芳华 / 2019-06-16 08:31:00 / 浏览数 8821 安全技术 WEB安全 顶(0) 踩(0)

SRC逻辑漏洞挖掘浅谈

[前言]

距离最近挖src到今天刚好一个月了,最近比较忙吧。具体应该算是5月份了,上一个月挖src的同时也被拉去参加《西安互联网安全城市巡回赛》了,还算比较幸运,通过几

1.资产收集

1.1业务范围

巧用搜索引擎首推谷歌查看了解SRC旗下涉及到的业务,收集其对应的业务下的域名,再进一步进行挖掘,如:



阿里巴巴 维基百科



全部

新闻

图片 地图

视频

更多

设署

T且

找到约 363,000 条结果 (用时 0.60 秒)

阿里巴巴集团-维基百科,自由的百科全书

https://zh.wikipedia.org/zh/阿里巴巴集团 ▼ 转为简体网页

阿里巴巴集團 (NYSE: BABA) 创立于1999年,是一家供電子商務線上交易平台的公司,業務包括B2B 貿易、網上零售、購物搜索引擎、第三方支付和雲計算服務。集團的 ...

发展历史·2014年·战略投资·其他投資

Alibaba Group - Wikipedia

https://en.wikipedia.org/wiki/Alibaba_Group ▼ 翻译此页

Alibaba Group Holding Limited is a Chinese multinational conglomerate specializing in e-commerce, retail, Internet and technology. Founded 4 April 1999, the ...

Founder: Jack Ma; Peng Lei

Revenue: CN¥250.266 billion (US\$39.898 billi...

Founded: 4 April 1999; 20 years ago; Hangzh... Total assets: CN¥717.124 billion (US\$114.326 ...

History · Companies and affiliated ... · Corporate governance · Controversies

阿里巴巴-维基百科,自由的百科全书

https://zh.wikipedia.org/zh-hans/阿里巴巴 ▼

阿里巴巴(阿拉伯语: على بابا) 是《一千零一夜》中《阿里巴巴和四十大盗》一篇的男主人公。该篇故事最早见于文字是《一千零一夜》的欧洲翻译者之一安托万·加朗擅自...

外部链接 [編輯] • 阿里巴巴中国站成 ((***)) 维基新闻相关报导: • 阿里巴巴国际站會 阿里巴巴进军台湾 力图协助中小企 • 台湾阿里巴巴❷ • Alibaba.com Taiwan 阿里巴巴台湾的Facebook专页配 阿里巴巴台湾的第三方合作服务商♥智汇文化有限公司♥ 酷开电视 **查论编** 阿里巴巴集团 在駅 马云・藤崇信・徳兆福・张勇・约翰·迈克·埃文斯・影響・孙正义・董建华・郭徳明・Borje E. Ekholm・義万仁・武卫・蒋芳・张建锋・刘振飞・戴珊・石义徳・金建杭・董本洪・命永福・古永裕・杨伟东・胡晓明・吴敏芝・郑俊芳・张旭豪 离职 杨致沅•程维 衛宝网・天猫・聚划道・全球速幸通・阿里巴巴国际交易市场・阿里巴巴创业者基金・阿里巴巴网络・阿里音乐・阿里坎仲・阿里玛姆・阿里云搜索・阿里云 - 1688・AliOS・劉欽金服・菜宮网络・飞獾・YunOS・阿里通信・阿里巴彫业集团(海票票)・一海・高徳地閣・ 其他 湖畔大学•广州恒大淘宝足球俱乐部 事件 淘宝售卖假货事件

阿里集团业务

萬职 杨致远・程维

海宝网·天猫·探划算·全球速費通·阿里巴巴国际交易市场·阿里巴巴创业者基金·阿里巴巴网络·阿里音乐·阿里软件·阿里妈妈·阿里云搜索·阿里云·1688·AIIOS·蚂蚁金服· 葉鸟网络·飞猪·YunOS·阿里通信·阿里巴巴影业集团(海票票)·一海·高德地图·万网·UC优视(UC浏览器)·友盟+·虾米音乐·阿里星球·阿里体育(世界电子竞技运动会)·合一集团(优酷·土豆网)·钉钉·点点虫·一达通·阿里健康·天下网商·《南华早报》·银泰商业·金马鲜生·饯了么(馆了么是选)·365翻译

其他 湖畔大学・广州恒大淘宝足球俱乐部

重性 治学性赤假保重位

淘宝网

www.taobao.com/

天猫

https://www.tmall.com/

聚划算

https://ju.taobao.com/

全球速卖通

https://www.aliexpress.com/

阿里巴巴国际交易市场

https://www.alibaba.com/

阿里巴巴创业者基金

https://www.ent-fund.org/

阿里巴巴网络

https://www.1688.com/

阿里音乐

https://www.xiami.com/

阿里软件

阿里软件(上海)有限公司

阿里妈妈

https://www.alimama.com/

阿里云搜索

https://m.aliyun.com/product/search#/?_k=obawx8

阿里云

1.2常规性质资产收集

基本的资产收集方式:子域名枚举、端口扫描、路径扫描、旁站c段查询

子域名

子域名爆破:

sublist3r、subdomainsBurte、DiscoverSubdomain、layer子域名挖掘机 (v1.0 RELEASE) Coded By Coco413 usage: DiscoverSubdomain -t 100 -f True -d target.com AutoInfoDetect of subdomain optional arguments: -h, --help -v. --version show this help message and exit -v, --version -d DOMAIN, --domain DOMAIN Domai show program's version number and exit DomainName of scan target -t THREAD, --thread THREAD Number of scan threads(default:100) Full dict files to brute(default:False) ▶ 先知社区 -f FULL, --full FULL

子域名枚举

通过网络空间安全搜索引擎

云恶资产、FOFA、Virustotal、Dnsdumpster、Threatcrowd









路径扫描

dirsearch 、御剑、

```
Extensions: php | Threads: 10 | Wordlist size: 2700

Error Log: D:\信息泄漏收集\dirsearch-master\logs\er

Target: http://svip.fang.anjuke.com

[17:33:44] Starting:
[17:33:44] 400 - 166B - /%2e%2e/google.com
[17:33:51] 400 - 166B - /cms/smarty/templates_c/%
[17:33:51] 200 - 8KB - /login
[17:33:52] 200 - 28B - /robots.txt
[17:33:52] 200 - 8KB - /login.html
[17:33:53] 200 - 8KB - /login.html
[17:33:53] 200 - 8KB - /login.htm
[17:33:53] 200 - 8KB - /login.htm
[17:33:55] 200 - 8KB - /login.htm
```

旁站C段查询

在线旁站C段查询:www.webscan.cc、www.5kik.com、phpinfo.me

- 1.3信息泄漏
- 敏感目录/文件

<u>猪猪侠weakfilescan、cansina、sensitivefilescan</u>、FileSensor cali:~/fuzz/FileSensor\$ python3 filesensor.py localhost -o [START] localhost [200]http://localhost/ [200]http://localhost/test.php [200]http://localhost/icons/openlogo-75.png [!][200]http://localhost/test.php.bak [!][200]http://localhost/test.php~ [!][200]http://localhost/test.php [!][200]http://localhost/.test.php.swp Crawled Page: 3 Sensitive File Found: 4 [200]http://localhost/test.php.bak [200]http://localhost/test.php~ [200]http://localhost/test.php [200]http://localhost/.test.php.swp Results saved in /home/xy/fuzz/FileSensor/output/localhost-20170228-150154

网页源码/js/json泄漏敏感接口

1)接口泄漏

```
1 (1)
```

```
//请求集合
"chageStatus" : "/seats/changeStatus.do",
"isOnline" : "/seats/isOnline.do",
                        "summary": "/seats/summary.do",
"initSeat": "/seats/initSeat.do",
                         "loadRecord" : "/seats/loadRecord.do",
"transList" : "/seats/seattree.do",
                         "getCommTypes" : "/seats/gettypes.do",
"addCommWord" : "/seats/addword.do",
                                "deleteCommWord" : "/seats/deleteword.do",
"updatePass" : "/seats/updatePass.do",
"validate" : "/seats/validate.do",
                                "validate": "/seats/validate.do",
"isLogin": "/seats/isLogin.do",
"userInfos": "/user/userInfo.do",
"getUserInfos": "/user/userInfo.do",
"getSmartUserInfos": "/user/userInfo.do",
"getGoodsInfos": "/user/goodsInfo.do",
"getSmartGoodsInfos": "/user/goodsInfo.do",
                                                                                                                                                                                                                                 后台接口地址泄露
                                 "sendLetter" : "/user/sendMsg.do",
"waitQueueCount" : "/chat/waitQueueCount.do",
"getChatIdsByStartTime" : "/chat/getChatIdsByStartTime.do",
"getChatIdsByEndTime": "/chat/getChatIdsByEndTime.do",
                                 getChatRecords": "/chat/getChatRecords.do",
"queryPhrase": "/phrase/queryPhrase.do",
                                 "queryHistoryRelate": "/chat/queryHistoryRelate.do",
                                                                                                                                               //当天历史列表-远东
                "hasLeaveMsgPower": "/chat/isLeaveMsg.do", //是否有留言权限"queryLeaveMsg": "/chat/getLeaveMsgVisit.do", //获取留言用户"getUserLeaveMsg": "/chat/getSeatUnreadMsg.do", //获取留言消
                 getUserLeaveMsg": "/chat/getSeatUnreadMsg.do", //获取留言消息
"getMoreLeaveMsgRecord":"/chat/getMoreLeaveMsg.do", //搜索-点击更多留言
                "msgRecordDetail":"/chat/leaveMsgDetail.do", //搜索-点击用户留言显示留言详情
```

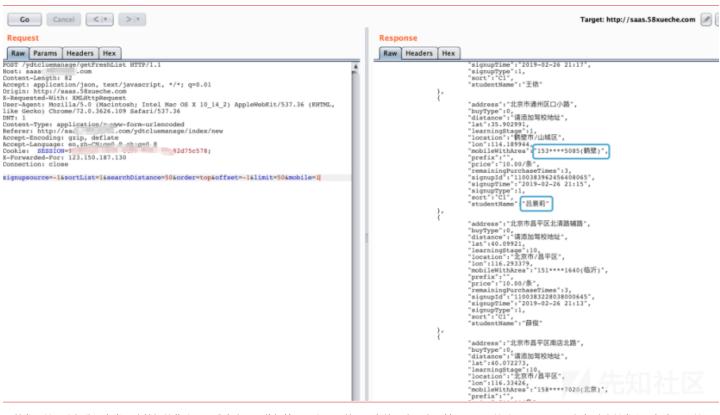
□ 2) json敏感信息泄漏

POST /job/resume/list HTTP/1.1

er=0&workingYear=0&expectSalary=0

Host: zhaopin com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0 Accept: application/json, text/plain, */* 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 Referer: https://zhacastk=6274eiq75d7d603a1d063 Content-Type: application/x-www-form-urlencoded X-Requested-With: XMLHttpRequest Content-Length: 209 Connection: close Cookie: BAIDUID=871A520DCA219664BBE4A618AEB80B07:EG=1: BIDUPSID=8E00100055010010013D18B68725736: PSTM=1552395855: BDUSS=03ZH55 YUEZZENXSU9UZAVWA... FBJ@ H_PS_PSSID=1427_21117_20698_28721_28558_28697_28584_26350_28605; Hm_lvt_3abe3fb0969d25e335f1fe7559defcc6=1553180835; Hm_lpvt_3abe3fb0969d25e335f1fe7559defcc6=1553180954; cas_st_480=a02e81c58f303e63adcddb50cf955bef7f658706c8428612d684f5341d21745047c4d4f3 _patcha_mct_key_=155344445527702701; uc_login_unique=e3c161e025bddbacb43c71637a6c8d64; mcttk=7283d3bb67ca5923b3b8 1000&curr⊂ 1Page=&jobType=&jobSubType

serPhone": "******", "type":2, "video":null, "workingYear": "\u65e0\u7ecf\u9a8c", "cashCost":10, "pointCos t":false,"platform":0},{"age":19,"birthday":"2000","resumefrom":"baipin","birthmonth":null,"education": "\u5927\u4e13","expectSalary":"\u9762\u8bae","maxSalary":-1,"minSalary":-1,"hasVideo":false,"gen der":"\u5973","jobCity":"\u676d\u5dde\\u4e0d\u9650","jobArea":"\u4e0d\u9650","jobIntention":"\u62a 4\u58eb","publishTime":"\u4eca\u5929","profStatus":"\u957f\u671f\u5173\u6ce8\u597d\u673a\u4f1a",
"portrait":null,"sortkey":"20190325","resumeld":"14764276","userld":"2852825695","userName":"\u4e 25\u5973\u58eb","userPhone":"******","type":2,"video":null,"workingYear":"1\u5e74\u4ee5\u4e0b","ca shCost":10,"pointCost":false,"platform":0},{"age":19,"birthday":"2000","resumefrom":"baipin","birthmo nth":null, "education": "\u9ad8\u4e2d\u4ee5\u4e0b", "expectSalary": "3000-5000", "maxSalary": "5000", " minSalary": "3000", "hasVideo": false, "gender": "\u7537", "jobCity": "\u5b9c\u5bbe\\u4e0d\u9650", "jobArea": "\u4e0d\u9650", "jobIntention": "\u666e\u5de5", "publishTime": "\u4eca\u5929", "profStatus": "\u6663 ea : \u4evatusess , jootiteentoir : \u5evasses , pasisiffinis : \u7evasses , pistestas : \u7evasses ; pistestas : \u7evasses : \u7evass "1-3\u5e74", "cashCost":10, "pointCost":false, "platform":0},{"age":19, "birthday": "2000", "resumefrom": baipin","birthmonth":null,"education":"\u9ad8\u4e2d\u4ee5\u4e0b","expectSalary":"3000-5000","max Salary", "5000", "minSalary": "3000", "hasVideo": false, "gender": "\u7537", "jobCity": "\u6606\u660e\Vu4e 0d\u9650", "jobArea": "\u4e0d\u9650", "jobIntention": "\u53f8\u673a", "publishTime": "\u4eca\u5929", "prof Status": "\u6b63\u5728\u627e\u5de5\u4f5c", "portrait": null, "sortkey": "20190325", "resumeld": "1476428 6","userId":"3424458962","userName":"\u5f20\u5148\u751f","userPhone":"******","type":2,"video":null ,"workingYear":"\u65e0\u7ecf\u9a8c","cashCost":10,"pointCost":false,"platform":0},{"age":19,"birthda y":2000,"resumefrom":"baixing","birthmonth":null,"education":"\u4e2d\u4e13\Vu6280\u6821","expect Salary": "3000-5000", "maxSalary": "5000", "minSalary": "3000", "hasVideo"; false, "gender": "\u5973", "job City": "\u8302\u540dV", "jobArea": "", "jobIntention": "\u62a4\u58ebV\u62a4\u7406", "publishTime": "\u4e ca\u5929","profStatus":0,"portrait":null,"sortkey":20190325,"resumeld":"5c97aed07b764f00013051b7 ","userId":null,"userName":"\u4e01\u5973\u58eb","userPhone":"******","type":2,"video":null,"workingY ear":"1\u5e74\u4ee5\u4e0b","cashCost":10,"pointCost":false,"platform":1}]}}



目前发现关于这部分没有发现比较好的收集工具或脚本,因此打算写一个,目前还正在编写中,主要基于chrom协议、pyppeteer框架动态触发爬取包含ajax以尽可能的收集

- a)网站源码涉及到的子域名ur接口资产爬取
- b)网站源码js中包含的请求或拼接的访问接口
- c高级功能) url接口中json信息泄漏识别

备注:该部分的具体内容将在下一篇文章【谈js静态文件在漏洞挖掘中的利用】继续更新

1.4其他业务查找

微信公众号绑定接口、app、老旧的登陆接口、版本迭代

2.越权

- 改识别用户参数
- 改cookie
- 越权访问
- 登陆后,修改密码未校验id与用户修改id即可该其他人密码
- · 修改个人数据时 页面源代码有用户标识符id 抓包修改或添加id
- 直接访问后台链接禁用js则不会跳转登录界面,直接登陆
- 登陆分为账号和游客登陆,游客功能有限,app端只前端检测,模拟发包即可
- 越权订单查看打印下载、越权操作他人收货地址、增删改查等。

3.逻辑漏洞

任意用户注册、密码重置、密码找回、

3.1本地验证、修改返回包

1)获取验证码后任意输入一个验证码。 账号信息(42945563741441) 认证管理 暂无 修改密码 企业信息管理 修改手机 邮箱未绑定 绑定 账号管理 权限管理 输入手机号 17128240046

获取验证码

取消

1234

确定

2)抓包放行,得到的返回包如下

周—至周五 9:00-18

客服: 400-050-808

资源管理

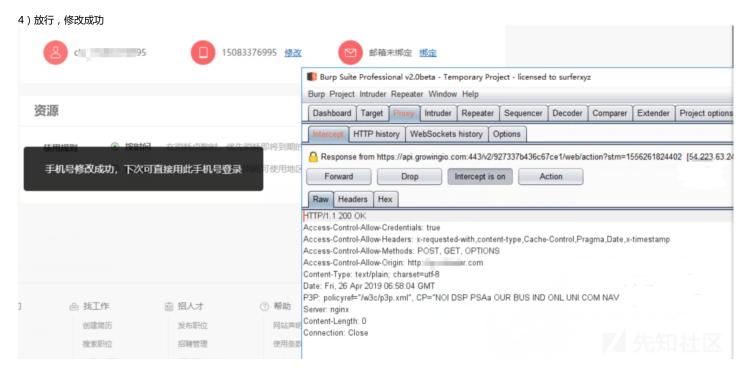
合同管理

HTTP/1.1 200 OK Server: Tengine Date: Fri, 26 Apr 2019 06:57:58 GMT Content-Type: text/json;charset=utf-8 Content-Length: 49 Connection: close Set-Cookie: bps=""; Domain=com; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/ Version=1; Domain= _____com; Max-Age=604800; Expires=Fri, 03-May-2019 06:57:58 GMT; Path=/ {"code":6,"msg":"手机验证码输入不正确"}

3)抓包改返回包修改为正确的返回包覆盖错误的返回包,如下

{"code":1,"data":"目标用户手机号","msg":"绑定成功Ÿ"}

HTTP/1.1 200 OK Server: Tengine Date: Fri, 26 Apr 2019 06:57:58 GMT Content-Type: text/json;charset=utf-8 Content-Length: 49 Connection: close Set-Cookie: bps=""; Domain=chinahr.com; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/ Set-Cookie: bps="buid=42945563741441&bst=1556261878247&bstSign=32c56f101b90dd37e82&blt=1556261878248&blt Version=1; Domain=chinahr.com; Max-Age=604800; Expires=Fri, 03-May-2019 06:57:58 GMT; Path=/ {"code":1,"data":"17121192606<mark>","msg":"绑定成功"}</mark>



3.2手机号、验证码、用户未统一验证问题

如密码找回重置时未对原绑定手机号验证进行任意账号密码重置

未对原绑定手机号、验证码、用户未统一验证,或验证码未绑定 只验证验证码正确,没判断用户id 或手机号,修改想改的id 正确手机验证码即可

```
POST /cppt/open/msg/send/smsCode HTTP/1.1
Host: user. com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101 Firefox/66.0
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
Referer:
http://use com/cppt/open/page/login?backUrl=http:// .com/home/index.html
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 99
Connection: close
Cookie: chrcsession=c81c0eeb-502a-4409-8247-2f0c80752762;
wechatId=b2744924-4db1-427d-bccf-632d8792e591;
token=5ca37a135c7549b582a6aa19cc48777e936pfn03;
gr_user_id=e5758f0e-ff8f-4491-ad5f-84586b0c6deb; _ga=GA1.2.640399965.1554215331;
_gid=GA1.2.1724795989.1554215331; 58tj_uuid=2a49ee03-1f03-41f6-80f3-3a45c084da20;
channel=campus; new_session=0;
init_refer=http%253A%252F%252F
                                          com%252Fjob%252F5b8cf26d7465577ccd2b5ab
0; new_uv=1; utm_source=; spm=; als=0;
gr session id b64eaae9599f79bd=cf5b4902-554a-4ffc-b19b-cf01dcd713e0;
gr session id b64eaae9599f79bd cf5b4902-554a-4ffc-b19b-cf01dcd713e0=true
account=150( 373&captcha=clg7&mobile=17f 350&type=5&timegap=1554219458600& rm
sLang=undefined
```

POST /cppt/open/pwd/m/preReset HTTP/1.1 Host: user com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101 Firefox/66.0

Accept: */*

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

Referer: http://user _____com/cppt/open/page/login?backUrl=http:// _____com/ncamp/xjh/

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Content-Length: 74 Connection: close

smsCode=588208&mobile=176 3850 ktimegap=1554223827949&_rmsLang=undefined

手机号改为验证码对应的手机号

★知社区

150\73账号被重置



重置密码成功!

下次登录请使用该密码

知道了

光 先知社区

3.3密码重置类其他逻辑问题

- 1. 以重置成功的token覆盖最后一步错误的token和1类似。
- 2. 密码重置时删除mobilephone参数值修改email参数值
- 3. 假如找回需要4部,最后一部有user参数,用自己账号正常到第三部,第四部修改user实现

4.支付逻辑漏洞

5.步骤,可跳过步骤

酒店..

6.爆破、枚举

撞库,登陆时无验证码且可无限被尝试,用户名验证时有无用户名错误回显、密码可被爆破

无验证码,验证码不刷新,验证码4位过于简单无尝试次数限制可被爆破、

枚举注册用户 输入用户名,发送请求验证用户名是否正确(若返回次数限制,可测试服务端未限制高频访问)

登陆失败有次数限制,若包中有限制参数可更改或删除参数

邮箱轰炸,短信轰炸,burp Repeate,短信轰炸验证码有60秒限制时,有的参数修改后可绕过如



改为0回显2绕过了验证码限制



7.其他

• cookie一直有效 , (修改密码后)

第三方账户登录绕过(拦截微博授权成功的请求地址: https://api.weibo.com/oauth2/sso_authorize?sflag=1 修改response中uid,服务端没有校验客户端提交的uid与授权成功的uid相同)

8.总结

在挖洞的过程中还是比较注重有耐心,细心测试更多参数、同时也需要我们不断的交流学习新思路,才会有更进一步的收获。另外也需要1>注重安全开发2>知识积累当然、

SRC逻辑漏洞挖掘浅谈.zip (0.003 MB) 下载附件

点击收藏 | 18 关注 | 2

上一篇:记一次真实的邮件钓鱼演练下一篇:内核漏洞挖掘技术系列(4)——sy...

1. 5 条回复



misskiki 2019-06-17 10:29:14

第三方账户登录绕过 这个楼主可以分享下姿势吗

0 回复Ta



Ph3mf0lk 2019-06-17 22:15:47

楼主可以说一下那个改返回包是怎么操作么。之前看见好几篇总结里有写到这点。但是我在实际日站的时候好像从来没遇到过。而且burp怎么拦截返回包呢 0 回复Ta



Ph3mf0lk 2019-06-17 22:26:28

嗷嗷,好像百度到方法了。

0 回复Ta



Tide 2019-06-18 08:21:55

@Ph3mf0lk 修改返回包信息本质上就是越权漏洞,要求服务端没有对用户的上一步操作进行验证,否则修改返回的数据包就是自欺欺人

0 回复Ta



173****4784 2019-06-18 12:08:42

逻辑漏洞大部分可以说是 客户端到服务器端验证步骤相对独立 才能钻空子 修改参数

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS <u>关于社区</u> <u>友情链接</u> <u>社区小黑板</u>