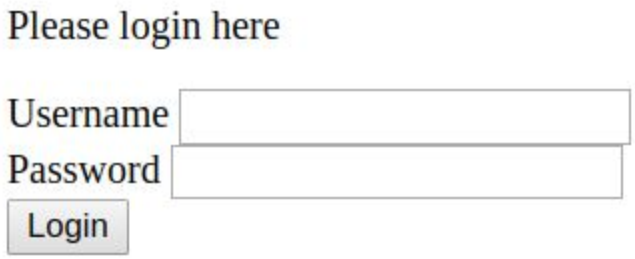
WEB: Das Blog

The webpage looks like the following:

We can then go into the login page.



If we insert "*test"* in the username and password, we receive the following message:

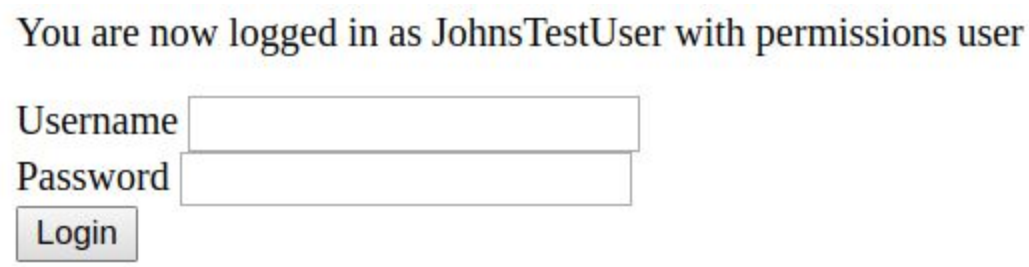
> *Sorry, That Username / Password is incorrect.*

Let's inspect the page:

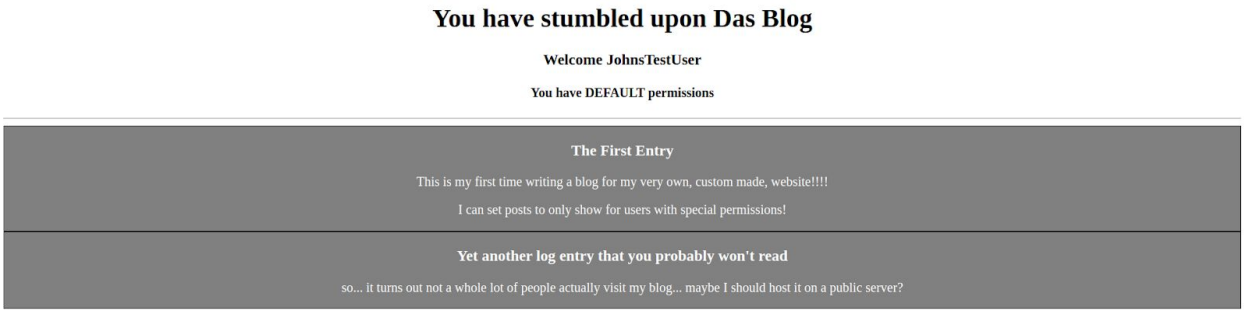
```
<!-- Development test account: user: JohnsTestUser, pass: AT3stAccountForT3sting -->
<!doctype html>
<html>
  <link type="text/css" id="dark-mode" rel="stylesheet" href(unknown)>
  <style type="text/css" id="dark-mode-custom-style"></style>
 ▼<head>
    <title>Das Blog Login page</title>
  </head>
..▼<body> == $0
    <p>Sorry, That Username / Password is incorrect.</p>
   ▼<form action="?" method="post">
      <label for="Username">Username</label>
      <input type="text" name="Username">
      <br>
      <label for="Password">Password</label>
      <input type="password" name="Password">
      <br>
      <input type="submit" name="submit" value="Login">
    </form>
  </body>
</html>
```

At the beginning, there is a suspicious line: maybe the programmers forgot to remove it …
We can try to insert the following credentials:

Username: JohnsTestUser
Password: AT3stAccountForT3sting

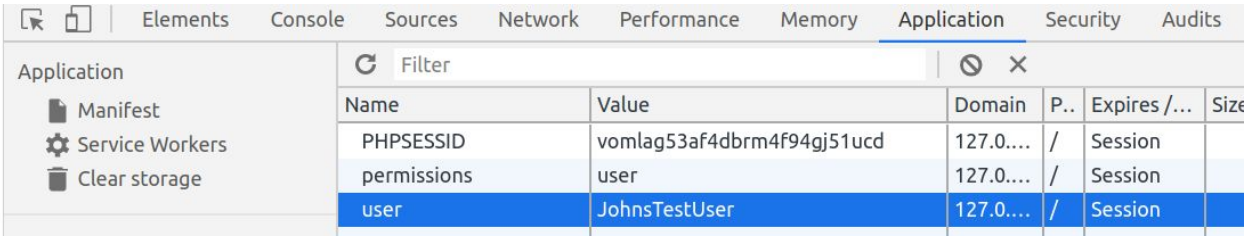


Great, we can try to go back to the home page and see the result.



It seems that we don’t have the permissions with this account to reach “sensible info”.

We need to find how permissions are handled, and we can try with the cookies. Cookies are under the “Application” section of our debugging tool.



By setting the permissions to “admin” we can reach the flag (after reloading the page).