CSE 5/7359 – Software Security

Lab 1 – Simple Web Server: Security Goals and Principles

**Name\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Objective: The Foundations book contains a java-based sample web server called SimpleWebServer. This lab requires you to work with simple web server in order to understand the security goals and design principles presented in section 1 of this course.

1. Develop a set of security requirements for the Simple Web Server example from the book. Be sure to include what needs to be protected, from whom, and for how long. Also indicate the cost of not protecting the data or assets as a note to each requirement.

2. Problem 6 on page 77-78 of the book asks you to consider threats against a web server with file upload capability. Complete all parts (*a* – *e*) of Problem 6 and…

Include the following considerations:

1. Reference the threat characters that we talked about, which of these threats are involved in the various attack scenarios in this problem?
2. Explain the steps that lead to each successful attack.
3. Explain which of the security goals is broken by the attacks.

3. Implement Problem 7 on page 78-79 of the book. Answer the questions in part *a* and *b*. Part *c* is optional, but you’ll receive a 1337 point for implementing it.

4. Complete parts *a*, *b* and *c* of problem 9 on page 79 of the book.

Hint: For part *a* it might help to observe how real websites use HTTP authorization. Use an HTTP proxy like Paros to view the HTTP headers involved in the negotiation.

Hint: For part *c* Ethereal is now known as Wireshark. The user manuals are pretty helpful in getting started, but use of the tool is relatively straightforward. I don’t mind questions and discussion on the use of the tool on the BlackBoard discussion forum (I created one called Security Tools Discussion).

## Submission:

Submit all work in a SINGLE .doc, .docx, or pdf file (this helps so that I don’t have a ton of files to download per student). For coding exercises, simply embed new or modified code snippets inside the document and include *screenshots* of **1) successful compilation** and **2) test cases** showing successful completion of the coding. If you see fit, you can embed other file objects in the document (i.e. an embedded Excel spreadsheet) if they will help explain or illustrate your points.