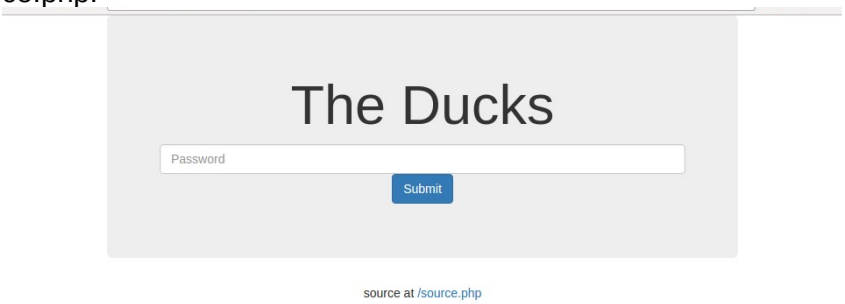
PHP overwrite

Problem: Submit the correct password.
Hint: send a POST variable
Given: index.php

Note: extract() is a vulnerable function in PHP, more information can be found here
http://stackoverflow.com/questions/829407/what-is-so-wrong-with-extract

Steps:
1) Open the page. We see that only a password can be entered. Notice that below the entry box is a link to /source.php.



2) Following the link will display the source code without the variable values. Search through the code and try to notice if anything can be exploited.

After searching through the code and using the hint, we can see a suspicious section of PHP code.

```
<?php if ($_SERVER["REQUEST_METHOD"] == "POST") { ?>
        <?php
        extract($_POST);
        if ($pass == $thepassword_123) { ?>
        <div class="alert alert-success">
                <code><?php echo $theflag; ?></code>
        </div>
        <?php } ?>
<?php } ?>
```

Note: There are two common methods for a HTTP request-response between the client and sever.
GET – Requests data from a specified source
POST – Submits data to be processed to a specific resource
More information on HTTP methods can be found here
http://www.w3schools.com/TAGS/ref_httpmethods.asp

This section of code uses PHP's extract function and a POST method for a request-response between the client and sever.

3) The extract function in PHP is vulnerable and can be used to overwrite other variables. In the case of this problem, we want to use the extract function and a POST request to overwrite the password for the system. This can be accomplished by using wget.

4) Use a wget command with a few options to overwrite the password variable with a value of our choosing.

Note: wget is used to retrieve content from web servers. Information on the options of wget can be found here http://www.computerhope.com/unix/wget.htm

We want to sent a POST data request, so we set the pass variable and thepassword_123 to both be abc. Enter into the terminal

sending two things to post data screenshot from terminal

wget -qO- --post-data="pass=abc&thepassword_123=abc" http://127.0.0.1:10800/