Notes ITC 240 May 13 2014

1. Prepared statements
2. Escaping SQL
3. Whitelisting

http://itc240.no-ip.org/~twilburn/itc240-2014/in-class/051314/addAnimal.php

Include must come before the variable

<?php

Include (“passwords.php”);

$mysql = new mysqli(“localhost”, “pbarke01”,”$mysql\_password”, “pbarke01”);

$result = $mysql-> query(‘SELECT \* FROM animals’);

echo “<pre>”;

foreach ($result as $row){

print\_r ($row);

}

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

<?php

Include (“passwords.php”);

$mysql = new mysqli(“localhost”, “pbarke01”,”$mysql\_password”, “pbarke01”);

$query = ‘SELECT \* FROM animals WHERE legs = ?’; //one question mark ..you can do more ….. ***AND WHERE carnivore = ?***

$prepared =$ mysql ->prepare ($query);

$legs = 4; //*normally this would come from some user input $\_REQUEST[“legs”]*

$prepared->bind\_param(“I”, $legs)

$prepared->execute();

$result = $prepared->get\_result();

***Can’t use a question mark to see a table or a column.***

[**www.php.net/manual/en/mysqli-stmt.bind-param.php**](http://www.php.net/manual/en/mysqli-stmt.bind-param.php)

**~~~~~~~~~~~~~~~~**

* **create column link to ? update=id**
* **SELECT \* row by id**
* **Fill form with result**
* **Add hidden input for id**
* **Change the row instead of inserting it UPDATE ///Once I post it…what do I do that’s different?**