

登录注册攻与防

安全建设 Murviet

 2019-04-16  3,283

1 关于登录注册

登录注册，是绝大多数互联网应用中的一项必备功能，作为开发者的我们，基本都对该功能非常熟悉。通常新手在进行编程练习时，会做大量与此相关的开发工作。我们往往对基础功能了如指掌，却忽略了登录注册功能可能遭受的其他风险。作者在多年的安全测试及研发工作中发现，不同场景下，大多数应用的登录注册功能，或多或少存在一些问题，该功能作为系统的主要入口，将严重影响到整个系统的安全性。

如果我们的系统，在面对的非常庞大的用户群体，并且伴随着某一方的利益时，登录注册功能应该设计的更加严谨。目前，大多数的“薅羊毛”团队，都是通过机器注册大量用户，以操纵这些虚假用户进行获利。

在此背景下，我们的登录系统必须设计的毫无漏洞，必要时刻更需要接入风险控制策略。同时，要更准确区分真实用户和虚假用户，防止系统遭受不必要的资金损失。

2 登录注册功能常见的漏洞

登录注册功能看似简单，其内部一般会引用一些相关功能：如图形验证码、短信或邮箱验证码等，这些功能一旦存在漏洞，对整体而言，将带来极大的安全风险。

登录注册功能常见的漏洞
账户密码明文传输
验证码失效
验证码重复使用
任意用户注册
登录账户泄露
短信验证码可被破解

上图这些漏洞中容易引发的攻击方式：

登录注册相关功能容易遭受到的攻击
撞库
中间人劫持账户密码
密码定向破解
破解任意账户短信验证
短信接口被恶意利用
批量注册账户
弱口令
验证码爆破和绕过

3 攻击案例





上图为某网站个人用户界面，url地址为：http://***.com/120456585

测试中发现，host后面的一串数字为系统中的用户ID，通过遍历ID可获得用户登录名。编写脚本批量获取系统中所有用户的登录名。

```
3
4   for ($i=12046581; $i < 12146581; $i++) {
5       # code...
6       $url = 'http://[REDACTED].$i';
7
8       $html = file_get_contents($url);
9       preg_match('/OwnerNickName = \'(.*)\'/i',$html,$match);
10      if($match[1]){
11          if (preg_match("/[\x7f-\xff]/", $match[1])) {
12              //echo "含有中文: ";
13          }else{
14              echo $match[1]."\n";
15              //echo "没有中文: ";
16          }
17      }
18  }
19
20
21  }
22  }
23
24
25
```

```
lixuan1437
lisa0615
ZLDS501
skylot
xiaohuli12345
d245713328
xuwei17774424
Q0513993928
Lovae7
l15317061093
uvwz15164567612
a532601334
ww13603874150
cswagfy
q123456789gagas
zzxxcc159753
Angelsir
hmtybs
lgs789456
aaaaa0123
QQ_12046609
du7757
ying894287
ewqyuy
```

进入登录页面发现网站无验证码，并且无任何安全策略防护。

4 风险安全问题

假如以上常见漏洞安全工作，做的已经很好了，就一定安全了吗？对于用户量少，或者仅限内部员工使用的平台来说做到这一步基本就可以了。

但如果我们的系统拥有庞大的用户量，并涉及利益相关，比如邀请好友送奖励的活动，这些安全措施却远远不足以保障庞大的用户体系以及公司利益。

当我们的业务拥有较大的用户量时，我们不单单保障系统的安全，也需要肩负保障系统中用户个人信息安全的责任，要确保客户的账户不被盗用，不出现事故。

而风险相关问题，主要体现在：攻击者会想尽一切办法来使用其他用户的信息登录到我们的系统中。这其中主要包括利益的驱使等动因。

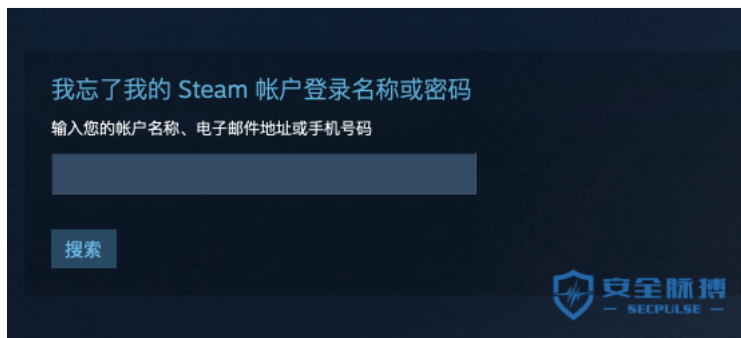
5 攻击案例

一、

游戏行业，面临最多的安全问题有用户账户被盗，这会直接或间接导致虚拟物品的丢失。这类问题会导致用户体验下降，严重的将导致用户财产损失等。盗号已然成为一个非常成熟的黑色产业。我们要做的，就是尽可能的提高用户的体验，同时保障用户的账户信息安全。

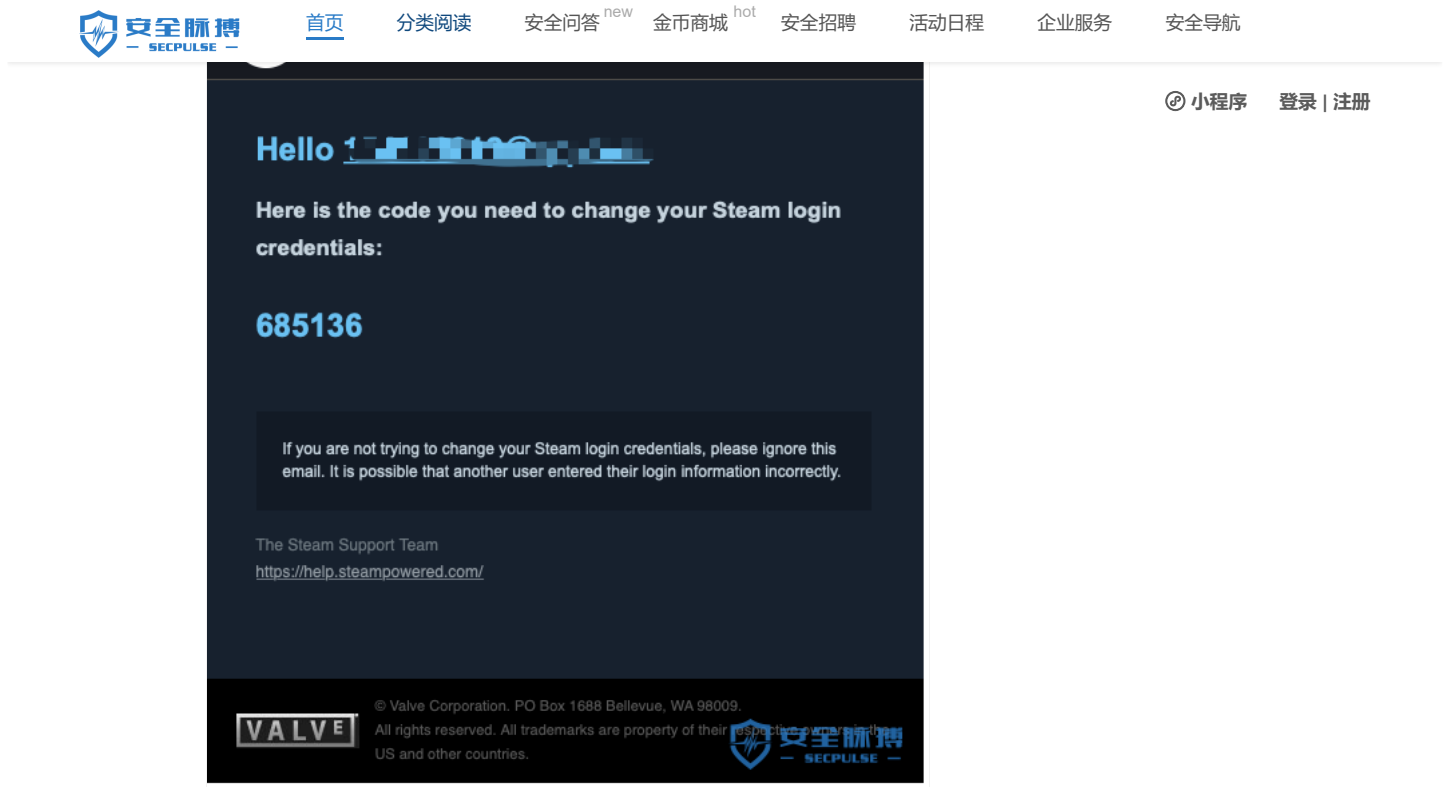
STEAM是众所周知的大型游戏平台，截止到2017年，Steam账户数量达到惊人的3亿个左右。如此庞大的用户量，难免成为众多黑产从业者眼里的香饽饽，各种各样的攻击层出不穷。常见的包括：钓鱼获取用户的账户密码、撞库等。以下案例，说一下一种针对STEAM用户的另类攻击手法。

在STEAM中有一个账户密码找回的功能，通过该功能，输入注册时使用的邮箱，



通过平台发送验证码执行找回密码的操作。





发送后用户的邮箱会收到一个六位数字的验证码。

这看似毫无问题的功能，在庞大的用户体系下，可能产生严重后果。

黑产工作者们会通过其他方式，收集大量的Steam用户邮箱，上百万或者上亿的邮箱，通过自动化脚本批量进行找回密码操作，因为攻击者没有登录邮箱的权限，无法提供收到的验证码。所以攻击者们将所有用户的验证码，统一设置为一个自定义的6位数字，来尝试验证码是否正确。

这种攻击方式虽然属于瞎猫碰死耗子的方式，但在如此规模的用户量下，此攻击方式效果出奇的好。目前，Steam平台已经将验证码修改为随机的六位字母和数字。极大的降低了被破解的几率。

6 设计安全的用户架构

当我们在设计一个登录注册功能时，有时过多的强调了安全性，从而忽略了用户体验。所以，我们不得不花更多的时间，在安全性与用户体验的改进上不断契合。

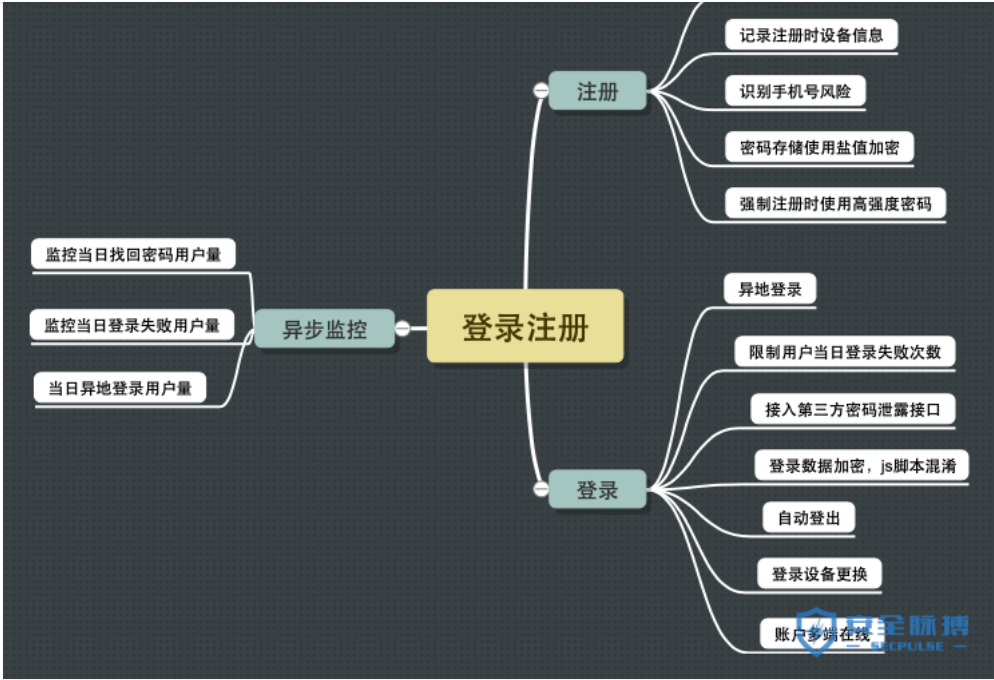
评定一个登录系统是否安全，核心在于这个系统是否能够高度识别，该账户在登录时，需要判断是正常登录抑或是被盗号。防止账户被盗的方式一般有以下几种方式：

- 密码是否正确
- 短信验证码是否正确
- 短信验证码和密码同时正确
- 回答密保问题正确等

当然，如果我们把这些验证，统一放在用户登陆界面，让用户第一时间填写信息的话，的确会给用户带来困扰，严重影响用户体验。

所以当我们设计登录时，依旧应该只让用户输入账户和密码，如果触发某个风险控制时，再让用户输入图形验证码、短信验证码等信息。

下图是一个登录注册系统部分风险控制的流程图：



小程序 登录 | 注册

根据思维导图依次往下看：

注册

注册功能里，我们的主要任务是判断用户所提交的这些信息是否真实可靠。比如：判断用户手机号是否真实，应该给用户填写的手机号发送一个验证码，通过验证码来判断手机号是否匹配。

记录注册时的设备信息和IP，是为了以后的风险等级做判定，判断设备是否是该用户常用设备信息。

通过接入第三方手机号风险控制，来识别该手机号是否属于正常手机号码，防止薅羊毛团队使用接码平台来恶意注册。

密码存储，一般我们使用简单的MD5进行加密，其实这种方式现如今已经非常不安全了，MD5虽然属于不可逆加密算法，但通过密文碰撞，实际明文密码是可以获取的。所以我们在加密用户密码，应进行加盐操作等加密方式，防止被碰撞破解。

在用户注册时，我们应强制用户使用高强度的密码，禁止用户使用纯数字或者简单的滚键盘方式输入密码，或者我们可以参考弱口令排行来限制用户使用弱口令。安全的密码规则包括：密码长度不得低于八位、密码必须包含大小写字母和数字等。

登录

异地登录，当用户在账户和密码正确后，但登录IP地址与常用IP地址不在统一区域内时，我们应触发风险控制，让用户输入短信验证码来进行验证。不单单输入账户和密码进行登录。

限制用户当日密码登录次数，主要防止攻击者定向破解该用户的密码。比如当该用户密码错误超过5次时，应该让该账户24小时内禁止登录。或引导用户找回密码。在找回密码的同时我们也应判断找回密码的IP地址是否属于常用登录地。

接入第三方密码泄露接口，该接口主要收集互联网上公开的账户泄露数据。通过接入该接口可提醒用户密码已泄露，强制用户进行修改密码等操作。

登录加密，无论浏览器端还是APP端在登录时我们的数据包应将用户账户密码进行加密，防止第三方截获，保障用户的信息安全。

设置自动登出，在一定时间内用户无操作，对账户进行强制退出，防止用户在离开时被他人恶意利用。

登录设备更换，当用户登录时检测到不是常用设备时，应及时作出相应的风险控制。

账户多端在线，用户的账户同时在两台设备登录时，我们应即时通知用户，或者强制下线，提醒用户重新进行登录，登录时必须输入短信验证码，或执行其他风控措施。

异步监控

当在设计登录功能时我们应设计一个系统安全级别：比如正常登录时只需要输入账户密码即可登录。触发一级风险控制时：需用户输入图形验证码进行登录。二级风险控制时需要用户使用短信进行验证。三级时需要用户在登

结尾


安全的系统，在根据自己的业务逻辑以及实际遭受到的攻击事件，来不断的演变出合理而又安全的架构，在安全的同时也要尽肯能考虑到用户的体验。

任何系统没有绝对的安全。有些安全设计并不是为了直接了断的阻断安全风险，而是为了提高攻击者攻击的成本。在缺乏利益趋势的情况下，攻击就会随之减少。

本文所讲的概念并非适用于所有业务或系统，只是为了扩展一下相关人员的思路。不足之处还请指正。

Tags: [Burp](#)、[hosts](#)、[Sql注入](#)、[代码](#)、[信息安全](#)、[密码](#)、[异步监控](#)、[弱口令](#)、[撞库](#)、[攻防](#)、[明文传输](#)、[漏洞](#)、[登录注册](#)、[破解](#)、[网络安全](#)、[脚本](#)、[邮箱](#)、[风险](#)、[验证码](#)、[黑色产业](#)

 点赞：3

 评论：0

 收藏：1

 积分 18


 金币 15



相关文章



国家认证！安识正式获得高新技术企业...



【漏洞预警】Spring Cloud C...



Spring Cloud Config目...

评论 (0)

昵称

必填 您当前尚未登录。 [登录?](#) [注册](#)

邮箱

必填 (保密)



Murviet

文章数：1 积分：18

安全问答社区



[首页](#)

[分类阅读](#)

[安全问答](#)^{new}

[金币商城](#)^{hot}

[安全招聘](#)

[活动日程](#)

[企业服务](#)

[安全导航](#)



脉搏官方公众号



安全脉搏

活动日程

[显示更多](#)

友情链接

网络尖刀 | E安全 | Sec-Wiki | 独自等待 | 中国红客联盟 | 娜迦信息 | SecSilo | armyzer0 | 易安在线 | i春秋 | 铁匠运维网 | 北京ITET培训中心 | 爱I
神刀安全网 | 吾爱漏洞 | 网易安全中心 | 安天365 | ChaMd5安全团队 | 破晓团队 | 黑白网 | ms08067

关注我们 SecPluse
官方微信 关于我们
安全问答 加入我们

合作伙伴



关于我们

安全脉搏 (secpulse.com) 是以互联网安全为核心的学习、交流、分享平台, 集媒体、培训、招聘、社群为一体, 全方位服务互联网安全相关的管理,



