



安全测试中 一些有趣的姿势和技巧

gdygdy

自我介绍



ID gdygdy

程序猿转行安全

多年搬砖背锅经验，目前在练习甩锅

曾经在多个SRC和漏洞平台打酱油

每天专心撸铁

聊些什么？

目 标

测试中那些总被忽略的目标

哪些目标？



APP

移动APP应用



微信

微信公众号，小程序



QQ

QQ公众号



支付宝

支付宝生活号、小程序

移动APP来源



安卓应用市场



AppStore



苹果企业证书安装



App Store



同开发者旗下APP



扩大目标范围

- I. 子业务
- II. 分公司
- III. 收购的业务
- IV.





微信公众号+小程序



#	Result	Protocol	Host	URL
40	200	HTTPS	wxapp.58.com	/log/track?pagePath=pages%2Fauthor
42	200	HTTPS	wxapp.58.com	/user/location?latitude=39.83023&long
43	200	HTTPS	wxapp.58.com	/log/click?pagePath=pages%2Fauthoriz
45	200	HTTPS	wxapp.58.com	/log/click?pagePath=pages%2Fauthoriz
47	200	HTTPS	wxapp.58.com	/user/info
48	200	HTTPS	wxapp.58.com	/user/thirdlogin?thirdKey=Y2XGMDN4n
49	200	HTTP	Tunnel to	passport.58.com:443
50	200	HTTPS	wxapp.58.com	/log/click?pagePath=pages%2Fauthoriz
52	200	HTTPS	passport.58.com	/fingerprint
53	200	HTTPS	wxapp.58.com	/user/wxalogin
54	200	HTTPS	wxapp.58.com	/load/config?thirdKey=Y2XGMDN4nZGI
55	200	HTTPS	wxapp.58.com	/weather/info?cityId=1&openId=055E
56	200	HTTPS	passport.58.com	/thd/proxylogin/wxapp/weixin?path=c
57	200	HTTPS	wxapp.58.com	/user/profile?thirdKey=dnIW9sw6GpUN
58	200	HTTPS	wxapp.58.com	/log/click?pagePath=pages%2Findex%
60	200	HTTPS	wxapp.58.com	/log/click?pagePath=pages%2Findex%
62	200	HTTPS	wxapp.58.com	/log/track?pagePath=pages%2Findex%
64	200	HTTP	Tunnel to	activity.58.com:443
65	200	HTTPS	activity.58.com	/wxa/wxsub/jobsubid?thirdKey=dnIW9
66	200	HTTP	Tunnel to	wxapp.58.com:443



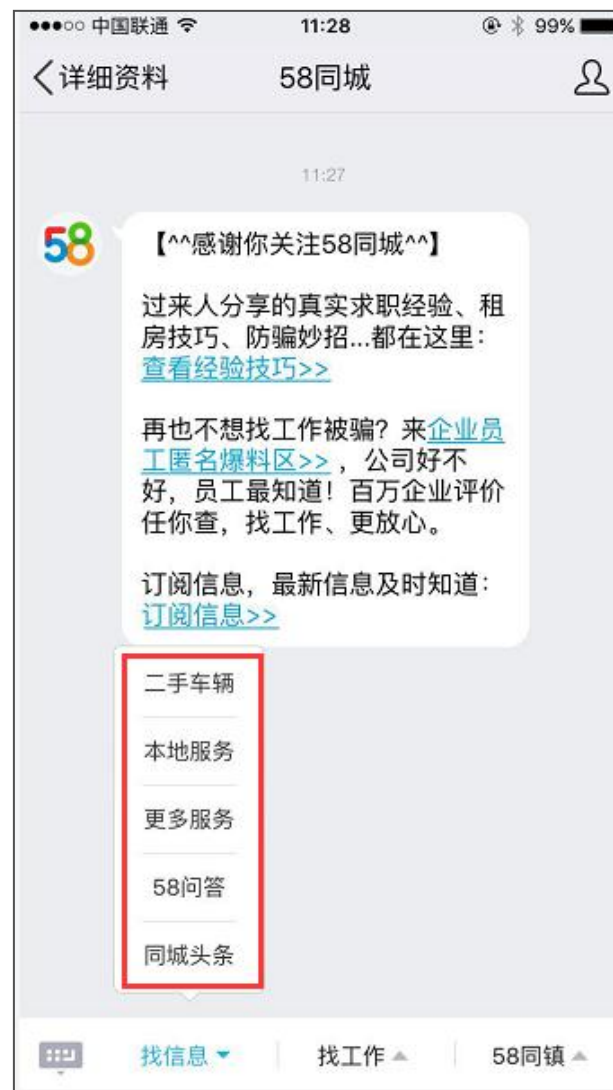
QQ



QQ



搜索公众号



下方菜单以及消息

支付宝生活号



支付宝



支付宝小程序



生活号入口



总入口



搜索

结束



什么？你们竟然都说我帅！

如何获得更多的目标？

01 社交功能

02 其他相关公众号

APP的不同版本

03

.....

04

社交功能



其他相关公众号、小程序



找驾校



科目一



科目二



科目三



科目四



拿本



驾校一点通订阅号
微信关注，驾考热点全知道



驾校一点通微信小程序
无需下载，考试做题快、准、稳

VIP真题

专家课程

分类练习

仿真模拟考试

智能模拟考试

专家模拟考试

精品推荐

学车动态

新手上路

理论考试

政策法规

报名须知

资格证

学车指南

驾驶技巧

交规秘笈

交通标志

场考路考

APP

顶部

APP的不同版本

← → ↻

安全 | <https://s.pc6.com/?cid=android&k=58同城app+v1>

pc6下载站: 安全、高速、放心的专业下载站!

最新软件 | 软件分类 |

 下载站
中国安全的下载站

58同城app v1.

搜索

全部 PC软件 安卓应用 手游 iPhone iPad MAC 小程序 VR 资讯 视频

58 58同城app下载 v8.13.6

大小: 51.76MB - 简体 - 免费软件

58同城手机客户端app, 58同城官方移动终端。58同城手机客户端app是界内评价很高的一个平台, 找房租房二手房, 应聘求职找工作, 全靠它, 还有更多便民服务功能等你来发现 [详情>>](#)

<http://www.pc6.com/az/66184.html> 更新: 2018-11-29

58 58同城HD下载 v5.0.1.2

大小: 16.7MB - 简体 - 免费软件

58同城app是全国最大的分类信息平台, 58同城app海量生活信息免费查询、发布, 房屋租售、二手买卖、招聘求职、汽车租售、宠物票务、餐饮娱乐, 覆盖全国所有大中城市, 汇聚大量个人和商家信息 [详情>>](#)

<http://www.pc6.com/az/303201.html> 更新: 2016-06-15

 58同城速聘下载 v1.0.0.1

大小: 13.17MB - 简体 - 免费软件

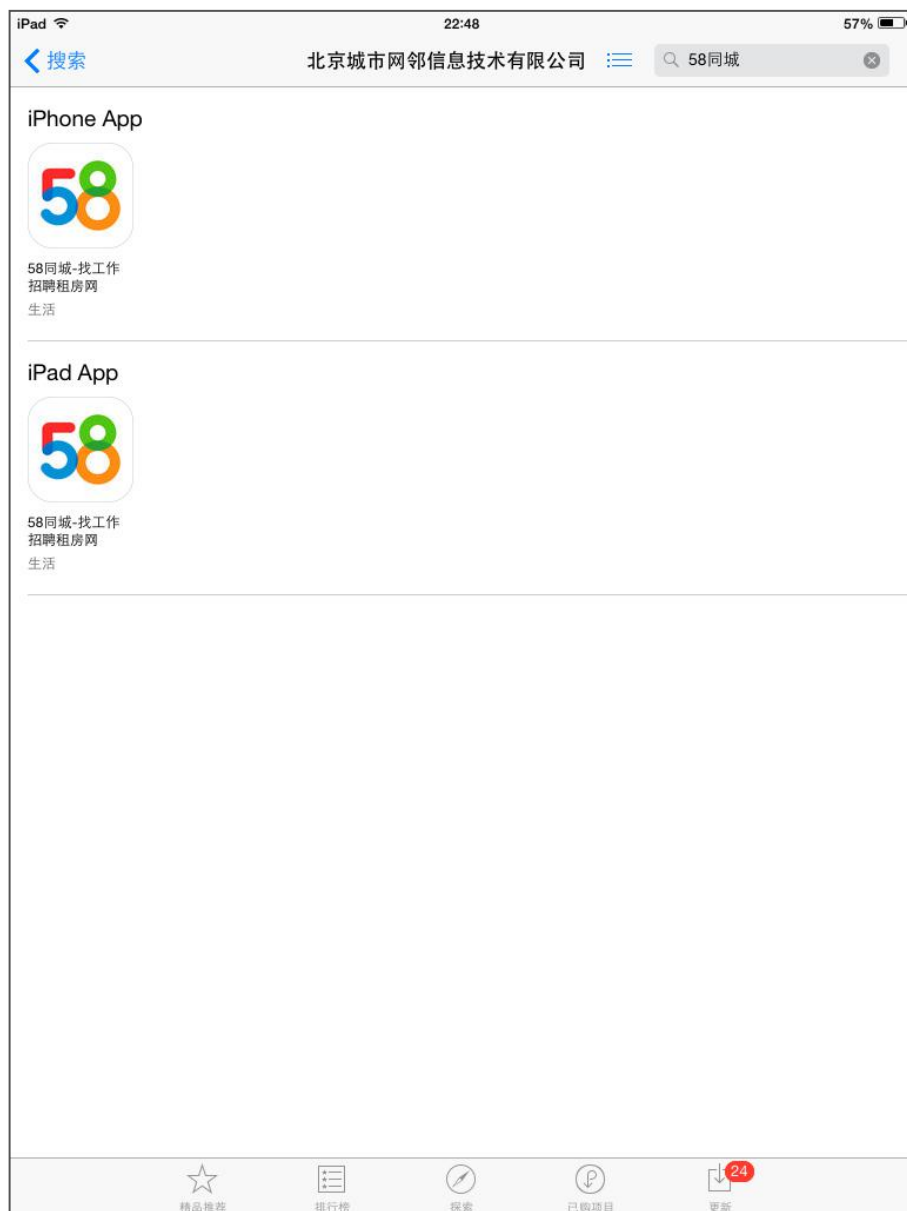
58同城速聘app是一款招聘求职应用, 58同城速聘app为企业与员工提供一个快速入职的平台, 员工可以迅速找到合适的工作, 企业也能解决人员紧缺的问题, 58同城速聘, 让找工作更快更有效率 [详情>>](#)

<http://www.pc6.com/az/212438.html> 更新: 2016-01-07

APP历史版本



其他版本



还有什么？

技 巧

几个解决问题的技巧

技巧1 2 3

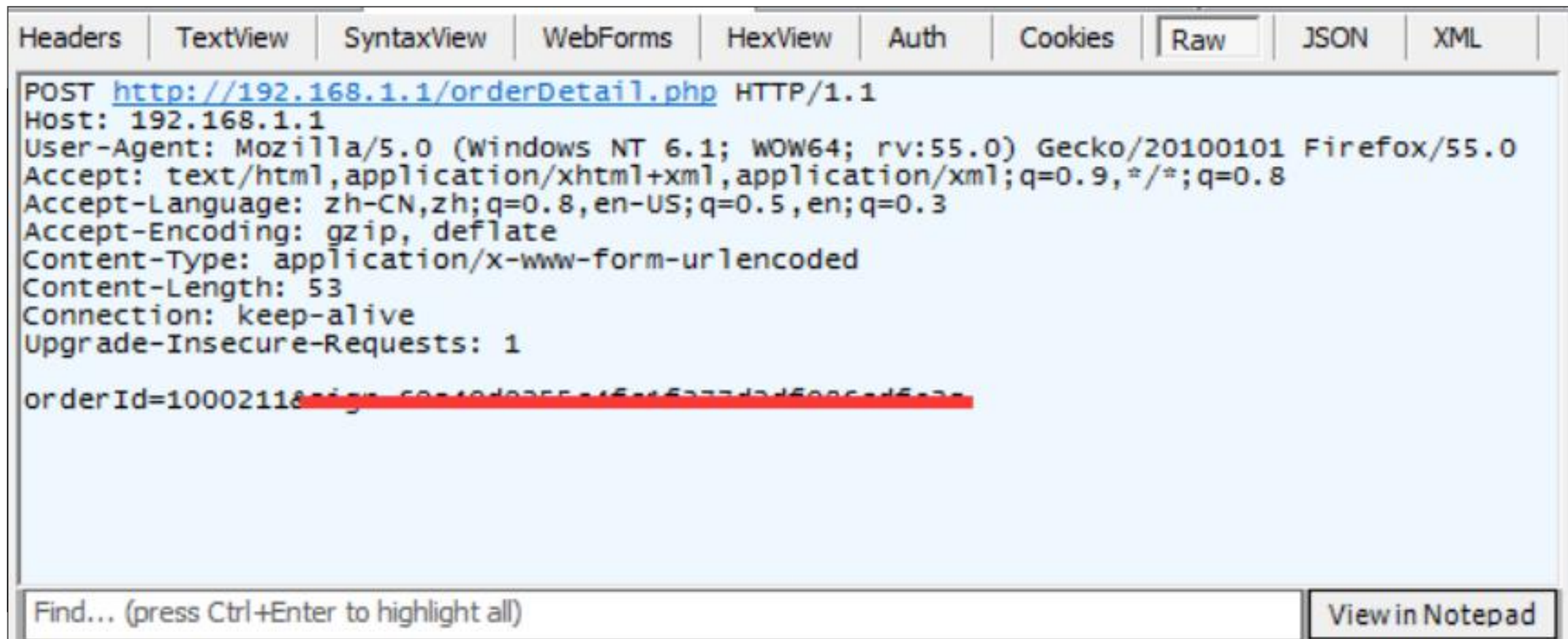
Headers	TextView	SyntaxView	WebForms	HexView	Auth	Cookies	Raw	JSON
---------	----------	------------	----------	---------	------	---------	-----	------

XML

```
POST http://192.168.1.1/updatepassword.php HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 47
Connection: keep-alive
Upgrade-Insecure-Requests: 1

newpwd=password&sms=123456&username=18888888888
```

技巧1 2 3



The image shows a web browser's developer tools window with the 'Raw' tab selected. It displays an HTTP POST request to `http://192.168.1.1/orderDetail.php`. The request headers include `Host: 192.168.1.1`, `User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0`, `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8`, `Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3`, `Accept-Encoding: gzip, deflate`, `Content-Type: application/x-www-form-urlencoded`, `Content-Length: 53`, `Connection: keep-alive`, and `Upgrade-Insecure-Requests: 1`. The request body is `orderId=10002118` followed by a redacted signature. At the bottom, there is a search bar and a 'View in Notepad' button.

```
POST http://192.168.1.1/orderDetail.php HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
Connection: keep-alive
Upgrade-Insecure-Requests: 1

orderId=10002118&sign=60740d0255e1f5e15277da2d5006cd5e2a
```

Find... (press Ctrl+Enter to highlight all) View in Notepad

技巧1 2 3

tType=1&channel=m_h5&userId=64774&accessToken=CSddCE...BMHKt&openId=&openChannel=&authCode...

tType=1&channel=m_h5&userId=64774&openId=&openChannel=&authCode= HTTP/1.1

Client

Accept: application/json
Accept-Encoding: gzip, deflate
Accept-Language: zh-cn
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 10_2_1 like Mac OS X) AppleWebKit/602.4.6 (KHTML, like Gecko) Mobile/14D27 PAHealth/3.2
X-Requested-With: XMLHttpRequest

Cookies / Login

☐ Cookie

from=direct

Get SyntaxView | Transformer | Headers | **TextView** | ImageView | HexView | WebView | Auth | Caching | Cookies | Raw

JSON | XML

{\"code\":1,\"msg\": \"成功\", \"data\": {\"idType\":1, \"idCardNo\": \"120...925\", \"realName\": \"吴...\", \"sex\":2, \"birthday\":-

难题

```
HTTP/1.1 200
Content-Type: application/json; charset=utf8
Date: Wed, 05 Dec 2018 12:27:28 GMT
Content-Length: 36
```

```
{"code":400,"msg":"验签不通过"}
```

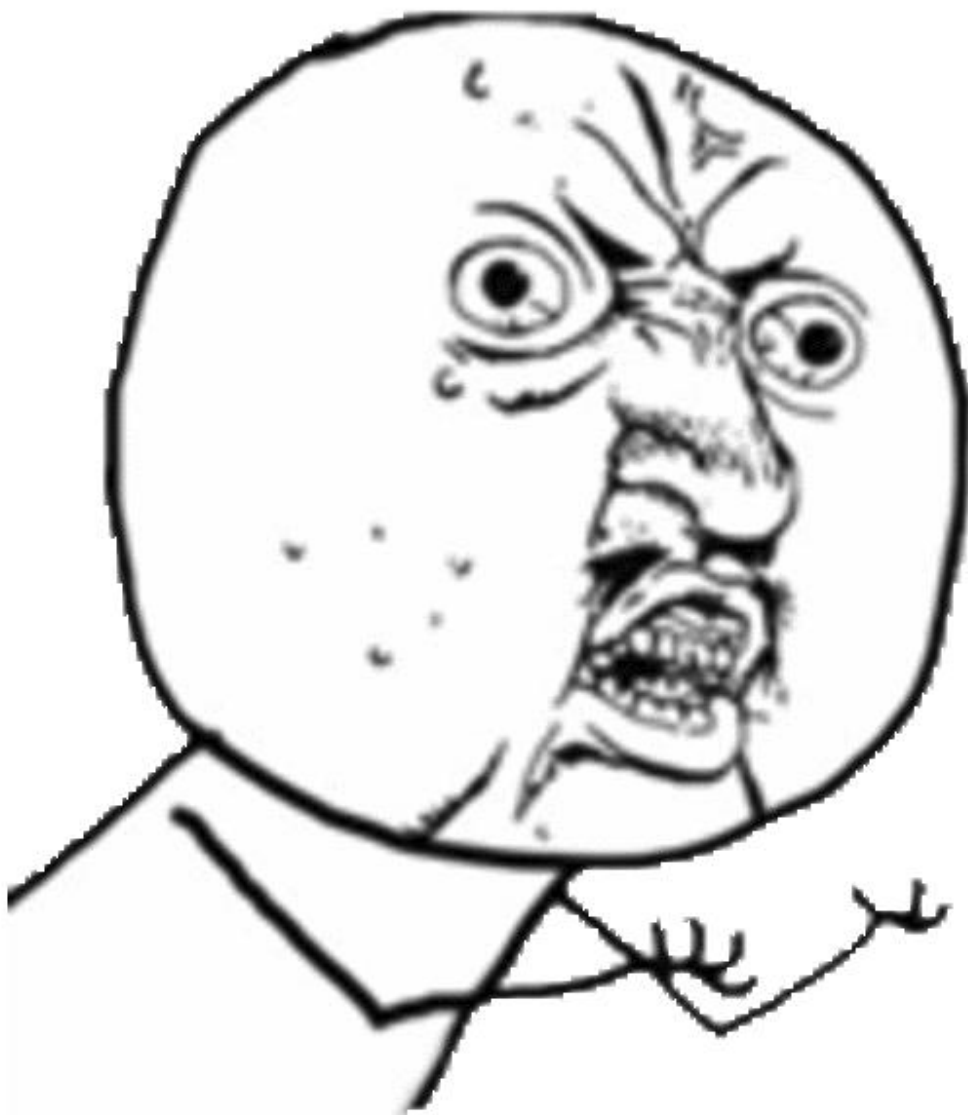
解决办法？



逆向思考

解决办法？

```
(function() {function q(a) {for(
==g&&(x=g); c=a.body; a=a.parent
b={r:parseInt(g[1], 10), g:parse
(g==void 0, (g=x.match(a))?d={r:
127<Math.max.apply(null, [b.r, b
")+")"}; b&&d?(a=Math.max.apply
1, 127<b&&
(a=1), b=Math.round(b+96*a), b=
{this.x=a; this.y=g; this.revers
_length=Math.sqrt(Math.pow(thi
==this.y)this._length=0; else
this.x)this._length=a, this.y=a
+Math.pow(g, 2))), g=g*b; this._l
0:Math.acos(Math.min(Math.max(
this.y));
this.getVectorFromCoordinates=
this.y}); this.getVectorFromPoi
0; f<d; f++) {j=a[f]; i=j.x.length
h; this.inStroke=!1; this._strok
_stroke={x:[a.x], y:[a.y]}; this
{b.call(n, g), 3); return a}retu
this._lastPoint.y)) {var g=
this._stroke.x.length; this._st
{n.call(c, b, g), 3); return a}re
_stroke, b=this.endStrokeFn, n=t
$(a), a=this.eventTokens={}; thi
new t(this); var h=$.fn[e]("glo
color": "#eee", lineWidth:0, minF
b.hasOwnProperty(j)&&b[j].call
height: 0 !important; margin-to
this.isCanvasEmulator=!1; b=thi
0 !important; margin-top:-1.5em
c=Math.max(Math.round(b.width/
this.fatFingerCompensation=0; v
f(Math.round(c.pageX+g), Math.r
catch(b) {} n.clear(); a.dataEngi
n.kick(); this.drawMoveHandler
this}.call({}, this), i=c.drawEn
$(1); this.isCanvasEmulator?(g
0; l.onmousemove=void 0; this.fa
-3*d.lineWidth; d.minFatFingerC
```



```
parent"!=g&&"rgba(0, 0, 0, 0)"!
o; g=void 0; (g=n.match(a))?
; var d;x?
16), b:parseInt(g[3], 16)}); d=b?
c.apply(null, [b.r, b.g, b.b]), a=
agth||(this.
function(a) {if(0==this.x&&0
pow(a, 2)/(1
gth(); return 0==g?
g){return new o(a-this.x, g-
-this.x, a.y-
gth)for(var d=a.length, j, i, f=
oStrokeFn=c; this.endStrokeFn=
setTimeout(function()
c-this._lastPoint.x)+Math.abs(a.y-
setTimeout(function()
var c=this.$parent=
o)
!important; width: 100% !important;
ant; width: 100% !important; height
this", this); c=(c=d.lineWidth)?
ss);
aw
ction(g) {try{g.preventDefault()}
top; a.dataEngine.startStroke(c(d)
oid 0; l.onmouseup=void
ontouchend=void
```

思考结果

```
POST [REDACTED] HTTP/1.1
signMsg: C5E83733A5B4A5BC22F8691B9C0188B1
token: 659d3c1977f1437c8535a4703c26e694
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Content-Length: 95
Host: [REDACTED]
Connection: Keep-Alive
Accept-Encoding: gzip
User-Agent: okhttp/3.3.0

borrowId=710&mobileType=2&token=659d3c1977f1437c8535a4703c26e694&userId=858&versionNumber=1.0.3
```

Find... (press Ctrl+Enter to highlight all)

Transformer	Headers	TextView	SyntaxView	ImageView	HexView	WebView	Auth	Caching	C
Raw	JSON	XML							

```
{"msg": "查询成功", "code": 200, "data": {"repay": [], "isBorrow": true, "borrow": [{"id": 710, "tppId": 3, "userId": 862, "orderNo": "0201378", "realAmount": 199.0, "fee": 0.4, "createTime": "2018-11-20 17:57:06", "timeLimit": "1", "state": "19", "cardId": 507, "serviceFee": 0.0, "infoAuthFee": 0.0, "interest": 0.4, "client": "[REDACTED]", "coordinate": "[REDACTED]", "ip": "[REDACTED]", "channelId": 16, "checkBackDetail": 1, "repayCount": 0, "isReborrow": 1, "cardNo": "62148801031000000000000000000000", "bank": "招商银行", "stateStr": "[REDACTED]"}]}
```



你们又在说我帅！

The background features a light gray field with several thin, dark blue lines intersecting. A large, dark blue, irregular polygonal shape is positioned in the upper right corner. Three small dark blue dots are located at the intersections of the lines: one near the top center, one near the middle right, and one near the bottom right.

感谢观看