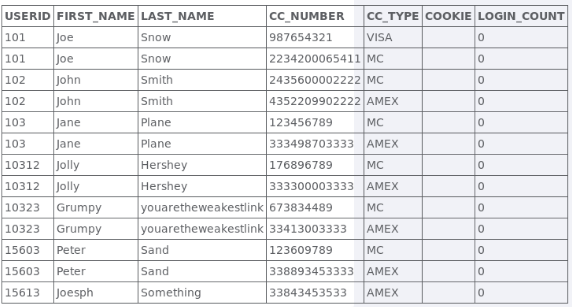
# Lab: WebGoat

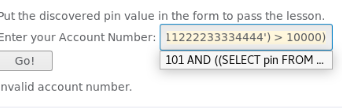
|  |
| --- |
| * This is due tonight and worth 10 points. * Use the following naming convention: homework, underscore, last name, first initial, and extension (e.g., Lab\_SQLi\_ImG.docx). |

**Task 1. String SQL Injection (3 points)**

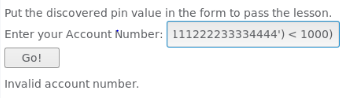
Provide a screenshot for the last result of the injection.



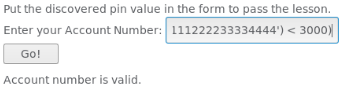
**Task 2. Blind Numeric SQL Injection (3 points)**

Provide screenshots for all the injections (min of three) you have tried following the guideline in the “Show Solutions.” Explain in your own words how you obtained the final outcome.  
 

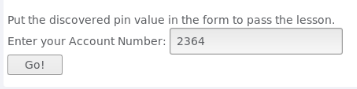
**Here we know that the number is not greater than 10000**



**Here we know the number is not less than 1000 so the number is in between 10000 and 1000**

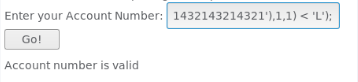


**Here we know the number is less than 3000 so the number is in between 3000 and 1000. After a while, if you keep switching the sign and the number, you will get the account number of 2364.**

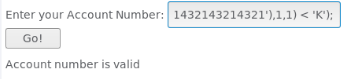


**Task 3. Blind String SQL Injection (4 points)**

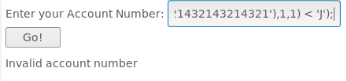
Provide screenshots for all the injections (min of five) you have tried following the guideline in the “Show Solutions.” Explain in your own words how you obtained the final outcome.



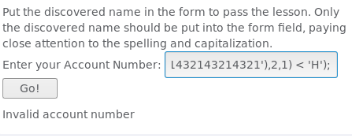
**Here we know the first letter is before the letter L**



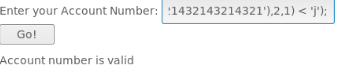
**Here we know the first letter is before the letter K**



**Here we know the first letter is a J because the previous statement is true and this statement is false.**



**Here we know the second letter is not below H**



**Here we know the second letter is below j. The only letter between H and J is I, so the second letter is I. Depending on whether it returns valid or invalid, you will know which letter goes on which spot.**

**Eventually through this process, the full name of ‘Jill’ will be found.**

