载等漏洞，然而只是just for fun。