



**QCon** 全球软件开发大会  
INTERNATIONAL SOFTWARE  
DEVELOPMENT CONFERENCE

BEIJING 2017

# 他山之石可以攻御

@呆子不开口 / 吕伟



促进软件开发领域知识与创新的传播



关注InfoQ官方信息  
及时获取QCon软件开发者  
大会演讲视频信息



扫码，获取限时优惠



全球架构师峰会 2017 [深圳站]

2017年7月7-8日 深圳·华侨城洲际酒店

咨询热线: 010-89880682



全球软件开发大会 [上海站]

2017年10月19-21日

咨询热线: 010-64738142

# 关于我

足球

安全从业者

厄齐尔

和蔼可亲

英俊( 网名 )

获锤子手机软  
文大赛一等奖

德扑

李霞

中年  
男子

胖

王刚

平凡

微博网友



# 他山之石可以攻御

- 💀 当攻击者想要攻击某个**安全防御**的时候，可能不会硬碰硬
- 💀 有一些其他正常功能或攻击方式可以帮他**绕过**你的防御
- 💀 “绕过”大多无需专业漏洞挖掘技术，其中有一些**没有“技术”含量**

各中超、中甲俱乐部：

为了深入贯彻《中国足球改革发展总体方案》的精神，加强中国足球本土人才的培养力度，促进中国足球与职业联赛的健康可持续发展。从 2017 赛季开始，中国足协对 U23 国内球员参加中超联赛、中甲联赛做出了相关规定（详见《2017 年中国足球协会超级联赛规程》和《2017 年中国足球协会甲级联赛规程》）。

为进一步落实 U23 国内球员报名、参赛的相关规定，现将相关实施细则通知如下：

一、如俱乐部在国内球员 27 人报名名单中未填报至少 4 名 U23 国内球员，则中国足协不接受俱乐部报名，俱乐部也将失去该年度职业联赛的参赛资格。

二、如俱乐部提交的首发出场 11 人名单中未填报至少 1 名 U23 国内球员，则该场比赛按弃权处理。中国足协纪律委员会赛后将依据《中国足球协会纪律准则》的有关条款对该

# 足协U23新政

**首发**必须得有一名23岁以下国内球员

上港的张华晨本轮再次刷新自己保持的最快被替换下场纪录，上一轮他14分钟被换下，本轮他11分钟就走下球场。第4轮比赛中国，18人首发的数据同中超首轮持平，第2及第3轮均17人出场。

随着中超联赛的进行，U23新政的积极和消极影响都在呈现。中超第4轮，中超16队25名球员出场，人数创出新高，但平均47分钟的出场时间却创出新低。同在本轮，中超有韦世豪和高准翼两名U23球员破门，上港的张华晨则刷新了被换下的新快纪录（11分钟）。对于延边富德及长春亚泰等成绩不佳的球队来说，U23球员的使用仍让他们感到为难。

# 足协目的是**锻炼年轻队员**

俱乐部选择**快速换下首发的U23队员**来绕过此新政

# 资产的概念

需要我们要保护的，可以是具体的对象，可以是预期实现的功能， .....



# U23新政的漏洞

足协的资产：想要实现的是锻炼年轻队员

足协的防护：至少一名U23球员必须首发

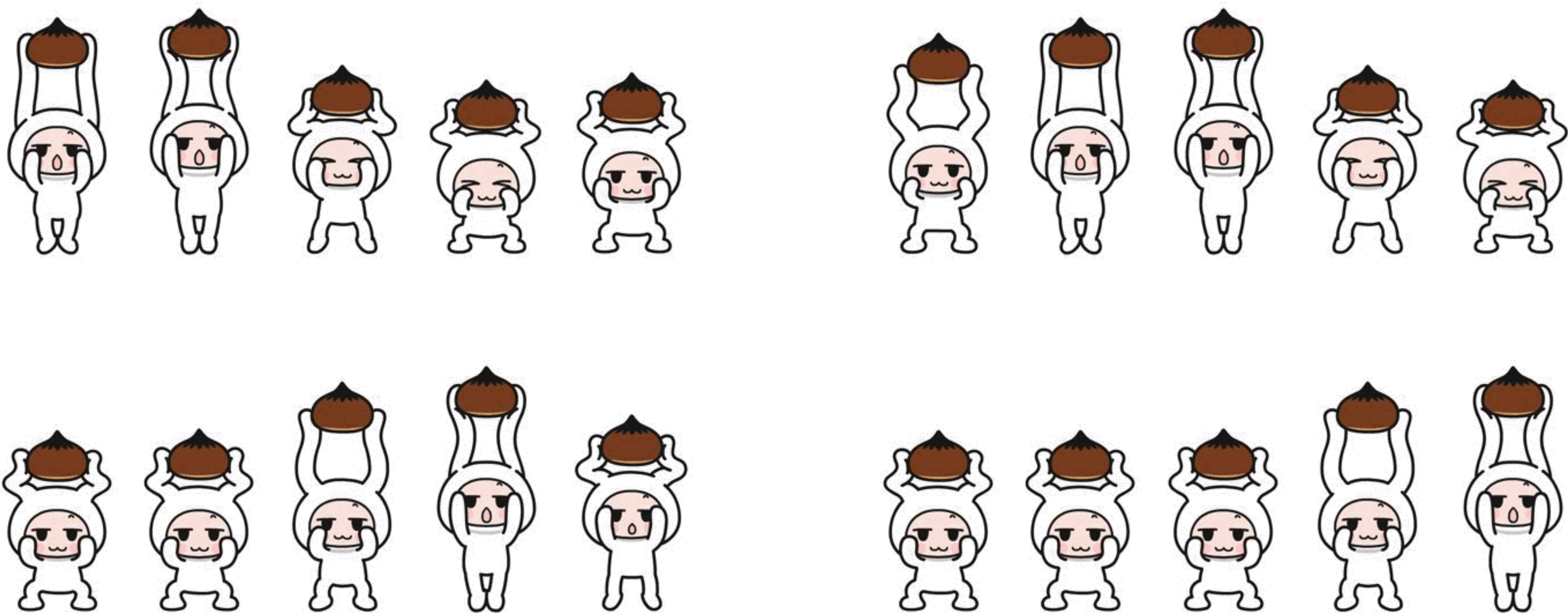
应该的防护：比如，至少一名U23球员必须打满80分钟以上，首不首发甚至都不重要

**治标不治本，误解了自己要防护的资产**



# 资产的防御被绕过

- 💀 事不关己——不清楚哪些是资产
- 💀 沧海桑田——不清楚自己有哪些资产
- 💀 忘了初心——治标不治本，误解了自己要防护的资产
- 💀 心有余而力不足——防御能力保护不了自己的资产
- 💀 心存侥幸——防护目前没有覆盖全
- 💀 我家大门常打开——隔离设计有问题，或其他功能非常接近你的资产
- 💀 眼前的黑不是黑，你说的白是什么白——白名单的防护薄弱



# 接下来我要举很多栗子

案例中的漏洞部分都已经修复



# 查看微博问答的匿名围观ID

0.00B/s

19:34

围观过的人

...

围观过的人

打赏过的人



想知道呆子老师最想告诉子女的，  
有关婚姻的经验是什么？谢谢您  
呆子不开口

加关注



二八八CD

加关注



Melody0946  
半生不熟 流动人口

加关注



花总有金箍棒了  
长期专注于中国经济乃至股市、期...

加关注



花梨木他们我们心自问呐m...  
积极向上，有点闷骚，有点任性，有...

加关注

查看全部

匿名围观

23人默默围观了此回答

查看Ta的其他回答

60.2B/s

19:35

问答收益

...

昨日总收益 (元)

0.55

2017年总收益 1275.20 元

查看详情

回答收益

提问收益

昨日关键指标

回答问题个数	0	回答问题收益(元)	0.00
围观人数	1	围观所得分成(元)	0.55

累计 (收入扣除个税后每月结算至支付宝，平台服务费10%)

回答问题总个数	19	回答问题总收益(元)	516.80
围观总人数	510	围观所得总分成(元)	280.50

322B/s

19:35

收益明细

...

全部

筛选



我就是那只音乐虫子  
2017-04-10 16:45:49  
围观收益 +0.55



小王子呀hey  
2017-04-09 19:29:13  
围观收益 +0.55



clic  
2017-04-07 11:57:46  
围观收益 +0.45



御弟昂  
2017-04-07 07:54:57  
围观收益 +0.55



大姐夫姜浩  
2017-04-07 02:21:46  
围观收益 +0.45



Mr\_Sflamingo  
2017-04-06 17:35:43  
围观收益 +0.55



Mr\_Sflamingo  
2017-04-06 17:28:22  
围观收益 +0.55



瓜英俊  
2017-04-06 14:55:55  
围观收益 +0.55

INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE

QCon[北京站]2017

# 查看微博问答的匿名围观ID

💀 事不关己——不清楚哪些是资产

💀 我家大门常打开——隔离设计有问题，或其他功能非常接近你的资产



# 张爱朋老师的故事



刘巍峰

刚刚 来自 iPhone 7 Plus

右边一串自己人竟然不知道超级话题有这功能？戳右边 #白百何# // @崔松岩:这数据不可能拿得到吧？ // @billy鹏的足迹:哪里来的数据？ // @胡波\_:这是哪儿的数据？ // @国东: // @Zodzod\_张浩:这数据怎么拿到的？！ // @田\_月:这。。。

@八哥专用 :白百何这会在不停的上微博又退出，看得出来她很忐忑和焦躁…

4月10日 4月11日 4月12日



00:00 4 8 12 16 20 24:00



白百何  
上线次数15 发微博条数0

13:16 13:22	在线	6min
13:05 13:12	在线	7min
12:50 12:56	在线	7min
12:42 12:48	在线	6min
11:58 12:14	在线	16min

1

评论

赞

名人动态



白百何  
微博在线了

白百何在线了 刚刚

@白百何  
于14:42在线了

签到，查看更多名人动态

上线啦

发博啦

空降啦

直播啦

签到

名人在线状态

4月10日 4月11日 4月12日



00:00 4 8 12 16 20 24:00



白百何  
上线次数16 发微博条数0

当前	在线	2min
13:16 13:22	在线	6min
13:05 13:12	在线	7min
12:50 12:56	在线	7min
12:42 12:48	在线	6min
11:58 12:14	在线	16min
09:42	在线	6min

# 张爱朋老师的故事

💀 事不关己——不清楚哪些是资产

💀 沧海桑田——不清楚自己有哪些资产





# 连接wifi就可以查看摄像头

某智能电视的手机app只要和电视在同一个wifi内就可以连接电视**遥控操作电视**

但给电视安装应用时，需输入电视上出现的验证码。但app上有个“横屏镜像”功能，此时**我再用另外一个手机去镜像查看这个验证码**就可以了

横屏镜像功能可以操作电视的系统桌面，但有些敏感功能无法点开，比如系统设置什么的。有个内置功能可以查看此账号绑定的家里的摄像头，也无法点击进入。但利用上面已经突破的安装应用功能，**可以给电视上装一个此品牌摄像头的管理app**，然后打开此app，也可以查看摄像头的内容

- 💀 事不关己——不清楚哪些是资产
- 💀 沧海桑田——不清楚自己有哪些资产
- 💀 忘了初心——治标不治本，误解了自己要防护的资产
- 💀 我家大门常打开——隔离设计有问题，或其他功能非常接近你的资产

# 绕过双因素验证

## 💀 突破双因素进微博

在一种攻击中，拿到用户sso的ticket可以登录进用户的微博。但如果用户开启双因素认证，进web版需要验证手机验证码。但如果跳到wap版本，则不需要

## 💀 淘宝异地登录风控绕过

拿到用户的某种自动登录凭证可以进入用户的淘宝，但如果是异地登录会验证手机。但淘宝旺旺的弹框中的自动登录的url则没有此限制，可能是因为用户体验的原因，弹框中没法再做双因素验证

## 💀 突破双因素登陆管理后台

某产品的web版管理员账号做了双因素认证，并且双因素登录后的凭证和非双因素的凭证一样。app没有管理员功能，但app端登录没有做双因素认证，盗号者可以用管理员的密码登录app端，获取cookie后再去web版登录

## 💀 某手机系统手机初始化同步照片功能绕过云端的手机验证码

某手机系统的云端查看用户照片短信等信息时需要验证手机验证码。但如果手机初始化的同步功能，可以不用手机验证码就可以同步用户的照片和短信



# 绕过双因素验证

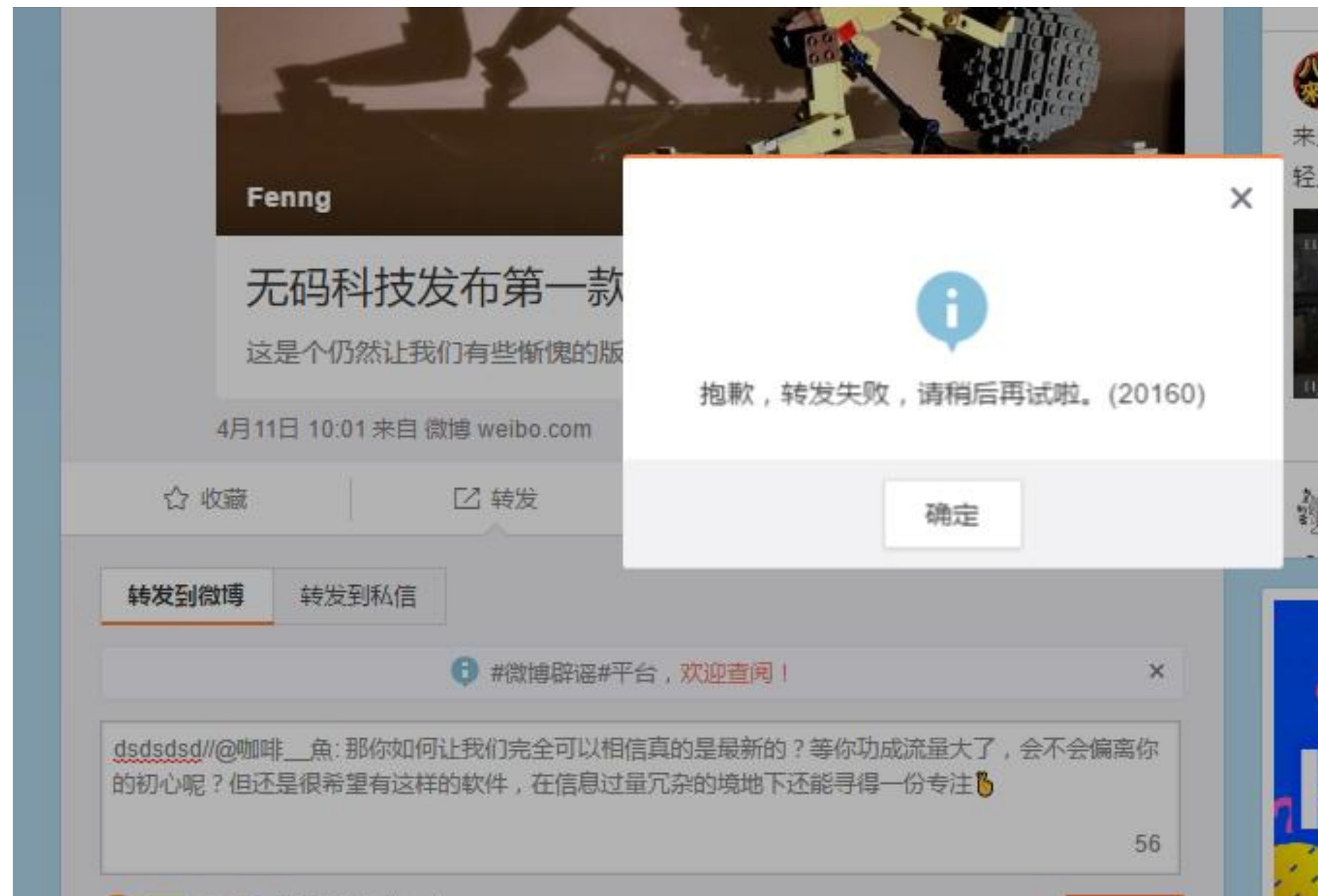
- 💀 沧海桑田——不清楚自己有哪些资产
- 💀 忘了初心——治标不治本，误解了自己要防护的资产
- 💀 心存侥幸——防护目前没有覆盖全
- 💀 我家大门常打开——隔离设计有问题，或其他功能非常接近你的资产

# 被拉黑后仍然可以转发他人微博



被拉黑后不能转发他的微博，也不能评论并转发  
但我觉得楼主说的棒，迫切想转发

# 被拉黑后仍然可以转发他人微博



别人转发了他的微博，发现我也不可以转别人的。我心急如焚



# 被拉黑后仍然可以转发他人微博

有个方式可以转发

找到一个转发此微博的他人的微博，然后评论并转发此微博，就可以转发成功



但这种方式易被看穿，并且不是直接转发，体验不好

可以找个转发语多的微博，然后再评论转发。由于总字数大于140，他人的转发语会被系统丢弃，就只剩你的转发语了






# 被拉黑后仍然可以转发他人微博

- ☠ 沧海桑田——不清楚自己有哪些资产
- ☠ 忘了初心——治标不治本，误解了自己要防护的资产
- ☠ 心存侥幸——防护目前没有覆盖全
- ☠ 我家大门常打开——隔离设计有问题，或其他功能非常接近你的资产

# https的劫持插入广告

 https的js服务被劫持，但证书是正确的，疑似证书泄露或后端服务被攻击

处理进度

提交漏洞

审核

修复

用户复查

完成

**回源请求使用http，被攻击者劫持**  
心存侥幸——防护目前没有覆盖全

# 查看被别人转发到朋友圈或私人可见的微博

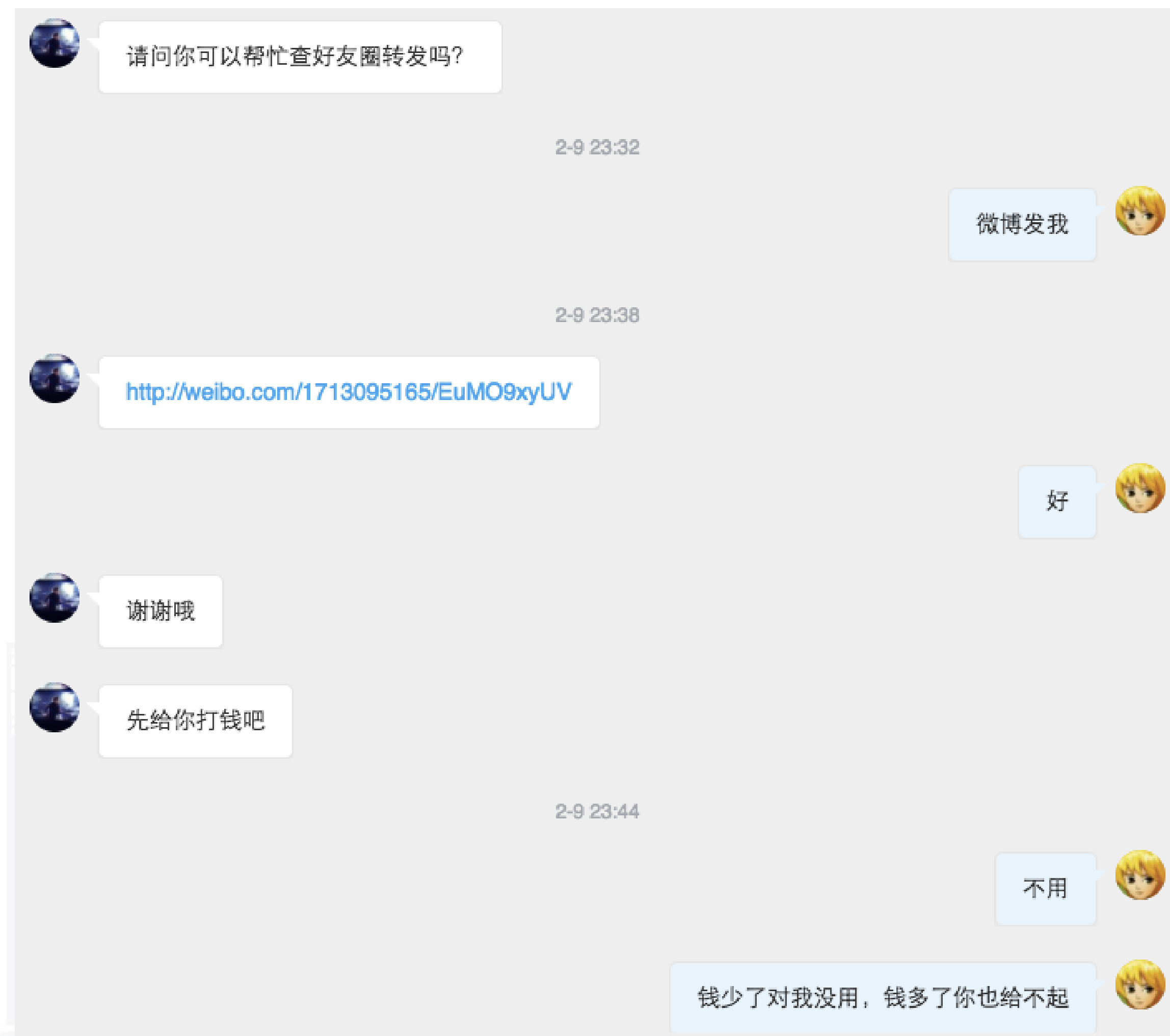
当你的微博被别人转发到他的朋友圈且你若不和他互粉，或者被转发到他的私人可见。你是看不到他的转发语的

但通过微博的一些其他功能的api可以获得转发id的列表。查出隐藏转发的id

再通过一个api可以查看到微博的内容

每一处都没有做权限限制

- 💀 事不关己——不清楚哪些是资产
- 💀 沧海桑田——不清楚自己有哪些资产
- 💀 我家大门常打开——隔离设计有问题，或其他功能非常接近你的资产



# 某支付功能可以变相信用卡套现

某支付产品转账功能不可以使用信用卡。但有一个代付功能。代付的人却可以使用信用卡完成代付

💀 忘了初心——治标不治本，误解了自己要防护的资产

💀 我家大门常打开——隔离设计有问题，或其他功能非常接近你的资产



# 某种方式发微博可以绕过广告屏蔽

微博会**不允许某些账号直发**广告内容

但是某**官方平台**上功能发出的微博可以任意发广告

只要发微博的**来源是此平台**就可以发广告。并且不通过平台合法功能，直接发出带此来源的微博的方式也有不少，所以被很多发广告的人利用

- 💀 事不关己——不清楚哪些是资产
- 💀 心有余而力不足——防御能力保护不了自己的资产
- 💀 心存侥幸——防护目前没有覆盖全
- 💀 眼前的黑不是黑，你说的白是什么白

# 一些常见敏感功能的副作用

## 💀 账号找回功能被坏人用来盗号

很多账号找回功能为了用于体验，在用户未提供足够可信身份的状态下，也允许用户找回账号成功。这样攻击者就也可以利用此功能盗号

## 💀 某支付产品收付款码在一起

存在一点风险，就是攻击者借付款的名义骗走你的条码，然后用于收款功能

## 💀 二维码扫描登录被盗号者利用

如果二维码扫描功能里的登录和加好友等功能没做隔离，并且防护薄弱。你若扫了他人发的二维码，若那个码是用来登录的，攻击者就可以登录你的账号了

💀 我家大门常打开——隔离设计有问题，或其他功能非常接近你的资产

# 几类风险

一些攻击或漏洞类型，也是用的此类思想





# 古老的旁注

## 旁注

[编辑](#)

 本词条缺少信息栏、名片图，补充相关内容使词条更完整，还能快速升级，赶紧来[编辑](#)吧！

旁注是最近网络上比较流行的一种入侵方法，在字面上解释就是—“从旁注入”，利用同一主机上面不同网站的漏洞得到webshell，从而利用主机上的程序或者是服务所暴露的用户所在的物理[路径](#)进行入侵。

 我家大门常打开——隔离设计有问题，或其他功能非常接近你的资产

# url跳转漏洞

**用可信白名单域的url来跳转到攻击url  
利用了信任关系完成对某些防御的绕过**

💀 忘了初心——治标不治本，误解了自己要防护的资产

💀 眼前的黑不是黑，你说的白是什么白

# 日志里泄露敏感信息

敏感数据在数据库中已经加密，但却在web或应用日志中被明文记录

- ☠ 事不关己——不清楚哪些是资产
- ☠ 沧海桑田——不清楚自己有哪些资产
- ☠ 忘了初心——治标不治本，误解了自己要防护的资产



# Github泄露大量资产

**Github上可以搜到大量公司的密码、key等敏感资产**

💀 事不关己——不清楚哪些是资产

💀 我家大门常打开——隔离设计有问题，或其他功能非常接近你的资产

# 解决方案

- ☠ 事不关己——不清楚哪些是资产（有安全意识，知道哪些是重要资产。别人值钱的东西要谨慎使用）
- ☠ 沧海桑田——不清楚自己有哪些资产（架构设计要低耦合，资产不要到处给别人）
- ☠ 忘了初心——治标不治本，误解了自己要防护的资产（知道自己要保护的是什么，尽量从底层做防护。条条大路通罗马，罗马城门设关卡）
- ☠ 心有余而力不足——防御能力保护不了自己的资产（提高防御能力。学习，培训，招人，花钱……）

# 解决方案

- 💀 心存侥幸——防护目前没有覆盖全（**尽量覆盖全，有客观条件限制的需要做其他安全策略来补充**）
- 💀 我家大门常打开——隔离设计有问题，其他功能非常接近你的资产（**资产做好隔离，对接近资产的功能做安全保护**）
- 💀 眼前的黑不是黑，你说的白是什么白——萧煌奇《你是我的眼》——白名单的防护薄弱（**对白名单功能做严格的4A**）



我的微博@呆子不开口



关注QCon微信公众号，  
获得更多干货！

# Thanks!



主办方 **Geekbang** > **InfoQ**  
极客邦科技