

PHP, MVC, SQL

# PHP

- PHP Hypertext Preprocessor
- server-side scripting language
- backend & logical underpinnings of our website

# PHP Syntax

- must start with `<?php` and end with `?>`

```
<?php
```

```
    // code goes here
```

```
?>
```

# PHP variables

- start with \$
- loosely typed
  - ▣ That doesn't mean that there aren't types - you just don't declare them!
- global scope (except for functions)
  - ▣ loops don't limit the scope of variables

```
<?php
```

```
    $number_int = 1;
```

```
    $number_string = "1";
```

```
    $number_float = 1.0;
```

```
?>
```

loops and conditions: if

```
if ($name == "Harry")  
{  
    printf("Yer a wizard!");  
}
```

loops and conditions: while

```
while ($voldy == false)
{
    printf("All was well");
}
```

loops and conditions: for

```
for ($i = 0; $i <= 8; $i++)  
{  
    submitPset($i);  
}
```

loops and conditions: for

```
$psets = [0, 1, 2, 3, 4, 5, 6, 7, 8];
```

```
foreach ($psets as $pset_i)
```

```
{
```

```
    submitPset($pset_i);
```

```
}
```



# arrays

indices	0	1	2	...
values	1	2	12	...

```
$my_list = [];  
$my_list[0] = 1;  
$my_list[1] = 2;  
$my_list[2] = 12;  
...
```

# associative arrays

indices	"cats"	"owls"	"dogs"	...
values	1	2	12	...

```
$my_list = [];  
$my_list["cats"] = 1;  
$my_list["owls"] = 2;  
$my_list["dogs"] = 12;  
...
```

# string concatenation: . operator

```
<?php
    $first = "Milo";
    $last = "Banana";

    $fullname = $first . " " . $last;

    // prints "Milo Banana"
    echo $fullname;
?>
```

# useful PHP functions

`require(filename.php)`

- includes PHP code from the specified file and evaluates it

`echo`

`exit`

`empty`

# PHP and HTML

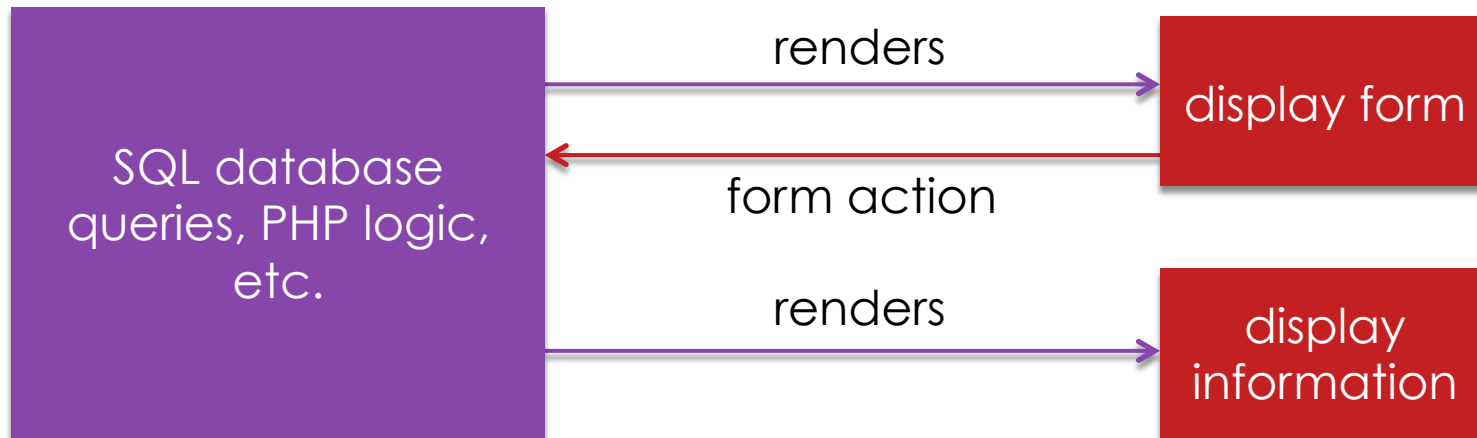
- PHP gives us the power to alter a page's HTML prior to loading, based on different conditions

```
<?= "Hello, " . $name . "! " ?>
```

# MVC

- Model
  - ▣ interactions with database
- View
  - ▣ aesthetics of the website
- Controller
  - ▣ handles user requests; passes data
- paradigm for organizing code

# MVC



# render

public/hello.php

```
render("hello.php",  
  ["msg" => "Who's a good boy?",  
   "name" => "Milo"]);
```

templates/hello.php

```
<p>  
  <?= htmlspecialchars($msg) ?>  
  <?= htmlspecialchars($name) ?> is!  
</p>
```



# render

public/hello.php

```
render("hello.php",  
  ["msg" => "Who's a good boy?",  
   "name" => "Milo"]);
```

templates/hello.php

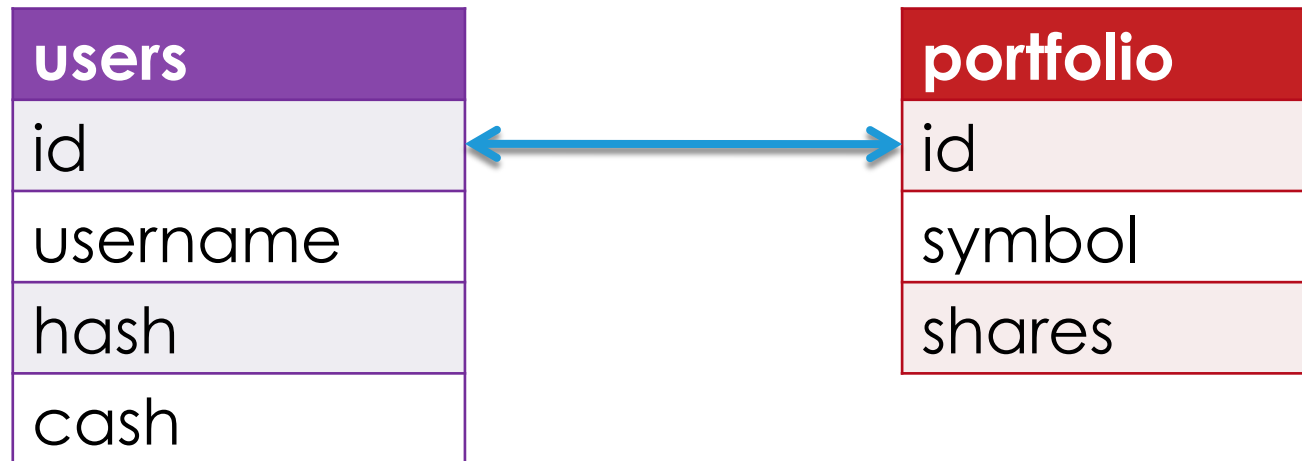
```
<p>  
  Who's a good boy?  
  Milo is!  
</p>
```

# SQL

- Structured Query Language
- programming language designed for managing databases

# why SQL?

- easy way to track and manage objects



how?

SELECT

INSERT

UPDATE

DELETE

# SELECT

```
SELECT * FROM wizards WHERE house = "Ravenclaw";
```

# query

- ? is a placeholder

```
$rows = query("SELECT * FROM wizards WHERE house = ?", $curr_house);  
if ($rows === false)  
{  
    apologize("Query failed");  
}
```

# SELECT

- query returns an array of rows

```
foreach ($rows as $row)
{
    print("<tr>");
    print("<td>{$row["Name"]}</td>");
    print("<td>{$row["Year"]}</td>");
    print("<td>{$row["House"]}</td>");
    print("</tr>");
}
```

# INSERT

```
INSERT INTO wizards (name, year, house)
VALUES("zamyła", 7, "Ravencław")
```

```
INSERT INTO gringotts (id, galleons)
VALUES(1, 500) ON DUPLICATE KEY UPDATE
galleons = galleons + VALUES(galleons)
```



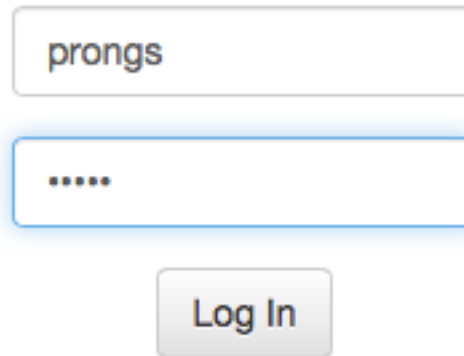
# UPDATE, DELETE

```
UPDATE gringotts SET galleons = galleons - 5  
WHERE id = 1
```

```
DELETE FROM gringotts WHERE id = 1
```

# SQL Injection Attack

```
$username = $_POST["username"];  
$password = $_POST["password"];  
$rows = query("SELECT * FROM users WHERE username='$username'  
AND password='$password'");
```



A login form consisting of two input fields and a button. The top input field contains the text "prongs". The bottom input field contains five dots, representing a password. Below the input fields is a button labeled "Log In".

# SQL Injection Attack

```
$username = $_POST["username"];  
$password = $_POST["password"];  
$rows = query("SELECT * FROM users WHERE username='$username'  
AND password='$password'");
```

prongs

lily' OR '1' = '1

Log In

```
SELECT * FROM users WHERE username='prongs'  
AND password='lily' OR '1' = '1'
```