

Правильные пароли

Руководство к пользованию



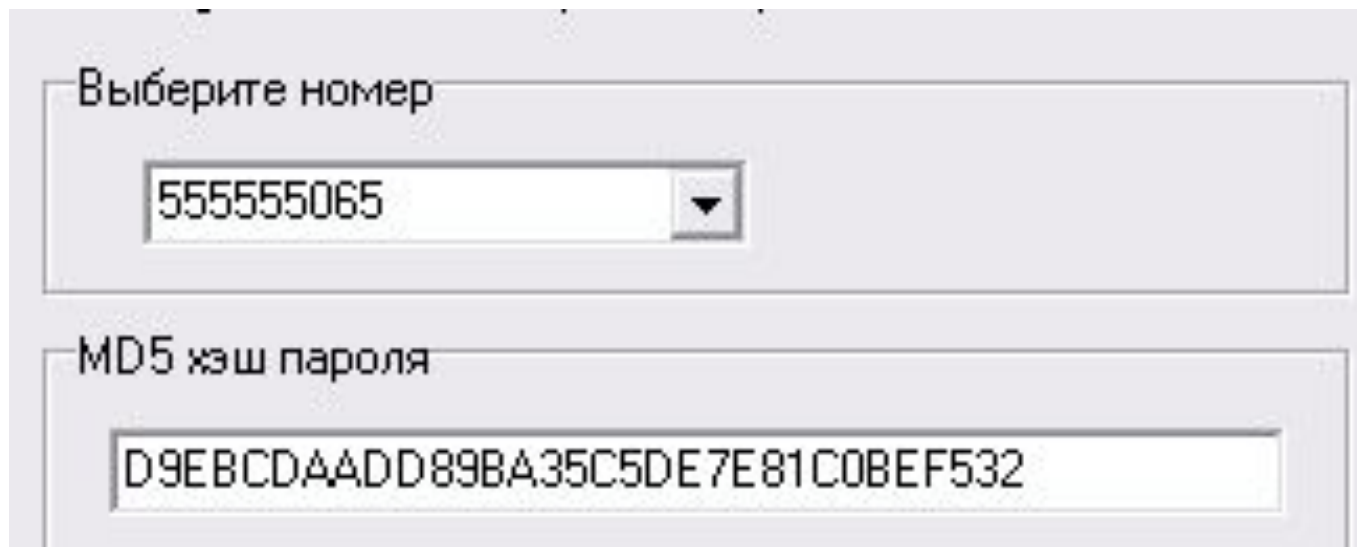
Пароль — условное слово или набор знаков, предназначенный для подтверждения личности или полномочий.



Пароли использовались в компьютерах с первых их дней. Например, CTSS от MIT, появившаяся в 1961 году, была одна из первых открытых систем. Она использовала команду LOGIN для запроса пароля пользователя



Роберт Моррис предложил идею хранения паролей в хэш-форме для операционной системы UNIX. Его алгоритм, известный как crypt, использует 12-битный salt и связывается для изменения формы с алгоритмом DES, снижая риск перебора по словарю



```
Выберите номер
555555065
MD5 хэш пароля
D9EBCDAAADD89BA35C5DE7E81C0BEF532
```

В конце 2017 года корпорация SplashData опубликовала 100 самых ненадежных паролей года. Первое место, уже 4 год подряд, занимает пароль - 123456. Его используют около 17% пользователей сети Интернет



Исходя из подходов к проведению атаки можно сформулировать критерии стойкости пароля к ней

- 1. Должен быть длинным.
- 2. Не должен быть словарным словом.
- 3. Не должен состоять только из общедоступной информации о пользователе.

Генератор паролей

СТАНДАРТНЫЙ ПАРОЛЬ 8 символов, цифры и буквы в нижнем и верхнем регистре, но без сочетаний 1100 (L в нижнем регистре, единица, ноль, O в верхнем регистре)	PkaYw75R
СТАНДАРТНЫЙ ПАРОЛЬ 12 символов, цифры и буквы в нижнем и верхнем регистре, но без сочетаний 1100 (L в нижнем регистре, единица, ноль, O в верхнем регистре)	PkaYw75RC49K
ПРОСТОЙ ПАРОЛЬ 8 символов, цифры и буквы в нижнем и верхнем регистре	Cybws63G
СУМАШЕДШИЙ ПАРОЛЬ 16 символов, любые символы, цифры и буквы в нижнем и верхнем регистре)Y>XSsj,+g~7)w4F

Чтобы создать новый пароль, обновите эту страницу (F5). Пароли никогда не повторяются, символы выбираются случайным образом.

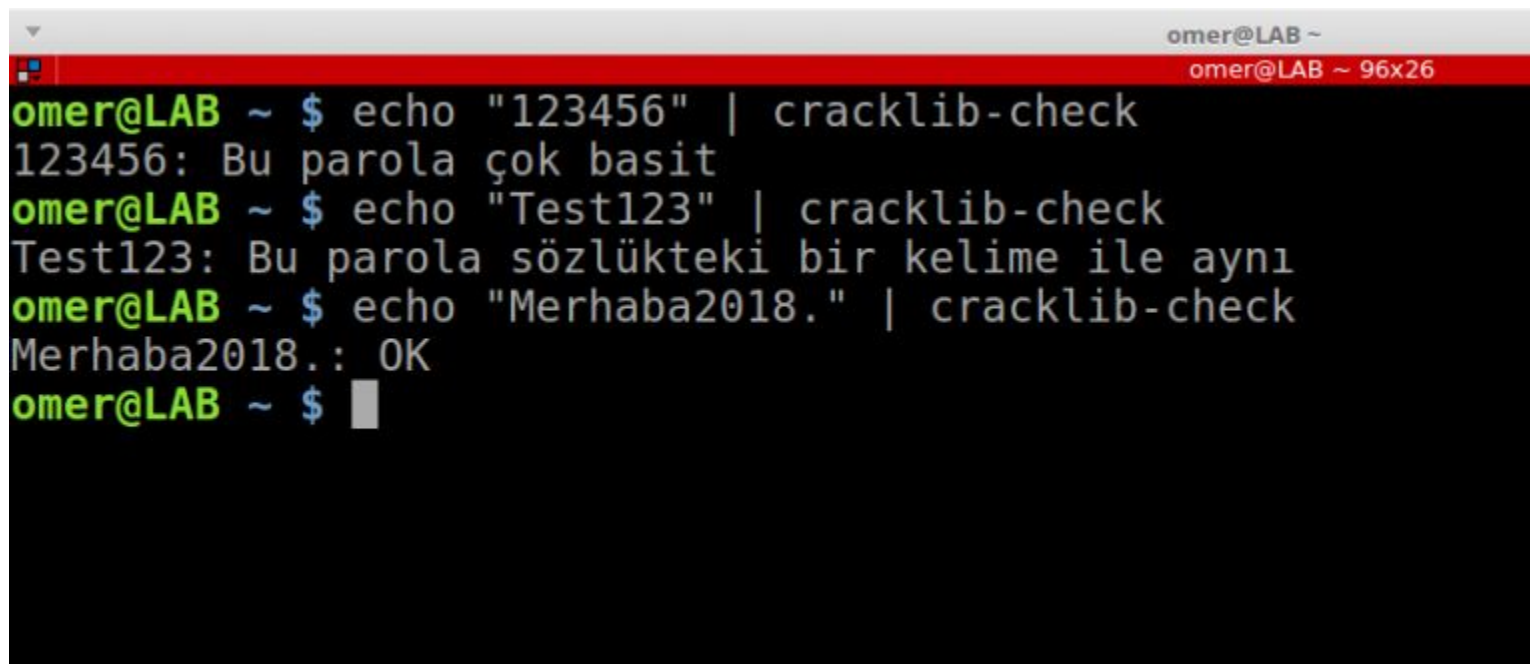
В качестве популярных рекомендаций к составлению пароля можно назвать использование сочетания слов с цифрами и специальными символами (#, \$, * и т. д.)



Методы защиты можно разделить на две категории:
обеспечение стойкости к взлому самого пароля,
и предотвращение реализации атаки

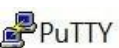


Первая цель может быть достигнута проверкой устанавливаемого пароля на соответствие критериям сложности. Для такой проверки существуют автоматизированные решения, как, например, cracklib.



```
omer@LAB ~  
omer@LAB ~ 96x26  
omer@LAB ~ $ echo "123456" | cracklib-check  
123456: Bu parola çok basit  
omer@LAB ~ $ echo "Test123" | cracklib-check  
Test123: Bu parola sözlükteki bir kelime ile aynı  
omer@LAB ~ $ echo "Merhaba2018." | cracklib-check  
Merhaba2018.: OK  
omer@LAB ~ $ █
```

Вторая цель — предотвращение захвата хэша передаваемого пароля и защиту от многократных попыток входа в систему. Обычно накладывают ограничение на число попыток в единицу времени (fail2ban)



GNU nano 2.5.1

File: /var/log/fail2ban.log

```
2016-07-22 10:05:25,381 fail2ban.filter [12445]: INFO [owncloud] Found 94.41.28.2
2016-07-22 10:05:32,471 fail2ban.filter [12445]: INFO [owncloud] Found 94.41.28.2
2016-07-22 10:05:50,681 fail2ban.filter [12445]: INFO [owncloud] Found 94.41.28.2
2016-07-22 10:05:57,751 fail2ban.filter [12445]: INFO [owncloud] Found 94.41.28.2
2016-07-22 10:05:58,139 fail2ban.actions [12445]: NOTICE [owncloud] Ban 94.41.28.2
2016-07-22 10:10:58,159 fail2ban.actions [12445]: NOTICE [owncloud] Unban 94.41.28.2
2016-07-22 11:25:33,592 fail2ban.filter [12445]: INFO [owncloud] Found 94.41.28.2
2016-07-22 11:25:38,661 fail2ban.filter [12445]: INFO [owncloud] Found 94.41.28.2
2016-07-22 11:26:16,051 fail2ban.filter [12445]: INFO [owncloud] Found 94.41.28.2
2016-07-22 11:26:22,131 fail2ban.filter [12445]: INFO [owncloud] Found 94.41.28.2
2016-07-22 11:26:23,139 fail2ban.actions [12445]: NOTICE [owncloud] Ban 94.41.28.2
```