

BugkuCTF-Web-你必须让他停下

原创

烟雨天青色 于 2018-12-13 18:26:17 发布 7083 收藏 1

分类专栏: [CTF](#) 文章标签: [BugkuCTF](#)

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/qq_38603541/article/details/84992941

版权



[CTF 专栏收录该内容](#)

29 篇文章 1 订阅

订阅专栏



看到题目的名字: 你必须让他停下, 嗯? 咋滴, 还跑了不成, 哈哈哈哈哈。点开题目地址, 额。。。。这刷新速度有点快啊, 快到我已经不能完整看完源码了。不过呢? 在没进行任何操作之前, 还是发现了源码里面有一句: “flag is here~” 嗯, 看来是隐藏掉了。。。。咋办? 咋办? 咋办? 看不到源码, 找不到flag。。那只能有一个办法: 抓包!!

上BurpSuite!!

说点题外话: 使用BurpSuite抓包时最好使用Firefox浏览器, 配置起来比较简单也比较好上手。

回归正题, 看图:

在Firefox浏览器中把链接贴过来, 然后打开BurpSuite进行抓包操作。。。



I want to play Dummy game with others;But I can't stop!
Stop at panda! u will get flag



刚开始抓包，抓了好长时间都没有抓到有用的包，都是一些类似“Not Found”的包，终于经过一番分析：从一开始抓包开始，始终没有发现10.jpg的包，这就很奇怪了，既然是随机生成的，怎么会没有这个包呢，还有就是抓的包的长度看起来不太对，经过一顿倒腾，终于找到包了，抓到包就能发现源码，发现源码，然后。。然后。。flag就在源码里面。嘻嘻

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP	Cookies
1853	http://123.206.87.240:8002	GET	/favicon.ico			404	305	HTML	ico	404 Not Found			123.206.87.240	
1854	http://123.206.87.240:8002	GET	/web12/			200	766	HTML		Dummy game			123.206.87.240	
1856	http://123.206.87.240:8002	GET	/favicon.ico			404	305	HTML	ico	404 Not Found			123.206.87.240	
1857	http://123.206.87.240:8002	GET	/web12/			200	749	HTML		Dummy game			123.206.87.240	
1858	http://123.206.87.240:8002	GET	/web12/1.jpg			404	305	HTML	jpg	404 Not Found			123.206.87.240	
1859	http://123.206.87.240:8002	GET	/favicon.ico			404	305	HTML	ico	404 Not Found			123.206.87.240	
1860	http://123.206.87.240:8002	GET	/web12/			200	750	HTML		Dummy game			123.206.87.240	

Request Response

Raw Headers Hex HTML Render

```
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<meta name="description" content="">
<meta name="author" content="">
<title>Dummy game</title>
</head>

<script language="JavaScript">
function myrefresh(){
window.location.reload();
}
setTimeout("myrefresh()",500);
</script>
</body>
<center><strong>I want to play Dummy game with others&But I can't stop!</strong></center>
<center>Stop at panda! u will get flag</center>
<center><div></div></center><br><ca style="display:none">flag(dummy_game_1s_s0_popular)</ca></body>
</html>
```

有flag了，这题就完成了，嘻嘻，好好玩。



[创作打卡挑战赛](#)
[赢取流量/现金/CSDN周边激励大奖](#)