CSEC-471
Penetration Testing Methodologies
Python Exercise 4

Given :

A mysql database (payload) and a website vulnerable to a blind SQL injection attack (blind/login.php), write a tool using Python and BeautifulSoup to perform a blind SQL injection attack. The tool can be specific to the website structure. In other words, it does not have to be adaptable to a different web page without some modification. The tool should be able to recover all of the user names from the database and their associated passwords.

Deliverables:

1. The python code that will perform the blind SQL injection against the specified website. Your code should use the URL http://localhost/blind/login.php
2. A note with any instructions necessary for the instructors to test your code including command line options and arguments if any. You should indicate in this document how well your code functions. i.e. Does it find all or just the first user name, can it handle mixed case characters, does it run very slow, etc? Grading will take into account whether you acknowledge problems your program has or we have to find them.
3. A file with the output of the command

Due date:

Submitted to the “Blind SQL code submission due 25-Feb @ 11:59pActions for Blind SQL code submission due 25-Feb @ 11:59p” by 11:59pm this Thursday, February 25, 2016.