那些年互联网金融的伤痛

魔方安全团队负责人
张佳发
网名：121

限制分发 © 2015 绿盟科技

1 那些年，我们挖掘过的漏洞背影

2 互联网金融P2P网贷攻击场景预演一

3 互联网金融P2P网贷攻击场景预演二

4 互联网金融P2P网贷攻击场景预演三

5 总结

那些年，我们挖掘过的漏洞背影

我们**魔方团队（原NSTRT）**曾负责过多家华南区互联网金融行业的业务渗透项目，曾发现过大量的互联网金融行业的高危业务漏洞。

越权类、手机短信验证码类、登录类、密码重置类

越权类

任意越权操作他人购买指定股票

某国际银行证券交易系统的**股票买卖功能**存在**任意越权操作他人购买指定股票漏洞**，攻击者以**自己的帐号**登录，在**买股卖股**时，把**userid**参数值**改为其他**用户的**userid**，即可**盗用**用户的**身份去买股或卖股**。

如果说光大证券的那次**A股事件**是**乌龙**，那么**这个漏洞**，则是完全可以用**黑客**的方式去**影响股市**。

任意越权删除他人银行卡

某网贷系统在**添加银行卡的功能**中，**银行卡**的**datavlue值参数**是根据添加的次序**依次增加**而生成，在**删除银行卡**时，**没有校验datavlue值**银行卡所属**用户是否是发起删除请求的用户**，通过遍历**datavlue值**实现恶意脚本批量删除平台上的会员添加的银行卡号，直接影响会员的使用，影响平台运行。

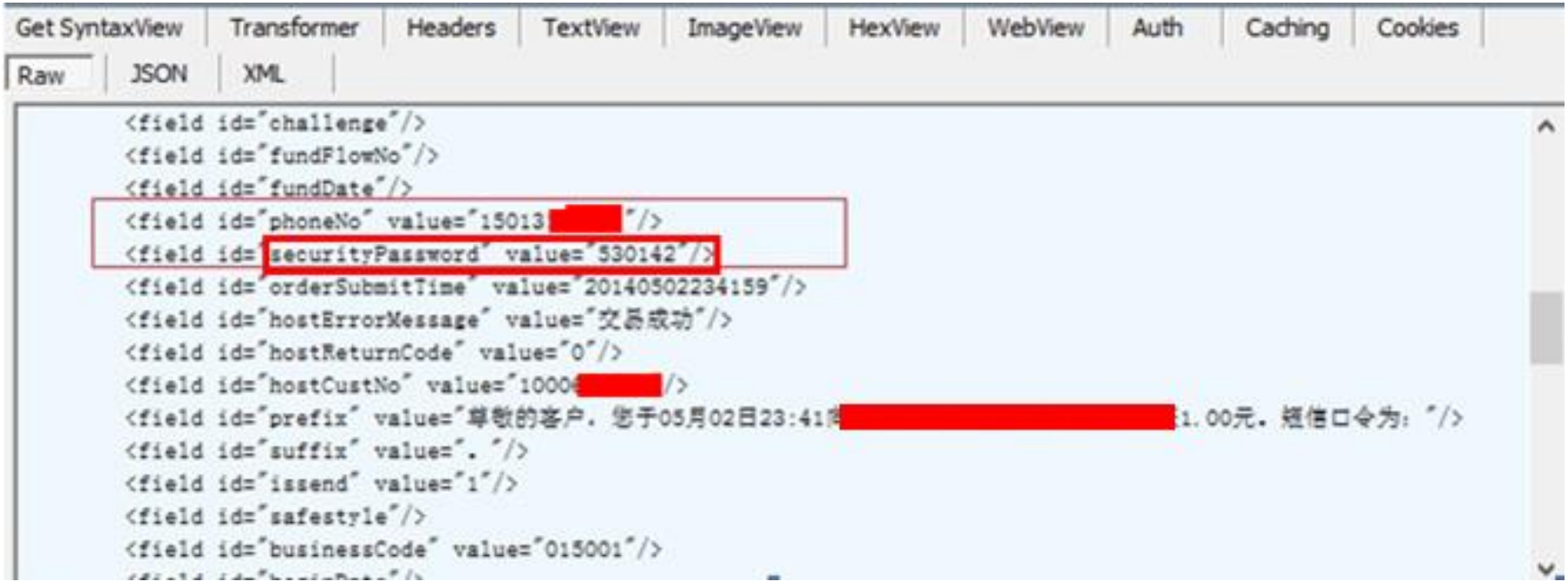
任意查看他人资金流水漏洞

某网贷系统在**资金流水查看**功能中，以**username参数值作为查询条件**，攻击者只需要**遍历username参数**，即可**任意查看他人的资金流水**。

手机验证码类

手机验证码明文泄露

某P2P网贷系统交易功能的**手机验证码明文泄露**，以**明文**的方式**返回客户端**。



获取明文动态口令漏洞

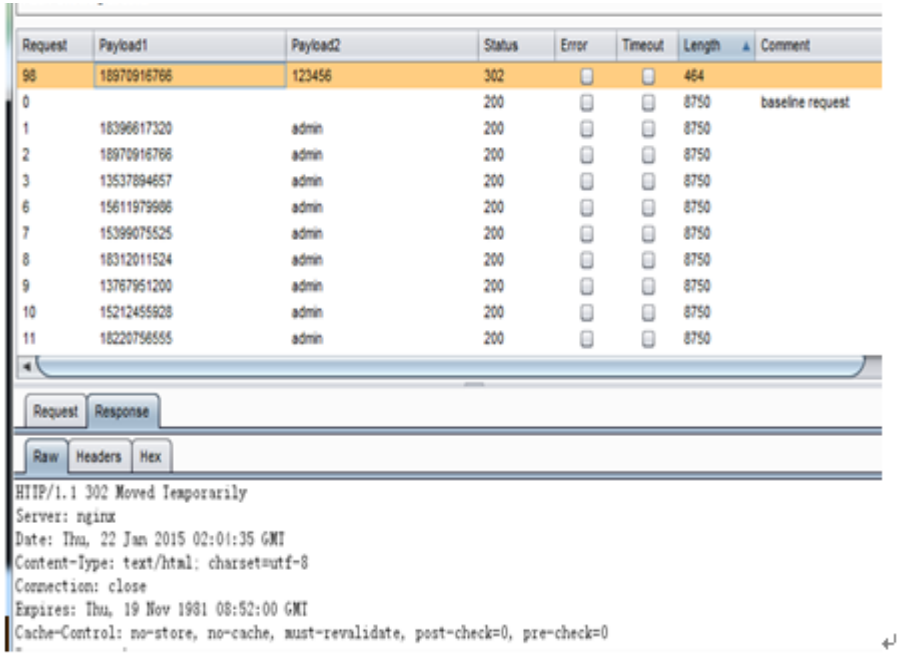
手机验证码一码多用

某P2P网贷系统的**手机验证码**可**一码多次使用**，**如同个验证码**在忘记密码功能使用后，又可在重置手机号功能上重复使用。

登录类

登录框撞库漏洞

由于某p2p网贷的**登录功能没有验证码，或验证码存在缺陷可被重复使用，又或验证码图形过于简单可被ocr识别**，故存在登录框撞库漏洞，可被攻击者通过密码库字典暴力破解获得可登录的帐号密码。



Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
98	18970916766	123456	302			464	
0			200			8750	baseline request
1	18396617320	admin	200			8750	
2	18970916766	admin	200			8750	
3	13537894657	admin	200			8750	
6	15611979986	admin	200			8750	
7	15399075525	admin	200			8750	
8	18312011524	admin	200			8750	
9	13767951200	admin	200			8750	
10	15212455928	admin	200			8750	
11	18220756555	admin	200			8750	

Request | Response

Raw | Headers | Hex

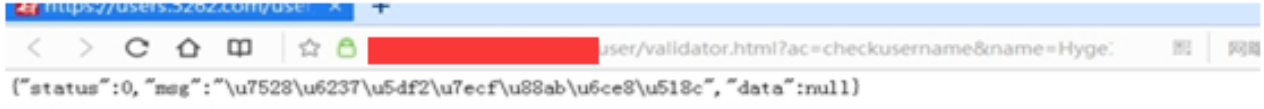
```
HTTP/1.1 302 Moved Temporarily
Server: nginx
Date: Thu, 22 Jan 2015 02:01:35 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
```

爆破成功，登录用户帐号。

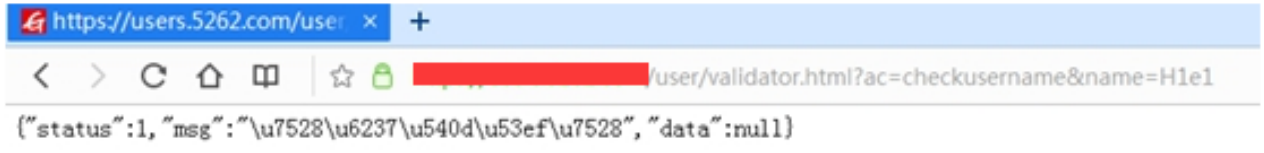
登录用户名遍历漏洞

某p2p网贷在注册用户模块的判断用户名是否已注册功能中，如用户**已注册（存在数据库中）则返回0**，如用户**未注册（不存在数据库中）则返回1**，攻击者根据这原理可**成功遍历**p2p网贷**所有可登录的用户名**。

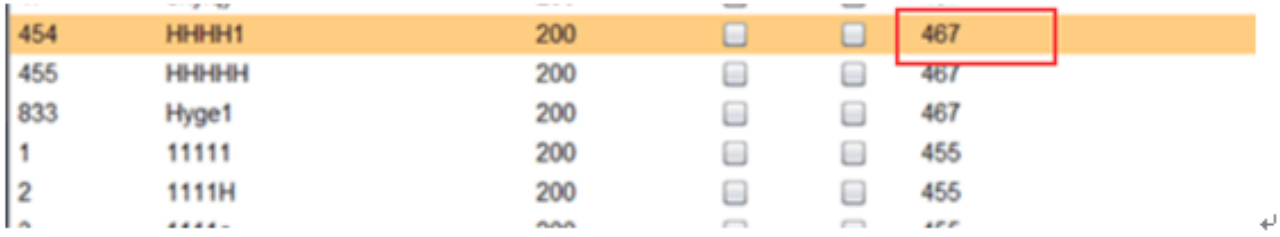
用户名存在返回的信息：



用户名不存在返回的信息：



载入字典进行暴力破解，
如图为成功爆破出用户名的数据包长度，用户名为 HHHH1



454	HHHH1	200			467
455	HHHHH	200			467
833	Hyge1	200			467
1	11111	200			455
2	1111H	200			455

绕过密码随机登录他人帐号漏洞

某证券网上交易系统的用户财产安全存在特大的高危漏洞，可以**绕过**他人**帐号密码**随机登录他人的证券交易帐号（**不需要知道他人的证券帐号或者密码**），即**拥有**他人证券**交易帐号**的**全部权限**。（漏洞的原因：在退出登录时session并未注销，而是随机分配给其他登录成功的用户）

服器即可成功随机授权一个帐号，比如成功登录资金帐号为 XXXX 用户的证券，并且拥有 XXXXX 用户的全部操作权限。如图：

密码重置类

异步漏洞重置任意用户密码

某P2P网贷系统的忘记密码功能存在**异步漏洞重置任意用户密码**，攻击者只需要**知道**任意用户的**帐号名及手机号**，输入**任意短信验证码**后，把返回包改为true，则可跳过验证，直接**重置**用户帐号**密码**。

进入到设置新密码的页面。

互联网金融P2P网贷攻击场景预演一

第一步：利用已注册用户名遍历漏洞，可成功遍历互联网金融p2p网贷所有有效用户名

在互联网金融p2p网贷注册用户功能中，会判断用户名是否已注册，如用户已注册（存在数据库中）则返回０，如用户未注册（不存在数据库中）则返回１，攻击者根据这原理可成功遍历p2p网贷所有可登录的用户名。

第二步：利用已验证手机号可遍历漏洞，可成功遍历某互联网金融所有已注册的有效手机号

在注册用户的手机验证功能中，会判断手机号是否已验证，如手机号已验证（存在数据库中）则返回０，如手机号未验证（不存在数据库中）则返回１，攻击者根据这原理可成功遍历p2p网贷所有已验证的手机号。

第三步：利用忘记密码功能把遍历出的用户名及手机号进行匹配对应

在忘记密码功能中，存在用户名及手机号的匹配校验，通过这个匹配校验，可把上述两步遍历出来的用户名及手机号进行匹配对应起来，如A的用户可对应到A的手机号

第四步：利用基于异步可修改任意用户的登录密码漏洞，改掉手机号对应起来的用户密码进行登录

同样在忘记密码的手机号修改密码功能中，存在异步漏洞，输入任意验证码后只需修改返回包（改为１）即可绕过手机短信验证码的验证，直接跳到下一步重置密码，利用此漏洞可无需接收他人用户手机号的短信验证码，即可成功改掉他人用户的密码,后进行登录。

第五步：成功登录他人的P2P网贷帐户

第六步：利用基于异步可修改任意用户的交易密码漏洞，改掉他人登录用户的交易密码

在重置交易密码功能中，存在异步漏洞，输入任意验证码后只需修改返回包（改为１）即可绕过手机短信验证码的验证，直接跳到下一步重置交易密码，利用此漏洞可无需接收他人用户手机号的短信验证码，即可成功改掉他人用户的交易密码。

第七步：利用已重置的交易密码，成功删除把登录的他人用户的银行卡删掉。

成功删除：

第八步：添加上攻击者自己的银行卡。

第九步：利用基于异步漏洞手机认证绕过验证漏洞，成功改掉登录用户的绑定手机，改成攻击者自已的手机号

在手机认证功能中，存在异步漏洞，输入任意验证码后只需修改返回包（改为１）即可绕过旧手机短信验证码的验证，直接跳到下一步设置新手机，利用此漏洞可无需接收他人用户手机号的短信验证码，即可成功改掉他人用户的手机号，改成攻击者自已的手机号。

第十步：重新绑定攻击者的手机号后，利用绑定的手机打电话到客服要求修改实名制，修改成攻击者自已的实名

第十一步：欺骗客服修改实名制后，对应了攻击者自己的实名，后攻击者成功把登录用户的余额取现到攻击者添加的银行卡上。

第十二步：成功取现，发财致富不是梦！

提现日期	平台账号	申请人	银行账号	开户名	提现金额（元）	备注
2015-07-01 09:48	[redacted]	李[redacted]	中国工商银行 中国工商银行三门峡分行灵宝市支行[redacted]	李[redacted]	11111.00	资金明细 拒绝

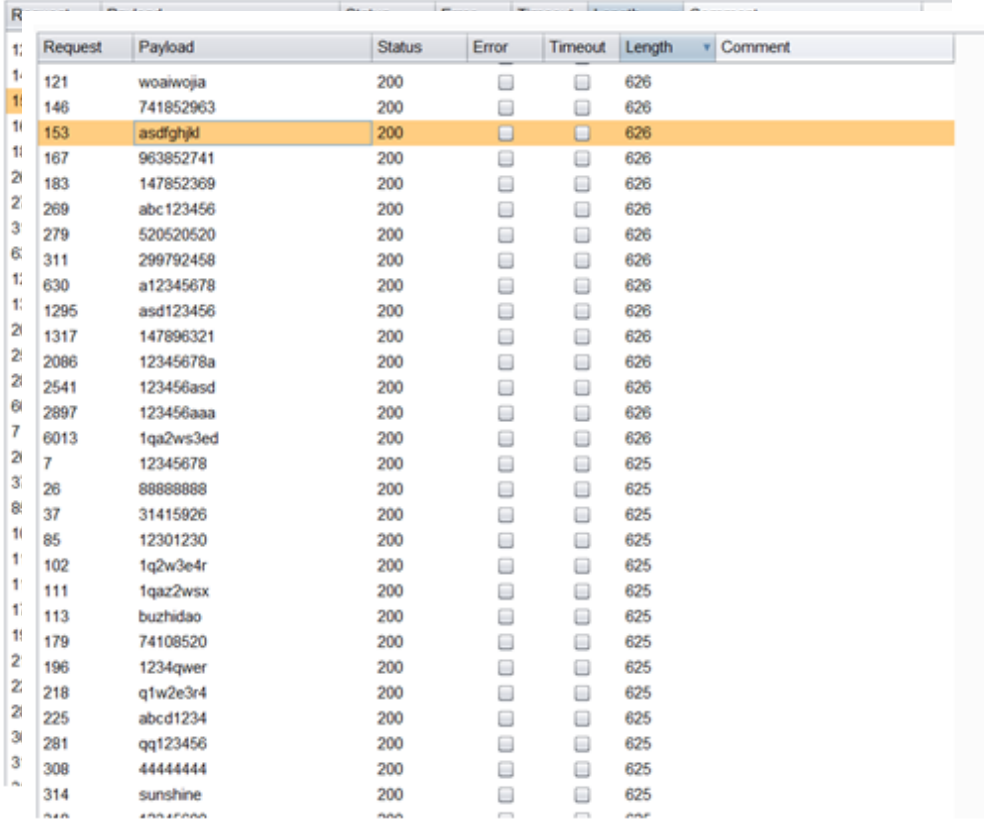
互联网金融P2P网贷攻击场景预演二

第一步：利用已注册用户名遍历漏洞，可成功遍历互联网金融p2p网贷所有有效用户名

在互联网金融p2p网贷注册用户功能中，会判断用户名是否已注册，如用户已注册（存在数据库中）则返回０，如用户未注册（不存在数据库中）则返回１，攻击者根据这原理可成功遍历p2p网贷所有可登录的用户名。

第二步：利用遍历出来的用户名进行登录撞库，成功撞得用户的密码并成功登录

由于P2P网贷登录功能没有验证码，或验证码存在缺陷可被重复使用，又或验证码图形过于简单可被ocr识别，故在登录功能上存在暴力破解漏洞，攻击者利用遍历出来的用户名，只需要一个合适的密码库字典，即可成功撞库。

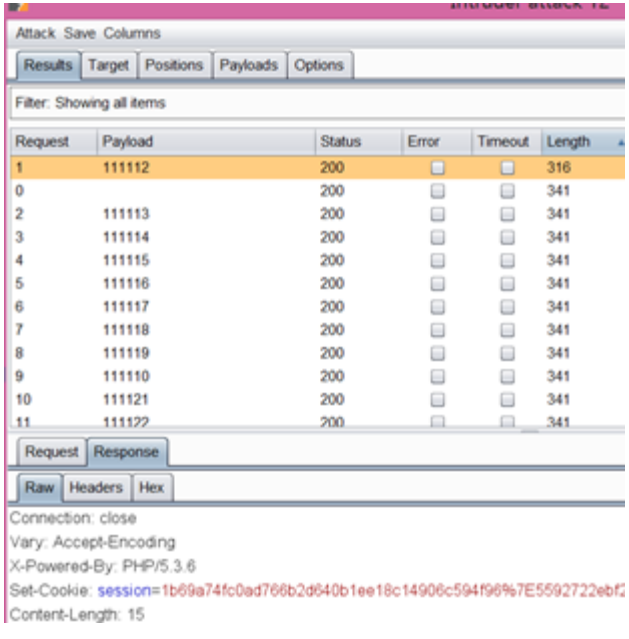


Request	Payload	Status	Error	Timeout	Length	Comment
121	woaiwojia	200			626	
146	741852963	200			626	
153	asdfghjkl	200			626	
167	963852741	200			626	
183	147852369	200			626	
269	abc123456	200			626	
279	520520520	200			626	
311	299792458	200			626	
630	a12345678	200			626	
1295	asd123456	200			626	
1317	147896321	200			626	
2086	12345678a	200			626	
2541	123456asd	200			626	
2897	123456aaa	200			626	
6013	1qa2ws3ed	200			626	
7	12345678	200			625	
26	88888888	200			625	
37	31415926	200			625	
85	12301230	200			625	
102	1q2w3e4r	200			625	
111	1qaz2wsx	200			625	
113	buzhidao	200			625	
179	74108520	200			625	
196	1234qwer	200			625	
218	q1w2e3r4	200			625	
225	abcd1234	200			625	
281	qq123456	200			625	
308	44444444	200			625	
314	sunshine	200			625	

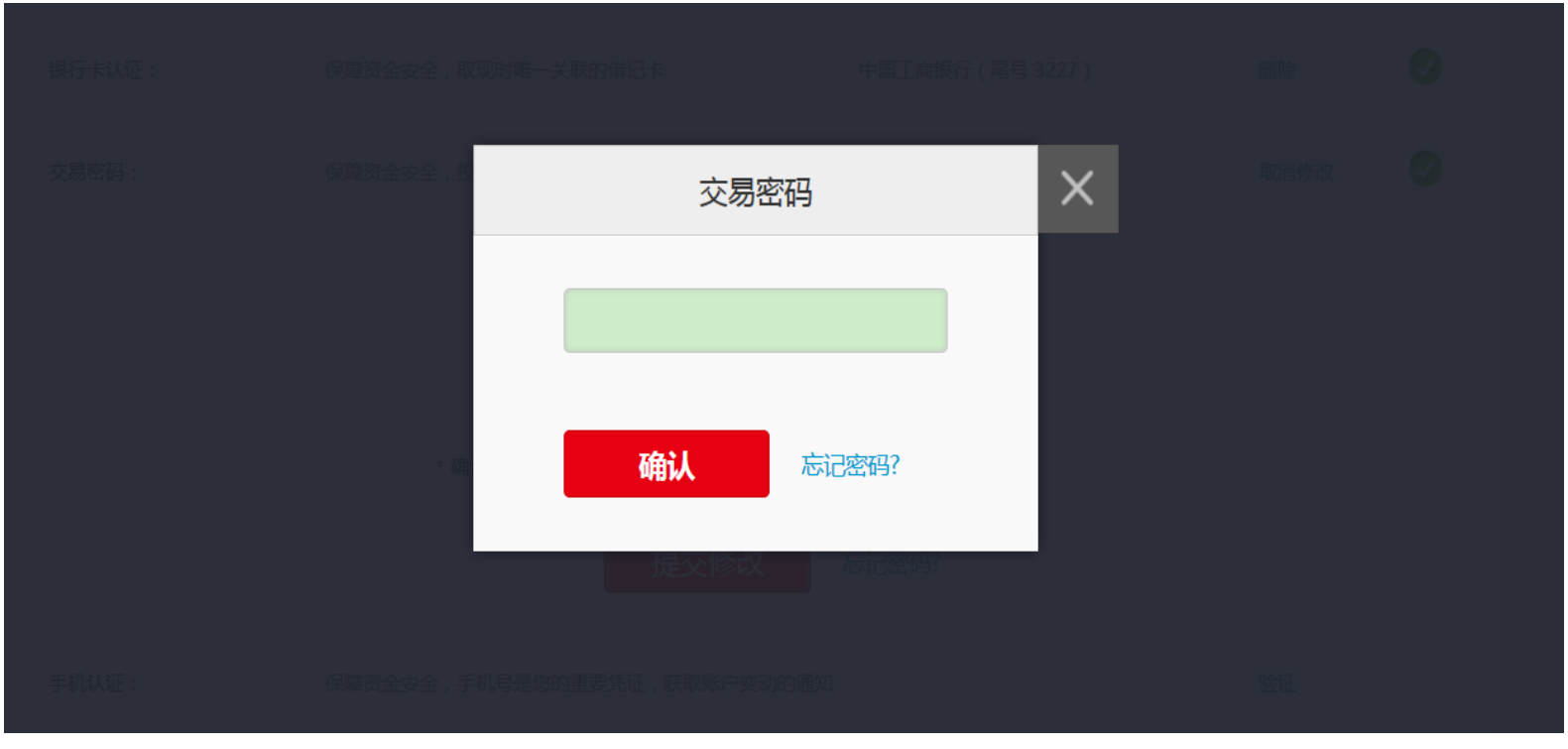
第三步：成功登录他人的P2P网贷帐户

第四步：利用交易密码修改暴力破解漏洞，成功破解出登录用户的交易密码

由于P2P网贷交易密码修改功能，只校验原密码是否正确，未设置有效的防暴力破解机制，故在交易密码修改功能上存在暴力破解漏洞，攻击者只需要一个合适的密码库字典，即可成功撞库，把交易密码改掉。



第五步：利用破解出的交易密码，把登录用户的银行卡删掉，改为攻击者自己的银行卡



第六步：利用手机验证码暴力破解漏洞成功改掉登录用户的绑定手机，改成攻击者自己的手机号

由于P2P网贷新手机绑定功能发送的手机短信验证码只有 6 位，且在30分钟内有效，故存在短信验证码暴力破解漏洞，通过短信验证码暴力破解漏洞即可在不需要收到旧手机短信的情况下，成功暴存破解出短信验证码，重新绑定新手机。

Request	Payload	Status	Error	Timeout	Length	Comment
7997	8007	200	☐	☐	565	
0		200	☐	☐	481	baseline request
1	1111	200	☐	☐	481	
2	1112	200	☐	☐	481	
3	1113	200	☐	☐	481	
4	1114	200	☐	☐	481	

第七步：重新绑定攻击者的手机号后，利用绑定的手机打电话到客服要求修改实名制，修改成攻击者自已的实名

第八步：欺骗客服修改实名制后，对应了攻击者自己的实名，后攻击者成功把登录用户的余额取现到攻击者添加的银行卡上。

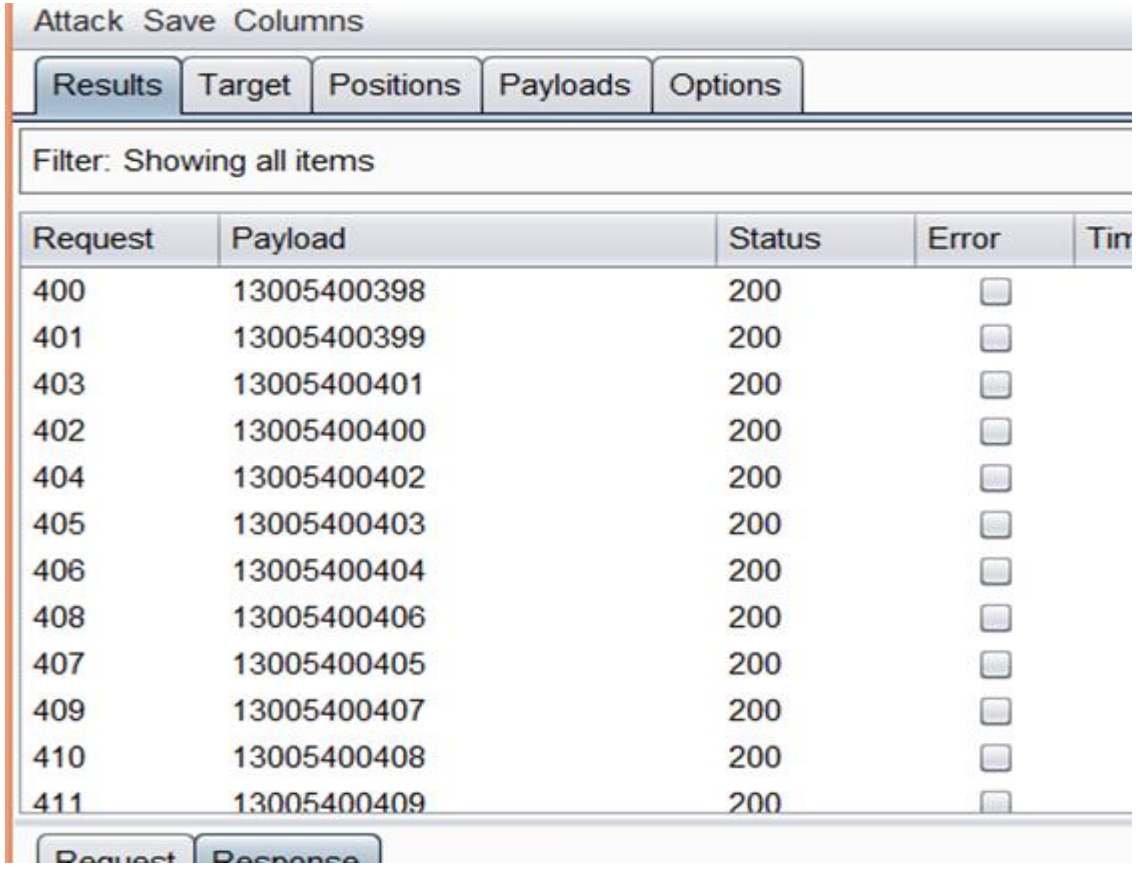
第九步：成功取现，发财致富不是梦！

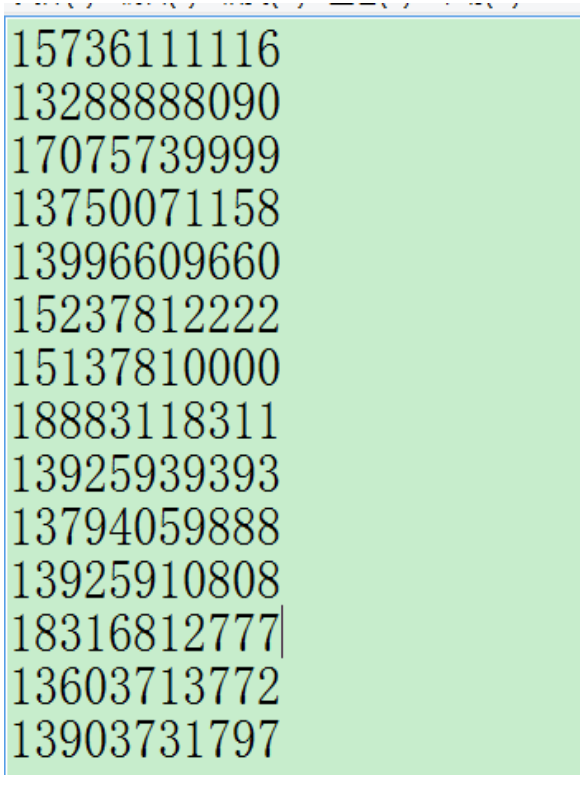
提现日期	平台账号	申请人	银行账号	开户名	提现金额（元）	备注
2015-07-01 09:48	[redacted]	李[redacted]	中国工商银行 中国工商银行三门峡分行灵宝市支行[redacted]	李[redacted]	11111.00	资金明细 拒绝

互联网金融P2P网贷攻击场景预演三

第一步：利用已验证手机号可遍历漏洞，可成功遍历某互联网金融所有已注册的有效手机号

在注册用户的手机验证功能中，会判断手机号是否已验证，如手机号已验证（存在数据库中）则返回０，如手机号未验证（不存在数据库中）则返回１，攻击者根据这原理可成功遍历p2p网贷所有已验证的手机号。





第二步：利用遍历出的手机号，卖给同行竞争对手，争抢客户资源

攻击者把遍历出的手机号卖给同业竞争者，同业的客服打电话给其中一个手机号，下面是聊天记录：

A：客户　　B：同行竞争对手的业务人员

B:你好，我是 xx 金融公司的，我们公司现在在搞新用户注册赠送 888 块红包的活动，能打扰你一些时间吗？

A：好吧，具体是什么的？

B：我们公司有几十年的历史和众多的资深人员，对于你投资理财更给你免费配私人助理，现在我们公司搞活动，新用户注册送 888 块，立刻注册立刻使用。

A：但是我在 AA 金融那已经注册会员。

B：不是我说别人坏话呀，AA 金融那边确实不如我们公司，首先我们公司历史悠久，且有众多的资深人员，更有众多成功案例，其次我们公司会定期搞送各种红包活动，很多客户在我们这里花少钱投资就能得到高收益，我们公司最大的亮点就是我们对每个客户免费配私人助理，你可以随时随地打电话咨询投资的所有问题。

A：这么好，我考虑一下吧。

B：嗯，那好，考虑好打电话给我好了。

总结

我们应该如何做？

我们无法做到预知黑客会在什么时候发动攻击，但我们能做到预知我们系统的漏洞在哪里，“攻击才是最好的动态防护”，当我们经常对我们系统不断的渗透检测时，我们系统隐藏的漏洞才会被不断的发现，我们的系统才能从根本上进行防护。

谢谢！