

微博存在支付逻辑漏洞

漏洞等级：高



搜索微博



## 首页

- 全部关注
- 最新微博
- 特别关注
- 好友圈

## 自定义分组

管理

- 游戏
- 11111
- 名人明星
- 同学
- 同事
- 悄悄关注

< 返回



一个带马的头像

精选

微博

相册

全部微博 (2)



6953 阅读 推广

按时间搜索

按

< 2021年  
1月 2月 3月 4月  
7月 8月 9月 10月

帮助中心  
微博客服 4000-960-960 自助服  
合作&服务  
微博营销 合作热线 4000-980-980  
举报中心

[点击此处](#)



## 我的粉丝



您的粉丝量太少了，请尝试推广给其它用户，积累粉丝后再来使用吧。

推广给更多用户

潜在粉丝

2000+人 40.00元 ▼

指定账号粉丝的相似用户

0元▼

兴趣用户

0元 ▼

### ① 绑定资质

选择资质 

## 资质管理

发现跳到此处

我的粉丝

您的粉丝量太少了, 请尝试推广给其它用户, 积累粉丝后再来使用吧。

推广给更多用户

潜在粉丝

覆盖用户数  + (输入范围 0-500000)

0 ————— 6000

指定账号粉丝的相似用户

0元 ▾

兴趣用户

0元 ▾

① 绑定资质 [选择资质 ▾](#) [资质管理](#)

预计覆盖人数: 100 +人 预计投放时长: 1小时

请阅读《服务协议》, 如无问题请完成支付

☒ 微博钱包(支持支付宝) ☐ 广告账户

2.00元 去支付

发现最低支付两元

← → ↻ https://pay.biz.weibo.com/promotenew?mid=4381767223721613&from=read\_profile\_v1pc\_04&ru=https://weibo.com 器 ☆

火狐官方网站 火狐官方网站 百度 新浪微博会员-精彩你... 新手上路 常用网址 京东商城 常用网址 京东商城 天猫 微博 爱淘宝 携程旅行 HTTP Status 404 - ... 京东商城 >> 移动设备上的书签

我的粉丝

您的粉丝量太少了，请尝试推广给其它用户，积累粉丝后再来使用吧。

推广给更多用户

潜在粉丝

输入范围 0 - 500000 10000.00元 ^

覆盖用户数 500000 + (输入范围 0-500000)

0 500000

指定账号粉丝的相似用户 0元 v

兴趣用户 0元 v

① 绑定资质 选择资质 v 资质管理

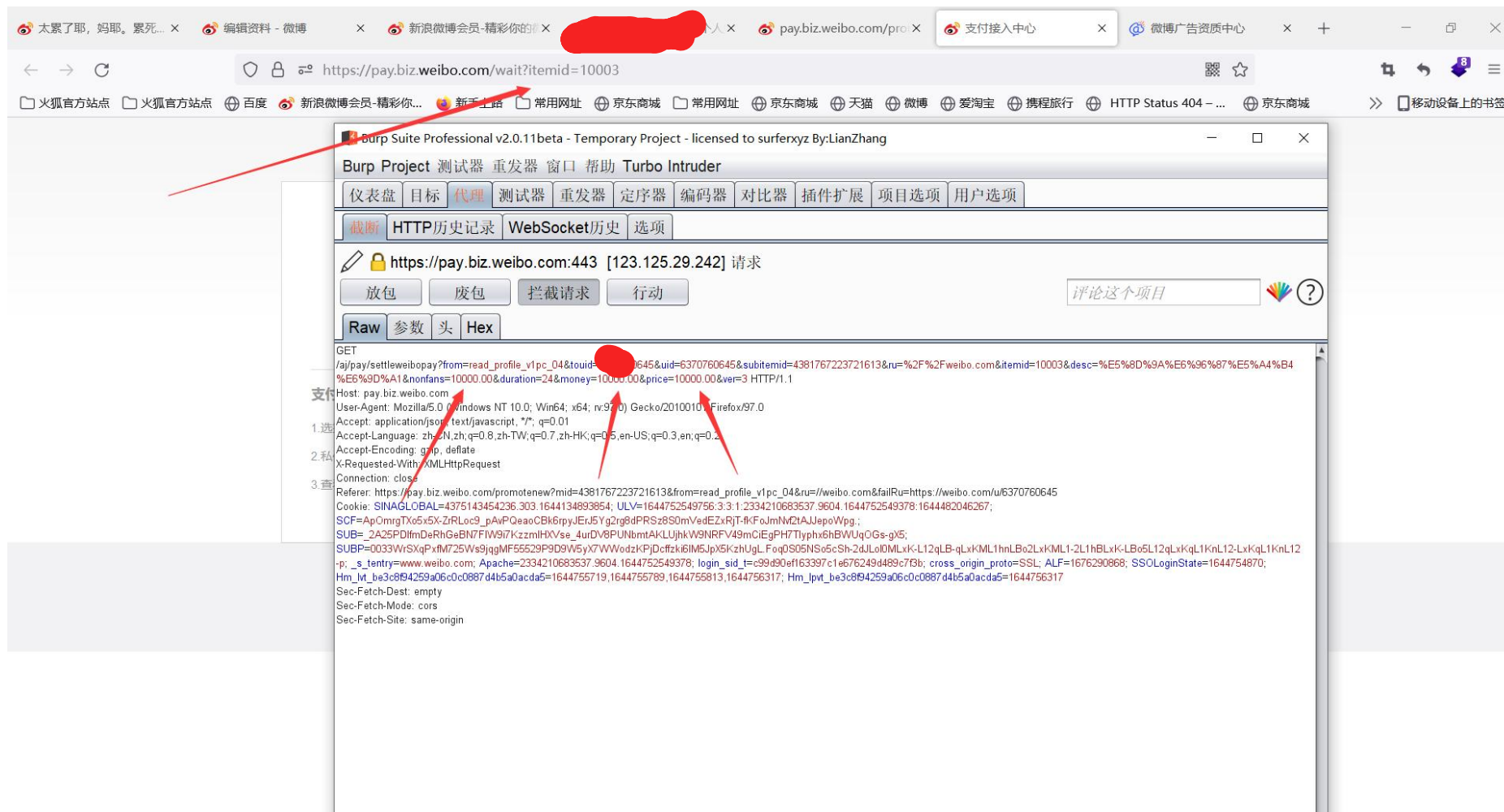
预计覆盖人数: 50.00万+人 预计投放时长: 24小时

请阅读《服务协议》，如无异议请完成支付

☒ 微博钱包(支持支付宝) ☐ 广告账户

10,000.00元 去支付

最高支付 1W 元  
我们点击去支付然后抓包



抓到此包修改 nonfans 参数为一百万尝试一下

Burp Project 测试器 重发器 窗口 帮助 Turbo Intruder

仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项

截断 HTTP历史记录 WebSocket历史 选项

 https://pay.biz.weibo.com:443 [123.125.29.242] 请求

放包

废包

拦截请求

行动

评论这个项目



Raw 参数 头 Hex

GET

/aj/pay/settleweibopay?from=read\_profile\_v1pc\_04&touid=6370760645&uid=6370760645&subitemid=4381767223721613&ru=%2F%2Fweibo.com&itemid=10003&desc=%E5%8D%9A%E6%96%87%E5%A4%B4%E6%9D%A1&nonfans=10000p0.00&duration=24&money=10000.00&price=10000.00&ver=3 HTTP/1.1

Host: pay.biz.weibo.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0

Accept: application/json, text/javascript, \*/\*; q=0.01

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

X-Requested-With: XMLHttpRequest

Connection: close

Referer: https://pay.biz.weibo.com/promotenew?mid=4381767223721613&from=read\_profile\_v1pc\_04&ru=//weibo.com&failRu=https://weibo.com/u/6370760645

Cookie: SINAGLOBAL=4375143454236.303.1644134893854; ULV=1644752549756:3:3:1:2334210683537.9604.1644752549378:1644482046267;

SCF=ApOmrqTXo5x5X-ZrRLoc9\_pAvPQeaoCBk6rpyJErJ5Yg2rg8dPRSz8S0mVedEZxRJT-fkFoJmNvf2tAJJepoWpg.;

SUB=\_2A25PDIfmDeRhGeBN7FIW9i7KzzmIHxVse\_4urDV8PUNbmtAKLUjhkW9NRFV49mCiEgPH7Tlyphx6hBWUqOGs-gX5;

SUBP=0033WvSXqPxfM725W9jqgMF55529P9D9W5yX7WWodzKPjDcfffki6IM5JpX5KzhUgLFoq0S05NSo5cSh-2dJLo10MLxK-L12qLB-qLxKML1hnLB02LxKML1-2L1hBLxK-LB05L12qLxKqL1KnL12-LxKqL1KnL12

-p; \_s\_tentry=www.weibo.com; Apache=2334210683537.9604.1644752549378; login\_sid\_t=c99d90ef163397c1e676249d489c7f3b; cross\_origin\_proto=SSL; ALF=1676290868; SSOLoginState=1644754870;

Hm\_lvt\_be3c8f94259a06c0c0887d4b5a0acda5=1644755719,1644755789,1644755813,1644756317; Hm\_lpv\_be3c8f94259a06c0c0887d4b5a0acda5=1644756317

Sec-Fetch-Dest: empty

Sec-Fetch-Mode: cors

Sec-Fetch-Site: same-origin



点击放包

太累了耶，妈耶。累死... - @... × 编辑资料 - 微博 × 新浪微博会员-精彩你的微博生 × @可爱的小明明1 的个人主页 × pay.biz.weibo.com/promote × pc端统一收银台 ×

← → ↺ https://pay.sc.weibo.com/pay/pc/cashier?sign\_type=md5&sign=2da5c2f85a5fe1f5753ef87fd02d5b8&seller\_id=3587960280&out\_pay 器 ☆

火狐官方网站 火狐官方网站 百度 新浪微博会员-精彩你... 新手上路 常用网址 京东商城 常用网址 京东商城 天猫 微博 爱淘宝 携程旅行 HTTP Status 404 - ... 京东商城 >> 移动设备上的...

微博 weibo.com 用户名: 2202032402210 121027408 1528

收款万 交易信息 应付金额 (元)

粉丝头条官方微博 博文头条 快速提升博文阅读量

1000000

请选择支付方式:

1 手机端扫码支付

用微博二维码完成支付

20%

2 电脑端支付

支付宝 立即支付



发现成功需要支付一百万  
我们再来试试 0.01

5站点

火狐官方网站

百度

新浪微博会员-精彩你...

新手上路

常用网址

京东商城

常用网址

京东商城

天猫

微博

爱淘宝

携程旅行

HTTP Status 404 - ...

京东商城

>>


微博

weibo.com

微博支付

订单号: 220203240227036681


交易号: 1210274095350587017

收款方	交易信息	应付金额 (元)
<div> 粉丝头条官方微博</div>	博文头条 快速提升博文阅读量	0.01

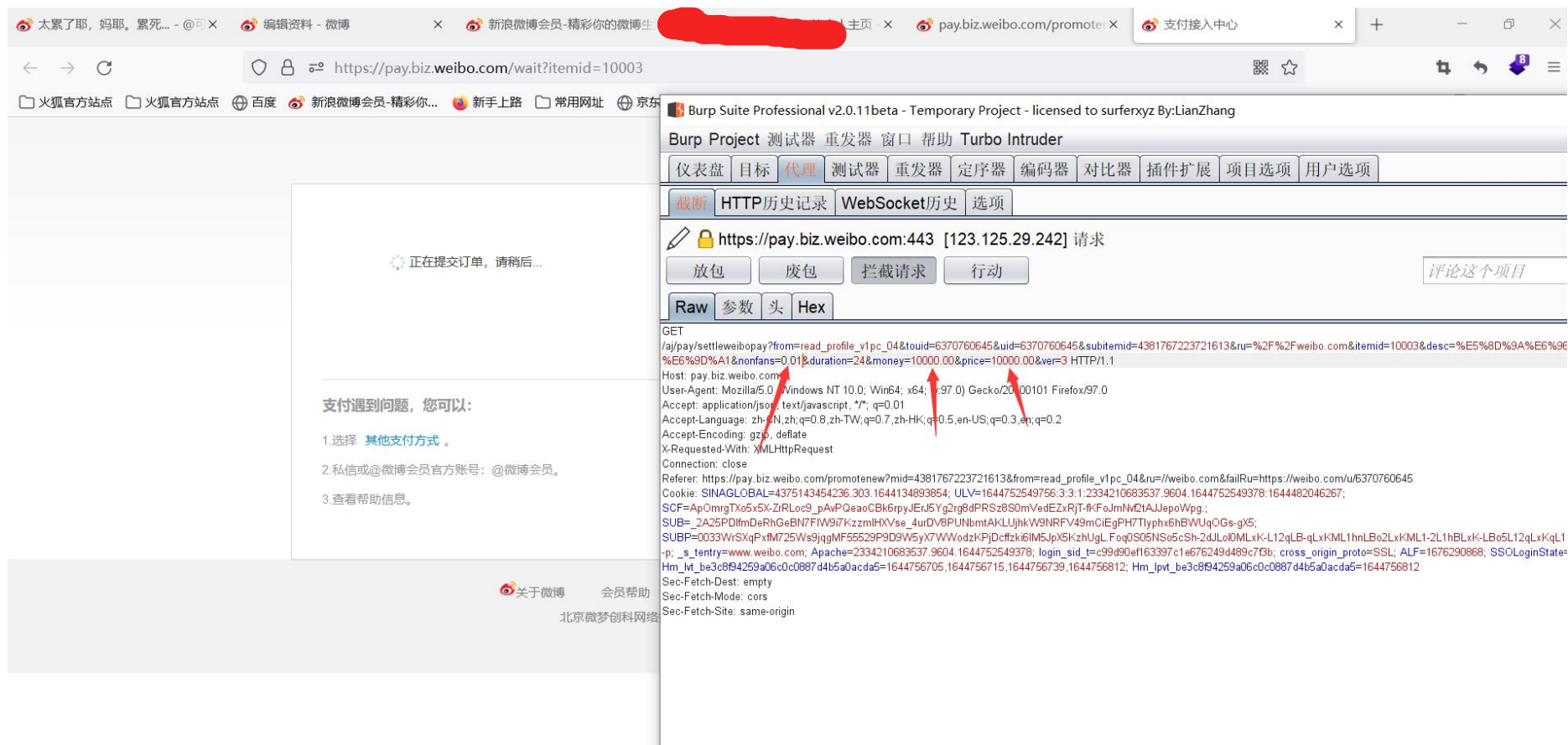
请选择支付方式:

1 手机端扫码支付

用微博扫描二维码完成支付




发现也可以进行



我们若将 1 万元价格改成 0.01 或许会有 1 万元推广但是为 0.01 元支付

微博支付




恭喜您，支付成功!

交易时间: 2022-02-13 20:55:21

双击可隐藏空白

订单号: 220203240227036744

交易号: 1210274095908771402

收款方	交易名称	应付金额 (元)
 粉丝头条官方微博	博文头条 快速提升博文阅读量	2.01

完成

发现支付成功