

WEB: Das Blog

The webpage looks like the following:

You have stumbled upon Das Blog

You must [login](#) to view posts

We can then go into the login page.

Please login here

| | |
|--------------------------------------|--------------------------|
| Username | <input type="text"/> |
| Password | <input type="password"/> |
| <input type="button" value="Login"/> | |

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

You are now logged in as JohnsTestUser with permissions user

Username

Password

Login

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

You have stumbled upon Das Blog

Welcome JohnsTestUser

You have DEFAULT permissions

| The First Entry |
|---|
| <p>This is my first time writing a blog for my very own, custom made, website!!!!</p> <p>I can set posts to only show for users with special permissions!</p> |
| Yet another log entry that you probably won't read |
| <p>so... it turns out not a whole lot of people actually visit my blog... maybe I should host it on a public server?</p> |

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.

| Application | | | | | | |
|--|-------------|----------------------------|-----------|-----|--------------|------|
| Application <ul style="list-style-type: none">ManifestService WorkersClear storage | Filter | | | | | |
| | Name | Value | Domain | P.. | Expires /... | Size |
| | PHPSESSID | vomlag53af4dbrm4f94gj51ucd | 127.0.... | / | Session | |
| | permissions | user | 127.0.... | / | Session | |
| | user | JohnsTestUser | 127.0.... | / | Session | |

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

You have stumbled upon Das Blog

Welcome JohnsTestUser

You have ADMIN permissions

| |
|---|
| <p>The Key, Oh my, The Key</p> <p>I know this post is only available for admins, and since I am the only admin on the blog, I decided to start keeping my passwords on here for quick access. Everyone says that it isn't a good idea, but I don't care, nobody reads this blog anyway...</p> <p>• flag{C00ki3s_c4n_b33_ch4ng3d_?}</p> |
| <p>The First Entry</p> <p>This is my first time writing a blog for my very own, custom made, website!!!!</p> <p>I can set posts to only show for users with special permissions!</p> |
| <p>Yet another log entry that you probably won't read</p> <p>so... it turns out not a whole lot of people actually visit my blog... maybe I should host it on a public server?</p> |