

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，再进行进一步挖掘，如：



阿里巴巴 维基百科



全部新闻图片地图视频更多

设置工具

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

阿里巴巴集团（NYSE：BABA）创立于1999年，是一家供电子商务线上交易平台的公司，业务包括B2B贸易、网上零售、购物搜索引擎、第三方支付和云计算服务。集团的 ...

发展历史 · 2014年 · 战略投资 · 其他投资

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 LeiRevenue: 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：علي 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 [编辑]

- 阿里巴巴中国站
- 阿里巴巴国际站
- 台湾阿里巴巴
 - Alibaba.com Taiwan 阿里巴巴台湾的Facebook专页
 - 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

 维基新闻相关报导：
阿里巴巴进军台湾 力图协助中小企业拓展商机

主·论·闻	阿里巴巴集团	[隐藏]
人物	在职 马云·蔡崇信·陆兆禧·张勇·约翰·迈克·埃文斯·彭蕾·孙正义·董建华·郭德明·Borje E. Ekholm·龚万仁·武卫·蒋芳·张建锋·刘振飞·戴珊·石义德·金建杭·董本洪·俞永福·古永锵·杨伟东·胡晓明·吴敏芝·郑俊芳·张旭豪	
离职	杨致远·程维	
业务	淘宝网·天猫·聚划算·全球速卖通·阿里巴巴国际交易市场·阿里巴巴创业基金·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·AliOS·蚂蚁金服·菜鸟网络·飞猪·YunOS·阿里通信·阿里巴巴影业集团 (淘票票)·一淘·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·盒马鲜生·饿了么 (饿了么星选)·365翻译	
其他	湖畔大学·广州恒大淘宝足球俱乐部	
事件	淘宝集卖假货事件	

整理，再进行常规资产收集

阿里集团业务

离职	杨致远·程维
业务	淘宝网·天猫·聚划算·全球速卖通·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·AliOS·蚂蚁金服·菜鸟网络·飞猪·YunOS·阿里通信·阿里巴巴影业集团(淘票票)·一淘·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·盒马鲜生·饿了么(饿了么星选)·365翻译
其他	湖畔大学·广州恒大淘宝足球俱乐部
地址	淘宝集团总部地址

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：

```
subdomain
  鎧€ 鎧€
  Coded By Coco413 (v1.0 RELEASE)

usage: DiscoverSubdomain -t 100 -f True -d target.com

AutoInfoDetect of subdomain

optional arguments:
  -h, --help            show this help message and exit
  -v, --version          show program's version number and exit
  -d DOMAIN, --domain DOMAIN
                        DomainName of scan target
  -t THREAD, --thread THREAD
                        Number of scan threads(default:100)
  -f FULL, --full FULL  Full dict files to brute(default:False)
```

子域名枚举

通过网络空间安全搜索引擎

云悉资产、FOFA、Virustotal、Dnsdumpster、Threatcrowd



Q收藏规则下载数据使用API

类型分布

网站

318

年份

2019

137

2018

181

国家排名

中国

318

端口排名

80

260

443

58

Server排名

Tengine

309

搜索 domain="58.com" 获得 318 条匹配结果 (独立IP数为 11 条), 用时 7 毫秒, 模式: extended.

默认只显示一年内的数据, 点击 all 链接查看所有.

← 上一页

1

2

3

4

5

6

7

...

32

下一页 →

jianli.58.com

80

2019最新个人简历库, 2019最新简历模板-58同城

154.8.240.21

Q

2019-05-01

Q

China

Q

58.com

Q

Tengine

HTTP/1.1 200 OK

Connection: close

Transfer-Encoding: chunked

Content-Type: text/html;charset=UTF-8

Date: Tue, 30 Apr 2019 18:14:17 GMT

Server: Tengine

Vary: Accept-Encoding

Vary: Accept-Encoding

https://mtongzhen.58.com

443

【58同镇乡镇生活信息服务平台|58同镇加盟方式】-58同城官网

先知社区

路径扫描

dirsearch、御剑、

```

dirsearch v0.3.8
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_form_admin.htm
[17:33:53] 200 - 8KB - /loginl
[17:33:53] 200 - 8KB - /login.htm
[17:33:55] 200 - 8KB - /login_A.html
[17:33:55] 200 - 8KB - /login/login
[17:33:55] 200 - 8KB - /login/index
[17:33:55] 200 - 8KB - /login/super
[17:33:55] 200 - 8KB - /login-redirect
[17:33:56] 200 - 8KB - /login/
[17:33:56] 200 - 8KB - /loginflat
[17:33:56] 200 - 8KB - /login_db
[17:33:57] 200 - 8KB - /login-us

```

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

猪猪侠weakfilesan、cansina、sensitivefilesan、FileSensor

```

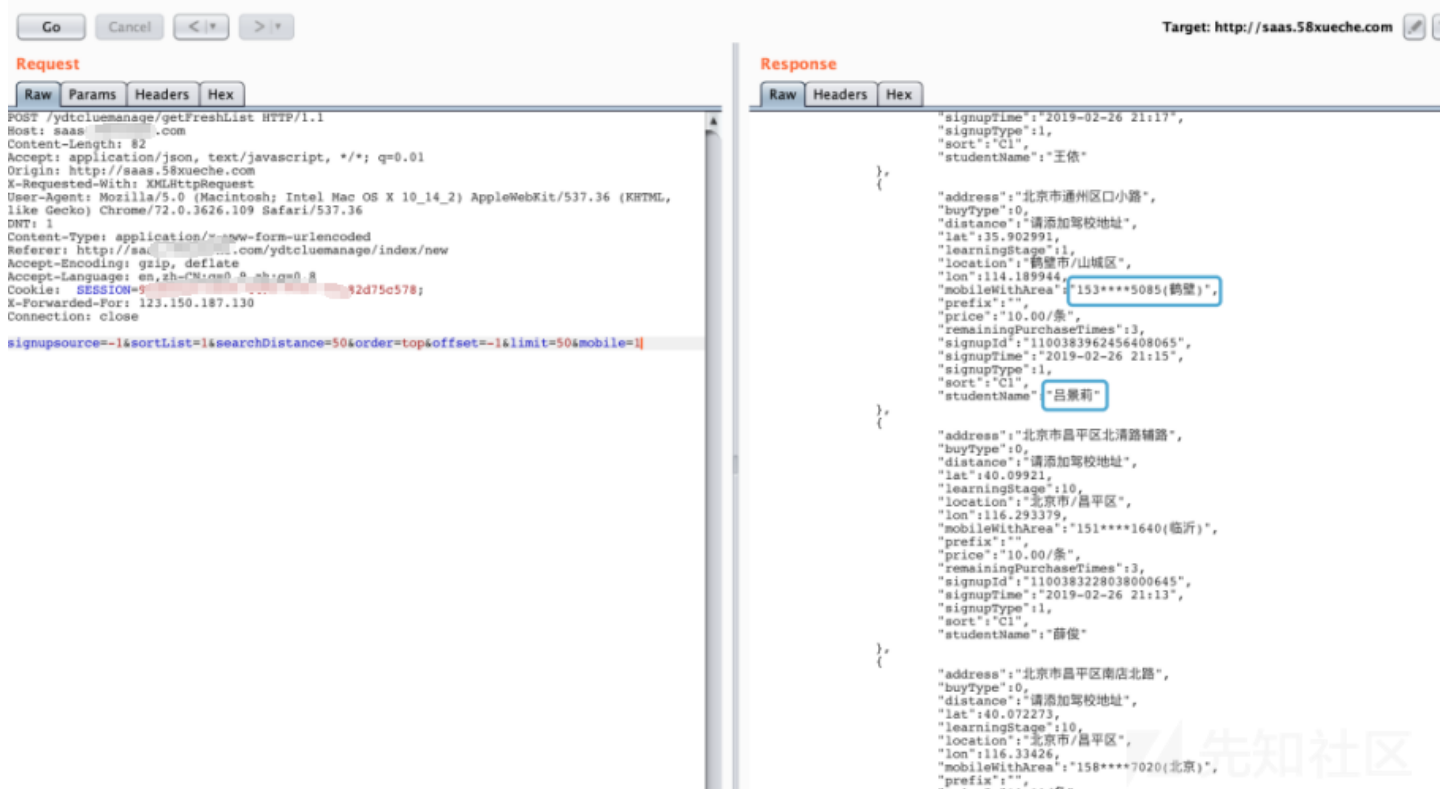
xy@kali:~/fuzz/FileSensor$ python3 filesensor.py localhost -o
[START] localhost
[200]http://localhost/
[200]http://localhost/test.php
[200]http://localhost/icons/openlogo-75.png
[!][200]http://localhost/test.php.bak
[!][200]http://localhost/test.php~
[!][200]http://localhost/test.php_
[!][200]http://localhost/.test.php.swp
-----
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



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

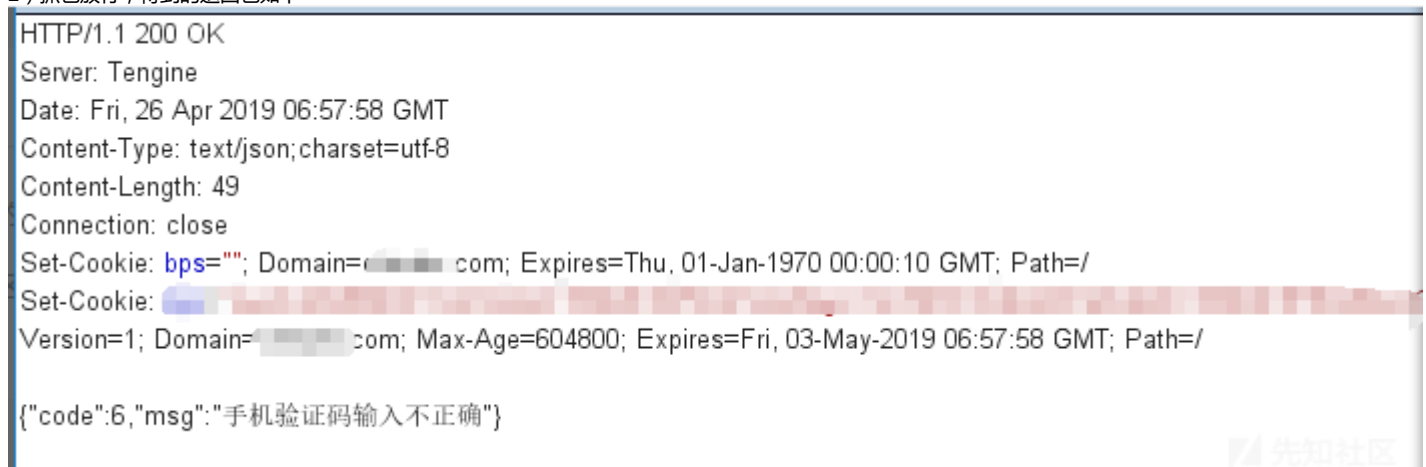
任意用户注册、密码重置、密码找回、

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。

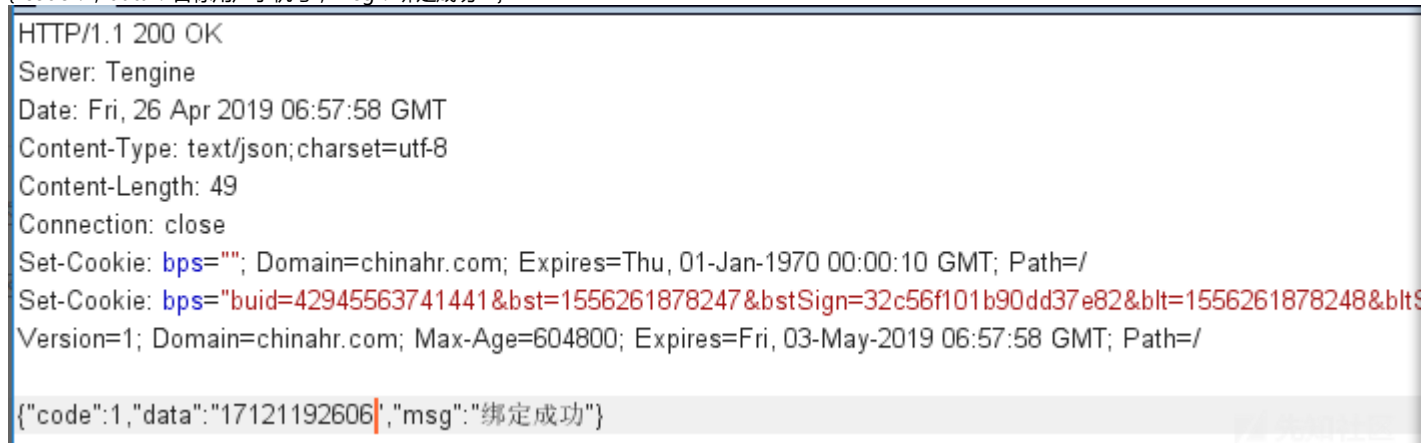


2) 抓包放行，得到的返回包如下

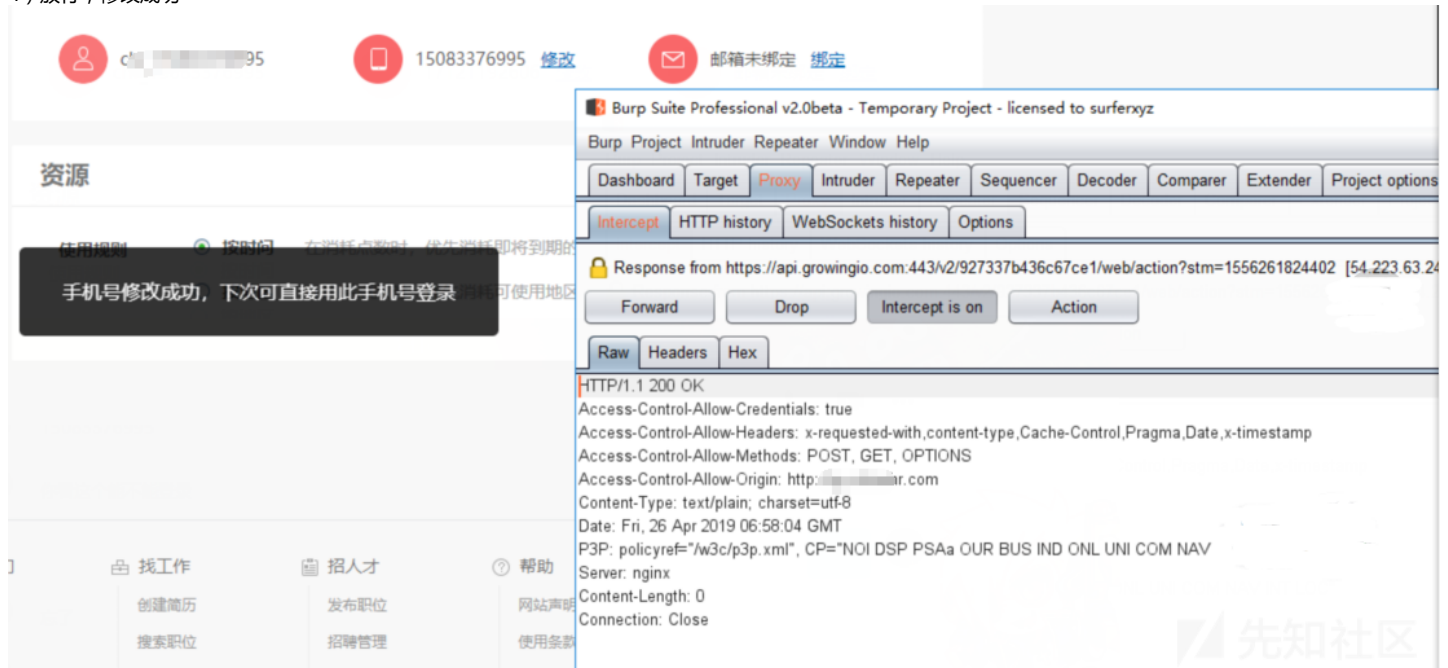


3) 抓包改返回包修改为正确的返回包覆盖错误的返回包，如下

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



4) 放行, 修改成功



3.2手机号、验证码、用户未统一验证问题

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

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

```
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: */*
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-f8f-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=1506. 373&captcha=clq7&mobile=176. 350&type=5&timegap=1554219458600&_rm
sLang=undefined
```



```
POST /cppt/open/pwd/m/preReset HTTP/1.1
Host: user[REDACTED].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[REDACTED].com/cppt/open/page/login?backUrl=http://[REDACTED].com/ncamp/xjh/
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 74
Connection: close
Cookie: c[REDACTED]=1189.44a9-8e71-1135465573ba; wechatId=d96a447f-8172-473a-ad96-a4f8a5a554b2; token=5ca3909
gr_user_id=e5758f0e-fb8f-4491-ad5f-b4[REDACTED]399965.1554215331; _gid=GA1.2.1724795989.1554215331; 58tj_
smsCode=588208&mobile=176[REDACTED]850&timegap=1554223827949&_rmsLang=undefined
```

手机号改为验证码对应的手机号

先知社区

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

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步，第四步修改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 Repeater，短信轰炸验证码有60秒限制时，有的参数修改后可绕过 如

1) isVerfi参数 这里是1 回包 3 手机没收到信息 存在验证码限制

```
GET /member/Handler/Regist...?Method=setMo
bile_Verification&phone=
e=dpol&sat=14958860679...
Host: www...
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/49.0.2623.139 Safari/537.36 SE 2.X MetaSr
1.0
Referer:
http://...
Cookie:
ASP.NET_SessionId=qjjbqabgdfr;
...672-4d015463
...100200-10...
CNZZDATA1000...47968-1...7C14958
31513; CheckCode=DPOL
Connection: close
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 1
Content-Type: text/plain; charset=utf-8
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Access-Control-Allow-Origin: *
Date: Sat, 27 May 2017 12:06:28 GMT
Connection: close
```

3

改为0 回显2 绕过了验证码限制

```
GET /member/Handler/Regist...?Method=setMo
bile_Verification&phone=
e=dpol&sat=1495886067992...
Host: www...
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/49.0.2623.139 Safari/537.36 SE 2.X MetaSr
1.0
Referer:
http://...
Cookie:
ASP.NET_SessionId=qjjbqabgdfr;
...5463
...CNZZDATA1000...81513-1...7C14958
81513; CheckCode=DPOL
Connection: close
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Length: 1
Content-Type: text/plain; charset=utf-8
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Access-Control-Allow-Origin: *
Date: Sat, 27 May 2017 12:07:20 GMT
Connection: close
```

2

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](#) [关于社区](#) [友情链接](#) [社区小黑板](#)