THE UNIVERSITY of NEW ORLEANS

CSCI 4621/5621 **INTRO TO CYBER SECURITY**

Assignment 1: Format String Fuzzing

Due: **Mar 22, 11:59pm**

Goal

The purpose of this lab is to demonstrate a format string attack leading to the modification of an environment variable.

VM

`csci4621-s23` on https://cyber-range.cs.uno.edu; create a VM for your work and include your login in the name. E.g.: if login is `jdoe`, VM name should be **`csci4621-s23-jdoe`**.

An OVA image (~8GB) is available from the class **repo/VM** folder, if you want to work locally.

Starter/submission code

- **repo:** code/4621-fmt.zip
- **sftp:** cook.cs.uno.edu:/home/vroussev/public/4621-fmt.zip

Deliverables

- Code:
  - your very own implementation of the `fuzzer()` function, such that it modifies the **`secret`** environment variable's value to **`hacked`** ***using the format string technique***
- Report:
  - a concise report documenting your work
- VM
  - if you have working code, leave running VM named **`csci4621-s23-<yourlogin>-lab1`** and describe how to use it in your report

Evaluation

You may consult all available on-/off-line resources, but you may not actively solicit help; e.g., you can read a discussion on *Stack Overflow*, but you may not post a question related to the assignment.

Submission

Bundle your whole submission—**a1.c**, **Makefile** and report file as a **zip** file named **4621-s23-<login>.zip** and submit via Moodle and (optionally) VM on `cyber-range.cs.uno.edu` as described above.

Bonus (+20%)

Remove (comment out) the first line of the `fuzzee` function:

```
char *env = envp[0];
```

Make you `fuzzer` code work again.

Note: simply moving it to your fuzzer function is not acceptable as a solution.

Graduate Credit

Graduate students must do the bonus version of the assignment for full credit

Grading

15% of final grade

Reference

repo: ref/Exploiting Format String Vulnerabilities (2001) v1.2.pdf