文章
Frank Ma · 三月 2 阅读大约需 3 分钟

Open Exchange

密码有多安全？

如何检查密码是否足够强大，使其不会很快被破解？ 又如何制作一个强大的密码？

我开发了一个工具，可能对这个问题有帮助。你可以在OpenExchange上找到它。用zpm安装。

```
zpm "install passwords-tool"
```

这个模块将只安装一个类 caretdev.Passwords中，其中包含一些有用的方法。

安全密码

要获得一个安全的密码，通常只需使用大写和小写的字母、数字和特殊符号，而且至少要有8个符号的长度。

Generate方法使用的参数：

- Length - 只是一个生成密码的长度，默认值为12。
- IncludeUpperLetter - 包括大写的ASCII字母，如果需要的话是2，默认是1。
- IncludeLowerLetter - 包括小写ASCII字母，如果需要的话，默认为2。
- IncludeNumber - 包括数字，如果需要的话，2个，默认为1个。
- IncludeSymbol - 包括特殊符号，如果需要的话，2个，默认为1个。

```
USER>w ##class(caretdev.Passwords).Generate(12,1,0,0,0)
FMXRQEQPOVBC
USER>w ##class(caretdev.Passwords).Generate(12,1,1,0,0)
rgbPyWApcUjp
USER>w ##class(caretdev.Passwords).Generate(12,1,1,1,0)
cDuLf8FqEDx7
USER>w ##class(caretdev.Passwords).Generate(12,1,1,1,1)
0J/ lLbW|T$
USER>w ##class(caretdev.Passwords).Generate()
w3}{OQA|T{h^
```

这个方法使用$System.Encryption.GenCryptRand()，而不是普通的$random
，后者对于密码来说可能不是那么安全。除了获得最佳密码外，它还在一个循环中生成一些密码，检查密码熵的值，并返回一个最高分。

密码熵 Entropy

密码熵预测了一个给定的密码通过猜测、暴力破解、字典攻击或其他常见方法破解的难度。熵本质上是衡量攻击者需要进行多少次猜测才能猜出你的密码。有几种方法来计算它。

```
USER>write ##class(caretdev.Passwords).Entropy("Pas$W0rD")
52.56
```

熵值公式

L = 密码长度；密码中的符号数
S = 独特的可能符号库的大小（字符集）。

比如：

数字（0-9）: 10
小写拉丁字母(a-z): 26
小写和大写拉丁字母（a-z，A-Z）：52
ASCII可打印字符集（a-z、A-Z、符号、空格）：95

可能的组合数=S**L

密码熵值 = log2(可能的组合数)

香农熵 Shannon Entropy

```
USER>write ##class(caretdev.Passwords).ShannonScore("Pas$W0rD")
24
```

这种方式是基于使用字符的频率，以及密码的整个长度。详情见 Wiki.

NIST得分

```
USER>write ##class(caretdev.Passwords).NISTScore("Pas$W0rD")
24
```

计算

- 第一个字符的熵是4比特；
- 接下来的七个字符的熵是每个字符2比特；
- 第九个到第二十个字符的熵为每字符1.5比特；
- 第21个及以上的字符，每个字符有1比特的熵；
- 如果同时使用大写字母和非字母字符，将增加6位的 "奖励"；
- 对于长度为1到19个字符的密码，在进行广泛的字典检查后，会增加6位的 "奖励"，以确保密码不包含在一个大的字典中。20个字符以上的密码不会得到这个奖励，因为它被认为是由多个字典词组成的密码。

强度 Strength

```
write ##class(caretdev.Passwords).DetermineStrength("Pas$W0rD")
REASONABLE
```

生成的密码

```
USER>write ##class(caretdev.Passwords).DetermineStrength(##class(caretdev.Passwords).
Generate())
STRONG
```

- 非常弱 VERYWEAK - 熵值Entropy <= 32
- 弱WEAK - 熵值Entropy <= 48
- 正常 REASONABLE - 熵值Entropy <= 64
- 强 STRONG - 熵值Entropy <= 80
- 非常强 VERYSTRONG - 熵值Entropy > 80

如果你喜欢这篇文章，请投票 。

#安全 #InterSystems IRIS
在 InterSystems Open Exchange 上检查相关应用程序

源 URL: https://cn.community.intersystems.com/post/%E5%AF%86%E7%A0%81%E6%9C%89%E5%A4%9A%E5%AE%89%E5%85%A8%EF%BC%9F