

19.02.06丨星期三丨晴天

# 第一种：验证码可爆破

标志为验证码为4/5位纯数字，以及验证码为前端进行刷新（该情况最为常见，一般在补天专属都是高危的）

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

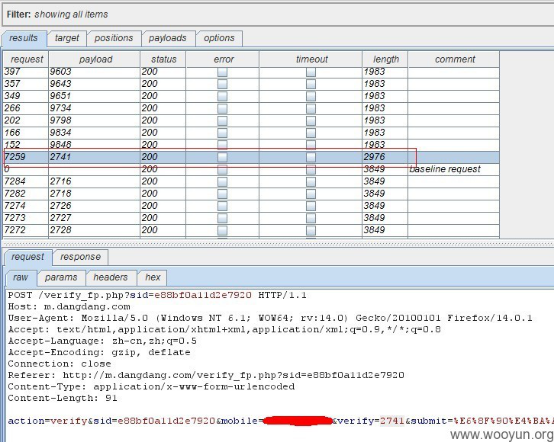
Accept-Encoding: gzip, deflate

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



# 第二种：验证码前端可控

也就是发送什么验证由你控制

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：

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

# 第三种：验证码在返回包内

就是简单地抓取返回包看到了验证码

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

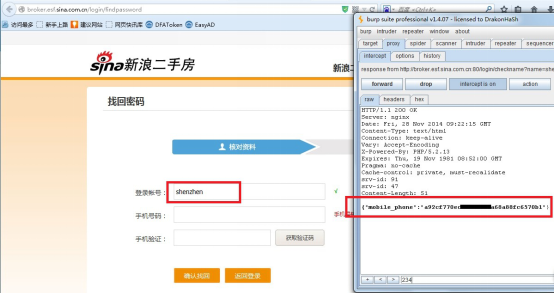
问题网站<http://esf.sina.com.cn/> 【新浪二手房】

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

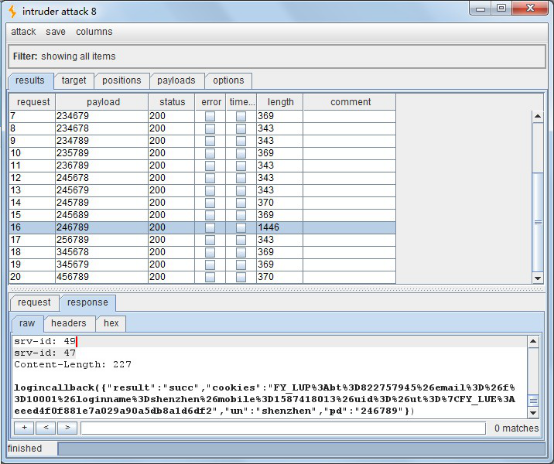
256789

345678

345679

456789

成功破出重置后的密码为246789



至此，成功登录该用户。



# 第四种：弱token

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

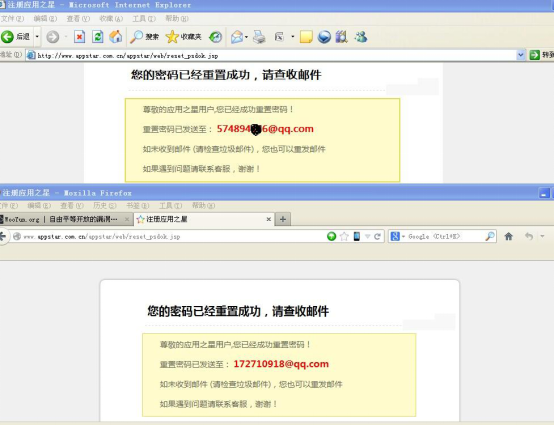
上面有积分可以换充值卡。

中兴某网站的积分商城充值卡等礼品任意兑换漏洞

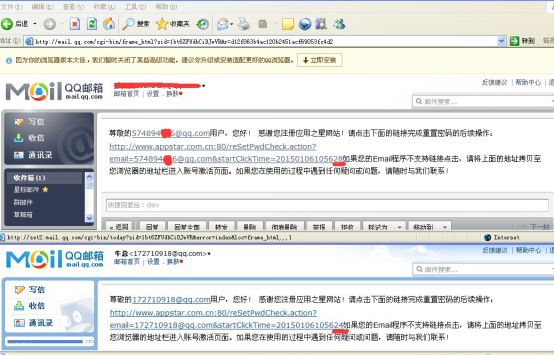
2.上面还有一个任意用户密码重置漏洞，找回密码链接的token不够随机，貌似就是当前时间。可以任意找回用户的密码而不用去查看邮箱中的找回链接是啥，重置别人的密码后就可以用别人的积分在积分商城里面来换取礼品。

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：



没被注册



# 第五种：越权修改密码

案例和越权结合的

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；



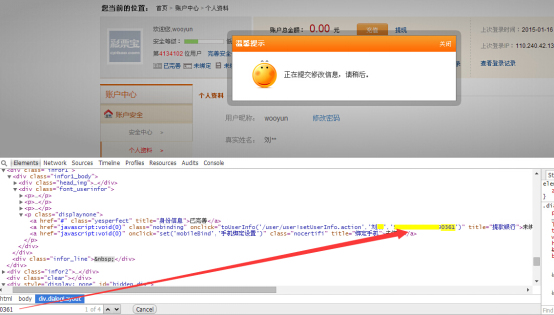
9、登录成功；

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！】

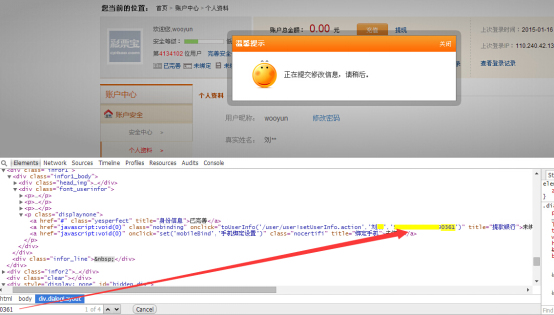
修改了、登录了也没有危害啊？是吗？他叫啥，哪里人，我都知道了！



漏洞证明：

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





# 第六种：前端跳过步骤

其实就是url等中含有步骤的标记，可以进行修改跳过某些验证

**2.5.1 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

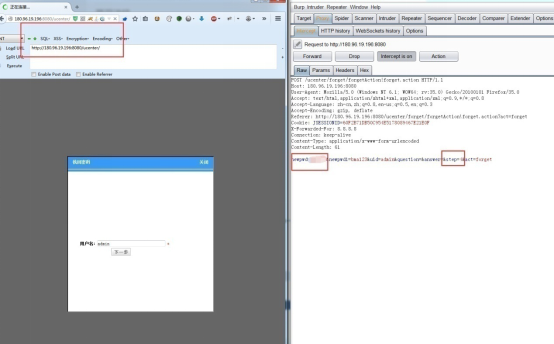
监控大量IP段

详细说明：

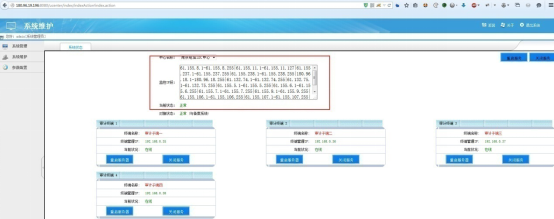
企业侧互联网综合管理平台

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

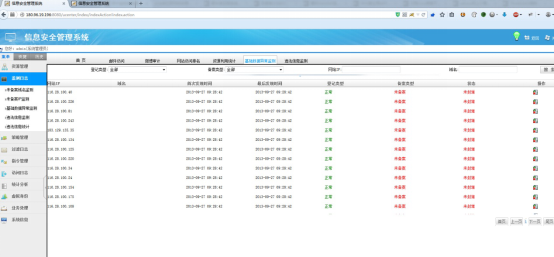
61.155.107.1-61.155.107.255

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



# 第七种：前端验证

一般指弹框那种验证/ajax的验证

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。

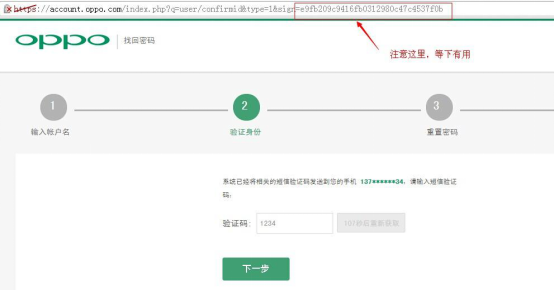
详细说明：

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

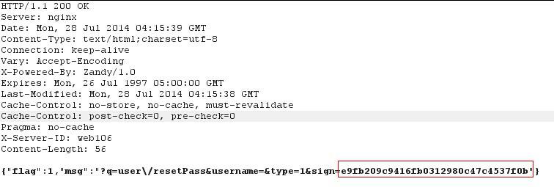
X-Server-ID: web106

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"}



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





# 第八种：注册覆盖重置密码

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

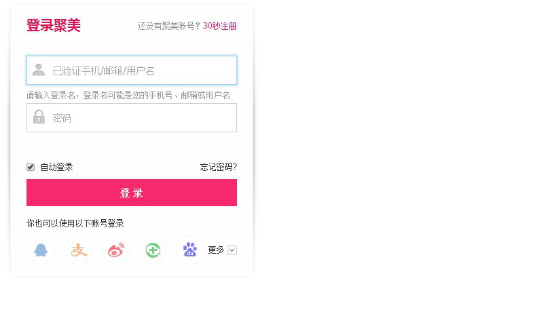
# 第九种：Session覆盖（牛皮的思路）

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



**2.1 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。