CS 50011 INTRODUCTION TO SYSTEMS II Summer 2017

Lab #4

Name: ____________________________________

Part 1: SQL Injection (20 points)

Some of the world’s greatest web developers have gotten together to create a professional grade book interface.

You can find it at http://endor.cs.purdue.edu:30NN/ where NN is your assigned port number. Note that it starts with a 3 this time.

The code used for this interface can be found in /var/www/html on your virtual machine.

Use the mysql command line interface to reset one of the user’s passwords so you can access the interface.

Identify and exploit at least two vulnerabilities, one of which must be a SQL injection attack.

[10 points] Exploit 1

[10 points] Exploit 2

Part 2: Secure It (20 points)

Identify and suggest patches for the vulnerabilities that were used in the above exploit(s).

This part may require you to do some research on proper PHP mysql interaction.

Note any overarching implementation details that may be flawed or beneficial. To be clear, in addition to code modifications, this part should have a brief (less than one page) write-up regarding the system, its flaws, and any benefits.

HINT: Read about PHP’s session_start() and friends. How might they be helpful?