Homework Assignment #1 – Web – Part I

Practical Cyber Security Fundamentals (CTF), Spring 2017
Department of Computer Science, Florida State University

Points: 50
Due: Beginning of the class (5:15pm) on January 30, 2017

Submission: You need to submit electronically via Blackboard by uploading a text file (named "**hw1-Firstname-Lastname.txt**") for your answers and programs to the problems; you need to combine all the parts into a single file. Here replace "Firstname" using your first name and replace "Lastname" using your last name in the file name.

The main purpose of this assignment is to let you be familiar and become comfortable with web fundamentals and be able to develop solutions toward solving CTF problems in the Web category. You need to show your work in order to receive full credit.

Problem 1 (10 points, 5 point each) Solve the following problems using Python; you need to submit the flags and your programs for full credit.

1) Decode this URL encoded string:
   %66%6c%61%67%7b%68%31%64%31%6e%67%5f%31%6e%5f%70%6c%34%31%6e%5f%73%31%74%33%7d
2) Do a while loop to decode this base64 string until you get the flag:
   Vm0xd1NtUXlWa1pPVldoVFlUSlNjRlJVVGtOamJGWnhVMjA1VlUxV2NIbFdiVEZIWVZaYWRW
   RnNhRmRXTTFKUVZrZDRXbVF3TlZsalJsWk9WakZLTmxaclVrZFVNVXB5VFZaV1dHSkhhRlJW
   YkZwM1ZGWlplVTFVVW1wTmF6VllWbGMxVjFaWFJqWldiRkpoVmpOb2FGUldXbHBrTWtaSldr
   WlNUbGRGU2paV2FrbzBZekZhV0ZKdVVtcGxiWE01

Problem 2 (10 points) Write a Python program to interact with the following website to get the flag:

http://ctf.hackucf.org:4000/calc/calc.php

Python is useful to overcome the race condition. For HTTP requests, use the Python requests library.

Problem 3 (30 points) Solve the following problems. You need to show the URLs and flags for full credit.

1) Exploit a SQL injection:
   http://ctf.hackucf.org:4001/index.php
2) Exploit LFI to download /etc/flag file from
   http://n0l3ptr.internetzninja.com/web1/index.php?page=home.html
3) Perform remote code execution (RCE) to download the hidden flag file in web1 directory:
   http://n0l3ptr.internetzninja.com/web1/upload.php
   (RCE hint: Use LFI.)