

PASSWORD STRENGTH CHECKERS ARE REALLY IMPORTANT?

SHARAN UDAYA SHETTY

Keraleeya Samajam's Model College , Dombivili East, Mumbai, Maharashtra, India

ABSTRACT

There are many purposes where regular users require different passwords whenever they send and receive emails, do online shopping and numerous other activities on the internet. Surprisingly since the invention of the password, it has not been capable to protect the user accounts until now. There is no problem in using the similar password, but different passwords are often difficult to remember and mistakes can creep in rather easily.

Many users do not know what kind of passwords should be chosen which will be strong enough to sorts of fraudulent activities ,so we are adding a password generating module which will generate a strong password if the user can't create a strong one which will match all the criteria and the user can create a custom generated password .This project is an attempt to develop a password strength checker along with password confirmation and a password generator so that combining all these together will indicate a close positive correlation between the difficulty of guessing and the quality of the passwords. Apart from these password validation will help the user to guide that if he has enter a wrong password and he can retype the password. In case if user is not able to create a strong password a password generator system will help him to set a strong and custom password which will be effective to secure the account or sensitive information.

Introduction

It is important to keep personal and organizational information safe and protected .Passwords have become the most used authentication to protect resources from unauthorized access A personalized password is a simple way for the user to create, implement and remember .A disadvantage with these kinds of passwords: they make an easy target for crackers If an unauthorized person has cracked a password and successfully entered a system ,login, account

etc. it is not unusual that the cracker can try to use the same password elsewhere .When reusing the same password, for instance on a more secure system, file or account can make it vulnerable for the user's sensitive data.

There are measurements for helping and encourage users to create and strengthen a better password, by using a password meter. Password meters are indicators that measures the password the user types in, and gives suggestions and guidance in the creation of the password. It shows the given password how weak or strong it is, also the mixture of characters, numbers, signs, symbols. Furthermore, there will be a password generator that creates random or customized passwords for users it helps users create stronger passwords that provide greater security for a given type of access .Password generators help those who have to constantly come up with new passwords to ensure authorized access and to

manage a large number of passwords for identity and access management.

Background study

To increase the strength of a passwords, users are typically required to know a set of rules when creating passwords. Users compose their passwords following the specific requirements given in the guidelines. For example, the password must contain at least eight characters including at least one number or one upper case letter, and it should not contain the username. There are various password guidelines that are used by organisations, and they should be written efficiently to provide good security. Nowadays, users may even have much more than 25 passwords.

As users are expected to use different passwords for each account to avoid security failures, it is difficult for the brain to remember many sets of illogical and random password. The user's response to this situation is generally adopting strategies such as choosing weak passwords or writing them down, which ultimately compromise the security of the systems so by implementing strict password creation guidelines will help the user to ensure a high security. There is a system called password generator which will generate custom password as per the user need adding some special characters so that it will be easy to remember the password and there will be no need to think too much about creating a strong password this system helps a lot to ensure that the user is good to remember the password and also maintain a good security.

Scope

Password strength checker helps users to choose hard to guess passwords and enhance the security

of systems based on password authentication. Password meters give simple and immediate visual feedback for what creates a strong password. Passwords generated with the help of meters increased from a median of nine characters to 10, included more special characters and contained more lower-case letters, up from a median of six characters to seven which will create a strong password.

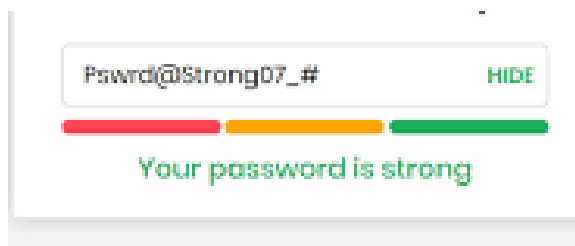


Password-strength meters based on length, complexity and unpredictability measure the effectiveness of a password in resisting both guessing and brute-force attacks. The first factor is determined by how long the password is, complexity is based on how large a set of characters or symbols it is drawn from, and unpredictability is based on whether the password is created randomly or by a more predictable process. If used correctly, a password meter helps the user choose more crack-resistant passwords, and length is a more effective requirement for producing strong passwords than the use of numerals and special characters. Password confirmation is an important part to confirm again the password which the user has created that will help user to make sure that password that he has created is valid and correct.

Objective

The objective of this project is to provide and generate a secure and safe password to the user many times user ignore or choose a weak password

which compromise the safety of the account. creating a password generator will help the user to use custom strong password and which will be easy to remember every time apart for that we also added a password validator to confirm the password if the user mistype their password ,they won't recognize it. The confirm password catches the type by helping user to type their password twice. By using this this confirm password field there is less or no chance to mistake password by user.



Purpose

The purpose is to find a balance between password strength. Hopefully to counterbalance with a complex secure password and be relatively easy for the user to remember for a long period of time. When creating a strong password it will not only keep the intruders away, it will also increase the safety of their personal information.



BACKGROUND OF THE PROBLEMS

This segment describes the most well-known strategies for secret phrase encryption. A. Hash Technologies Hash encryption innovation is the most regularly utilized procedure for scrambling and putting away client data and passwords in PC and organization frameworks. It is a function to pack messages of any length into a proper length message digest. Additionally hash is a refinement of data, normally a lot more modest than the data, and is of a decent length [6]. A solid hash should be irreversible, which implies that any of the first data can't be inferred by the hash esteem. Additionally, any adjustment of the info data will bring about a huge change in the hash esteem, which is known as the avalanche effect. The hash should also be anti-collision, that is, two snippets of data with a similar hash esteem can't be found. So these highlights are reasonable for saving passwords in the mean time individuals need to utilize an irreversible calculation to encrypt saved passwords.

Password Cracking Algorithms

Brute Force Attack, also known as method of exhaustion, tries every combination of characters at a given length [3, 13].

This method consumes a lot of computation and is usually the least efficient way to crack hash encryption, but as long as the device runs fast enough and time permits, it will eventually find the correct password [13]. The so-called given length is depending on the password policy of target website that

displays the minimum limit of the number of textual password

characters when creating passwords and modifying passwords

[14]. Some websites are 6-bit characters (no need to try the

length less than 6 characters), most websites are 8-bit

characters (no need to try the length less than 8 characters)

Password Cracking Algorithms Brute Force

Attack, also called technique for depletion, attempts each blend of characters at a given length

. This technique devours a ton of calculation and is generally the most un-effective method for

breaking hash encryption, yet as long as the gadget runs adequately quick and time grants, it

will ultimately find the right password The so-called given length is relying upon the secret

phrase strategy of target site that he minimum limit of the number of textual password characters

while making passwords and adjusting passwords . A few sites are 6-bit characters (no need to try

the length under 6 characters), most sites are 8-bit characters (no need to try the length less than 8

characters) For the most part, secret phrase entropy gives a decent sign of the strength of the

passwords and compare to the time expected to break the secret phrase using brute force for

example the bigger the secret phrase entropy, the additional time is expected to break the secret key

using brute force. Dictionary attacks on the other hand works distinctively and relies upon the size

of the dictionary utilized and may not relate in a similar way as secret phrase entropy.

Notwithstanding, utilizing both brute force and dictionary attack can provide client with a superior

sign of the genuine strength of the passwords as a solid secret key (for a decent length) should not be

clear or just somewhat adjusted from a readable word.

Password algorithm

Password Algorithm is the backend code of the various sites for mirroring the secret word strength meter.

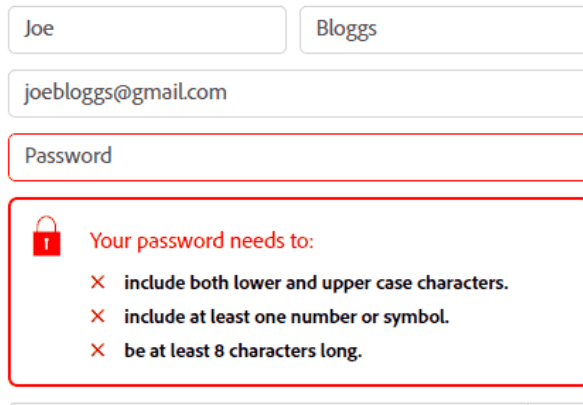
it is an expansion calculation framework which breaks down the secret phrase, consolidates the weight distribution, and acquires the secret word strength score. The higher the score, the safer the secret phrase and the more secure it is. As indicated by the secret word score, the secret phrase level is separated into seven levels from very weak(score of 0) to extremely protected (score ≥ 90). Focuses are given dependent on secret key length, uppercase and lowercase letters being utilized, number of digits and symbols utilized.

The conditions to be met for a good password is that users can only get extra points if they meet the minimum conditions

The lowest condition is as follows:

1. The secret key length is no under 8 characters;
2. Contains capitalized letters;
3. Contains lowercase letters
4. Contains numbers;
5. Contains symbols like (*#@!)

Password Policies:



The base condition requires that thing 1 be fulfilled and any three of things 2 - 5 be fulfilled. As indicated by the secret phrase score, the secret key level is divided into the accompanying five levels from very weak (score of 0) to extremely amazing (score ≥ 80)

Results and discussions

This review gives an understanding that encryption technologies are turning out to be more complex although breaking strategies are arising endlessly. A portion of the hash encryption algorithms have disadvantages as examined previously, yet they are still generally protected and broadly utilized by expanding the length of the hash esteem and adding salt.



. In any case, when the time needed to break a secret phrase surpasses the worth of the data it protects, the brute force assault becomes pointless. Dictionary attacks and rainbow-table attacks despite the fact that their library records are sufficiently amazing, the hardware cost of the capacity unit that necessities to store this data is additionally increased. However long the client can intermittently refresh and refresh the first secret phrase, even a single character change will make the library files of the dictionary attack and the rainbow-table attack lists huge and unbearable. What's more, mainstream Internet platforms should be more answerable for ensuring the security of its clients' passwords and decreasing the chance of being leaked.

Conclusions

To summarize, the internet based world has turned into a basic part of people's lives. At the point when individuals access the Internet, they need to manage clear text passwords. Although most mainstream Internet platforms have taken on their own secret phrase strength meters to assist clients with setting solid passwords, it just so happens, these efforts are not acceptable and counterproductive on account of their own particular secret key strategies. Future work includes client testing of the new secret key strength meter to existing ones.

REFERENCES

1. M ,Xu and W, Han, "An Explainable Password Srength Meter"

2. W.C., Summers and E, Bosworth, "Password policy: the good, the bad, and the ugly".
3. D, Pleacher (n.d.). "Password Entropy". [online] Pleacher.com. Available at: www.pleacher.com/mp/mlessons/algebra/entropy.html [Accessed 28 May 2019]