Assignment 1 – IDATT2503

Task 1:

After making “name” executable and typing anything and adding %s behind, there occurs an segmentation fault. This is because the %s will try to modify the string literal. If I don’t write the %s, then the program proceeds and prints out what was written.

When looking at the code, the line “printf(local\_28);” should be the culprit. To fix the problem, the print function needs to be forced to print out as a string, like “printf(“%s”, local\_28);” should prevent the issue.

Task 2:

Flag 0 – The page numbers in the URL goes from 1,2 which already exist to 6 as the first new page created. When I tested the pages between, I found page 4 to be “restricted access” to. I changed the URL to .../page/edit/4, and the flag was displayed in the text field.

^FLAG^15700e4fd6309a224a017d0977cd8c523a2aa284e685356c8d574d6c9fc7fe22$FLAG$

Flag 1 – I proceeded to play around with the URL when editing a page. The edit address always expects a number at the end, so I tried replacing it with ‘, which then redirected me to a page with the flag.

^FLAG^a7ca3a95dc84c282d8796ab20a21aace41d2cdb6ef332a96efd860c675645b9a$FLAG$

Flag 2 – I created a new page with the alert() function, and the flag was not displayed after creation, but when the home page was displayed again. An alert box with the flag appeared. XSS injection with javascript.

^FLAG^d346bda8484f36a097568a2100c7c5a265923a30d4060e8d103e4373c81a2a48$FLAG$

Flag 3 – Tried doing the same thing as with flag 2, but in the description box. After testing around a bit, I found it possible to create my own html elements, such as buttons. I created a <p> tag with a <button onClick=flag> inside. In console, the flag was displayed.

^FLAG^a0d39da691fc0ca24af78680a82db403662db0d183ab3130fa4d275f2188e925$FLAG$