CSC564A Computer Security

Project 2

(due by midnight on Wednesday, April 9th)

Problem. Consider the following C program that checks a user password and grants or denies access. The access is granted only if the user enters the correct password ("goodpassword").

There is a security flaw in the program that allows an attacker to get access by entering a string different from the correct password.

Try to carry out the attack on a particular computer. You need to schedule an appointment (before April 9th) and show me that you can carry out the attack. You don't need to submit anything.

To carry the attack, you need to enter a special string, different from goodpassword, which causes the main program to print:
Access granted!

Find the string for your computer!

```
int IsPasswordOk() {
      char password[13];
      gets(password);
      if(!strcmp(password,"goodpassword")) return 1;
      else return 0;
}

int main() {
      int pwdStatus;
      puts("Enter password");
      pwdStatus = IsPasswordOk();
      if(!pwdStatus) {
            puts("Access denied!");
            exit(-1);
      }
      else puts("Access granted!");
      exit(0);
}
```