HashTeam web_阴间2048 writeup

原创

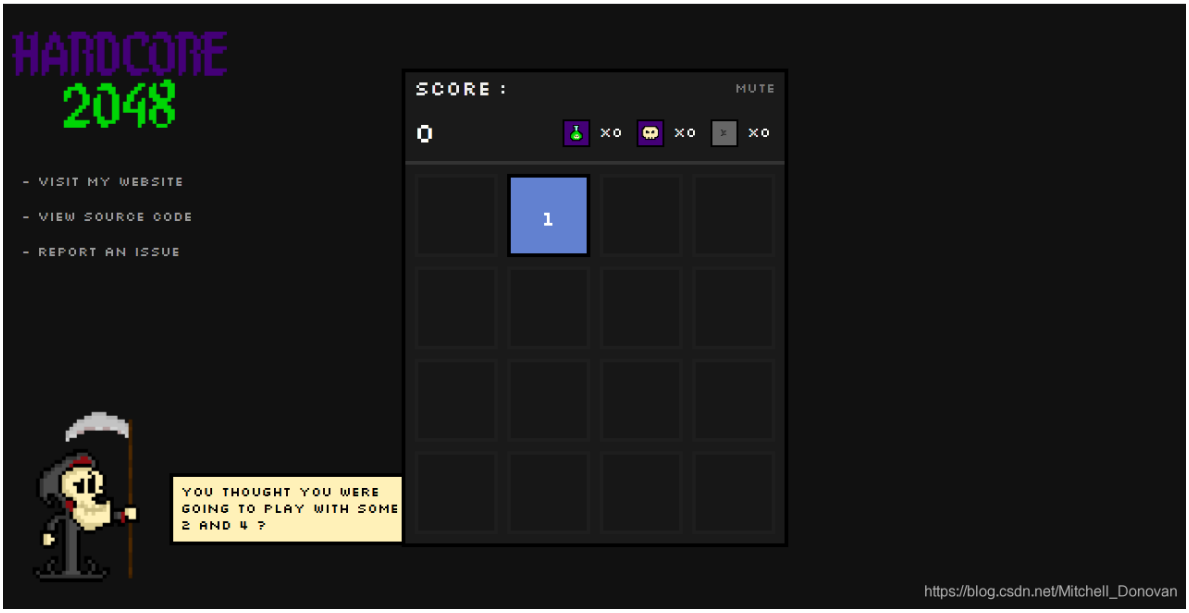
Mitch311 于 2020-12-29 21:01:46 发布 637 收藏
分类专栏： CTF 文章标签： unctf

HashTeam web_阴间2048

原题链接

key:JS代码审计(假)+控制台URL(真)

①原题界面长这样式的□



看不出来啥，怎么操作也没用，习惯性地F12看一下源码（这种签到题提示一般都在源码里给）

得到提示，where is game.js?

②按照提示，来网络这里找到game.js

点进去md全是黑白的代码，眼要瞎了，还是来vscode里审计吧

③进行js代码审计，先大致浏览一下，发现了可疑代码段

```
check_lose: function()
{
    if(this.score>233333)
    {
        url="?OrbicQu4ck_is_="+('h'+'a'+'n'+'d'+'s'+'o'+'m'+'e').toLowerCase();
        this.lose();
    }
    if (this.find_pos()) return ;
    for (var x = 0; x < 4; ++x)
    {
        for (var y = 0; y < 4; ++y)
        {
```


这里给了提示url，我们把这段代码复制到控制台中执行一下

```
>> url="?OrbicQu4ck_is_="+('h'+'a'+'n'+'d'+'s'+'o'+'m'+'e').toLowerCase();
<- "?OrbicQu4ck_is_=handsome"
```

④可以看到结果字符串前有一个?，后面是一个变量等于一个值

结合前面的url可以知道这里大概是要你get提交一下这个值

get提交参数OrbicQu4ck_is_=handsome，得到flag