# 聊聊弱口令的危害(一)——安全小课堂第十八期

2016-07-15 京东安全应急响应中心

## 安全小课堂第十八期

打个比方,你有一个保险柜,里面有几千万人民币现金,而口令则是进入保险柜的钥匙,当别人也有一把这样的钥匙。因为弱口令很容易被他人猜到或破解,所以如果你使用弱口令,就相当于把家门的锁是很老旧,拿个铁丝就可以打开,这是相当危险的。本期我们来聊一聊弱口令的危害。

### 本期邀请到 唯品会安全专家cookie 新浪安全专家吗啡 大家欢迎~





豌豆妹

什么是弱口令?



弱口令通俗来讲就是口令太简单,容易被别人猜到或被破解工具破解的口令,如仅包含简单数字或字母的口令,"123456"、"abcde"等,这种口令很容易被别人破解,存在相当大的安全隐患,会给黑客留下可乘之机,因此不推荐用户使用。









#### 豌豆妹

常见弱口令有哪些?



弱口令也是分场景的,对于IT管理员来说,他们喜欢用admin,88888,admin123, test, root, root123这样的弱口令。对于互联网用户来说,用户喜欢使用qwerty, gazwsx123,这种键盘的特殊位置字母构成的弱口令。 除此之外,生日、姓名这些组合 成的密码也是用户喜欢使用的弱口令。





- 1、连续或重复的数字,如123123、123456、987654、111111、222333等;
- 2、连续或重复的字母,如aaa、abc、abcdef、zyx等;
- 3、键盘上常见的连续按键,如:1gaz@wsx、gwert、asdfghjkl;、!@#、 147258369 (数字键盘)等;
- 4、日期或年份,如800128(生日)、2012、19251120等;
- 5、与用户相关的名称信息,如newdoone(公司名称)、shaoyuanming(姓名全 拼)、sym(姓名缩写)、oa(产品名称)、admin(用户名)、手机号等;
- 6、具有特殊含义的字符串,如520、1314、woaini;
- 7、其他常用的字符串:root、abc123!、administrator、test等。
- 以上元素被许多人用来构成好记的口令,而攻击者也会使用上述素材相互组合来生成弱 口令字典。如newdoone123(公司名称+连续数字)、abc!@#(连续字母+键盘按 键)、asdf520(键盘按键+特殊含义字符)、shaoyuanming2012(用户名+年份) 等,符合上述规律的都可以认为是弱口令。



#### 豌豆妹

弱口令的产生是为什么?





弱口令的产生主要是因为用户没有安全意识,用户认为不会有人猜到他们的弱口令。不过也实在是因为现在的互联网产品越来越多,当我们要去使用它们的时候,不得不注册一个新的账户,那么用户为了方便记忆,当然会优先使用好记忆的密码。这样就大大提高了弱口令出现的概率。





#### 豌豆妹

哪些地方出现弱口令的危害最大呢?





个人认为不管什么地方出现弱口令都会有相当大的安全风险,一旦被利用,都将产生重大危害···

葫芦娃



危害的话通常是结合场景的,对于企业来说,vpn用户的弱口令很严重。直接暴露在外网的SSH,RDP3389,mysql的业务弱口令很严重。 然后对于普通用户来说,网银、支付或者其他存在很多个人信息的互联网应用的弱口令也很严重。





#### 豌豆妹

弱口令的危害有哪些?



显而易见,密码是互联网世界的通行证。如果别人可以轻易拿到你的密码,就可以你的名义在互联网里穿梭。这时候,你的钱就是别人的钱,你的信誉就是别人的信誉,你的好友,你的服务器就是别人的服务器。





打个比方吧,你有一个保险柜,里面有几千万人民币现金,而口令则是进入保险柜的钥匙,当别人也有一把这样的钥匙。因为弱口令很容易被他人猜到或破解,所以如果你使用弱口令,就相当于把家门的锁是很老旧,拿个铁丝就可以打开,这是相当危险的。



### 豌豆妹

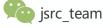
┗哈~说的太棒啦~本期话题未完待续哟~重磅信息在朝你招手~请拭目以待,下期见!

#### 安全小课堂往期回顾:

- 1、论安全响应中心的初衷;
- 2、安全应急响应中心之威胁情报探索;
- 3、论安全漏洞响应机制扩展;
- 4、企业级未授权访问漏洞防御实践;
- 5、浅谈企业SQL注入漏洞的危害与防御;
- 6、信息泄露之配置不当;
- 7、XSS之攻击与防御;
- 8、电商和O2O行业诈骗那些事儿(上);
- 9、电商和O2O行业诈骗那些事儿(下);
- 10、CSRF的攻击与防御;
- 11、账户体系安全管理探讨;
- 12、远程代码执行漏洞的探讨;
- 13、服务器安全管控的探讨;
- 14、畅谈端口安全配置;
- 15、谈一谈github泄露;
- 16、撞库攻击是场持久战;
- 17、url重定向攻击的探讨。

6-9







京东安全应急响应中心

动动手指~关注下呗~