Ćwiczenie – Stwórz i przechowuj silne hasła

1. Zadania

Poznaj tajniki najbezpieczniejszych haseł.

Część 1: Poznaj techniki tworzenia silnego hasła.

Część 2: Zapoznaj się z tajnikami bezpiecznego przechowywania haseł.

1. Scenariusz

Hasła są stosowane na szeroką skalę w celu kontrolowania dostępu do różnych zasobów. Atakujący wykorzystają różne techniki w celu zdobycia haseł użytkowników, co pozwoli im uzyskać nieuprawniony dostęp do zasobów i danych.

W celu lepszego zabezpieczenia się ważne jest właściwe zrozumienie zasad tworzenia silnych haseł i sposobów bezpiecznego ich przechowywania.

1. Wymagane zasoby

* Komputer lub urządzenie mobilne z dostępem do Internetu

1. Tworzenie silnego hasła

Silne hasła muszą spełniać cztery wymogi, wymienione w kolejności od najważniejszego:

* + - 1. Użytkownik powinien móc łatwo zapamiętać hasło.
      2. Hasło nie może być proste, musi być trudne do odgadnięcia.
      3. Nie może być również proste do zgadnięcia przez specjalne programy służące do łamania haseł.
      4. Hasło musi być złożone i zawierać: liczby, symbole oraz kombinację wielkich i małych liter.

W powyższej liście pierwszy z wymogów wydaje się najważniejszy, ponieważ podstawą jest możliwość zapamiętania hasła. Na przykład hasło **# 4ssFrX ^ -aartPOknx25\_70! XAdk <d!** jest uważane za silne (spełnia trzy ostatnie wymagania), choć niezwykle trudne do zapamiętania.

W wielu systemach wymagane są hasła zawierające kombinację cyfr, symboli oraz małych i wielkich liter. Hasła zgodne z tymi wymogami są dobre, o ile tylko użytkownik nie ma problemu z ich zapamiętaniem. Oto przykładowy często spotykany zestaw reguł tworzenia hasła:

* Hasło musi mieć co najmniej 8 znaków
* Hasło musi zawierać wielkie i małe litery
* Hasło musi zawierać cyfrę
* Hasło musi zawierać znak specjalny (np. #, $, @, &)

Poświęć teraz chwilę, aby przeanalizować cechy charakterystyczne silnych haseł oraz powyżej przedstawiony zestaw reguł. Jak myślisz, dlaczego zestaw reguł często pomija dwa pierwsze elementy? Postaraj się wyjaśnić. Wyjaśnij.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dobrym sposobem na tworzenie silnych haseł jest wybieranie czterech lub więcej losowych słów i łączenie ich razem. Hasło **telewizjażababutykościół** jest silniejsze niż **J0ann@#81** Zauważ, że chociaż drugie z nich jest zgodne z wszystkimi wymienionymi wyżej zasadami, to jednak programy do łamania haseł są bardzo skuteczne w odgadywaniu haseł tego typu. Mimo, że wiele zestawów reguł dotyczących haseł nie zaakceptowałoby tego pierwszego, to jednak hasło **telewizjażababutykościół** jest znacznie silniejsze od drugiego. Jest łatwiejsze do zapamiętania (szczególnie w skojarzeniu z konkretnym wyobrażeniem lub obrazem), jest bardzo długie, a brak oczywistego powiązania ze sobą składających się na niego wyrazów utrudnia złamanie lub zgadnięcie.

Skorzystaj z internetowego narzędzia do tworzenia haseł i utwórz hasła opierając się na podstawie opisanego wyżej zestawu reguł.

* + 1. Otwórz przeglądarkę internetową i przejdź do <http://passwordsgenerator.net>
    2. Ustaw opcje zgodnie z zestawem reguł tworzenia haseł.
    3. Wygeneruj hasło.

Czy wygenerowane hasło jest łatwe do zapamiętania?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Skorzystaj z internetowego narzędzia do tworzenia haseł i utwórz hasła złożone z przypadkowej kombinacji słów. Zwróć uwagę, że połączenie wielu słów w jedno powoduje, że poszczególne części nie są traktowane jako wyrazy ze słownika.

* + 1. Otwórz przeglądarkę internetową i przejdź do <http://preshing.com/20110811/xkcd-password-generator/>
    2. Wygeneruj hasło składające się z przypadkowych słów poprzez kliknięcie w **Generate Another!** w górnej części strony.
    3. Czy wygenerowane hasło jest łatwe do zapamiętania?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Bezpieczne przechowywanie haseł

Użycie menedżera haseł powoduje, że pierwszą regułę silnego hasła można pominąć, ponieważ użytkownik ma zawsze dostęp do menedżera haseł. Zauważ, że niektórzy użytkownicy mają zaufanie tylko do tych haseł, które sami mogą zapamiętać. Każdy menedżer haseł musi je przechowywać w „magazynie", co daje możliwość dokonania ich kradzieży.

"Magazyn" haseł musi być silnie zaszyfrowany, a dostęp do niego musi być ściśle kontrolowany. Dzięki aplikacjom mobilnym i interfejsom sieciowym menedżer haseł dostępny w chmurze jest zawsze dostępny dla użytkowników.

Popularnym menedżerem haseł jest LastPass.

Utwórz testowe konto LastPass:

* + 1. Otwórz przeglądarkę internetową i przejdź do <https://lastpass.com/>
    2. Kliknij **Start Trial**, aby utworzyć konto testowe.
    3. Wypełnij pola zgodnie z instrukcjami.
    4. Ustaw główne hasło. To hasło będzie zapewniać dostęp do Twojego konta LastPass.
    5. Pobierz i zainstaluj aplikację kliencką LastPass dla swojego systemu operacyjnego.
    6. Otwórz aplikację kliencką i zaloguj się za pomocą hasła głównego LastPass.
    7. Poznaj menadżera haseł LastPass testując różne funkcje.

Jak myślisz, gdy dodajesz hasła do LastPass, gdzie są one zapisywane?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Oprócz Ciebie przynajmniej jeden inny podmiot ma dostęp do Twoich haseł. Kim jest ten podmiot?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Przechowywanie wszystkich haseł w jednym miejscu może być wygodne, jednak istnieją wady takiego rozwiązania. Czy jesteś w stanie wymienić te wady?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Czym jest zatem silne hasło?

Korzystając z cech silnego hasła podanych na początku tego ćwiczenia, wybierz hasło, które jest łatwe do zapamiętania, lecz trudne do odgadnięcia. Złożone hasła są w porządku, o ile nie wpływają negatywnie na spełnienie ważniejszych reguł, np. wymogu ich łatwego zapamiętywania.

Używając menedżera haseł możesz nie martwić się o to, czy hasło jest łatwe do zapamiętania.

Poniżej znajduje się krótkie podsumowanie:

Wybierz hasło, które jesteś w stanie zapamiętać.

Wybierz hasło, którego nikt nie skojarzy z Twoją osobą.

Stwórz różne hasła i nigdy nie używaj tego samego hasła do różnych usług.

Złożone hasła są w porządku, o ile nie utrudniają ich zapamiętania.