Security Injections @Towson

Security Injections, Java CS1 - Input Validation

1. Background   **2. Code Responsibly**   **3. Laboratory Assignment**

4. Discussion Questions

Code Responsibly-- How Can I Properly Validate Input?

Check all input: Below is a partial list of some checks to include:

- **Type check:**vinput should be checked to ensure it is the datatype expected, e.g., age must be integer.
- **Length check:** variables are checked to ensure they are the appropriate length, for example, a US telephone number has 10 digits.
- **Range check** - numbers checked to ensure they are within a range of possible values, for example, the value for month should lie between 1 and 12.
- **Reasonable check:** values are checked for their reasonableness, e.g. (age > 16) && (age < 100)
- **Divide by Zero:** variables are checked for values that might cause problems such as division by zero.
- **Format check** - Checks that the data is in a specified format (template), e.g., dates have to be in the format DD/MM/YYYY.

Input checking can be difficult. Checking a telephone number may require consideration of the many differing telephone formats used by countries around the world.

Recover Appropriately: A robust program will respond to invalid input in a manner that is appropriate, correct, and secure. When your program runs across invalid input, it should recover as much as possible, and then repeat the request, or otherwise continue on. Arbitrary decisions such as truncating or otherwise reformatting data to "make it fit" should be avoided.

The following method shows input validation to check range and/or reasonableness:

```java
static int validNum(int min, int max)
{
    Scanner scan = new Scanner(System.in);
    int value = scan.nextInt();
    while ((value < min || value > max))
    {
      System.out.println("Enter a number between [" + min + "," + max + "]" );
      value = scan.nextInt();
    }
    return value;
}
```

Answer the following questions:

Question 1:

Which of the following inputs should be checked for reasonableness?

- ☑ ✓ age
- ☐ first name
- ☐ city
- ☑ ✓ Item Price

(HINT: Read sections *Check your input* to answer this question)

Question 2:

Which of the following inputs would require a specific template or format to be appropriate?

- ☑ ✓ social security number
- ☐ national debt
- ☑ ✓ Telephone number

☑ ✓ birthdate

(HINT: Read sections *Check your input* to answer this question)

Go To Next Section

Powered by a modified version of Class2Go

☑ ✓ birthdate

(HINT: Read sections *Check your input* to answer this question)