SECU73000 - Assignment 4

Check eConestoga for due date.

Introduction

In class we have experimented with different tools and techniques to assist us in source code assessment. In this assignment, we will perform a source code review on some unknown code. You are welcome to use any and all of the tools and techniques we used in class, as well as any other tools you may enjoy.

Once identified, you will offer an opinion on how bad the discovered vulnerability is and how one might best remediate the vulnerability.

Specification

1. Download the source code from eConestoga
2. unzip the archive
3. Double click on the .sln file to open the project in Visual Studio
4. Now that you know the solution is readable, proceed to review and identify the issues.

Deliverable

Using all the tools at your disposal, review this code base and identify as many security issues as you can. For each issue you identify, be sure to both explain why the finding is an issue and how an attacker might leverage the issue. Follow that short discussion with some overview thoughts on how you would suggest the developer fix the issue.

Please note that we are slightly more interested in the weakness itself, rather than the fix, so when discussing a finding, spend 60% of your time/effort on the vulnerability and 40% on potential mitigation strategies.

You will submit a written report (MSWord or PDF only) containing screen shots, filename and line number pairs, and the three discussion points noted above (finding explanation, likely exploit scenarios and mitigation strategies).

Marking Rubric

I will be looking for the following:

- Number and validity of findings
- Accuracy and completeness of finding explanation
- Reasonableness of exploit scenario
- Appropriateness of mitigation strategies.

Standard Deductions

- 5% for not having name and assignment # in your Word/PDF document
- 10% for submitting a "zip"ed (compressed) document
- Regular late submission penalty (see Program Handbook)
- Penalties applied as per the Student Handbook for any plagiarism and/or academic dishonesty.