Bugku CTF 每日一题 game1

原创

彼岸花苏陌 于 2022-01-10 19:31:11 发布 1523 收藏

分类专栏： ctf 文章标签： ctf web

本文链接：https://blog.csdn.net/qq_42263820/article/details/122417464

首先这是一个网页游戏

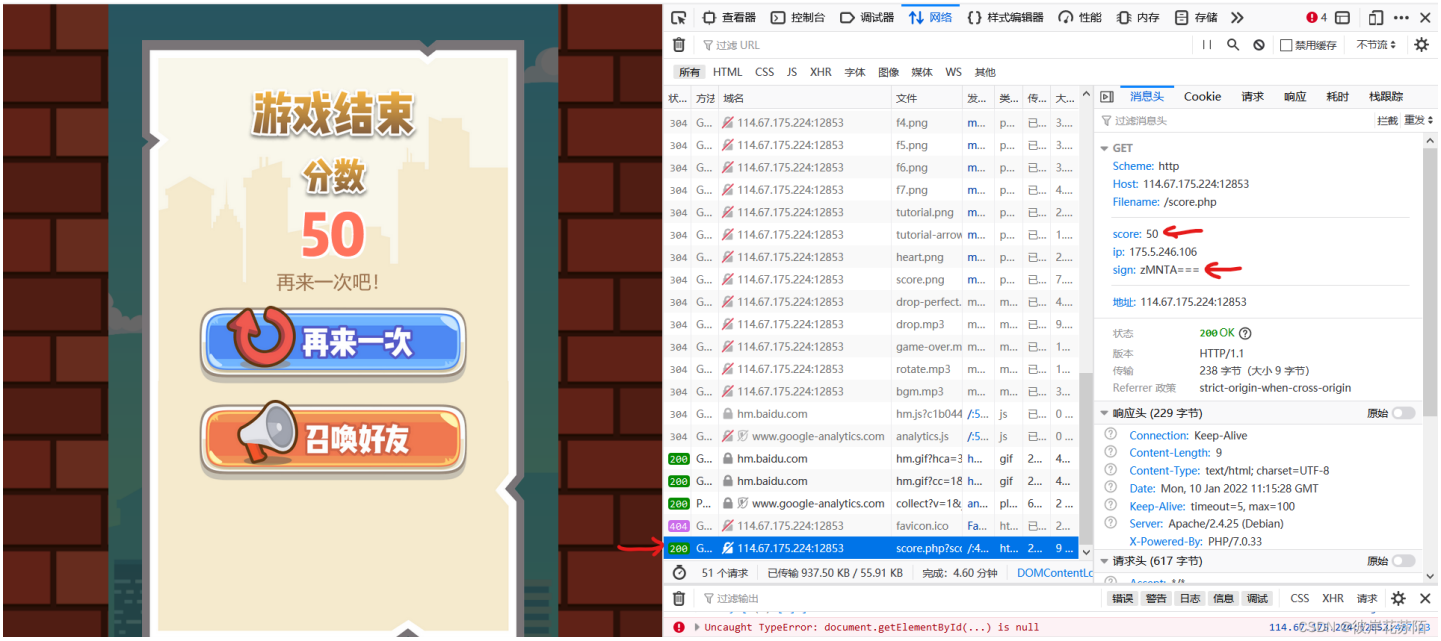
解这类题的方法要查看网页源码 在源码中找到端倪

首先玩一下游戏 发现到后面越来越难 所以这类解题要动手修改一下数值

1.先抓包，发现出现了这个

使用repeater修改后提交发现不行

于是网页上又玩了一把 打完后发现了这个



发现有个sign的值，右键查看源码后ctrl+f搜索sign发现了这个

```
            }
        }
        var ppp='175.5.246.106';
        var sign = Base64.encode(score.toString());
        xmlhttp.open("GET","score.php?score="+score+"&ip="+ppp+"&sign="+sign,true);
        xmlhttp.send();
    $('#over-zero').show()
}

// game customization options
```


原来是base64加密，再回到上图中把50的值加密看看？

发现50加密后是NTA=

于是猜测sign的组成是zM+数值+==提交一次试一下发现

Request

Raw | Params | Headers | Hex

```
GET /score.php?score=999999&ip=175.5.246.106&sign=zMOTk5OTk5==
HTTP/1.1
Host: 114.67.175.224:12853
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0)
Gecko/20100101 Firefox/88.0
Accept: */*
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
Connection: close
Referer:
http://114.67.175.224:12853/?s=1641812333919?s=1641812416044?s=1
641812676374?s=1641812771746
Cookie: Hm_lvt_c1b044f909411ac4213045f0478e96fc=1641812247;
Hm_lpvt_c1b044f909411ac4213045f0478e96fc=1641812772;
_ga=GA1.1.2106414304.1641812250;
_gid=GA1.1.1796833814.1641812250; _gat=1
Pragma: no-cache
Cache-Control: no-cache
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Mon, 10 Jan 2022 11:24:14 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/7.0.33
Content-Length: 38
Connection: close
Content-Type: text/html; charset=UTF-8

flag{2997bed68456a978c4dd20b49d0d4e7a}
```


得到flag！