Easy to Remember, Hard to Guess: A Password Generation Tool for the Digital Age

Ioana-Ilona BRĂSLAȘU, Andrei-Daniel ANDRONESCU, Dumitru-Iulian NĂSTAC
Faculty of Electronics, Telecommunications and Information Technology,
University POLITEHNICA of Bucharest, Romania
ioanabraslasu2000@gmail.com, andronescu.andreidaniel@gmail.com, iulian.nastac@upb.ro

Abstract

A brute force attack is a common method used by cybercriminals to gain unauthorized access to user accounts. It is essential for individuals and organizations to take proactive measures to protect themselves from such attacks. One way to do this is by improving their knowledge of cybersecurity and implementing measures to safeguard their online presence. Using programming languages like Python and web-frameworks like Django, websites can be developed to help individuals generate secure and memorable passwords that align with the latest password security standards. This can help anyone who wants to improve their password security, irrespective of whether they have been a victim of a cyber-attack or not.

Index terms: hackers, Python, secure password, website, memorable

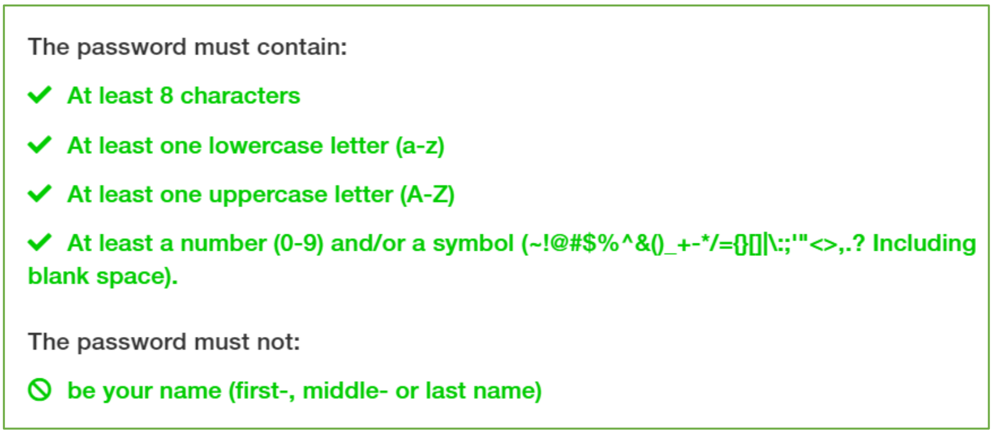
1. Introduction

The Internet dependency has increased significantly in the post-pandemic era and therefore people create frequently accounts using their credentials when they perform online shopping, work remotely or in e-learning. As a result, the most crucial factor in this context is the password. With the large number of accounts created online, it can be challenging to remember every password created for each website and, in particular, to generate new password every time, as it is recommended by the well-known password-manager tool of Google [1]. People tend to ignore such suggestions and instead, they use identical passwords across multiple platforms because it is more comfortable in this way. What is more, the risks of using personal information based on birthdays, names or addresses in passwords tend to be ignored even if any information posted on social media can be used by a hacker as they can craft a social engineering attack [2].

Since password authentication is the cheapest mechanism to access a system, passwords turn into the most vulnerable component in this equation [3] and this issue was a source of inspiration. In this paper, an easy-to-remember password generator is proposed and it is presented as a website. The user must enter two words that represents him, excluding personal information, such as: favorite sports team, city, season, food, activity or animal and a number. After inputting the necessary requirements, the implemented code modifies the words by converting some lower-case letters into upper-case or changing certain letters into symbols or numbers. These modified words are then combined with the entered number to create a secure character combination that is resistant to cyber-attacks.

2. What does a secure password need?

Generally, each website offers the user general information regarding what a secure password should contain, without requiring additional research on security risks. This is just an example from a university's website [4] of suggestions that usually pop up when creating a password:



The password must contain:

✓ At least 8 characters

✓ At least one lowercase letter (a-z)

✓ At least one uppercase letter (A-Z)

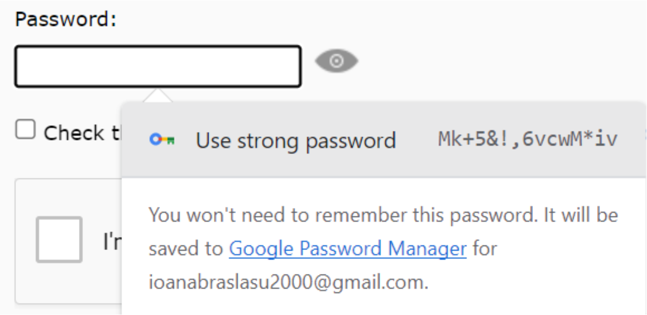
✓ At least a number (0-9) and/or a symbol (~!@#$%^&()_+-*/={}[]|\:;'"<>,.? Including blank space).

The password must not:

⃠ be your name (first-, middle- or last name)

Fig. 1. A website's recommendation for a secure password

Also, Google Password Manager always suggests strong passwords, which can be stored in this tool, but it can be extremely difficult to remember since it represents just a random combination of characters, but very solid at the same time.



Password:

□ Check t

Use strong password Mk+5&!,6vcwM*iv

You won't need to remember this password. It will be saved to Google Password Manager for ioanabraslasu2000@gmail.com.

Fig. 2. Google Password Manager suggestion

2.1. General standards for a secure password

To ensure the safety and security of our online presence, it is important to follow certain guidelines and standards when creating and managing passwords. By following this set of rules, we can greatly reduce the risk of our personal information being compromised by hackers and cybercriminals.

- **Avoid using personal information**: ExpressVPN's study on the most common passwords around the world showed that 42% of people use their first name in their passwords, while 43% of them use their birth date [5], data that ca be easily guessed by unauthorized people who can search on your social media for such details. It is also advisable to refrain from using personal information, such as the names of pets or children, as well as addresses.
- **The longer the password the better**: According to the Center for Internet Security (CIS) [6], length is the most important aspect of a good password. Passwords that are more than 8 characters are statistically harder to guess than shorter ones. When a password cracker has more characters to fill to guess the correct password, it becomes exponentially less likely to get it right.

- **Mixed symbols, numbers and caps:** A mix of characters increases the number of possible combinations and makes it more difficult for an attacker to guess or crack the password. For instance, a password such as "password123" can be easily guessed, while a password such as "Pa$$w0rd!23" is more complex and difficult to guess. The use of numbers and capitalization also adds an extra layer of complexity to the password [7].
- **A password should not be shared with any other account:** If a shared password is compromised, it can potentially give an attacker access to all accounts associated with that password. Additionally, sharing them with other accounts can lead to a loss of control over personal information such as bank accounts, as it can be difficult to track who has access to what information. In some cases, sharing passwords may even be a violation of the terms of service of certain websites or applications.
- **A password should not contain any consecutive letters or numbers**
- **Easy to remember, hard to guess:** the users' real issue
- **The password should be confidential:** It is important to keep our passwords confidential because they are the primary means of securing personal and sensitive information online. If passwords are not kept confidential, they can be easily compromised, giving unauthorized individuals access to our accounts and personal information.

Not only is the complexity of a password essential, but also the safety of the 'place' where it is stored. Cybersecurity experts from the U.S. government (CISA) have recommended using password managers [8]. A password manager is a software application that helps users generate, store, and manage their passwords for various online accounts. It typically stores passwords in an encrypted database that is protected by a master password or passphrase that must be remembered by the user. Such tools can also help users generate strong, unique passwords for each account, which reduces the risk of a password being compromised.

Eventually, to add extra safety to the password and to the sensitive information, individuals can opt for two-authentication security measure. It can take different forms such as SMS codes, authentication as an option to increase security for their users.

2.2. Most used combinations for passwords

When it comes to creating an online account, many of us would rather remember a code than create an unbreakable password. Defending our position, it can be challenging to keep track of numerous login credentials. According to technology expert Burton Kelso [9], it is human nature to fall into a predictable routine when it comes to our passwords list.

To make matters worse, the analysis reveals that 64 percent of breached passwords were used for at least two accounts [10] which can lead to a domino effect in the case when a hacker succeeds in guessing a password because several accounts are compromised as well.

According to NordPass.com [11], the most common passwords used in 2022 are: *password*, *123456*, *123456789*, *guest*, *123123*, *col123456*, *000000*, *querty*.

Security.org created a website [12] that check how secure a password is and in how many years or seconds they can be guessed. The passwords listed above can be breached in less than one second. It is an interesting tool that makes the user understand how technology evolves in terms of decrypting passwords.

3. Real cases of weak passwords guessing and the consequences

Weak passwords are a common cause of data breaches and cyber-attacks, leading to serious consequences for individuals, businesses, and organizations. In 2019, a massive data breach at Capital

One Bank [13] exposed the personal information of over 100 million customers, due to a vulnerability in the company's cloud infrastructure caused by a weak password. In another case, on January 17th 2022, approximately 500 individuals' cryptocurrency wallets were targeted in an attack that resulted in the theft of approximately $18 million worth of Bitcoin, $15 million worth of Ethereum, and other cryptocurrencies [14]. The hackers were able to gain access to the wallets by bypassing two-factor authentication, demonstrating the vulnerability of this security measure. This incident highlights the importance of using a password manager to store and manage strong, unique passwords for online accounts, as it can help protect against Brute force attacks, where attackers use automated tools to try many possible passwords, can be successful against weak passwords that are easy to guess, such as "123456" or "password." Similarly, phishing attacks, where attackers trick users into revealing their passwords through fraudulent emails or websites, can be effective against users with weak passwords who may be more easily fooled. Moreover, dictionary attacks, where attackers use pre-computed lists of common passwords, can be successful against weak passwords that are commonly used, such as "qwerty" or "letmein".

All these examples illustrate the importance of using strong, unique passwords and taking other measures to protect against cyber-attacks. A solution to this issue would be to make those passwords as memorable as possible to be more appealing to not only individuals, but also big companies.

4. Description of the Website Implementation

Since passwords are mainly used in different Internet browsers, implementation of a website that comes in handy in securing the online experience is proposed. In this process, both Python programming language and web development languages were used in order to create a fully functional website that is called *My Secure Password*. Here, the user can enter two words that represents him and also one number to prevent the risk of decryption, elements that eventually will build a robust password.

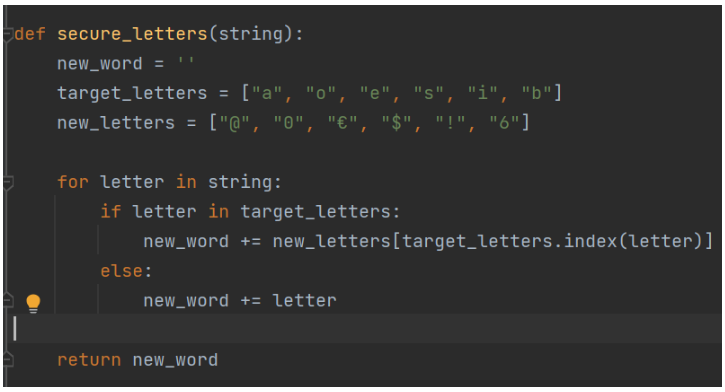
4.1. Backend Part of the Website

For creating the server where the website will be running, Django framework is used. Django is a high-level Python web framework that encourages rapid development and clean, pragmatic design. The efficiency of rendering HTML pages was demonstrated by including CSS and JavaScript files in the HTML templates, which allowed for customization of the website's styling and incorporation of interactive features like a copy-to-clipboard button.

In this framework's inputs, Python functions were created to perform the most important part of the project, the creation of the secure password. Those are:

- upper_vowels ()
- secure_letters ()

In designing these functions, two widely recognized criteria were used for enhancing password security, namely the substitution of lower-case characters with their corresponding upper-case letters and the use of special characters as substitutes for some of the alphabetic letters. In practice, individuals are typically more responsive to the manipulation of vowel characters in a word, hence, the decision was made to replace only lower-case vowels with their respective upper-case counterparts. This approach reduces the potential for confusion and facilitates memorization of the password. When it comes to replacing some letters with special characters, substituting *a* with '@' or *i* with '!' will impact the user visually. There are other character substitution ideas:

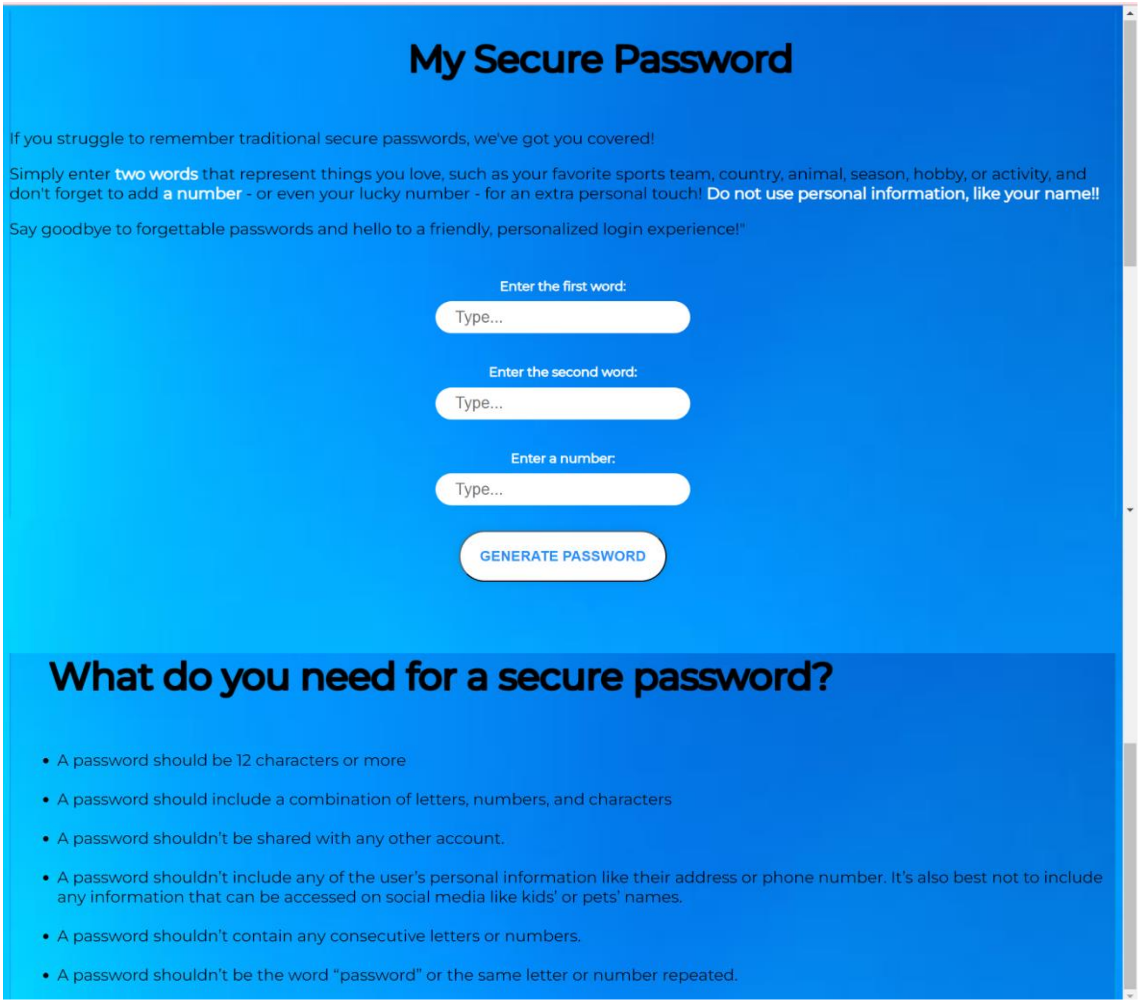


```
def secure_letters(string):
    new_word = ''
    target_letters = ["a", "o", "e", "s", "i", "b"]
    new_letters = ["@", "0", "€", "$", "!", "6"]

    for letter in string:
        if letter in target_letters:
            new_word += new_letters[target_letters.index(letter)]
        else:
            new_word += letter

    return new_word
```

Fig. 3. Special Characters replacement in Python Code

As the most important function, the password generation one, has two words and one number as input, it was decided to randomly allocate those letter-manipulation functions to the input words for making the code as general as possible. Next, the processed words plus the number are combined into a complex union of characters. If the user typed words that consists of a word or less, an error message will pop up and if the combination of letters has less than twelve letters, random characters such as: ‘*’,’ #’, ‘- ‘or ‘.’will be placed between the elements until the desired number of characters is reached. Also, if there are any spaces in the input words, they will be also replaced with special characters.

4.2. Frontend Part of the Website



My Secure Password

If you struggle to remember traditional secure passwords, we've got you covered!

Simply enter **two words** that represent things you love, such as your favorite sports team, country, animal, season, hobby, or activity, and don't forget to add **a number** - or even your lucky number - for an extra personal touch! **Do not use personal information, like your name!!**

Say goodbye to forgettable passwords and hello to a friendly, personalized login experience!"

Enter the first word:

Enter the second word:

Enter a number:

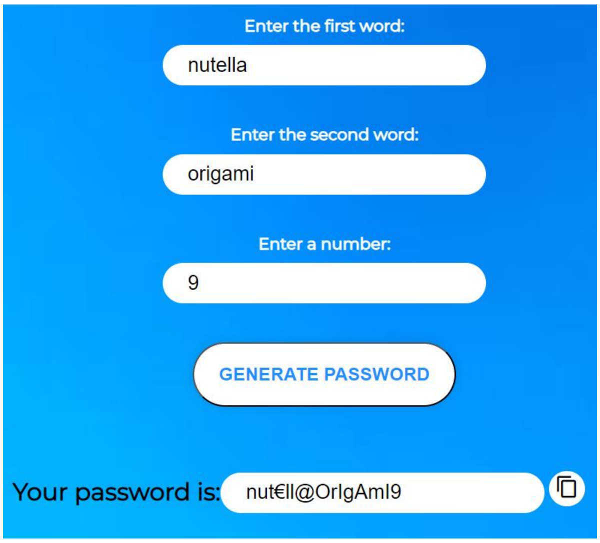
What do you need for a secure password?

- A password should be 12 characters or more
- A password should include a combination of letters, numbers, and characters
- A password shouldn't be shared with any other account.
- A password shouldn't include any of the user's personal information like their address or phone number. It's also best not to include any information that can be accessed on social media like kids' or pets' names.
- A password shouldn't contain any consecutive letters or numbers.
- A password shouldn't be the word "password" or the same letter or number repeated.

Fig. 4. The website’s design

To ensure a seamless design for the website, widely recognized languages such as HTML, CSS, and JavaScript were used. The user receives clearly what is needed for generating a secure and memorable password and additionally some recommendations to protect personal data online. After pressing the ‘Generate Password’ button, an input will appear with the result, along with the copy-to-clipboard button.

Towards the end of the webpage, a section has been included that offers a concise summary of necessary recommendations and principles for designing a secure password based on standard practices.



Enter the first word: nutella

Enter the second word: origami

Enter a number: 9

Your password is: nut€ll@OrIgAmI9

Fig. 5. Example of a Secure Password

5. Conclusion

In conclusion, the proposed website offers an efficient solution to the common problem of weak passwords. By generating strong and memorable passwords that comply with the latest password security standards, the website can significantly reduce the risk of cyber-attacks and prevent users from reusing the same password across different websites. In today's digital world, where cyber threats are constantly evolving, it is imperative for individuals to take proactive measures to ensure the security of their personal information. The website's approach to generating secure passwords is a simple yet effective way for users to improve their online security and safeguard themselves against potential data breaches. By implementing this method, users can rest assured that their accounts are well-protected, and their sensitive information is kept secure. Overall, the website's contribution to enhancing password security serves as a crucial step towards improving the overall cybersecurity landscape.

When it comes to improving the presented website, displaying errors accordingly on the interface is on the list for future plans. In present, only the error when the user enters a word of 2 characters or less appears on the screen. Also, the error display is not well formatted and many other error cases should pop up. For example, when the user enters consecutive numbers or letters and when words such as passwords and user are chosen should not give the permission for creating a strong password.

References

[1]. Google. (n.d.). Manage your Google Account password. [Online]. Available: https://passwords.google.com/options?ep=1. [Accessed: Apr. 19, 2023].

[2]. J. Miller and Z. Snyder, "Innocuous Facebook Quizzes: Attacker Intel Goldmines," ZeroFOX, 2016. [Online]. Available: https://www.zerofox.com/blog/innocuous-facebook-quizzes-attacker-intel-goldmines/. [Accessed: May 06, 2023]

[3]. Sadat, S. E., Hedayathllah, H., & Ahamadzai, N. (2023). Highly Secure and Easy to Remember Password-Based Authentication Approach. Journal for Research in Applied Sciences and Biotechnology, 2(1), 18-25. DOI: 10.55544/jrasb.2.1.18. [Accessed: Apr. 19, 2023].

[4]. University Admissions. (n.d.). Log in. [Online]. Available: https://www.university admissions.se/intl/login. [Accessed: Mar. 20, 2023].

[5]. HackRead. (2019, Feb. 8). People use their names as passwords: Study. [Online]. Available: https://www.hackread.com/people-use-their-names-passwords-study/. [Accessed: Apr. 20, 2023].

[6]. Georgetown University. (2020, Oct. 27). Password size matters. [Online]. Available: https://security.georgetown.edu/csam-2020/password-size-matters/. [Accessed: Apr. 20, 2023].

[7]. Google. (n.d.). Create a strong password. [Online]. Available: https://support.google.com/accounts/answer/32040?hl=en. [Accessed: Apr. 23, 2023].

[8]. Cybersecurity and Infrastructure Security Agency. (2022, Mar. 10). Choosing and protecting passwords. [Online]. Available: https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords. [Accessed: Apr. 23, 2023].

[9]. Reader's Digest. (n.d.). Passwords hackers can guess first. [Online]. Available: https://www.rd.com/article/passwords-hackers-guess-first/. [Accessed: Apr. 23, 2023].

[10]. Techzine. (2022, Mar. 2). Most people still use the same password for multiple accounts. [Online]. Available: https://www.techzine.eu/news/security/74094/most-people-still-use-the-same-password-for-multiple-accounts/. [Accessed: Apr. 23, 2023].

[11]. NordPass. (n.d.). Most common passwords list. [Online]. Available: https://nordpass.com/most-common-passwords-list/. [Accessed: Apr. 23, 2023].

[12]. Security.org. (2022, Mar. 18). How secure is my password? [Online]. Available: https://www.security.org/how-secure-is-my-password/. [Accessed: Apr. 23, 2023].

[13]. Capital One, "Facts 2019," Capital One, [Online]. Available: https://www.capitalone.com /digital/facts2019/. [Accessed: Apr. 24, 2023].

[14]. ERMProtect, "Top 10 Data Breaches So Far in 2022," ERMProtect, [Online]. Available: https://ermprotect.com/blog/top-10-data-breaches-so-far-in-2022/. [Accessed: Apr. 24, 2023].