

## Ćwiczenie – Tworzenie i przechowywanie silnych haseł (Wersja dla nauczyciela)

**Informacja dla instruktora:** Fragmenty tekstu oznaczone czcionką czerwoną lub podświetlone na szaro są dostępne wyłącznie w wersji dokumentu dla instruktora.

### Zadania

Poznaj tajniki najbezpieczniejszych haseł.

**Część 1: Poznaj techniki stojące za stworzeniem silnego hasła.**

**Część 2: Zapoznaj się z tajnikami bezpiecznego przechowywania haseł.**

### Wprowadzenie

Hasła są stosowane na szeroką skalę w celu kontrolowania dostępu do różnych zasobów. Atakujący wykorzystują 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.

### Wymagane zasoby

- Komputer lub urządzenie mobilne z dostępem do Internetu

### Część1 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 zbyt proste do odgadnięcia.
- 3) Nie może być proste do zgadnięcia przez specjalne programy komputerowe.
- 4) Hasło musi być złożone, musi zawierać cyfry, symbole i kombinacje 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:

- Długość hasła musi wynosić przynajmniej 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.

---

---

---

---

---

Dodawanie symboli, cyfr oraz mieszanie wielkich i małych liter utrudnia użytkownikowi zapamiętanie go. Zazwyczaj użytkownik, który wymyśli hasło zgodne z obowiązującym powszechnie zestawem zasad, będzie skłonny używać tego samego sposobu konstrukcji lub nawet całego hasła podczas każdorazowej rejestracji. Niektóre systemy zmuszają użytkownika do okresowej zmiany hasła, co powoduje, że użytkownicy używają haseł z przeszłości. Użytkownicy często wprowadzają drobne modyfikacje hasła zamiast stworzyć całkowicie nowe, co jednak w świetle obowiązujących zasad jest poprawne.

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.

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

Czy wygenerowane hasło jest łatwe do zapamiętania?

---

---

Odpowiedzi mogą być różne. Ale jest bardzo prawdopodobne, że wygenerowane hasło nie 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.

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

---

---

Odpowiedzi mogą być różne. Jest bardzo prawdopodobne, że wygenerowane hasło będzie łatwe do zapamiętania.

## Część2 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 powinien być ściśle kontrolowany. Dzięki aplikacjom na telefony komórkowe i interfejsom sieciowym, menedżer haseł w chmurze zapewnia nieprzerwany dostęp do usług.

Popularnym menedżerem haseł jest LastPass.

Utwórz testowe konto LastPass:

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

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

---

Hasła są przechowywane w chmurze na serwerach firmy LastPass.

Poza tobą przynajmniej jeden inny podmiot ma dostęp do twoich haseł. Kim jest ten podmiot?

---

LastPass

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

---

Odpowiedzi mogą być różne. Serwery firmy LastPass są atrakcyjnym celem dla atakujących, ponieważ zawierają hasła wielu użytkowników. Odpowiedzialność za przechowywanie haseł zostaje przekazana firmie zewnętrznej. To powoduje, że nie masz żadnej kontroli nad stosowanymi zabezpieczeniami. Decydujesz się zaufać tej firmie oraz ich działaniom w zakresie ochrony haseł. Pamiętaj jednak, że nie masz żadnej gwarancji, że Twoje hasła są bezpieczne.

## Część3 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 możesz zapamiętać.

## Ćwiczenie – Stwórz i przechowuj silne hasła

---

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.