hgame第一周wp

原创

不毅 于 2021-02-05 21:49:12 发布 143 收藏

分类专栏： ctf 文章标签： web 安全

本文链接：https://blog.csdn.net/strange_stv/article/details/113678954

文章目录

前言

开始参加hgame之后才发现自己实在是太菜了。不停地问大佬们才搞出了几道签到题。有点灰心，不过本来参加的目的就是借此多学点东西，所以也无所谓了。

---

web

Hitchhiking_in_the_Galaxy

Description

第一次在银河系里搭顺风车，要准备啥，在线等，挺急的

Challenge Address http://hitchhiker42.0727.site:42420

首先F12一下，发现源码中有这样一个文件

```
<html>
 <head>…</head>
 <body> == $0
  <div class="page-wrap d-flex flex-row align-items-center">
   <div class="container">
    <div class="row justify-content-center">
     <div class="col-md-12 text-center">
      <span class="display-1 d-block">404</span>
      <div class="mb-4 lead">你来晚了，地球已经被沃贡人摧毁了。原因是地球挡住了它们的超空间快速通道。</div>
      <a href="HitchhikerGuide.php" class="btn btn-link">我要搭顺风车！</a>
     </div>
    </div>
   </div>
  </div>
 </body>
</html>
```



```
href="HitchhikerGuide.php"
```

因为啥都不会，先找了一遍文件，果然没有。那就只好抓包。先改了一下请求方法，get换post，把请求头改成了上面那个文件，出了一个提示,要什么无限非概率引擎。好家伙，我还以为是什么浏览器引擎之类的。后来修改了UA，跳出提示，要通过指定网址访问。

```
你知道吗？<a href="https://github.com/wuhan005">茄子</a>
特别要求：你得从他的<a href="https://cardinal.ink/">Cardinal</a>
过来
```

在头部增加referer，得到如下所示

Request

Pretty | Raw | \n | Actions

```
1 POST /HitchhikerGuide.php HTTP/1.1
2 referer:https://cardinal.ink/
3 Host: hitchhiker42.0727.site:42420
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Infinite Improbability Drive/87.0.4280.88 Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.
  8,application/signed-exchange;v=b3;q=0.9
7 Accept-Encoding: gzip, deflate
8 Accept-Language: zh-CN,zh;q=0.9
9 Connection: close
```

Response

Pretty | Raw | Render | \n | Actions

```
1 HTTP/1.1 200 OK
2 Date: Tue, 02 Feb 2021 07:52:17 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Content-Length: 39
5 Connection: close
6 Content-Type: text/html; charset=UTF-8
7
8 flag仅能通过本地访问获得
9
```


要本地访问，那就添加X-Forwarded-For: 127.0.0.1得到flag。

watermelon

Description

简单且上头的游戏

Challenge Address http://watermelon.ryen.xyz:800/

首先发现，大西瓜真好玩）抓包了一下，想看看有没有返回分数的post请求，发现啥也没有。然后F12，找js文件中的游戏分数变量啥的（我都不知道有Ctrl+f快速搜索这种东西，眼睛都瞎了），还是没有。想想看显示flag还有两种可能，一种是游戏结束，一种是跳出弹窗。游戏结束的地方没有方法，果断搜alert。

```
gameOverShowText: function(e, t) {
    if (e > 1999) {
        alert(window.atob("aGdhbWV7ZG9feW91X2tub3dfY29jb3NfZ2FtZT99"))
    }
```

居然还是写了文件加密的。查了百度了之后知道，同个网页下js代码可以直接拖到控制台运行。然后就跳出一个带有弹窗的flag了。

智商检测鸡

Description
又有谁不爱高数呢？反正我不爱（请使用firefox浏览器打开题目）
Challenge Address http://r4u.top:5000/

不说了，写了一个计算器，硬怼出来的。。还在学js

misc

Base全家福

Description
新年即将来临之际，Base家族也团聚了，他们用他们特有的打招呼方式向你问了个好，你知道他们在说什么吗？
R1k0RE1OWldHRTNFSU5SVkc1QkRLTlpXR1VaVENOUlRHTVlETVJCV0dVMlVNTlpVR01ZREtSUlVlQTJET01aVUdSQ0RHTVpWSVlaVEVNWlFHTVpER01KWElRPT09PT09
本次比赛为招新赛，请各位选手不要在当周比赛进行期间至结束后24小时内发布当周比赛题目的writeup
Challenge Address https://www.baidu.com

绝了啊，Base64、Base32、Base16一路解过去就完事了

总结

提示：这里对文章进行总结：
例如：以上就是今天要讲的内容，本文仅仅简单介绍了pandas的使用，而pandas提供了大量能使我们快速便捷地处理数据的函数和方法。