HackRush 2021 CTF Write-Up

Team - Navi
Members :-

- Inderjeet Singh Bhullar
- Harshvardhan Vala

Reverse Engineering

Challenge simple_check :

Solution - The source C code for simple_check was given. I opened the code and found that the flag was an input char array of size 50. There were many conditional statements in the code which gave information about each element or flag, size of flag. A loop specified that the first 12 characters of the array should be “HackRushCTF{“. Another conditional statement specified that the length of the final flag should be 28 characters. After that there were many conditional statements regarding each element of the flag array. Assuming each element of the array to be a variable, I solved the expressions I got from the conditional statement. After solving for all the conditional statements, I got integer values assigned to the remaining elements of the flag array. Every character in C has an integer associated with it, ASCII CODE. So to convert the integers I got for each element to a character, all I had to do was add a ‘0’ to the integer and assign a char to it. Like:-

Let i be the integer and c be the character associated to it, then to find c :

char c = i + ‘0’;

Now that I had a character assigned to the 28 elements of the flag array, I have the flag. I put the flag as the input of the C code and it turned out to be correct.

Flag - HackRushCTF{x86_f1r5t_t1m3?}

Challenge Ancient:

The symbols given in the language looked a bit familiar and the name of the problem gave a hint that it might be a historical language. I searched few symbols there and found out that it was written in Brahmi Script. Finally I found a Brahmi Script converter and put the given text in it to find out the flag:

HackRushCTF{ashoka}