Authentication

Class 37

- universally, systems use username - password pairs for authentication and login
- someday that will change, but not yet

- two big criteria
  - usernames must be unique
  - passwords must be secure
- these are usually stored in a database

```
create table user
(
  username varchar(255) not null,
  password varchar(255) not null,
  first_name varchar(255) not null,
  last_name varchar(255) not null,
  phonenumber varchar(255) not null,
  key(username)
);
```

Passwords

- it's easy to write code to ensure that passwords are long enough, contain characters of multiple types, etc.
- but the one unbreakable rule is that actual passwords must never be stored on the server

- this is accomplished with a pair of PHP functions:

password_hash() takes a cleartext password as input and returns a (currently) 60-character one-way encrypted version of the input

password_verify() takes a cleartext password and a previously generated hash and returns true or false depending on whether the password matches the hash