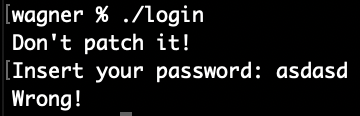
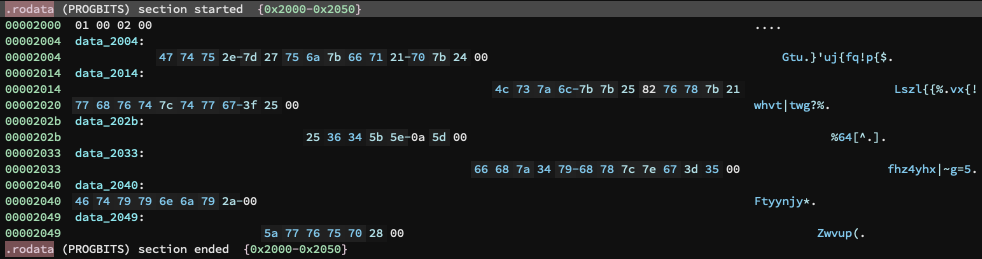
Link: <https://crackmes.one/crackme/5db0ef9f33c5d46f00e2c729>



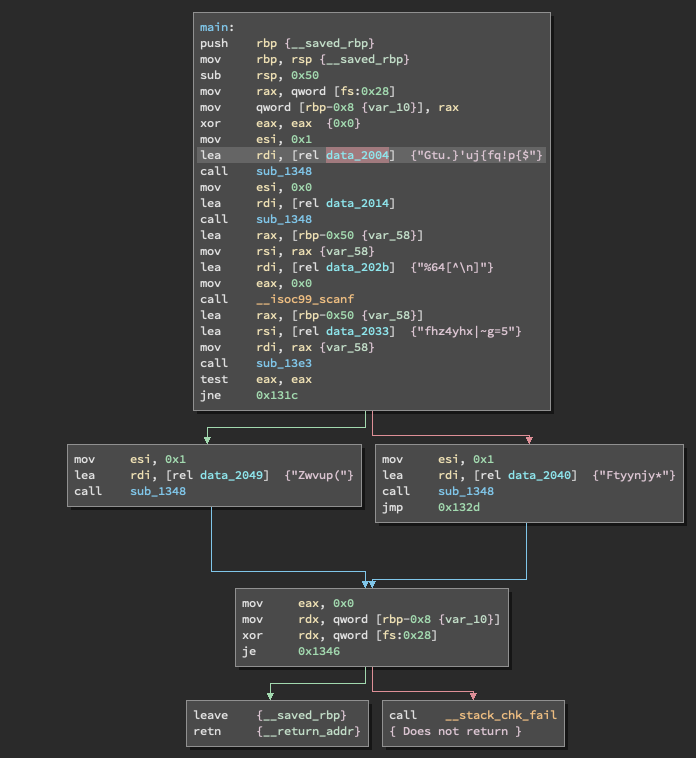
While running the program it gave the instructions to not patch. I entered a set of random characters that were incorrect. Upon disassembling the code, I found the following sets of string:

1. "Gtu.}'uj{fq!p{$"

2. "fhz4yhx|~g=5"

3. "Zwvup("

4. "Ftyynjy\*"

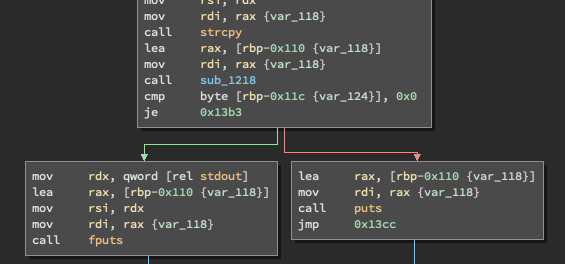
 5. "Lszl{{%\x82vx{!whvt|twg?%"

There is definitely some sort of encryption used here. Furthermore, it seems the messages are decrypted before being sent stdout. So, the message: "Don't patch it!", "Insert your password:" and "Wrong!" are probably encrypted as one of the texts above. This is made evident as these data are sent to either puts or fputs.

From inspection on the lengths of the messages I have, most likely:

1. "Gtu.}'uj{fq!p{$" => "Don't patch it!"

2. "Zwvup(" => "Wrong!"

 3. "Lszl{{%\x82vx{!whvt|twg?%" => "Insert your password:"

Using the ASCII table, I was able to determine the following.

For 1,

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| G | t | u | . | } | ‘ | u | j | { | f | q | ! | p | { | $ |
| 3 | 5 | 7 | 7 | 9 | 7 | 5 | 9 | 7 | 3 | 9 | 1 | 7 | 7 | 3 |
| D | o | n | ‘ | t |  | p | a | t | c | h |  | i | t | ! |

For 2,

Z w v u p (

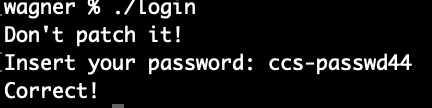
3 5 7 7 9 7

W r o n g !

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Z | w | v | u | p | ( |
| 3 | 5 | 7 | 7 | 9 | 7 |
| W | r | o | n | g | ! |

Looking at the shift for the numbers, this seems to be a pattern for the shift in characters. Based on the flow of control in the disassembled code, we see "Zwvup(" exists in one and "Ftyynjy\*" in the other. It seems safe to assume the latter represents the branch that is correct. Also "fhz4yhx|~g=5" seems to be used before choosing which branch to go. Based on the decryption above, we get the following:

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| f | h | z | 4 | y | h | x | | | ~ | g | = | 5 |
| 3 | 5 | 7 | 7 | 9 | 7 | 5 | 9 | 7 | 3 | 9 | 1 |
| c | c | s | - | p | a | s | s | w | d | 4 | 4 |



Entering "ccs-passwd44" was successful, with message being sent back being "Correct!".