我是如何挖各SRC漏洞的

目　录

一、作为外行对信息安全的理解和看法

二、为什么会喜欢挖漏洞

三、对此事定位、布局

四、了解游戏规则

五、了解自己想做的和能做的

目　录

六、情报收集，从远处看细节

七、选择容易忽视的问题，避开高手

八、了解(开发、实施、安全)人员的细微关系和情绪

九、一个有意思的漏洞

十、一个有意义的漏洞

一、作为外行对信息安全的理解和看法

由于之前不知道什么是信息安全，一开始的想法就是：信息安全 = 黑客　　，然后就是下面这样的。

二、为什么喜欢挖漏洞

如果说追女朋友是hrm太旺盛，那么挖漏洞可能就是因为女朋友不在家。。。

其实可能是因为小时候电视的影响，一直对“黑客”这个词有很大的向往，但是一直没找到机会去接触这个行业。

在去年底的某一天，刚好有个同事喜欢刷微博，提到有“SRC”这个词,原来这个黑安全相关。

三、对此事的定位和布局

确定了自己喜欢做的事情，选择目标很重要，为什么会在众多”SRC”里面选择，阿里和携程。

四、了解游戏规则

漏洞评分标准

贡献值计算方法

贡献值分值由漏洞对应用的危害程度以及应用的重要程度决定：贡献值分值=漏洞基础贡献值X应用贡献值系数

例如：一个淘宝核心应用远程执行漏洞的贡献值为100，计算方法为：漏洞基础贡献值（严重：10）X应用贡献值系

而一个淘宝天下的反射型XSS漏洞的贡献值为3，计算方法为：漏洞基础贡献值（中：3）X应用贡献值系数（边缘应

漏洞等级

根据漏洞的危害程度将漏洞等级分为【严重】、【高】、【中】、【低】、【无】五个等级。每个漏洞总基础贡献

利用场景中漏洞的严重程度、利用难度等综合因素给予相应分值的贡献值和漏洞定级，每种等级包含的评分标准及

【严重】

基础贡献值分值【9~10】，本等级包括：

1、 直接获取系统权限的漏洞（服务器权限、客户端权限）。包括但不仅限于远程命令执行、任意代码执行、上传

获取系统权限、缓冲区溢出（包括可利用的 ActiveX 缓冲区溢出）。

2、 直接导致业务拒绝服务的漏洞。包括但不仅限于远程拒绝服务漏洞。

3、 严重的敏感信息泄漏。包括但不仅限于核心 DB（资金、身份、交易相关）的 SQL 注入漏洞。

4、 严重的逻辑设计缺陷和流程缺陷。包括但不仅限于伪造任意号码发送消息、任意账号资金消费、任意帐号密码

【高】

基础贡献值分值【6~8】，本等级包括：

1、 敏感信息泄漏。包括但不仅限于非核心DB SQL注入、源代码压缩包泄漏、可获取大量用户交易信息的接口、服务器、应用加密可逆或明文的敏感信息泄露。

2、 越权访问。包括但不仅限于绕过认证直接访问管理后台、后台弱密码。

3、 大范围影响用户的其他漏洞。包括但不仅限于可造成自动传播的存储型XSS（包括存储型DOM-XSS）、涉及交易、资金、密码的CSRF。

4、 影响到服务器的本地提权漏洞。

【中】

基础贡献值分值【3~5】，本等级包括：

1、 需交互方可影响用户的漏洞。包括但不仅限于反射型 XSS（包括反射型 DOM-XSS）、CSRF、URL跳转漏洞。

2、 本地拒绝服务漏洞。包括但不仅限于客户端本地拒绝服务（解析文件格式、网络协议产生的崩溃）。

3、 普通越权操作。包括但不仅限于不正确的直接对象引用。

4、 普通信息泄漏。包括但不仅限于客户端明文存储密码、客户端密码明文传输以及web路径遍历、系统路径遍历。

5、 普通的逻辑设计缺陷和流程缺陷。

【低】

基础贡献值分值【1~2】，本等级包括：

1、 轻微信息泄漏。包括但不仅限于路径信息泄漏、svn信息泄漏、phpinfo、异常信息泄露。

2、 难以利用但存在安全隐患的漏洞，包括但不仅限于可引起传播和利用的 Self-XSS

其实最关键是什么不能做，什么能做

评分标准通用原则

1) 评分标准仅适用于阿里巴巴集团产品和业务。与阿里巴巴集团完全无关的漏洞，不计贡献值。

2) 对于非阿里巴巴集团自身发布的产品和业务，如阿里巴巴集团的投资公司、合资公司、合作区业务，贡献值不超过 5，等级不高于【中】，且不保证能按照预定时间处理；如果是阿里巴巴开放平台的第三方应用的漏洞，不计贡献值。

3) 第三方产品的漏洞只给第一个提交者计贡献值，最高不超过5贡献值，等级不高于【中】，且不保证修复时长，包括但不限于阿里巴巴集团正在使用的wordpress、flash插件以及apache等服务端相关组件等；不同版本的同一处漏洞视为相同漏洞。

4) 同一个漏洞源产生的多个漏洞计漏洞数量为一。例如 phpwind 的安全漏洞、同一个 JS 引起的多个安全漏洞、同一个发布系统引起的多个页面的安全漏洞、框架导致的整站的安全漏洞、泛域名解析产生的多个 安全漏洞等。

5) 各等级漏洞的最终贡献值数量由漏洞利用难度及影响范围等综合因素决定，若漏洞触发条件非常苛刻，包括但不限于特定浏览器才可触发的xss漏洞，则可跨等级调整贡献值数量。

6) 同一漏洞，首位报告者计贡献值，其他报告者均不计。

7) 在漏洞未修复之前，被公开的漏洞不计分。

8) 报告网上已公开的漏洞不计贡献值。

9) 同一份报告中提交多个漏洞，只按危害级别最高的漏洞计贡献值。

10) 以测试漏洞为借口，利用漏洞进行损害用户利益、影响业务运作、盗取用户数据等行为的，将不会计贡献值，同时阿里巴巴集团保留采取进一步法律行动的权利。

争议解决办法

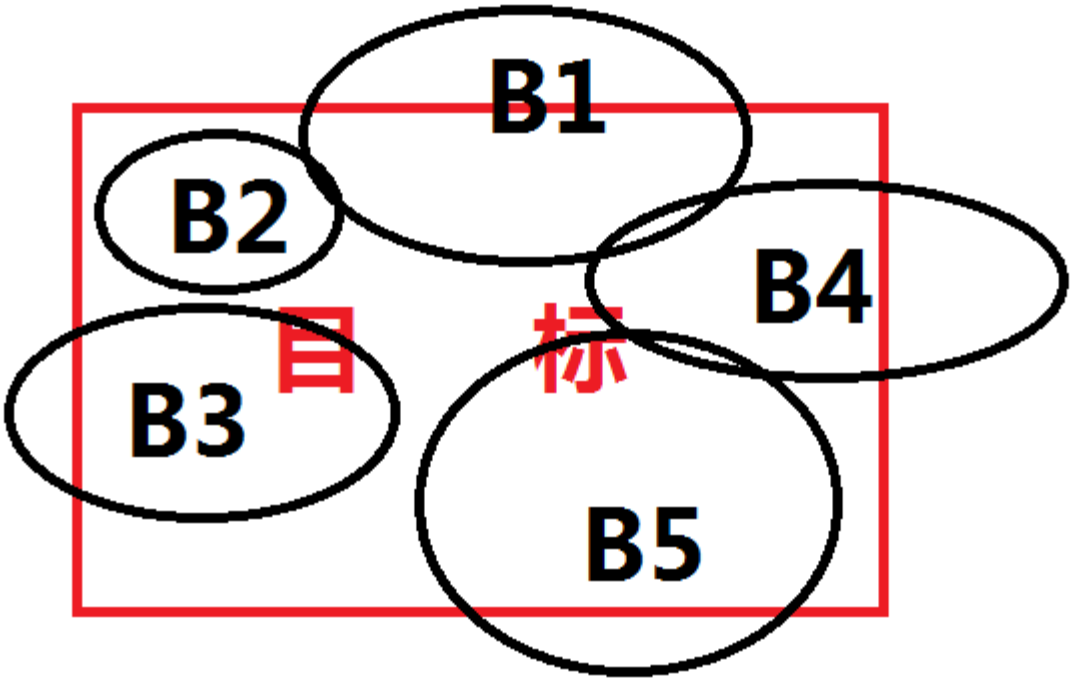
在漏洞报告处理过程中，如果报告者对流程处理、漏洞定级、漏洞评分等有异议的，可以通过漏洞详情页面的留言板或者通过即时通讯联系在线工作人员及时沟通。

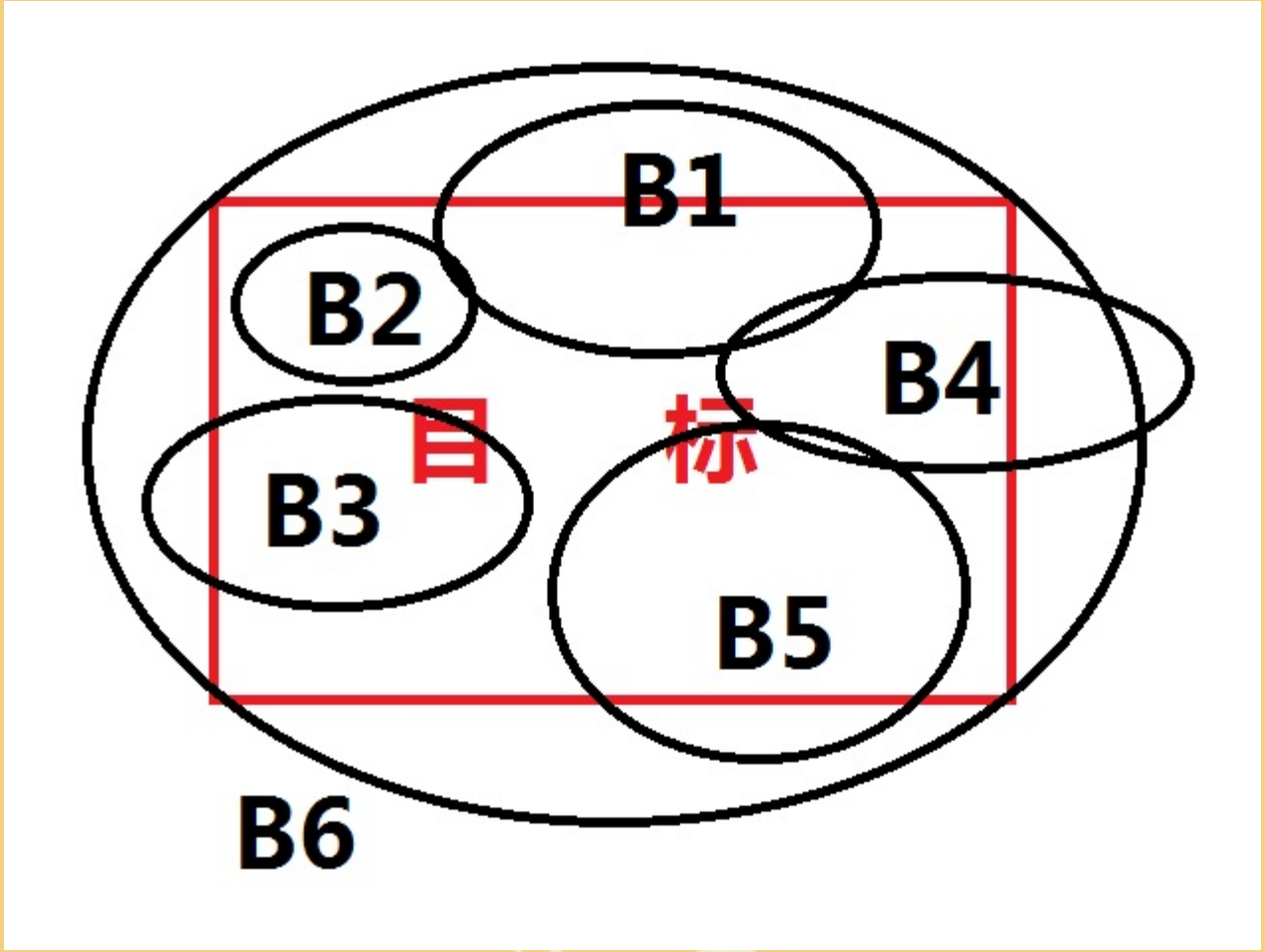
五、了解自己想做的和能做的

由于不懂什么是漏洞，在了解规则后，发现自己会的只有那么一点，那么，如何把尽会的一点点东西利用在这个漏洞挖掘场景中呢？

六、情报收集，从远处看细节

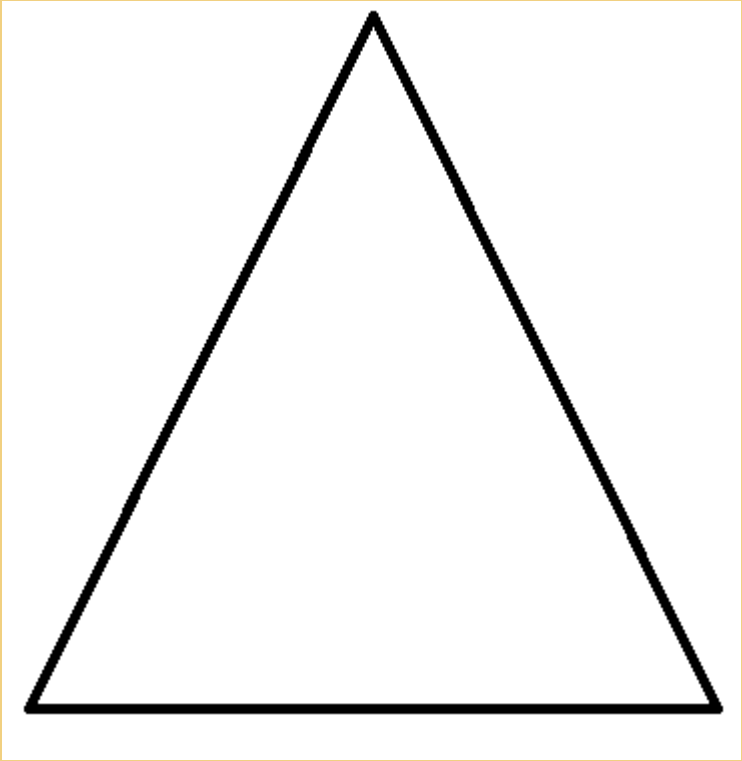
- 以业务为驱动，了解目标旗下所有的子公司、分公司以及并购等相关业务。
- 以渗透测试的思维收集目标信息，主要包括域名、ip范围、开源社区关于公司相关的代码、员工信息等。


B1
B2
B4
目
标
B3
B5


B1
B2
B4
目
标
B3
B5
B6

七、选择容易忽视的问题，避开高手

- 实施、运维问题，从乌云公开的漏洞统计来看，实施和运维过程产生的问题尤为严重，其数量和影响面都非常大。
- 核心业务逻辑问题，由于不懂技术，但对核心业务比较敢兴趣，只好用逻辑来撬动技术。
- 边缘业务问题，这个地方一般会被公司安全人员忽视（不重视），但往往是可以四两拨千斤的。



设计

开发

实施

八、了解(开发、实施、安全)人员的细微关系和情绪

听说程序员的天敌是产品经理和安全人员，那么由于心理矛盾，多少会在工作配合方面出现写问题。

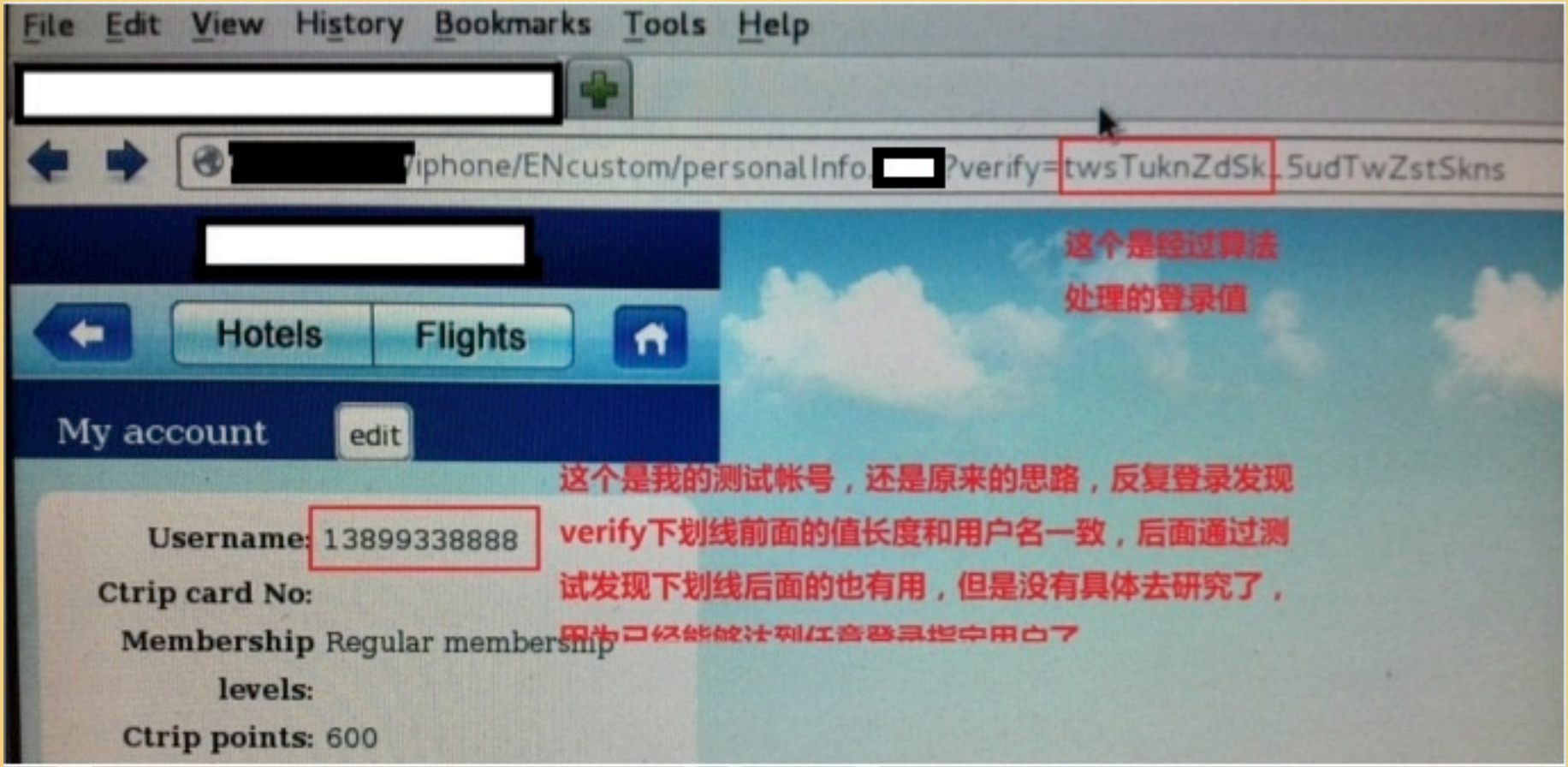
这里的细微关系和一些综合因素，就很容易造成如：漏洞修复不完整，漏哪补哪等等现象。

九、一个有意思的漏洞

在逛西湖的过程中，感觉自己之前看到某系统有些问题，回去经过仔细观察，果然别有洞天，大致情况如以下URL：

http://***.******.***/iphone/ENIndex.****?verify=tuTwunsZnn_5Tttw

灵感出现

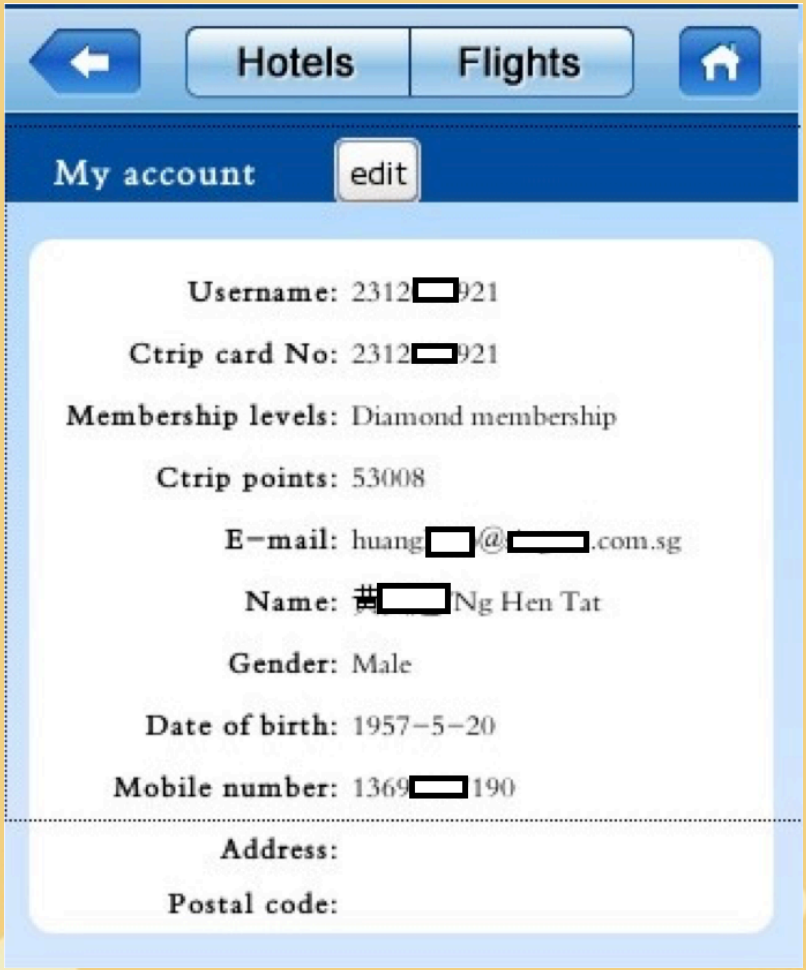

File Edit View History Bookmarks Tools Help
[redacted]iphone/ENcustom/personalInfo[redacted]?verify=twsTuknZdSk_SudTwZstSkns
这个是经过算法
处理的登录值
Hotels
Flights
My account
edit
这个是我的测试帐号，还是原来的思路，反复登录发现
verify下划线前面的值长度和用户名一致，后面通过测
试发现下划线后面的也有用，但是没有具体去研究了，
Username: 13899338888
Ctrip card No:
Membership levels: Regular membership
Ctrip points: 600

对算法的理解

加算法形成的值		原始用户名信息
aaaaaaaaaaa	a	srqponmlkji
bbbbbbbbbbb	b	vutsrqponml
ccccccccccc	c	YXWVUTSRQPO
ddddddddddd	d	65432109876
eeeeeeeeeee	e	rqponmlkjih
fffffffffff	f	ONMLKJIHGFE
ggggggggggg	g	mlkjihgfedc
hhhhhhhhhhh	h	SRQPONMLKJI
iiiiiiiiiii	i	lkjihgfedcb
jjjjjjjjjjj	j	EDCBAZYXWVU
kkkkkkkkkkk	k	87654321098
lllllllllll	l	gfedcbazyxw
mmmmmmmmmmmmm	m	RQPONMLKJIH
nnnnnnnnnnn	n	98765432109
ooooooooooo	o	xwvutsrqpon
ppppppppppp	p	MLKJIHGFEDC
qqqqqqqqqqq	q	fedcbazyxwv
rrrrrrrrrrr	r	FEDCBAZYXWV
sssssssssss	s	09876543210
ttttttttttt	t	10987654321
uuuuuuuuuuu	u	32109876543
vvvvvvvvvvv	v	UTSRQPONMLK
wwwwwwwwwwwww	w	43210987654
xxxxxxxxxxx	x	ZYXWVUTSRQP
yyyyyyyyyyy	y	TSRQPONMLKJ
zzzzzzzzzzz	z	KJIHGFEDCBA

加算法形成的值		原始用户名信息
sssssssssss	s	09876543210
ttttttttttt	t	10987654321
TTTTTTTTTTT	T	21098765432
uuuuuuuuuuu	u	32109876543
wwwwwwwwwwwww	w	43210987654
ZZZZZZZZZZZ	Z	54321098765
ddddddddddd	d	65432109876
SSSSSSSSSSS	S	76543210987
kkkkkkkkkkk	k	87654321098
nnnnnnnnnnn	n	98765432109

通过算法重构验证参数，最终实现任意用户登陆



十、一个有意义的漏洞

在一次扫马路的过程中，发现一运维问题，无意中进了大公司内网，第一件事想着就是继续测试，但后来在前辈的指导下，才发现这是不符合游戏规则的。但在此同时，也发现这是自己很有兴趣做的一件事，好像是叫渗透测试。

运气很重要

谢 谢 ！