Secure Programming, Assignment 3:

Application and Web Security

Strict deadline: December 10, 2018, 23:59 Amsterdam time

Question 1 (10 points)

The file secprog.c contains a C program with multiple vulnerabilities. Analyze the program (you may compile it with the given Makefile and run it, or just read the source code) and document all the vulnerabilities you find in the form of a table that details, for each vulnerability:

- The line number where you found the vulnerability
- The type of vulnerability (i.e., buffer overflow)
- How an attacker can exploit the vulnerability
- How to fix the vulnerability

Note that you don't have to create a fixed program. Submit your table as a .xlsx or .xls spreadsheet. At the top of the spreadsheet, please include your name, student number, VUnet ID, and e-mail address. Please keep your answers brief. A few lines should be enough to describe how to exploit and fix each vulnerability.

Question 2 (10 points)

At http://130.37.198.90 , you'll find a simple web site that contains a reflected XSS vulnerability. Create an exploit for the vulnerability that displays a javascript popup containing the user's session cookie. Send us a .txt file containing your exploit URL and any other necessary steps to complete the exploit. At the top of your .txt file, include your name, student number, VUnet ID, and e-mail address.

Note: *If you have problems with the browser detecting and blocking the XSS attack, feel free to try your exploit in another browser.* We've verified that the bug is exploitable in Firefox Quantum 63.0.3 (64-bit). On the other hand, the latest version of Chrome blocks the exploit, and so that browser is not recommended for doing this assignment.

How to Submit

To hand in the assignment, submit a zip file on Canvas called <your vunet id>.zip that contains:

- The table (.xlsx or .xls) containing your answers to Question 1.
- The .txt file containing your exploit for Question 2.