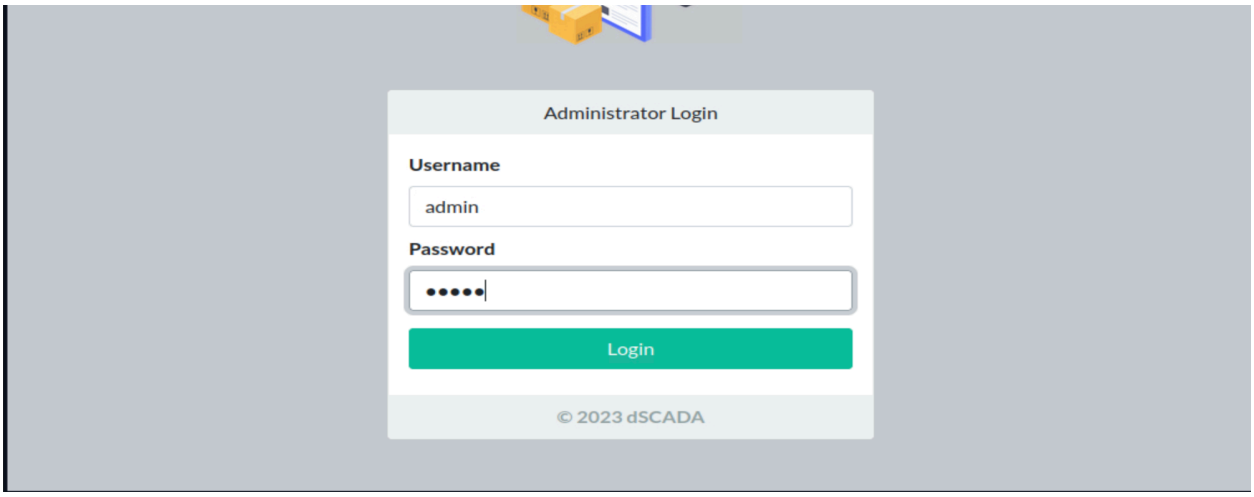
dSCADA Challenge

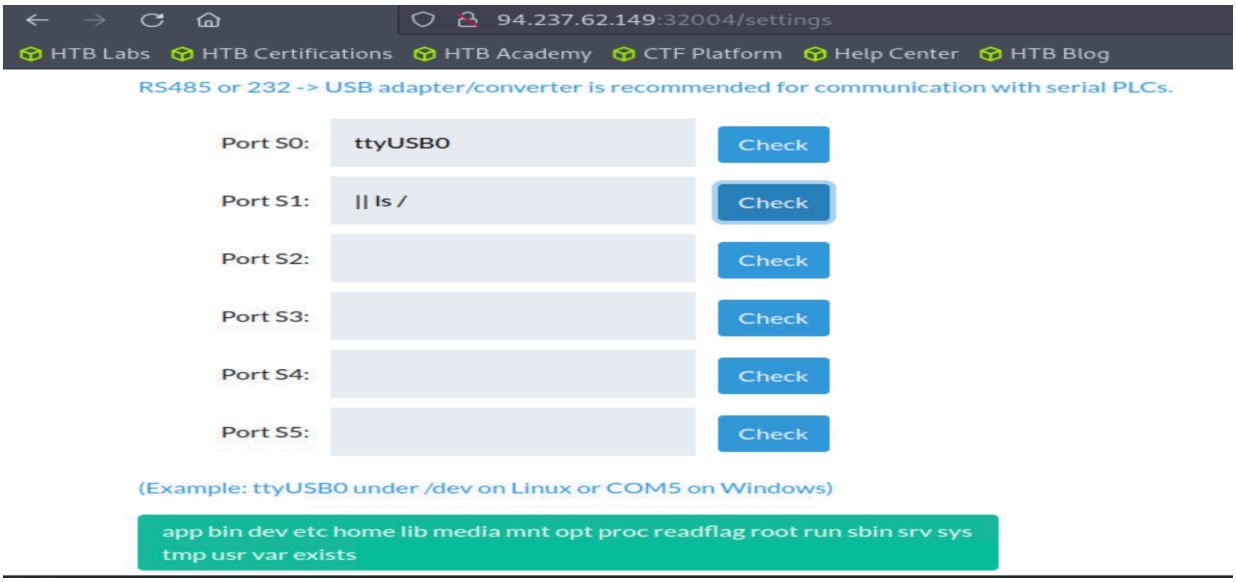
Step1: First visited http://94.237.62.195:31684/

Step2: Then tried few default credentials and logged in with credentials(admin: admin)



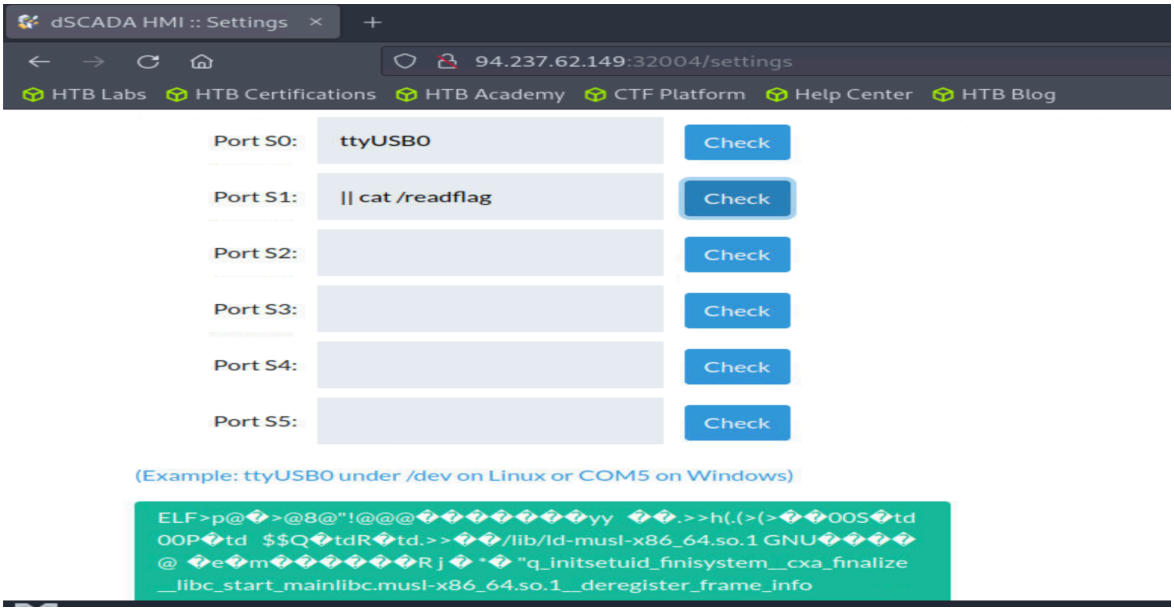
Step3: Then checked all the available user input fields and found command injection vulnerability with all user input fields in the 'serial settings'.

Step4: Then exploited files names using the following command - **|| ls /** as shown in the below.

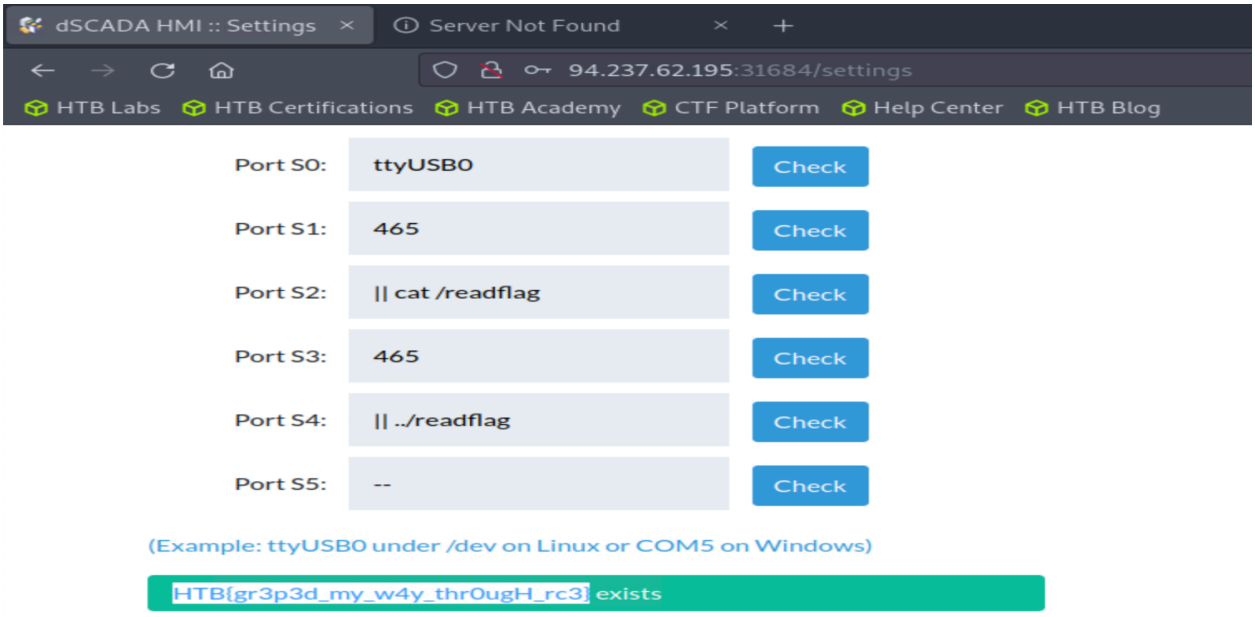


Step5: Found 'readflag' file in '/' directory.

Step6: First used **|| cat /readflag** but the content of the flag is uninterpretable but found that the file is ELF file type from the visible content.



Step7: Then checked the permissions of the file, if we have execute permission or not. And we do have permission to execute the file. Hence, executed the ELF file and got the flag as shown in the below.



Risk Mitigation Strategy:

We can mitigate week login credentials of 'dSCADA' by change the default credentials, and implementing strong password policies, two-factor authentication (2FA) and account lockout policies.

We can mitigate command injection vulnerabilities by sanitization or validation of the input user, using input whitelisting filter, providing less privileges to the file and using parameterized commands or by avoiding shell execution by user-controlled input.