```
$value = strip_tags($value); // Strips html and PHP tags
        if (get_magic_quotes_gpc())
        {
                $value = stripslashes($value); // Gets rid of unwanted quotes
        }
return $value;
}
if ((isset($_POST['dog_name'])) && (isset($_POST['dog_breed'])) && (isset($_POST['dog_
color'])) && (isset($_POST['dog_weight'])))
{
$dog_name = clean_input($_POST['dog_name']);
$dog_breed = clean_input($_POST['dog_breed']);
$dog_color = clean_input($_POST['dog_color']);
$dog_weight = clean_input($_POST['dog_weight']);
$lab = new Dog($dog_name,$dog_breed,$dog_color,$dog_weight);
list($name_error, $breed_error, $color_error, $weight_error) = explode(',', $lab);
...
```

For more information on the PHP function `isset`*, visit*

Examples: *http://php.net/manual/en/function.isset.php*

Videos: *https://www.thenewboston.com/videos.php?cat=11&video=17087*

For more information on $_POST, visit

Examples: *http://php.net/manual/en/reserved.variables.post.php*

Videos: *https://www.thenewboston.com/videos.php?cat=11&video=17087*

At the top of `lab.php`, you are adding several items to provide more secure code.

```
if ((isset($_POST['dog_name'])) && (isset($_POST['dog_breed'])) &&
(isset($_POST['dog_color'])) && (isset($_POST['dog_weight'])))
```

This `if` statement uses the `isset` method and `$_POST` to verify that all four properties (`dog_name`, `dog_breed`, `dog_color`, and `dog_weight`) have been passed into the program with the `POST` method. If all items have been passed, you then will filter (clean) those items. If any of them have not been passed, an `else` statement (that you will look at later) will request the user go back to the `lab.html` page to enter all needed information.

```
$dog_name = clean_input($_POST['dog_name']);
Each property is passed to the clean_input method (after it has been retrieved using the
$_POST method) to remove harmful tags. In this example, the $dog_name property (on the left
side of the = sign) will receive the cleaned information.
function clean_input($value)
{
$bad_chars = array("{", "}", "(", ")", ";", ":", "<", ">", "/", "$");
$value = str_ireplace($bad_chars,"",$value);
$value = strip_tags($value); // Strips html and PHP tags
$value = htmlentities($value); // Removes any html from the string and turns it into &lt; format
```