To define the credentials for accessing your onedev.io repository, you can use the Jenkins Credentials plugin to securely store and retrieve the necessary credentials. Here's an example of how you can define the credentials:

1**. In Jenkins, go to the dashboard and click on "Credentials" in the sidebar.**

**2. Click on "Global credentials (unrestricted)" or "System" depending on your Jenkins configuration.**

**3. Click on "Add Credentials" to create a new set of credentials.**

**4. Choose the appropriate credential type for your onedev.io repository. For example, if you're using SSH key-based authentication, select "SSH Username with private key" or if you're using a username and password, select "Username with password".**

**5. Fill in the necessary details based on your authentication method:**

**- For SSH key-based authentication:**

**- Username: Your onedev.io username or the username associated with the SSH key.**

**- Private Key: Select "Enter directly" and paste your private key.**

**- Passphrase: If your private key is encrypted with a passphrase, enter it here.**

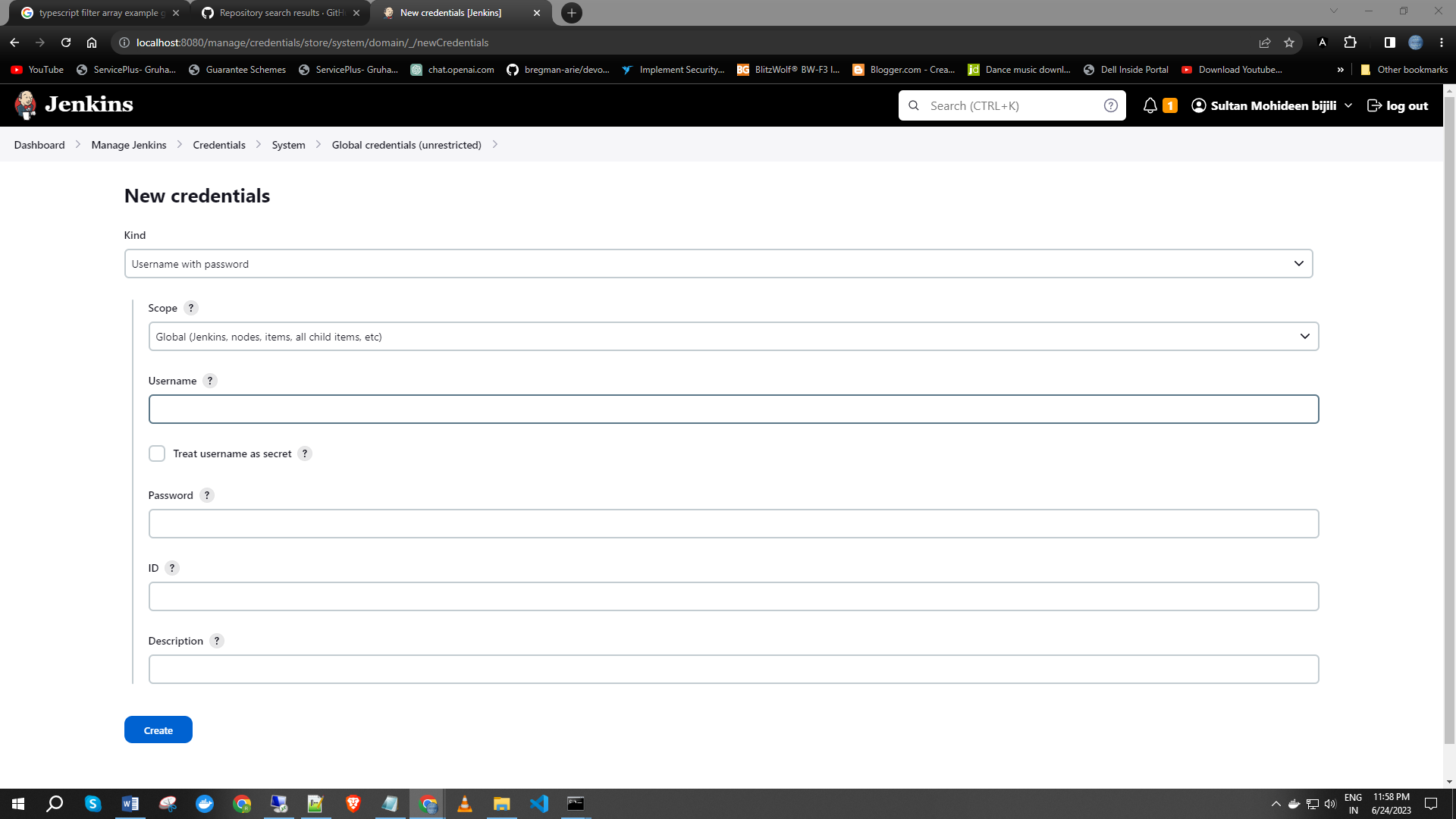
**- For username and password authentication:**

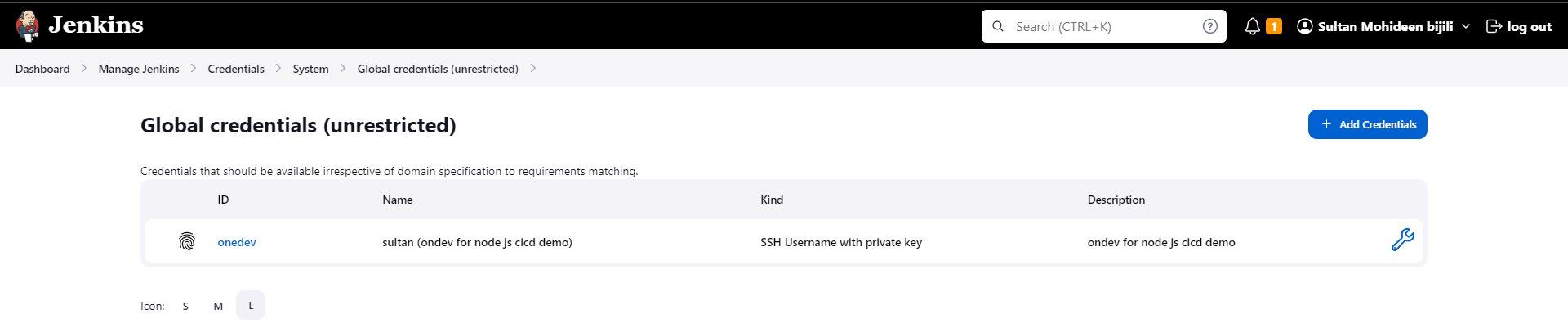
**- Username: Your onedev.io username.**

**- Password: Your onedev.io password.**

**6. Give your credentials a meaningful ID, such as "onedev-credentials", and optionally provide a description.**

7. Click on "OK" to save the credentials.





In the Jenkins pipeline script mentioned earlier, you would replace `'your-credentials-id'` with the ID you provided for the onedev.io repository credentials.