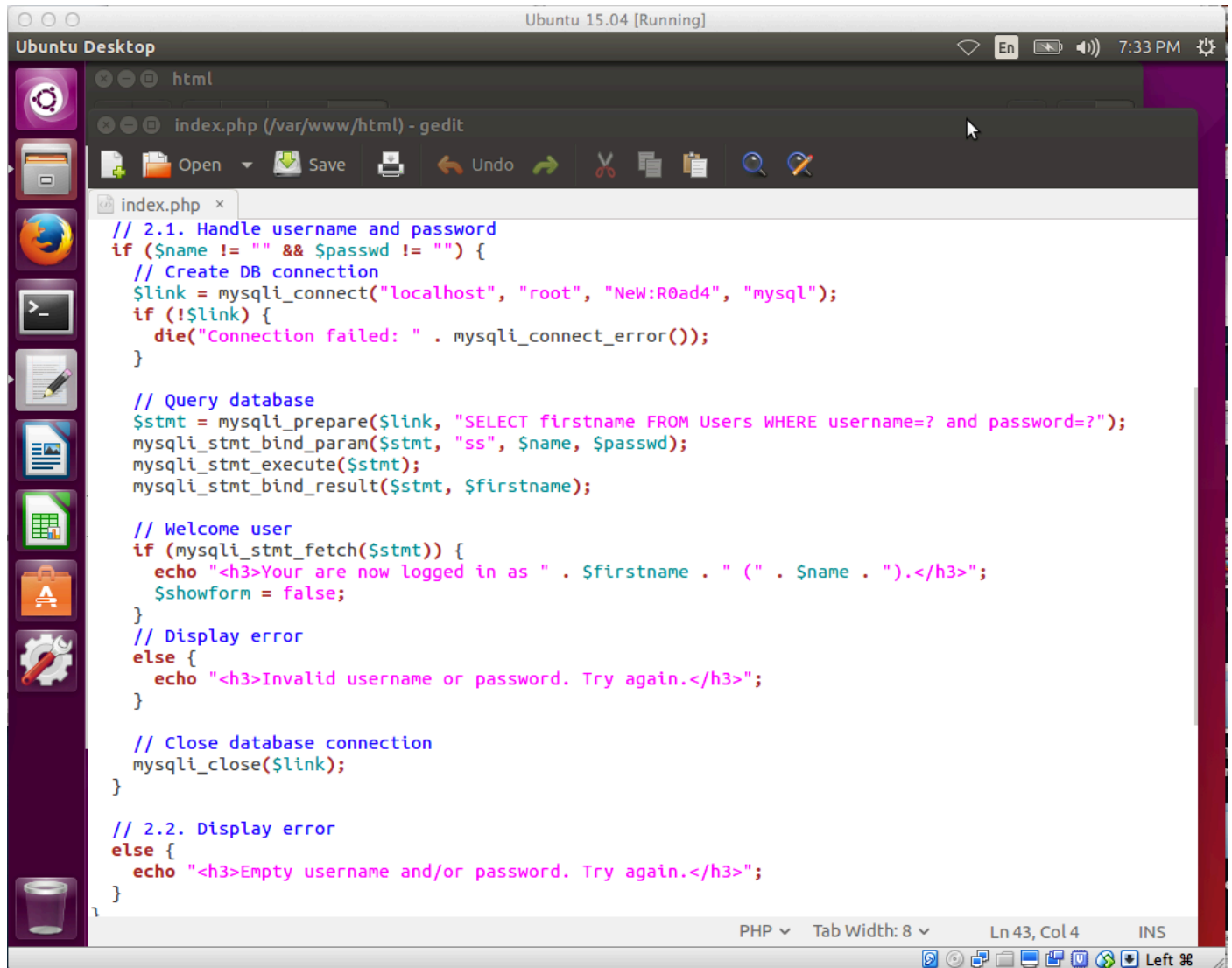


Exercise 8

Username: foo' or '1'='1

Password: bar' or '1'='1

Exercise 9



The screenshot shows an Ubuntu 15.04 desktop environment. A gedit text editor window is open, editing a file named 'index.php' located at '/var/www/html'. The script is a PHP file that handles user login. It starts with a comment '// 2.1. Handle username and password' and checks if the username and password are not empty. If they are, it attempts to connect to a MySQL database on localhost with the username 'root' and password 'New:R0ad4'. If the connection fails, it dies with an error message. If successful, it prepares a SQL query to select the first name from the 'Users' table where the username and password match the provided values. It then fetches the result and displays a welcome message. If the connection fails or the query returns no results, it displays an error message. The script ends with a comment '// 2.2. Display error' and an echo statement that displays an error message if the username or password is empty.

```
// 2.1. Handle username and password
if ($name != "" && $passwd != "") {
    // Create DB connection
    $link = mysqli_connect("localhost", "root", "New:R0ad4", "mysql");
    if (!$link) {
        die("Connection failed: " . mysqli_connect_error());
    }

    // Query database
    $stmt = mysqli_prepare($link, "SELECT firstname FROM Users WHERE username=? and password=?");
    mysqli_stmt_bind_param($stmt, "ss", $name, $passwd);
    mysqli_stmt_execute($stmt);
    mysqli_stmt_bind_result($stmt, $firstname);

    // Welcome user
    if (mysqli_stmt_fetch($stmt)) {
        echo "<h3>Your are now logged in as " . $firstname . " (" . $name . ").</h3>";
        $showform = false;
    }
    // Display error
    else {
        echo "<h3>Invalid username or password. Try again.</h3>";
    }

    // Close database connection
    mysqli_close($link);
}

// 2.2. Display error
else {
    echo "<h3>Empty username and/or password. Try again.</h3>";
}
```