链滴

江湖魔头 Writeup

作者：moddemod

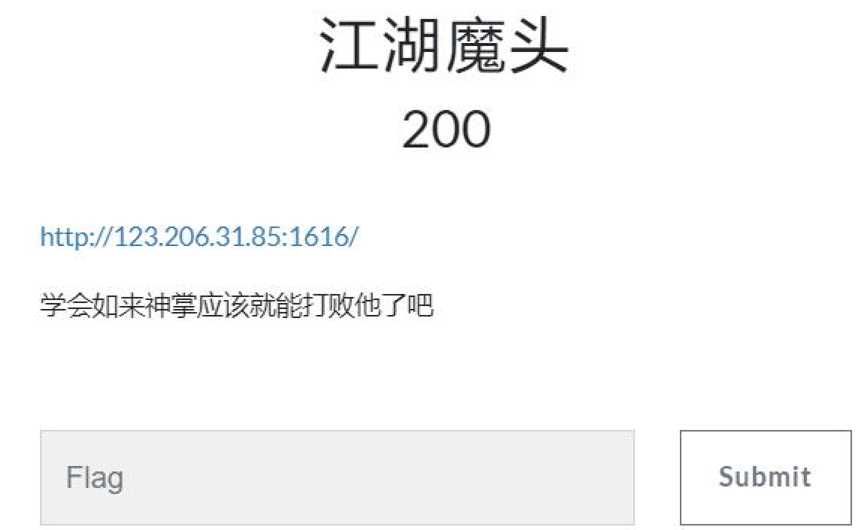
原文链接：https://ld246.com/article/1567311660712

来源网站：链滴

写在前面的话

打怪需要装备，装备需要钱，如果这句话没能帮到你，那么就继续看吧

这是一道来自Bugku上的一道题，题目地址：http://123.206.31.85/



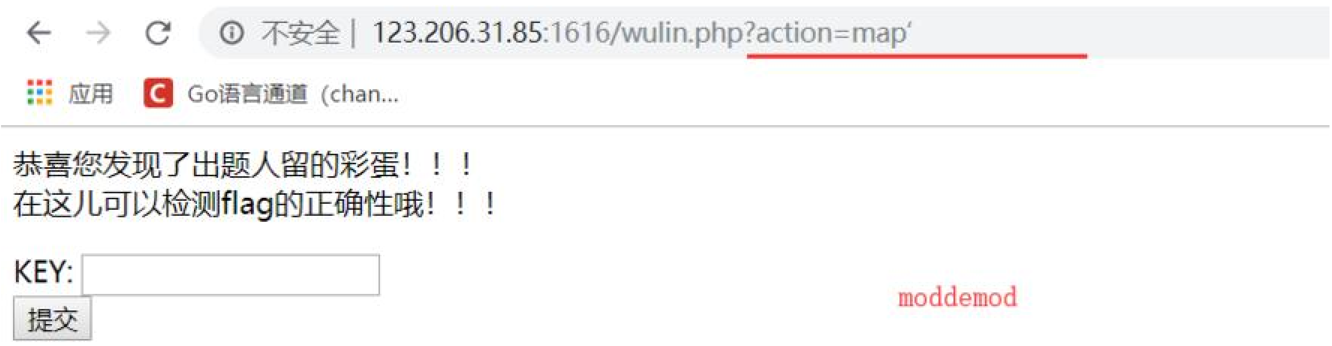
江湖魔头

200

http://123.206.31.85:1616/

学会如来神掌应该就能打败他了吧

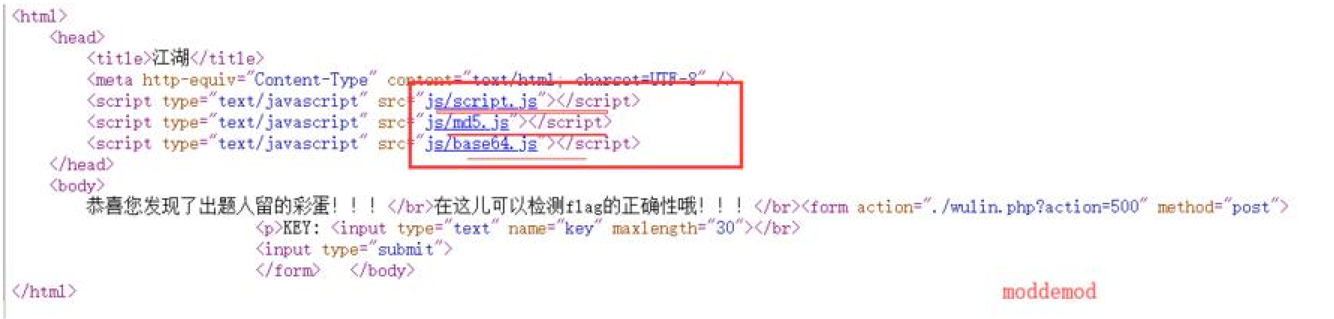
随便观察了一下没有发现什么特殊的地方，看参数的地方加了'出现如下：



恭喜您发现了出题人留的彩蛋！！！
在这儿可以检测flag的正确性哦！！！

KEY:

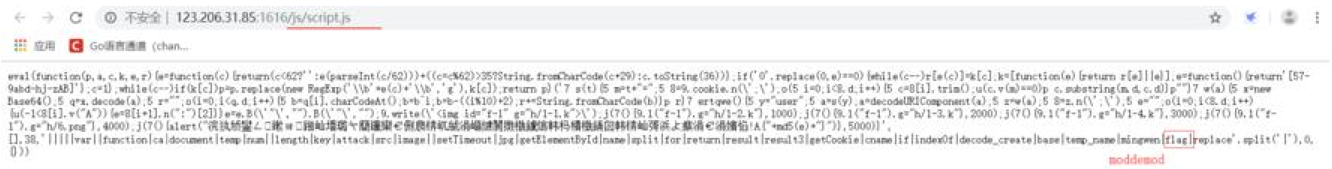
打开源码只发现三个js文件



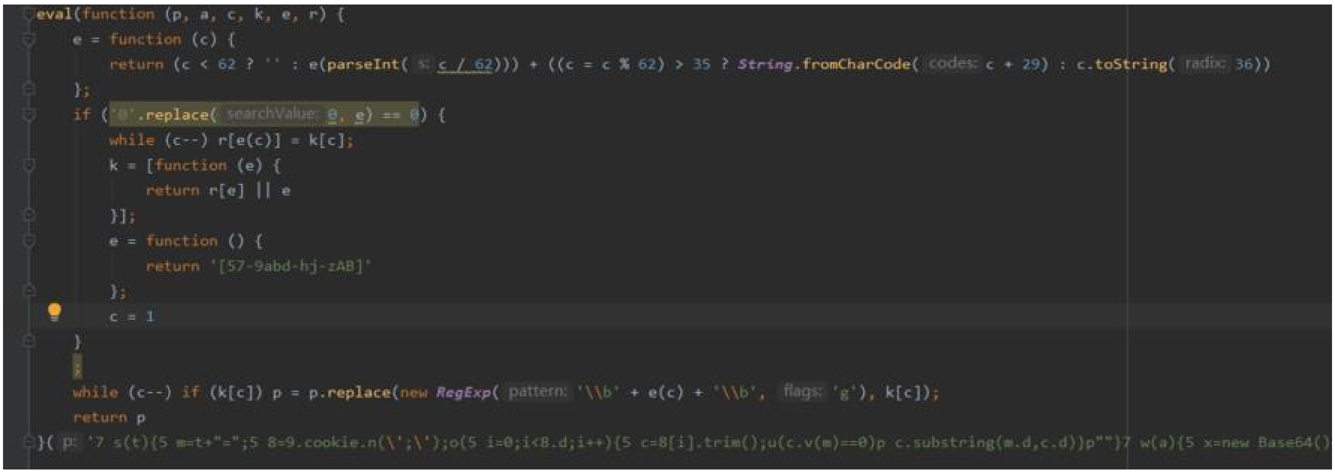
```
<html>
    <head>
        <title>江湖</title>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
        <script type="text/javascript" src="js/script.js"></script>
        <script type="text/javascript" src="js/md5.js"></script>
        <script type="text/javascript" src="js/base64.js"></script>
    </head>
    <body>
        恭喜您发现了出题人留的彩蛋！！！</br>在这儿可以检测flag的正确性哦！！！</br><form action="./wulin.php?action=500" method="post">
                            <p>KEY: <input type="text" name="key" maxlength="30"></br>
                            <input type="submit">
                            </form>    </body>
</html>
```

接下来就是代码审计的时间了，这里主要是Javascript.

在script.js中发现flag，随便打开一个编辑器格式化一下。



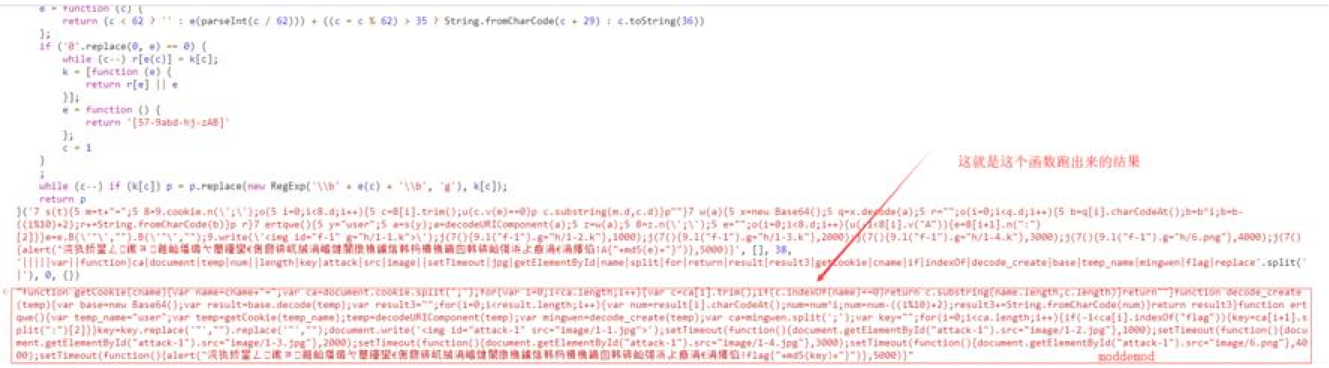
```
eval(function(p,a,c,k,e,r){e=function(c){return(c<62?'':e(parseInt(c/62)))+((c=c%62)>35?String.fromCharCode(c+29):c.toString(36))};if('0'.replace(0,e)==0){while(c--)r[e(c)]=k[c];k=[function(e){return r[e]||e}];e=function(){return'[57-
9abd-hj-zAB]'};c=1};while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p}('7 s(t){5 m=t+"=";5 8=9.cookie.n(\';\');o(5 i=0;i<8.d;i++){5 c=8[i].trim();u(c.v(m)==0)p c.substring(m.d,c.d)}p""}7 w(a){5 x=new
Base64();5 q=x.decode(a);5 r="";o(i=0;i<q.d;i++){5 b=q[i].charCodeAt();b=b^i;b=b-((i%10)+2);r+=String.fromCharCode(b)}p r}7 ertqwe(){5 y="user";5 a=s(y);a=decodeURIComponent(a);5 z=w(a);5 8=z.n(\';\');5 e="";o(i=0;i<8.d;i++)
{u(-1<8[i].v("A")){e=8[i+1].n(":")[2]}}e=e.B(\'"\',"").B(\'"\',"");9.write(\'<img id="f-1" g="h/1-1.k">\');j(7(){9.1("f-1").g="h/1-2.k"},1000);j(7(){9.1("f-1").g="h/1-3.k"},2000);j(7(){9.1("f-1").g="h/1-4.k"},3000);j(7(){9.1("f-
1").g="h/6.png"},4000);j(7(){alert("[illegible]A("+md5(e)+"]")},5000)}',
[],38,'||||var||function|ca|document|temp|num||length|key|attack|src|image||setTimeout|jpg|getElementById|name|split|for|return|result|result3|getCookie|cname|if|indexOf|decode_create|base|temp_name|mingwen|flag|replace'.split('|'),0,
{}))
```



```
eval(function (p, a, c, k, e, r) {
    e = function (c) {
        return (c < 62 ? '' : e(parseInt( s: c / 62))) + ((c = c % 62) > 35 ? String.fromCharCode( codes: c + 29) : c.toString( radix: 36))
    };
    if ('0'.replace( searchValue: 0, e) == 0) {
        while (c--) r[e(c)] = k[c];
        k = [function (e) {
            return r[e] || e
        }];
        e = function () {
            return '[57-9abd-hj-zAB]'
        };
        c = 1
    }
    ;
    while (c--) if (k[c]) p = p.replace(new RegExp( pattern: '\\b' + e(c) + '\\b',  flags: 'g'), k[c]);
    return p
}( p: '7 s(t){5 m=t+"=";5 8=9.cookie.n(\';\');o(5 i=0;i<8.d;i++){5 c=8[i].trim();u(c.v(m)==0)p c.substring(m.d,c.d)}p""}7 w(a){5 x=new Base64()
```

eval()就不用解释了吧，首先这是一个匿名函数，我们直接把eval去掉然后在Chorme中跑一下。

```
fun = function (p, a, c, k, e, r) {
    e = function (c) {
        return (c < 62 ? '' : e(parseInt(c / 62))) + ((c = c % 62) > 35 ? String.fromCharCode(c + 29)
 c.toString(36))
    };
    if ('0'.replace(0, e) == 0) {
        while (c--) r[e(c)] = k[c];
        k = [function (e) {
            return r[e] || e
        }];
        e = function () {
            return '[57-9abd-hj-zAB]'
        };
        c = 1
    }
    ;
    while (c--) if (k[c]) p = p.replace(new RegExp('\\b' + e(c) + '\\b', 'g'), k[c]);
    return p
}('7 s(t){5 m=t+"=";5 8=9.cookie.n(\';\');o(5 i=0;i<8.d;i++){5 c=8[i].trim();u(c.v(m)==0)p c.substr
ng(m.d,c.d)}p""}7 w(a){5 x=new Base64();5 q=x.decode(a);5 r="";o(i=0;i<q.d;i++){5 b=q[i].char
odeAt();b=b^i;b=b-((i%10)+2);r+=String.fromCharCode(b)}p r}7 ertqwe(){5 y="user";5 a=s(y);
=decodeURIComponent(a);5 z=w(a);5 8=z.n(\';\');5 e="";o(i=0;i<8.d;i++){u(-1<8[i].v("A")){e=8[
+1].n(":")[2]}}e=e.B(\'"\',"").B(\'"\',"");9.write(\'<img id="f-1" g="h/1-1.k">\');j(7(){9.l("f-1").g="
/1-2.k"},1000);j(7(){9.l("f-1").g="h/1-3.k"},2000);j(7(){9.l("f-1").g="h/1-4.k"},3000);j(7(){9.l("f-1").
="h/6.png"},4000);j(7(){alert("浣犳娇鐢ㄥ∟鍬ョ∃鍓屾墦璐ヤ簡鐮鑲鑾€佩爬锛屼綘鍦嶇閬撴綘鍗囧嚑闂撴墫瀵ㄩ煩韓
槓橹鍋囧韓锛屼綘鍦ㄦ潵鍫ㄥ嚑!A{"+md5(e)+"}")},5000)}', [], 38, '|||||var||function|ca|documen
|temp|num||length|key|attack|src|image||setTimeout|jpg|getElementById|name|split|for|return|
esult|result3|getCookie|cname|if|indexOf|decode_create|base|temp_name|mingwen|flag|repla
e'.split('|'), 0, {})
```



```
    e = function (c) {
        return (c < 62 ? '' : e(parseInt(c / 62))) + ((c = c % 62) > 35 ? String.fromCharCode(c + 29) : c.toString(36))
    };
    if ('0'.replace(0, e) == 0) {
        while (c--) r[e(c)] = k[c];
        k = [function (e) {
            return r[e] || e
        }];
        e = function () {
            return '[57-9abd-hj-zAB]'
        };
        c = 1
    }
    ;
    while (c--) if (k[c]) p = p.replace(new RegExp('\\b' + e(c) + '\\b', 'g'), k[c]);
    return p
}('7 s(t){5 m=t+"=";5 8=9.cookie.n(\';\');o(5 i=0;i<8.d;i++){5 c=8[i].trim();u(c.v(m)==0)p c.substring(m.d,c.d)}p""}7 w(a){5 x=new Base64();5 q=x.decode(a);5 r="";o(i=0;i<q.d;i++){5 b=q[i].charCodeAt();b=b^i;b=b-
((i%10)+2);r+=String.fromCharCode(b)}p r}7 ertqwe(){5 y="user";5 a=s(y);a=decodeURIComponent(a);5 z=w(a);5 8=z.n(\';\');5 e="";o(i=0;i<8.d;i++){u(-1<8[i].v("A")){e=8[i+1].n(":")
[2]}}e=e.B(\'"\',"").B(\'"\',"");9.write(\'<img id="f-1" g="h/1-1.k">\');j(7(){9.l("f-1").g="h/1-2.k"},1000);j(7(){9.l("f-1").g="h/1-3.k"},2000);j(7(){9.l("f-1").g="h/1-4.k"},3000);j(7(){9.l("f-1").g="h/6.png"},4000);j(7()
{alert("浣犳娇鐢ㄥ∟鍬ョ∃鍓屾墦璐ヤ簡鐮鑲鑾€佩爬锛屼綘鍦嶇閬撴綘鍗囧嚑闂撴墫瀵ㄩ煩韓槓橹鍋囧韓锛屼綘鍦ㄦ潵鍫ㄥ嚑!A{"+md5(e)+"}")},5000)}', [], 38,
'|||||var||function|ca|document|temp|num||length|key|attack|src|image||setTimeout|jpg|getElementById|name|split|for|return|result|result3|getCookie|cname|if|indexOf|decode_create|base|temp_name|mingwen|flag|replace'.split('
|'), 0, {})
"function getCookie(cname){var name=cname+"=";var ca=document.cookie.split(";");for(var i=0;i<ca.length;i++){var c=ca[i].trim();if(c.indexOf(name)==0)return c.substring(name.length,c.length)}return""}function decode_create
(temp){var base=new Base64();var result=base.decode(temp);var result3="";for(i=0;i<result.length;i++){var num=result[i].charCodeAt();num=num^i;num=num-((i%10)+2);result3+=String.fromCharCode(num)}return result3}function ert
qwe(){var temp_name="user";var temp=getCookie(temp_name);temp=decodeURIComponent(temp);var mingwen=decode_create(temp);var ca=mingwen.split(';');var key="";for(i=0;i<ca.length;i++){if(-1<ca[i].indexOf("flag")){key=ca[i+1].s
plit(":")[2]}}key=key.replace('"',"").replace('"',"");document.write('<img id="attack-1" src="image/1-1.jpg">');setTimeout(function(){document.getElementById("attack-1").src="image/1-2.jpg"},1000);setTimeout(function(){docu
ment.getElementById("attack-1").src="image/1-3.jpg"},2000);setTimeout(function(){document.getElementById("attack-1").src="image/1-4.jpg"},3000);setTimeout(function(){document.getElementById("attack-1").src="image/6.png"},40
00);setTimeout(function(){alert("浣犳娇鐢ㄥ∟鍬ョ∃鍓屾墦璐ヤ簡鐮鑲鑾€佩爬锛屼綘鍦嶇閬撴綘鍗囧嚑闂撴墫瀵ㄩ煩韓槓橹鍋囧韓锛屼綘鍦ㄦ潵鍫ㄥ嚑!flag{"+md5(key)+"}")},5000)}"
```

原文链接：江湖魔头 Writeup

同样我们再格式化一下这段代码,

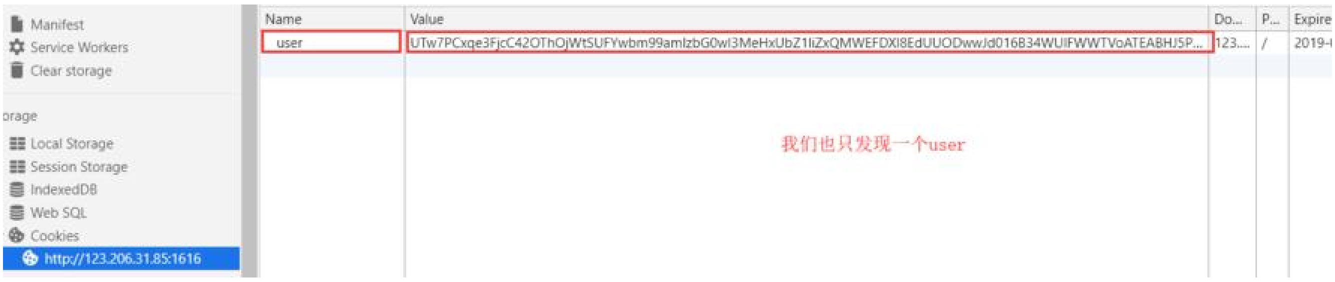
```
function getCookie(cname) {
    var name = cname + "=";
    var ca = document.cookie.split(';');
    for (var i = 0; i < ca.length; i++) {
        var c = ca[i].trim();
        if (c.indexOf(name) == 0) return c.substring(name.length, c.length)
    }
    return ""
}

function decode_create(temp) {
    var base = new Base64();
    var result = base.decode(temp);
    var result3 = "";
    for (i = 0; i < result.length; i++) {
        var num = result[i].charCodeAt();
        num = num ^ i;
        num = num - ((i % 10) + 2);
        result3 += String.fromCharCode(num)
    }
    return result3
}

function ertqwe() {
    var temp_name = "user";
    var temp = getCookie(temp_name);
    temp = decodeURIComponent(temp);
    var mingwen = decode_create(temp);
    var ca = mingwen.split(';');
    var key = "";
    for (i = 0; i < ca.length; i++) {
        if (-1 < ca[i].indexOf("flag")) {
            key = ca[i + 1].split(":")[2]
        }
    }
    key = key.replace('"', "").replace('"', "");
    document.write('<img id="attack-1" src="image/1-1.jpg">');
    setTimeout(function () {
        document.getElementById("attack-1").src = "image/1-2.jpg"
    }, 1000);
    setTimeout(function () {
        document.getElementById("attack-1").src = "image/1-3.jpg"
    }, 2000);
    setTimeout(function () {
        document.getElementById("attack-1").src = "image/1-4.jpg"
    }, 3000);
    setTimeout(function () {
        document.getElementById("attack-1").src = "image/6.png"
    }, 4000);
    setTimeout(function () {
        alert("浣犱娇鐢ㄥ□鏁ョ□鎺屾墦璐ヤ簡鑷€佸爮锛屼綘鍏嶇敓闃撳槸鍖熷韩杩樻槸鍋囧韩锛屾
浜よ瘯涓€涓嬪惂!flag{" + md5(key) + "}")
```

原文链接：江湖魔头 Writeup

```
    }, 5000)
}
```

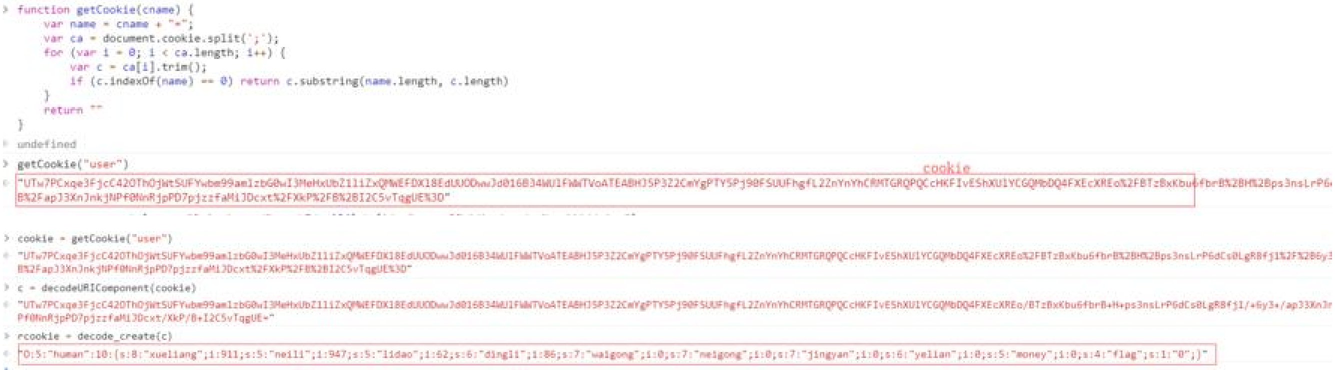
getCookie()是为了获取cookie，在ertqwe()中传入user,接下来我们还发现了decodeURIComponent)以及decode_create(),后面的for循环里面处理得到key,最后会得到一下MD5加密的flag。

说白了这里唯一可以做文章的地方就是cookie了，因为经过了几个函数我们都还没研究过。接下来继跟踪具体函数吧。



Name	Value	Do...	P...	Expire
user	UTw7PCxqe3FjcC42OThOjWtSUFYwbm99amlzbG0wI3MeHxUbZ1IiZxQMWEFDXI8EdUUODwwJd016B34WUlFWWTVoATEABHJ5P...	123....	/	2019-(

我们也只发现一个user



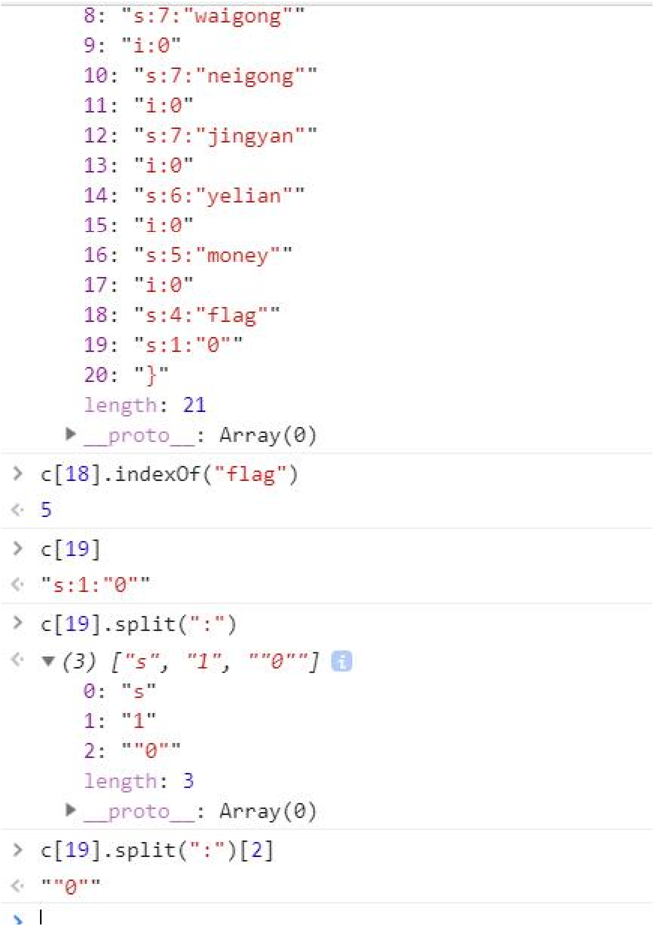
```
> function getCookie(cname) {
      var name = cname + "=";
      var ca = document.cookie.split(';');
      for (var i = 0; i < ca.length; i++) {
          var c = ca[i].trim();
          if (c.indexOf(name) == 0) return c.substring(name.length, c.length)
      }
      return ""
  }
< undefined
> getCookie("user")
< "UTw7PCxqe3FjcC42OThOjWtSUFYwbm99amlzbG0wI3MeHxUbZ11iZxQMWEFDX18EdUUODwwJd016B34WU1FWWTVoATEABHJ5P3Z2CmYgPTY5Pj90FSUUFhgfL2ZnYnYhCRMTGRQPQCcHKFIvEShXU1YCGQMbDQ4FXEcXREo%2FBTzBxKbu6fbrB%2BH%2Bps3nsLrP6
  B%2FapJ3XnJnkjNPf0NnRjpPD7pjzzfaMiJDcxt%2FXkP%2FB%2BI2C5vTqgUE%3D"
                                                                                    cookie
> cookie = getCookie("user")
< "UTw7PCxqe3FjcC42OThOjWtSUFYwbm99amlzbG0wI3MeHxUbZ11iZxQMWEFDX18EdUUODwwJd016B34WU1FWWTVoATEABHJ5P3Z2CmYgPTY5Pj90FSUUFhgfL2ZnYnYhCRMTGRQPQCcHKFIvEShXU1YCGQMbDQ4FXEcXREo%2FBTzBxKbu6fbrB%2BH%2Bps3nsLrP6dCs0LgR8fj1%2F%2B6y3
  B%2FapJ3XnJnkjNPf0NnRjpPD7pjzzfaMiJDcxt%2FXkP%2FB%2BI2C5vTqgUE%3D"
> c = decodeURIComponent(cookie)
< "UTw7PCxqe3FjcC42OThOjWtSUFYwbm99amlzbG0wI3MeHxUbZ11iZxQMWEFDX18EdUUODwwJd016B34WU1FWWTVoATEABHJ5P3Z2CmYgPTY5Pj90FSUUFhgfL2ZnYnYhCRMTGRQPQCcHKFIvEShXU1YCGQMbDQ4FXEcXREo/BTzBxKbu6fbrB+H+ps3nsLrP6dCs0LgR8fj1/+6y3+/ap33XnJr
  Pf0NnRjpPD7pjzzfaMiJDcxt/XkP/B+I2C5vTqgUE="
> rcookie = decode_create(c)
< "O:5:"human":10:{s:8:"xueliang";i:911;s:5:"neili";i:947;s:5:"lidao";i:62;s:6:"dingli";i:86;s:7:"waigong";i:0;s:7:"neigong";i:0;s:7:"jingyan";i:0;s:6:"yelian";i:0;s:5:"money";i:0;s:4:"flag";s:1:"0";}"
```

O:5:"human":10:{s:8:"xueliang";i:911;s:5:"neili";i:947;s:5:"lidao";i:62;s:6:"dingli";i:86;s:7:"waigong" i:0;s:7:"neigong";i:0;s:7:"jingyan";i:0;s:6:"yelian";i:0;s:5:"money";i:0;s:4:"flag";s:1:"0";}

这里看到了最后得到的是cookie反序列化后的字符串，但同时我们发现money为0，太穷了！！！

怎么才能有钱呢?

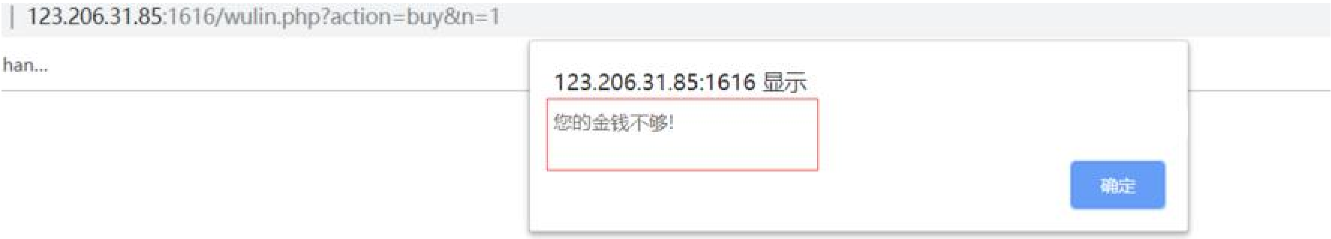
我们先来看看for循环哦



```
      8: "s:7:"waigong""
      9: "i:0"
      10: "s:7:"neigong""
      11: "i:0"
      12: "s:7:"jingyan""
      13: "i:0"
      14: "s:6:"yelian""
      15: "i:0"
      16: "s:5:"money""
      17: "i:0"
      18: "s:4:"flag""
      19: "s:1:"0""
      20: "}"
      length: 21
    ▶ __proto__: Array(0)
> c[18].indexOf("flag")
< 5
> c[19]
< "s:1:"0""
> c[19].split(":")
< ▼ (3) ["s", "1", ""0""]
      0: "s"
      1: "1"
      2: ""0""
      length: 3
    ▶ __proto__: Array(0)
> c[19].split(":")[2]
< ""0""
>
```

这里的意思也就是即使你把这段代码直接跑也会的得到一个MD5，只是为空值。 显然不是flag。

现在我们来看一下直接去买装备是啥情况！



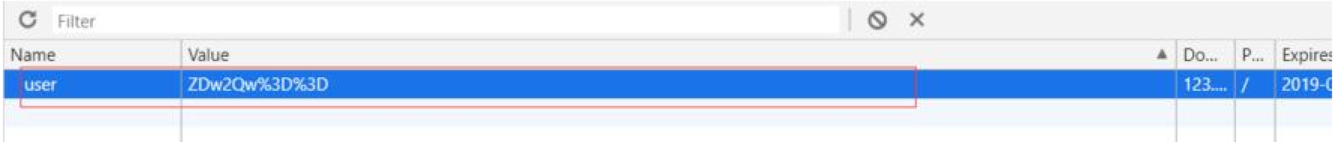
123.206.31.85:1616/wulin.php?action=buy&n=1

han...

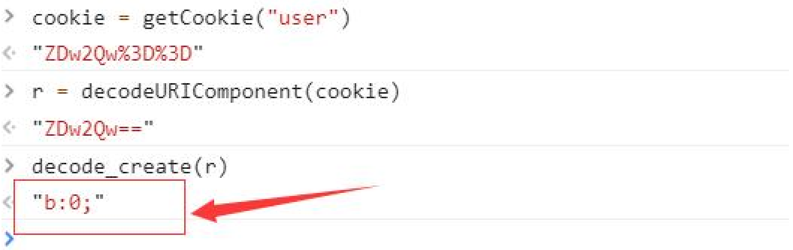
123.206.31.85:1616 显示

您的金钱不够!

买不起，我们打开cookie看一下。



Name	Value	Do...	P...	Expires
user	ZDw2Qw%3D%3D	123....	/	2019-(



```
> cookie = getCookie("user")
< "ZDw2Qw%3D%3D"
> r = decodeURIComponent(cookie)
< "ZDw2Qw=="
> decode_create(r)
< "b:0;"
>
```

原文链接：江湖魔头 Writeup

关键字段，也就是这里面都是钱啊！！！知道为什么这么穷了吧，因为你没钱！

现在的目的很明显，就是要有钱！

`"money";i:0;`

现在目标就转为逆向加密。

encodeURIComponent()函数已经提供给我们，但是我们还想有一个encode_create()那就更完美了。

可是天上哪有掉馅饼的好事呢？

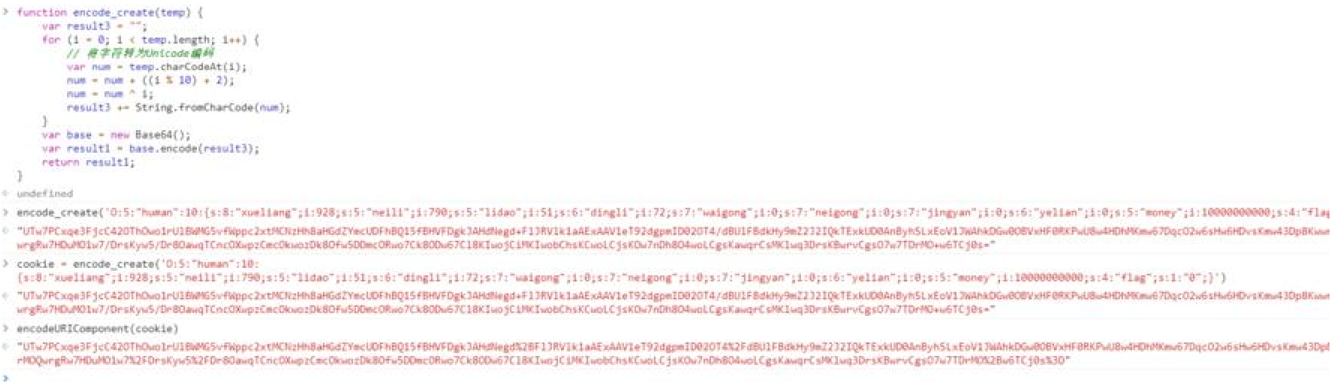
现在进入decode_create()分析阶段。

```
function decode_create(temp) {
    var base = new Base64();  // Base64
    var result = base.decode(temp);  //decode()
    var result3 = "";
    for (i = 0; i < result.length; i++) {
        var num = result[i].charCodeAt(); // decode后进行按位获取Ascii值
        num = num ^ i; // 与位置进行异或
        num = num - ((i % 10) + 2); // 进行运算
        result3 += String.fromCharCode(num) // 最后转为字符
    }
    return result3
}
```

下面开始编写加密函数(重点！！)：

```
function encode_create(temp) {
    var result3 = "";
    for (i = 0; i < temp.length; i++) {
        // 将字符转为Unicode编码
        var num = temp.charCodeAt(i);
        num = num + ((i % 10) + 2);
        num = num ^ i;
        result3 += String.fromCharCode(num);
    }
    var base = new Base64();
    var result1 = base.encode(result3);
    return result1;
}
```

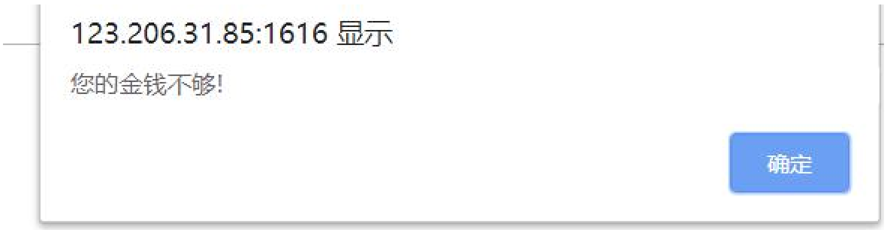
下面我们就开始变有钱的操作！



```
> function encode_create(temp) {
      var result3 = "";
      for (i = 0; i < temp.length; i++) {
          // 将字符转为Unicode编码
          var num = temp.charCodeAt(i);
          num = num + ((i % 10) + 2);
          num = num ^ i;
          result3 += String.fromCharCode(num);
      }
      var base = new Base64();
      var result1 = base.encode(result3);
      return result1;
  }
< undefined
> encode_create('O:5:"human":10:{s:8:"xueliang";i:928;s:5:"neili";i:790;s:5:"lidao";i:51;s:6:"dingli";i:72;s:7:"waigong";i:0;s:7:"neigong";i:0;s:7:"jingyan";i:0;s:6:"yelian";i:0;s:5:"money";i:10000000000;s:4:"flag
< "UTw7PCxqe3FjcC420ThOwo1rU1BWMG5vfWppc2xtMCNzHhBaHGdZYmcUDFhBQ15fBHVFDgkJAHdNegd+F1JRV1k1aAExAAV1eT92dgpmID02OT4/dBU1FBdkHy9mZ2J2IQkTExkUD0AnByh5LxEoV1JWAhkDGw0OBVxHF0RKPwU8w4HDhMKmw67DqcO2w6sHw6HDvsKmw43DpBKww
  wrgRw7HDuMO1w7/DrsKyw5/Dr8OawqTCncOXwpzCmcOkwozDk8OfwSDDmcORwo7Ck8ODw67C18KIwojCiMKIwobChsKCwolCjsKOw7nDh8O4woLCgsKawqrCsMK1wq3DrsKBwrvCgsO7w7TDrMO+w6TCj0s="
> cookie = encode_create('O:5:"human":10:
  {s:8:"xueliang";i:928;s:5:"neili";i:790;s:5:"lidao";i:51;s:6:"dingli";i:72;s:7:"waigong";i:0;s:7:"neigong";i:0;s:7:"jingyan";i:0;s:6:"yelian";i:0;s:5:"money";i:10000000000;s:4:"flag";s:1:"0";}')
< "UTw7PCxqe3FjcC420ThOwo1rU1BWMG5vfWppc2xtMCNzHhBaHGdZYmcUDFhBQ15fBHVFDgkJAHdNegd+F1JRV1k1aAExAAV1eT92dgpmID02OT4/dBU1FBdkHy9mZ2J2IQkTExkUD0AnByh5LxEoV1JWAhkDGw0OBVxHF0RKPwU8w4HDhMKmw67DqcO2w6sHw6HDvsKmw43DpBKww
  wrgRw7HDuMO1w7/DrsKyw5/Dr8OawqTCncOXwpzCmcOkwozDk8OfwSDDmcORwo7Ck8ODw67C18KIwojCiMKIwobChsKCwolCjsKOw7nDh8O4woLCgsKawqrCsMK1wq3DrsKBwrvCgsO7w7TDrMO+w6TCj0s="
> encodeURIComponent(cookie)
< "UTw7PCxqe3FjcC420ThOwo1rU1BWMG5vfWppc2xtMCNzHhBaHGdZYmcUDFhBQ15fBHVFDgkJAHdNegd%2BF1JRV1k1aAExAAV1eT92dgpmID02OT4%2FdBU1FBdkHy9mZ2J2IQkTExkUD0AnByh5LxEoV1JWAhkDGw0OBVxHF0RKPwU8w4HDhMKmw67DqcO2w6sHw6HDvsKmw43DpB
  rMOQwrgRw7HDuMO1w7%2FDrsKyw5%2FDr8OawqTCncOXwpzCmcOkwozDk8OfwSDDmcORwo7Ck8ODw67C18KIwojCiMKIwobChsKCwolCjsKOw7nDh8O4woLCgsKawqrCsMK1wq3DrsKBwrvCgsO7w7TDrMO%2Bw6TCj0s%3D"
>
```

原文链接：江湖魔头 Writeup

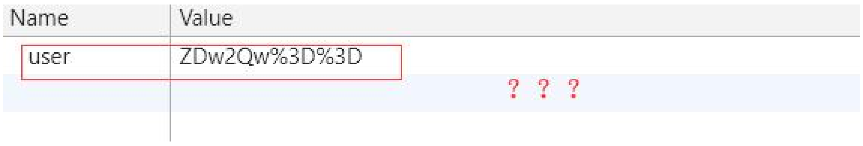
但是我们发现还是买不了？？？



123.206.31.85:1616 显示

您的金钱不够!

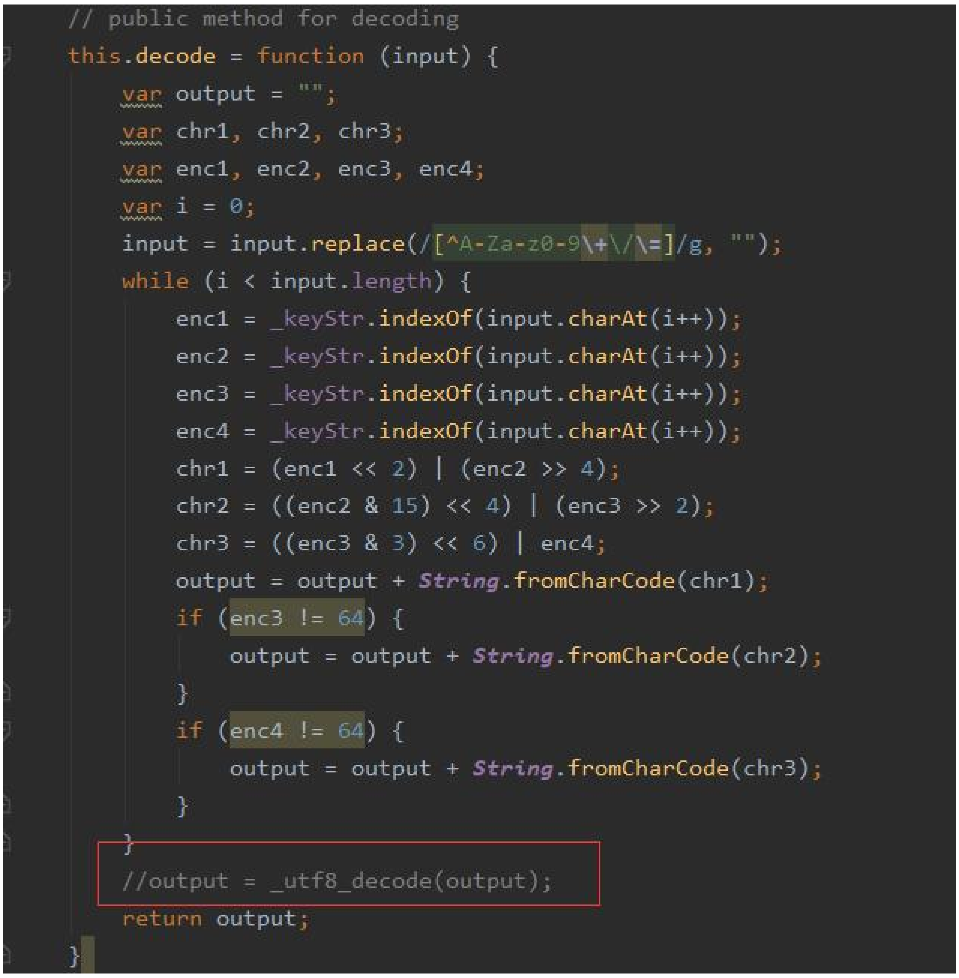
查看cookie发现没有修改成功!



Name	Value
user	ZDw2Qw%3D%3D

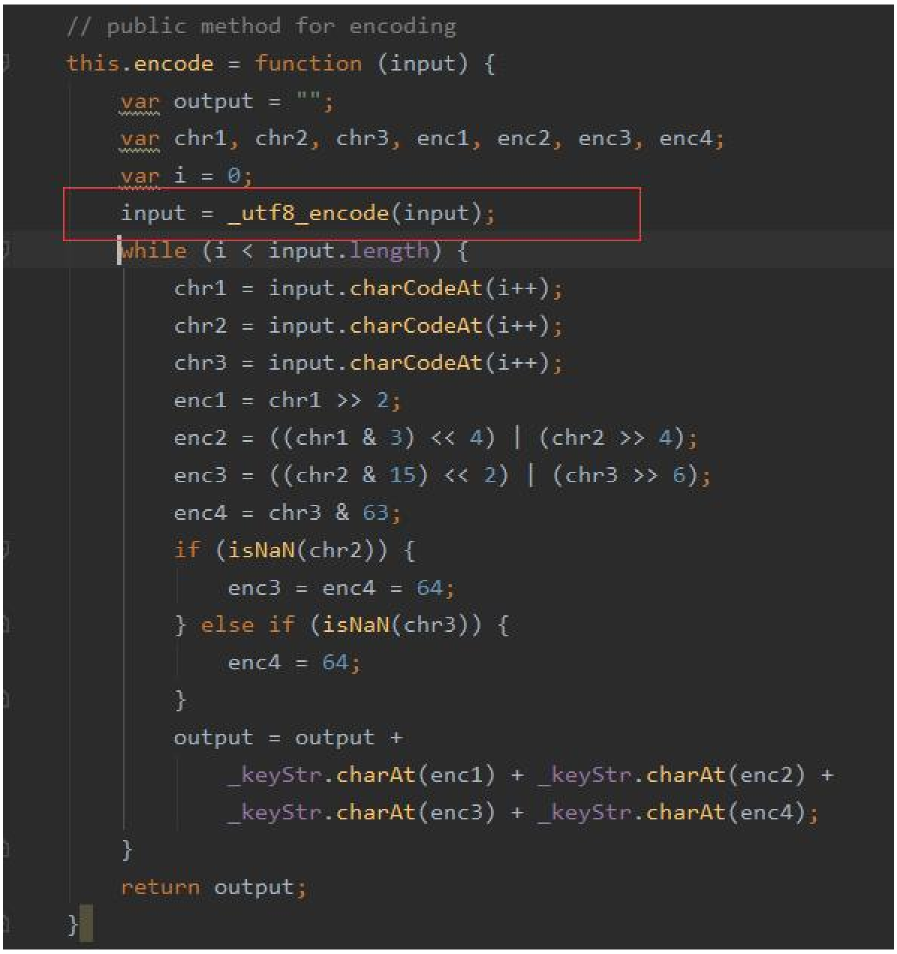
？？？

仔细思考发现刚才的Base64我们没有跟踪进去看，肯定是它搞的鬼!



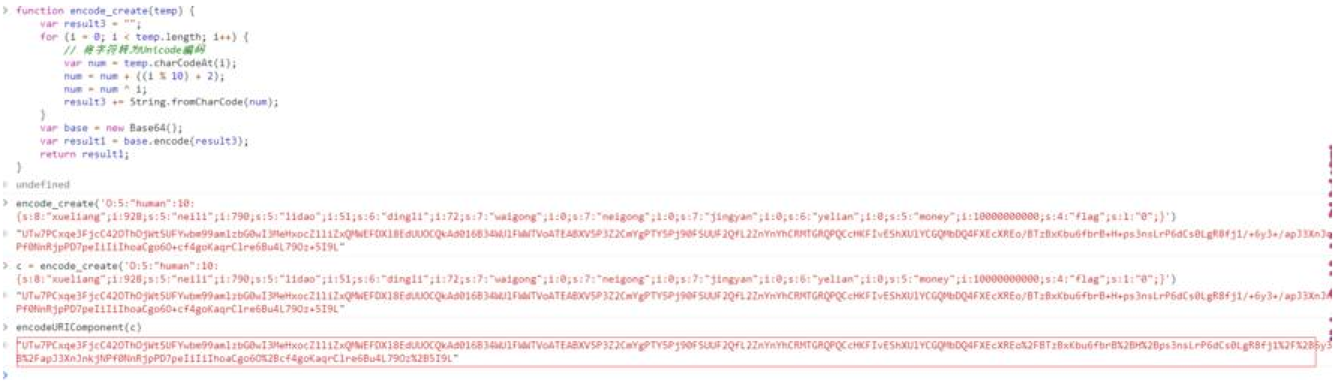
```
    // public method for decoding
    this.decode = function (input) {
        var output = "";
        var chr1, chr2, chr3;
        var enc1, enc2, enc3, enc4;
        var i = 0;
        input = input.replace(/[^A-Za-z0-9\+\/\=]/g, "");
        while (i < input.length) {
            enc1 = _keyStr.indexOf(input.charAt(i++));
            enc2 = _keyStr.indexOf(input.charAt(i++));
            enc3 = _keyStr.indexOf(input.charAt(i++));
            enc4 = _keyStr.indexOf(input.charAt(i++));
            chr1 = (enc1 << 2) | (enc2 >> 4);
            chr2 = ((enc2 & 15) << 4) | (enc3 >> 2);
            chr3 = ((enc3 & 3) << 6) | enc4;
            output = output + String.fromCharCode(chr1);
            if (enc3 != 64) {
                output = output + String.fromCharCode(chr2);
            }
            if (enc4 != 64) {
                output = output + String.fromCharCode(chr3);
            }
        }
        //output = _utf8_decode(output);
        return output;
    }
```

在decode这个方法中，我们发现很诡异的地方这里被注释掉了，但是在encode方法中是这样的。



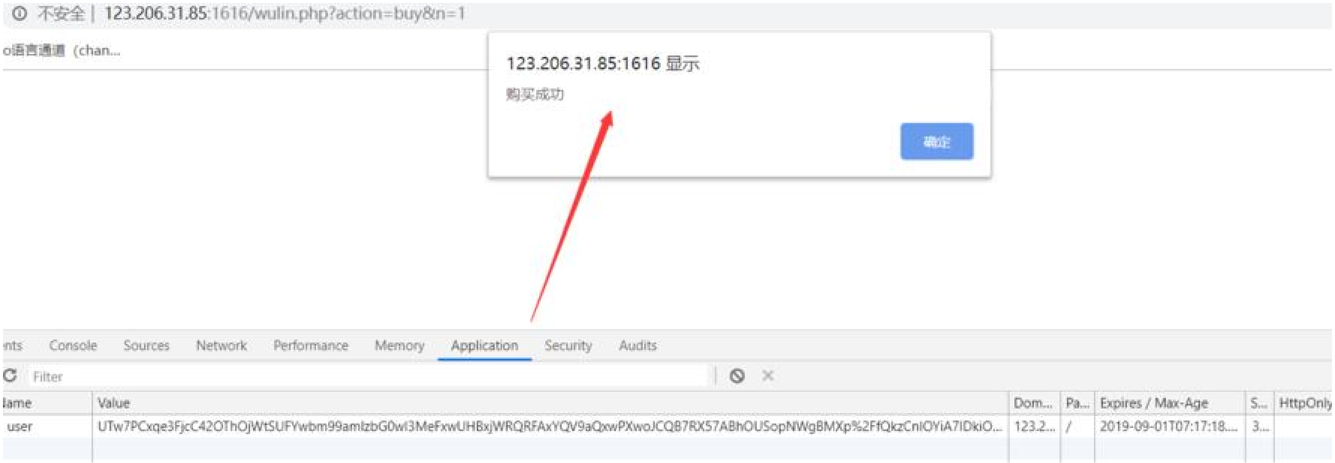
```
    // public method for encoding
    this.encode = function (input) {
        var output = "";
        var chr1, chr2, chr3, enc1, enc2, enc3, enc4;
        var i = 0;
        input = _utf8_encode(input);
        while (i < input.length) {
            chr1 = input.charCodeAt(i++);
            chr2 = input.charCodeAt(i++);
            chr3 = input.charCodeAt(i++);
            enc1 = chr1 >> 2;
            enc2 = ((chr1 & 3) << 4) | (chr2 >> 4);
            enc3 = ((chr2 & 15) << 2) | (chr3 >> 6);
            enc4 = chr3 & 63;
            if (isNaN(chr2)) {
                enc3 = enc4 = 64;
            } else if (isNaN(chr3)) {
                enc4 = 64;
            }
            output = output +
                _keyStr.charAt(enc1) + _keyStr.charAt(enc2) +
                _keyStr.charAt(enc3) + _keyStr.charAt(enc4);
        }
        return output;
    }
```

所以明白了吧，我们现在的目的就要把这里注释掉，然后覆盖一下这个函数！



```
> function encode_create(temp) {
      var result3 = "";
      for (i = 0; i < temp.length; i++) {
          // 将字符转为Unicode编码
          var num = temp.charCodeAt(i);
          num = num + ((i % 10) + 2);
          num = num ^ i;
          result3 += String.fromCharCode(num);
      }
      var base = new Base64();
      var result1 = base.encode(result3);
      return result1;
  }
< undefined
> encode_create('O:5:"human":10:
  {s:8:"xueliang";i:928;s:5:"neili";i:790;s:5:"lidao";i:51;s:6:"dingli";i:72;s:7:"waigong";i:0;s:7:"neigong";i:0;s:7:"jingyan";i:0;s:6:"yelian";i:0;s:5:"money";i:10000000000;s:4:"flag";s:1:"0";}')
< "UTw7PCxqe3FjcC42OThOjWtSUFYwbm99amlzbG0wI3MeHxocZ111ZxQMWEFDX18EdUUOCQkAd016B34WU1FWWTVoATEABXV5P3Z2CmYgPTY5Pj90FSUUF2QfL22nYnYhCRMTGRQPQCcHKFIvEShXU1YCGQMbDQ4FXEcXREo/BTzBxKbu6fbrB+H+ps3nsLrP6dCs0LgR8fj1/+6y3+/apJ3XnJq
  PF0NnRjpPD7peIiIiIhoaCgo60+cf4goKaqrClre6Bu4L79Oz+5I9L"
> c = encode_create('O:5:"human":10:
  {s:8:"xueliang";i:928;s:5:"neili";i:790;s:5:"lidao";i:51;s:6:"dingli";i:72;s:7:"waigong";i:0;s:7:"neigong";i:0;s:7:"jingyan";i:0;s:6:"yelian";i:0;s:5:"money";i:10000000000;s:4:"flag";s:1:"0";}')
< "UTw7PCxqe3FjcC42OThOjWtSUFYwbm99amlzbG0wI3MeHxocZ111ZxQMWEFDX18EdUUOCQkAd016B34WU1FWWTVoATEABXV5P3Z2CmYgPTY5Pj90FSUUF2QfL22nYnYhCRMTGRQPQCcHKFIvEShXU1YCGQMbDQ4FXEcXREo/BTzBxKbu6fbrB+H+ps3nsLrP6dCs0LgR8fj1/+6y3+/apJ3XnJ4
  PF0NnRjpPD7peIiIiIhoaCgo60+cf4goKaqrClre6Bu4L79Oz+5I9L"
> encodeURIComponent(c)
< "UTw7PCxqe3FjcC42OThOjWtSUFYwbm99amlzbG0wI3MeHxocZ111ZxQMWEFDX18EdUUOCQkAd016B34WU1FWWTVoATEABXV5P3Z2CmYgPTY5Pj90FSUUF2QfL22nYnYhCRMTGRQPQCcHKFIvEShXU1YCGQMbDQ4FXEcXREo%2FBTzBxKbu6fbrB%2BH%2Bps3nsLrP6dCs0LgR8fj1%2F%2B6y3
  B%2FapJ3XnJnkjNPF0NnRjpPD7peIiIiIhoaCgo60%2Bcf4goKaqrClre6Bu4L79Oz%2B5I9L"
>
```

现在购买成功了



ⓘ 不安全 | 123.206.31.85:1616/wulin.php?action=buy&n=1
o语言通道 (chan...

123.206.31.85:1616 显示

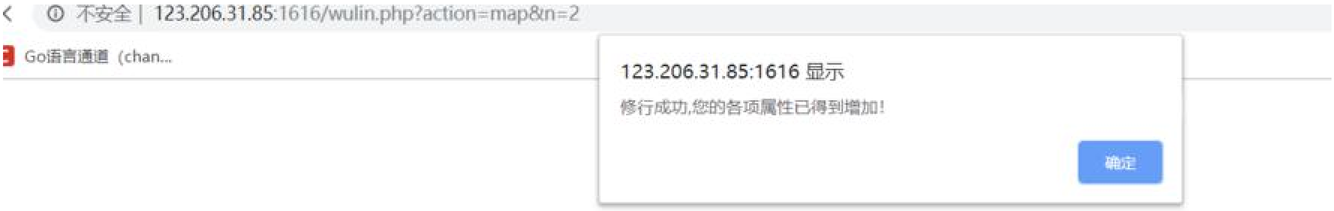
购买成功

确定
nts Console Sources Network Performance Memory Application Security Audits
C Filter

lame	Value	Dom...	Pa...	Expires / Max-Age	S...	HttpOnly
user	UTw7PCxqe3FjcC42OThOjWtSUFYwbm99amlzbG0wI3MeFxwUHBxjWRQRFAxYQV9aQxwPXwoJCQB7RX57ABhOUSopNWgBMXp%2FfQkzCnlOYiA7lDkiO...	123.2...	/	2019-09-01T07:17:18....	3...	

原文链接：江湖魔头 Writeup

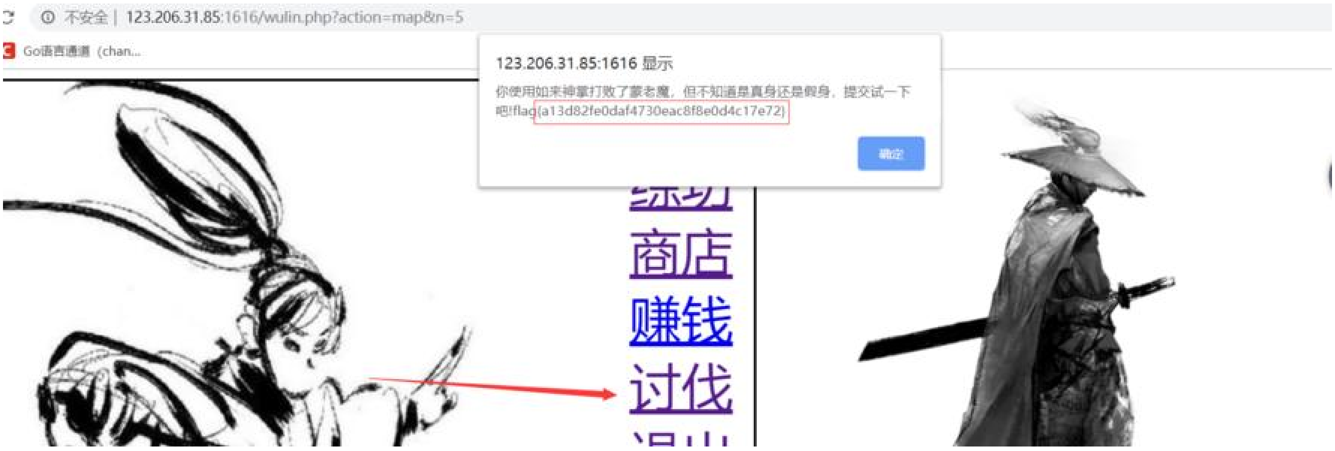
然后练功！



123.206.31.85:1616 显示

修行成功,您的各项属性已得到增加！

讨伐就成功拿到flag！！！



123.206.31.85:1616 显示

你使用如来神掌打败了蒙老魔，但不知道是真身还是假身，提交试一下吧!flag{a13d82fe0daf4730eac8f8e0d4c17e72}

原文链接：江湖魔头 Writeup