CS380 Exercise 6

Programmer: David Shin

Github URL: www.github.com/davidws22/CS380-EX6

1. Logging in as ‘ted’ without providing password field

Input: ted’);#

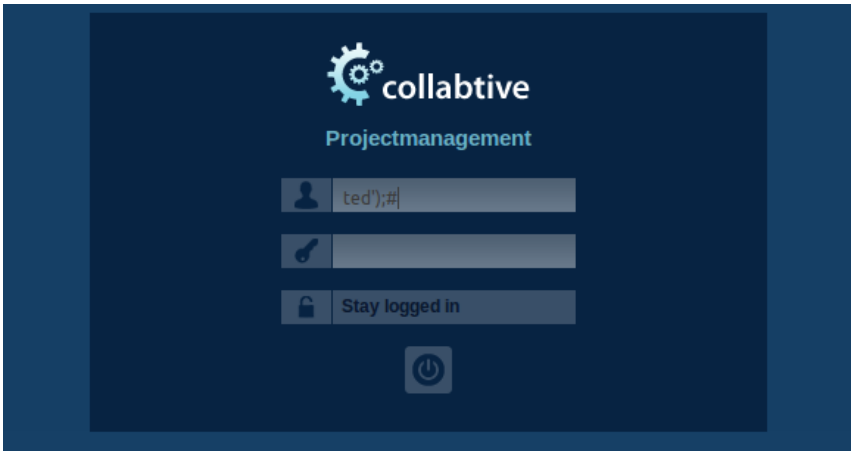
$sel1 = mysql_query(

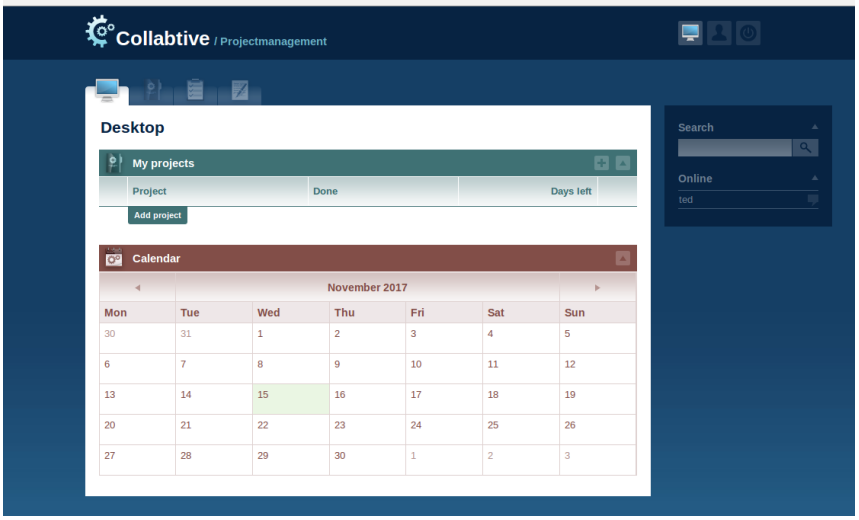
"SELECT ID, name, locale, lastlogin, gender

FROM USERS_TABLE

WHERE (name = ’$user’ OR email = ’$user’) AND pass = ’$pass’");

This works because our input would force the SQL interpreter to end the query early, and completely bypass the password field with the ‘#’ symbol, which is recognized as the beginning of a comment in php.

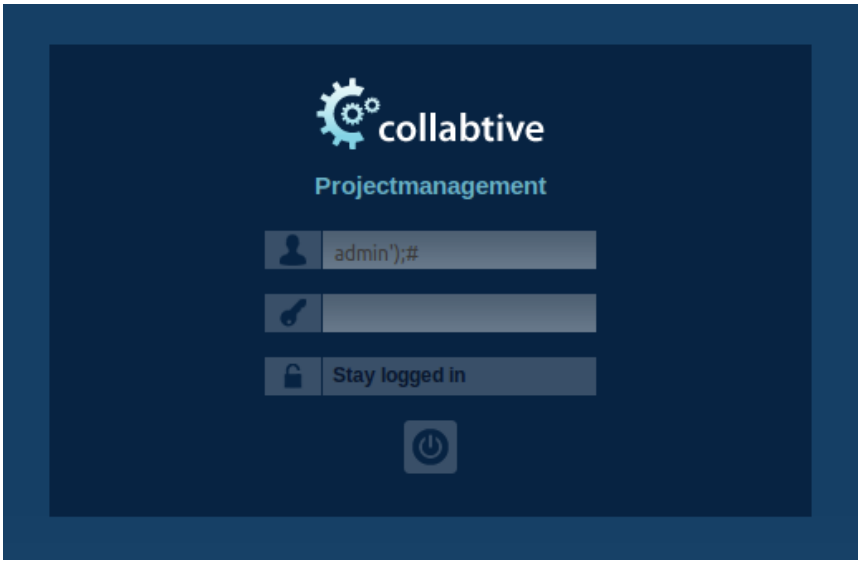


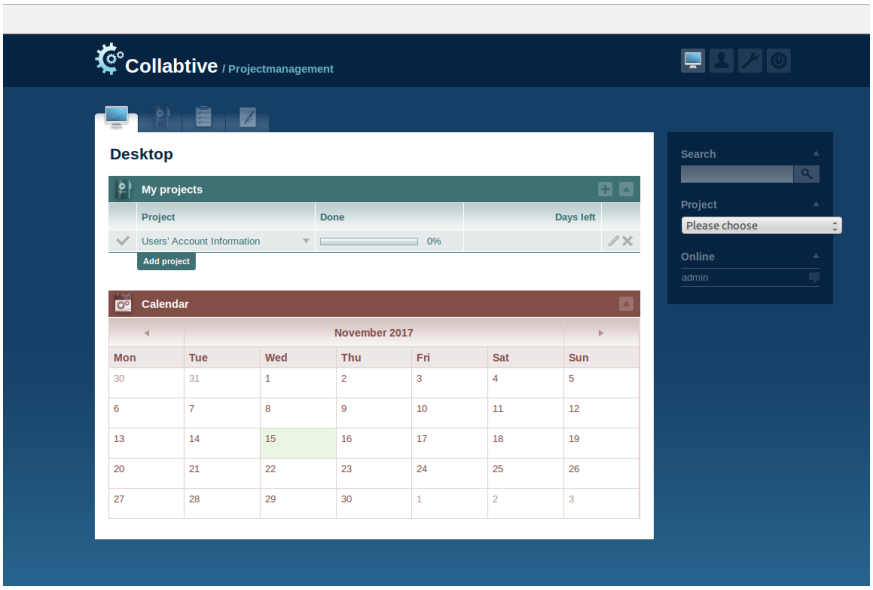


2. Logging in as ‘admin’ without providing password field

Input: admin’);#

The same logic from the previous example still applies, even if admin is the new username.





3. Logging in with a blank username (i.e., the user name in the query is considered blank but the user field in the login form is not necessarily blank).

Input: ‘ OR name = name);#

The reason why this works is because OR is a binary operator, and by having one expression equate to true, we are granted access by a successful SQL query. We can apply the same logic for examples 1 and 2 when we terminate the SQL query early with the sequence of);# characters.

After executing this command, the website thinks the user ‘admin’ is logged in.