Arbitrary object injection in PHP

1. This lab uses a serialization-based session mechanism and is vulnerable to arbitrary object injection as a result. You will need to obtain source code access to solve this lab.
2. While browsing the website, I didn't find any interesting things except the serialized object in session in cookie, but still I can't use it to solve the lab.
3. In page source, I found interested end point as a comment:

```
  </section>
  <!-- TODO: Refactor once /libs/CustomTemplate.php is updated --
div>
```

   I tried to navigate to this end point, but the response is an empty page.
4. From the lab's hint, I noticed that if I append tilde symbol (**~**) to the file name, I can read the content of the file. I do it and already the content of the file appeared. It is a php code that contains a class with some properties. The interesting thing is that the **destruct** function. The body of this function is unlinking the file that is stored in the **lock_file_path**. Unlinking means deleting the file.
5. The mission is to create a new object that contains the value of the lock_file_path, while deserializing this object, the destruct called by default. So, the file will be deleted.
6. I created this object:
   `O:14:"CustomTemplate":1:{s:14:"lock_file_path";s:23:"/home/carlos/morale.txt";}`
   and encode it then replace it with the session value in the request then sent it.
7. The file unlinked successfully and the lab solved.