COURSEWARE

Passwords

Contents

- [Overview](#)
- [Weak Passwords](#)
- [Strong Passwords](#)
- [Storing Passwords](#)
- [Tutorial](#)
- [Exercises](#)

Overview

What makes a good password? What should we do when storing passwords? These questions will be answered in this module.

Weak Passwords

The strength of a password is left to interpretation for the most part. Some believe it's secure enough to have more than 8 characters, a number and special character.
Some don't even go that far.
But the characteristics of a weak password are:

- Common Passwords e.g. password, root
- Common Combinations e.g. 123
- Personal inclusions e.g. A Loved one's name, Date of Birth
- Short password e.g. dog
- One type of character, whether that be numbers, letter or special characters
- Common words and phrases e.g. ILoveFootball

Strong Passwords

A strong password consists of a balance between security and accessibility.
What is the point of a password being so secure it is impossible to remember?
For example: eoisjcmeioce£$%"££"£$£344522e2e34cfdmle$ is a very secure password.
But unless you keep that password stored somewhere, you will never be able to remember this password to access your account.

So what should a password be?
A good strong password normally contains the following:

- 4 unrelated words
- At least 1 special character
- At least 1 number

For example: eggf00tballwirespeaker!

This is a good strong password and is a lot more rememberable.

Storing Passwords

Sometimes you may need to store peoples passwords and it's important that you do this securely so that anyone authorised to access your users' information, still cannot see passwords.
The password should only be known by the user themselves.

To make this possible you will need to hash any passwords before storing them.

Tutorial

There is no tutorial for this module.

Exercises

Go here and try entering some passwords you think are weak or strong. To see how long it would take for a password attack to gain access.