Password Hashing
IN618 Security

Introduction

In your future work, the probability that you will be responsible for handling user names and passwords is basically 100% In this lab you will start learning how to do this correctly.

1 Examining a trivially exploitable system

Extract a copy of the IN618-Password-Example-One project onto your lab machine's desktop. Open the project with Visual Studio, inspect the source code, and run the program. It implements a very simple username/password check and allows you to enter new usernames and passwords.

Problem 1: There are several username/password pairs already set up on the system. By inspecting it, find them and verify that you are able to log into the system using stolen credentials. Write one username/password pair that you found.

Why was it so easy to do this?

2 Examining a more secure, but still flawed, system

After the password hashing method is discussed, implement it on your system. and verify that it works. Then, get a copy of the pre-hashed passwords and set them up on your system.

Problem 2: One of the passwords in the pre-hashed set is poorly chosen and can be discovered using the system. Which user has the bad password and what is it?

Briefly describe the method you used to find the password. Given enough time, could you use it to find all the passwords in the file?

Challenge question: Without consulting any references, can you think of a way to make this password system harder to break? How?

3 Wrapping up

Save a copy of your project in your home directory or other location where you can save it for the next lab session.