Ford's Notes: Password Testing

The goal of this exercise is to learn about the 'strength' of the passwords and demonstrate methods used to make passwords more secure.

This exercise will use tools available from various sites on the Internet. These sites were all operational when this exercise was written.

https://www.uic.edu/apps/strong-password/

https://www.whatismyip.com/password-strength-test/

Important note: Do not test your own passwords using these web sites.

Testing Password Strength

1) Test these passwords.

   password

   123456789

   Security+701

   Which password is most secure? Why?

   Which password is least secure? Why?

2) Why is the password 'Squawkbox' better than 'PoloPool'?

3) A salt is a piece of random data added to a password. Use the following strings to add salt to the passwords from (1).

   SY0701

   SQUAWK

4) Test the following passphrases.

   Its only rock and roll

   You can check out anytime you want but you can never leave.

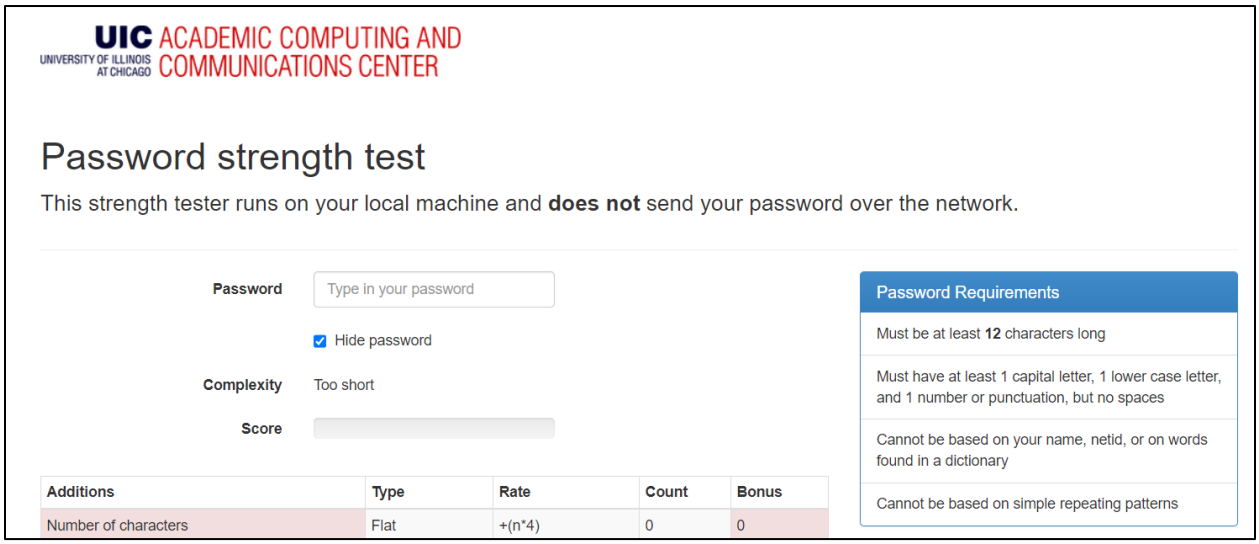
   Did you include space characters and punctuation?

The following pages are references and answers to the questions on this page.

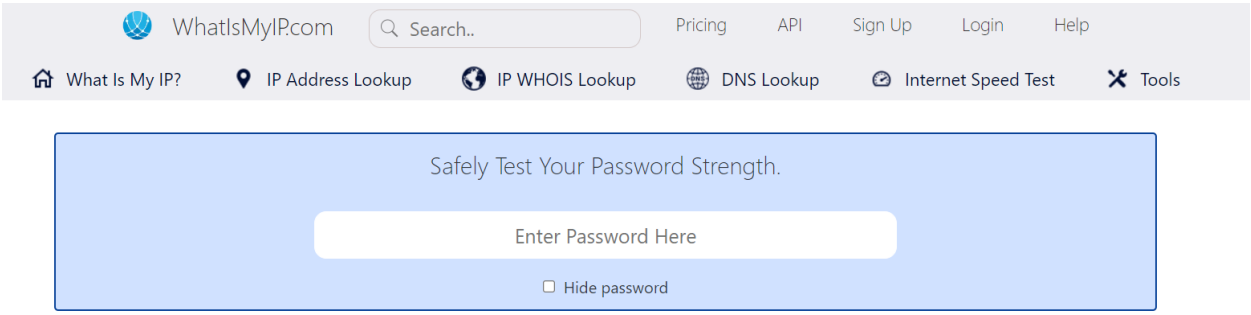
Brian Ford, 2023

Ford's Notes: Password Testing

Password testing websites



https://www.uic.edu/apps/strong-password/



https://www.whatismyip.com/password-strength-test/

Ford's Notes: Password Testing

Solutions

1) Test these passwords.

    password

    123456789

    Security+701

The University of Illinois at Chicago (UIC) Computing Center Password Strength Test displays two tables for each submitted password. The first table (Additions) scores submitted passwords. The second table deducts from that score based on factors that weaken the password.

Rows marked in green denote positive aspects of the password.

Rows marked in red or yellow denote negative aspects.

Any row that is gray denotes no score because that factor was not present.

WhatsMyIP offers a password strength test that tests on the complexity of the entered value based on different measures of difficulty to reverse that value. The output is in time to crack the password. There are four different measures of difficulty: throttled online, and unthrottled online attacks.

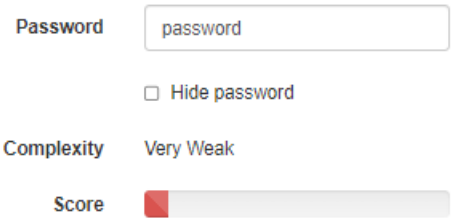
A throttled attack implies that passwords would be rate limited by the target device. That throttled rate is 100 per hour. An unthrottled attack assumes that passwords can be sent to a target device as fast as they can be generated and transmitted. The unthrottled rate is 10 per second.

Fast hashes are cryptographic hash algorithms used to compute a hash that is compared to a previously stored value. They are designed to be fast and generate 10 billion passwords per second.

Slow hashes are designed to be inefficient (slow) and more difficult to calculate. The slow hashing rate is 10,000 passwords per second.

Ford's Notes: Password Testing

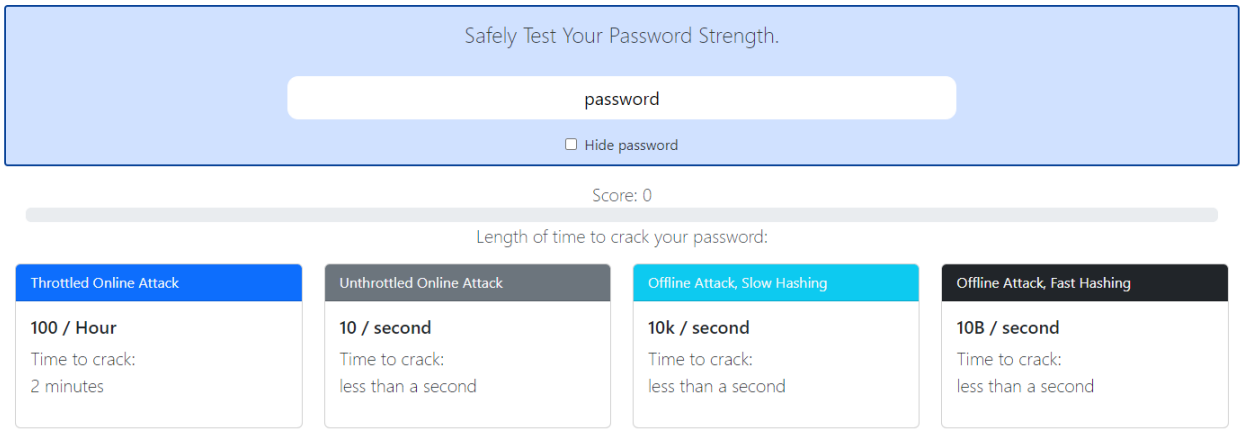
password



Additions	Type	Rate	Count	Bonus
Number of characters	Flat	+(n*4)	8	+ 32
Uppercase letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	8	0
Numbers	Cond	+(n*4)	0	0
Symbols	Flat	+(n*6)	0	0
Middle numbers or symbols	Flat	+(n*2)	0	0
Requirements	Flat	+(n*2)	2	0

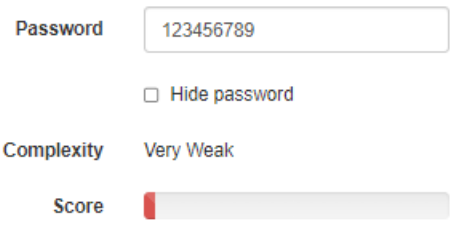
Deductions	Type	Rate	Count	Bonus
Letters only	Flat	-n	8	- 8
Numbers only	Flat	-n	0	0
Repeat Characters (case insensitive)	Comp	-	2	- 2
Consecutive uppercase letters	Flat	-(n*2)	0	0
Consecutive lowercase letters	Flat	-(n*2)	7	- 14
Consecutive numbers	Flat	-(n*2)	0	0
Sequential letters (3+)	Flat	-(n*3)	0	0
Sequential numbers (3+)	Flat	-(n*3)	0	0
Sequential symbols (3+)	Flat	-(n*3)	0	0

Using the term 'password' produced a score of 8 (very weak). That was 32 additions from which it subtracts 24 (deductions).



Ford's Notes: Password Testing

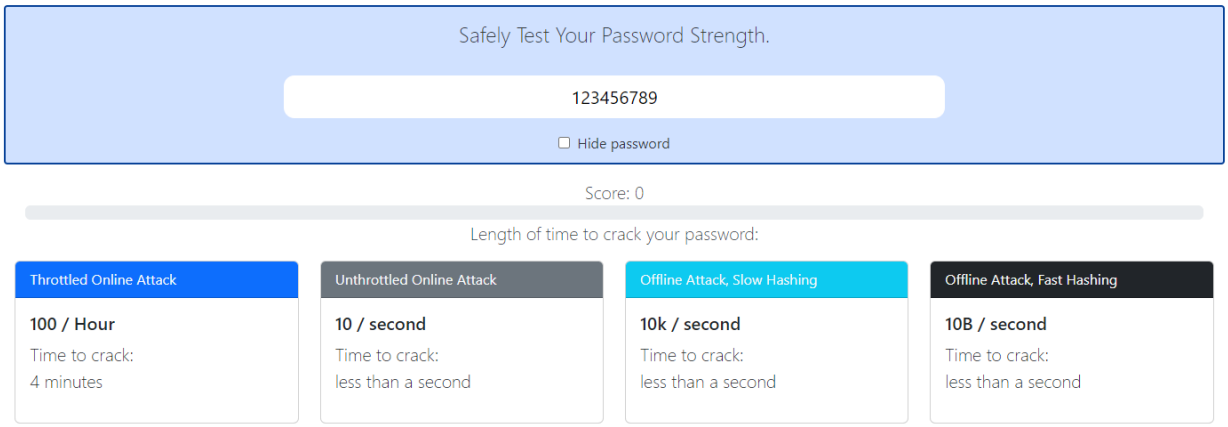
123456789



Additions	Type	Rate	Count	Bonus
Number of characters	Flat	+(n*4)	9	+ 36
Uppercase letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	0	0
Numbers	Cond	+(n*4)	9	0
Symbols	Flat	+(n*6)	0	0
Middle numbers or symbols	Flat	+(n*2)	7	+ 14
Requirements	Flat	+(n*2)	2	0

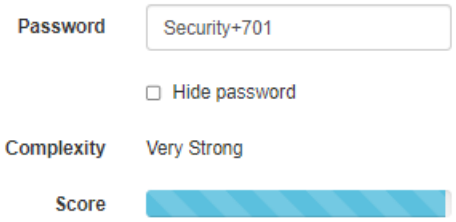
Deductions	Type	Rate	Count	Bonus
Letters only	Flat	-n	0	0
Numbers only	Flat	-n	9	- 9
Repeat Characters (case insensitive)	Comp	-	0	0
Consecutive uppercase letters	Flat	-(n*2)	0	0
Consecutive lowercase letters	Flat	-(n*2)	0	0
Consecutive numbers	Flat	-(n*2)	8	- 16
Sequential letters (3+)	Flat	-(n*3)	0	0
Sequential numbers (3+)	Flat	-(n*3)	7	- 21
Sequential symbols (3+)	Flat	-(n*3)	0	0

Using the term '123456789' produced a score of 4 (very weak). That was 40 additions from which it subtracts 36 (deductions).



Ford's Notes: Password Testing

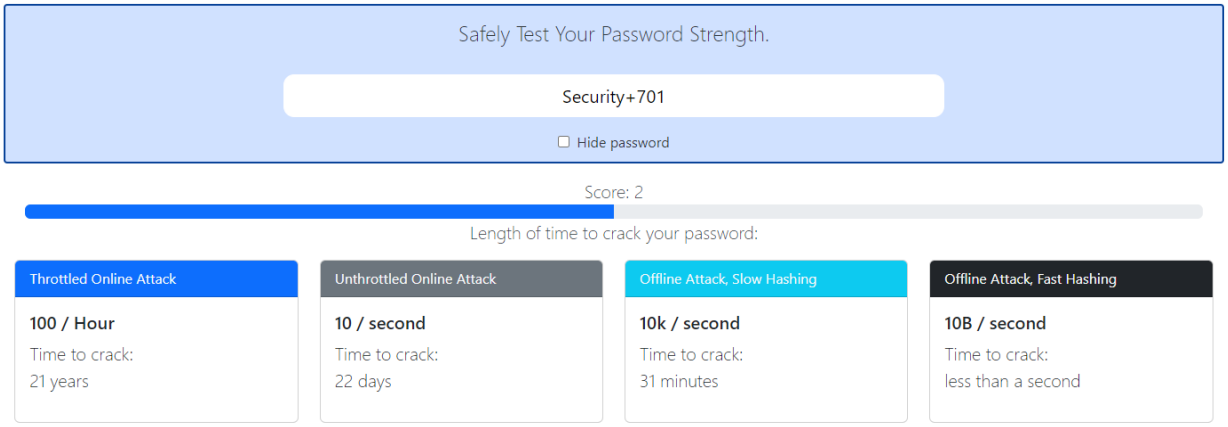
Security+701



Additions	Type	Rate	Count	Bonus
Number of characters	Flat	+(n*4)	12	+ 48
Uppercase letters	Cond/Incr	+((len-n)*2)	1	+ 22
Lowercase Letters	Cond/Incr	+((len-n)*2)	7	+ 10
Numbers	Cond	+(n*4)	3	+ 12
Symbols	Flat	+(n*6)	1	+ 6
Middle numbers or symbols	Flat	+(n*2)	3	+ 6
Requirements	Flat	+(n*2)	5	+ 10

Deductions	Type	Rate	Count	Bonus
Letters only	Flat	-n	0	0
Numbers only	Flat	-n	0	0
Repeat Characters (case insensitive)	Comp	-	0	0
Consecutive uppercase letters	Flat	-(n*2)	0	0
Consecutive lowercase letters	Flat	-(n*2)	6	- 12
Consecutive numbers	Flat	-(n*2)	2	- 4
Sequential letters (3+)	Flat	-(n*3)	0	0
Sequential numbers (3+)	Flat	-(n*3)	0	0
Sequential symbols (3+)	Flat	-(n*3)	0	0

Using the term 'Security+701' produced a score of 70 (very strong). That was 86 additions from which it subtracts 16 (deductions).



2) Why is the password 'Squawkbox' better than 'PoloPool'?

Surprise! Squawkbox is a weak password. There are no numbers or special characters used. PoloPool is a very weak password for the same reasons but is very weak because of the three repeated characters (P, O, L).

3) Adding salt

Adding SY0701 or Sqwaukbox at the start or at the end of each password improves the complexity and the time needed to crack the passwords. Using Sqwaukbox as a salt produced longer times to crack using the WhatsMyIP strength test.

4) Using passphrases:

Its only rock and roll

You can check out anytime you want but you can never leave.

The UIC Password Strength Test scored both of these passphrases higher based on their length but neither includes numbers or special characters. The time to crack measures for passphrases were in years or centuries.

Including the " " or space character between the words slightly increased the scores and complexity of the passphrases as it makes them longer. The " " was not identified as a special character by the UIC tool.