Project 2

Program 1

Andrew Beers acb75@pitt.edu

Procedure:

Knowing the program was written in C, I knew it would have a main function. I initially set a breakpoint at main. I looked at all the calls in main and saw a call to the function strcmp. I thought this might be where the comparison of the strings would be made in the program so I made a break in the program at this point. I noticed that before this call to strcmp there was a move from a pointer on the stack pointer to an address location of 0x08090b08. I thought this might be where the string answer of the program might be loaded so in gdb I looked at the value in this address at the strcmp breakpoint.

Solution:

The value of this register was “QDdQUfltpuUQPVrOynvdHJpO”. I then ran the program again and inputted the value QDdQUfltpuUQPVrOynvdHJpO as my string. I received the message Congratulations! Unlocked with passphrase QDdQUfltpuUQPVrOynvdHJpO Program exited normally, as this was the key the program was looking for.

Notes:

This program seems like a basic program with only a main function that calls strcmp and other basic functions that are a part of the standard c library. The nuance that I noticed in this program was that the string literal pointer wasn’t loaded to $eax or one of the named registers, it was just loaded into an arbitrary address value.

Pass phrase = QDdQUfltpuUQPVrOynvdHJpO