**CSE 484 In-class Worksheet #3i+5 (Fall 2016)**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ UWNetID: \_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Email address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Student ID #: \_\_\_\_\_\_\_\_\_\_\_

Partner names for this activity: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Q1.** This command injection lets you copy a file to an arbitrary location. But there’s more! What could you do as an attacker that’s even more severe?

**Q2.** What are some of the challenges with SQL injection? What makes SQL injections hard? Is it easier to extract data or change data with a SQL injection?

**Q3.** What are some of the problems with storing session state in the URL instead of in a cookie? What vulnerabilities does it create? What other problems would arise in such a web app?

**Q4.** What would you try first if you were looking for vulnerabilities in this shopping cart system?