

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

版权声明: 本文为博主原创文章, 遵循 CC 4.0 BY-SA 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/Mitchell_Donovan/article/details/111936262

版权



[CTF 专栏收录该内容](#)

51 篇文章 3 订阅

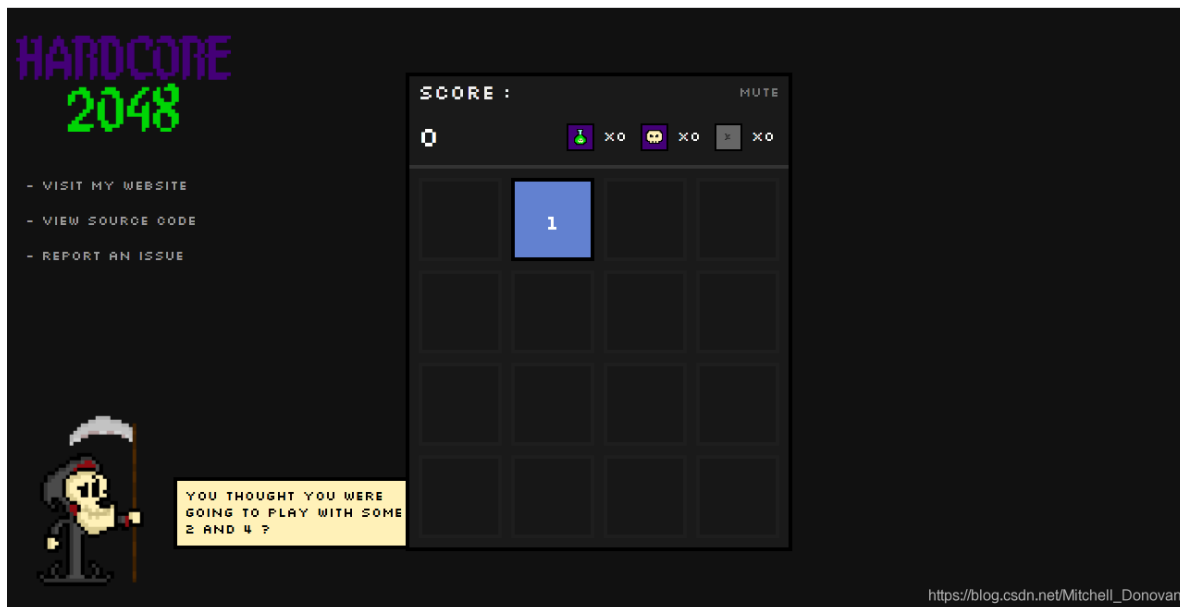
订阅专栏

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)

```
<!DOCTYPE html>
<html> event 滚动 登山
  <head> ... </head>
  <body>
    <!--where is game.js?-->
    <header id="main_header"> ... </header>
    <div id="loading_div" style="display: none;"> ... </div>
    <main id="main" role="main" style="display: block;"> ... </main>
    <div id="finish_div"> ... </div>
    <div id="reaper" class="stand" style="display: block;"> ... </div>
    <p id="reaper_text" style="display: block;"> ... </p>
    <script asvnc="" src="https://www.goole-analytics.com/analytics.js"></script>
  </body>
```

得到提示, where is game.js?

②按照提示，来网络这里找到game.js



状态	方法	域名	文件
200	GET	47.103.222.234:28734	/
200	GET	47.103.222.234:28734	resources.js
200	GET	47.103.222.234:28734	index.js
200	GET	47.103.222.234:28734	ui.js
304	GET	47.103.222.234:28734	game.js
304	GET	47.103.222.234:28734	animation.js
304	GET	47.103.222.234:28734	reaper.js

30 个请求 | 已传输 406.84 KB / 244.38 KB | 完成: 2.44 秒 | DOMContentLoaded: 1.02 秒 | load: 1.52 秒

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)
    {
```

https://blog.csdn.net/Mitchell_Donovan

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

