Part 1 Documentation

*Flag String*: **34gdfh340234**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Methodology to Bypass Authentication*: For simple adjustments to print the flag string regardless of what username and password are input, I modified the comparisons to effectively make the validation checks for the username and password dysfunctional. Essentially, each code block (involving the user input) of the form

mov dl, [e?x]

cmp dl, [e?x]

I made both ‘?’ equal so the test compares each value to itself always true.

Therefore, I did not add or delete instructions, simply modify some of the register operands.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Instructions Changed*: Format (Address: Original **New Instruction**)

1. (004B10D5: mov dl, [eax] **move dl, [ecx]**)
2. (004B10DF: mov dl, [eax+1] **move dl, [ecx+1]**)
3. (004B1106: mov dl, [ecx] **mov dl, [eax]**)
4. (004B1110: mov dl, [ecx+1] **mov dl, [eax+1]**)