Lab 04: Format String Problems

Goals

- Identify vulnerabilities of a specified type in an application
- Remediate identified vulnerabilities using specified method

Notes

The lab is available in the Learn org of Dakota State University's Information Assurance Lab within the vApp <username>_CSC234_Zwach_Base. It's accessible at https://ialab.dsu.edu. You can start the vApp by clicking Actions and Start in the HTML5 client.

The code that comprises the entire application is available within the /home/student/course_files/_assignments/format_string_problems directory. Make your changes there using a text editor of your choosing. Compile using gcc. Remember to use the **-m32** flag. You may use the **-no-pie** and **-g** flags if you want to do more poking around, but neither of those are required for the assignment. Remember, you can permanently revert your changes to the codebase at any time with the command `revertall`.

The username is **student** and the password is **Password1!**.

Discovery

This program has one or more flaws. Identify changes you'd make for security reasons and why.

1. Review the source code for the application of interest (a7.c).
   a. Provide screenshots of vulnerable or otherwise flawed code segments.
   b. Explain each issue in your own words.
2. Compile and run the program
   a. Provide a screenshot demonstrating each of the vulnerabilities using a method of your choice. Ideally in this case, you'd beat the game.

Remediation

After confirming the vulnerability, use your knowledge and available resources to modify the source to follow best practices and avoid integer overflows.

3. Modify the source code to gracefully the flaws.
   a. Document your resulting source code with a screenshot
4. Test your changes
   a. Are your attempts at entering further malicious input successful? Why or why not?
   b. Provide screenshots documenting proper handling of malicious input.

Scoring

The rubric will be published at scoring time. Each portion of the assignment has the following points assigned.

Section	Points
1	**6**
2	2
3	**6**
4	**6**
Total	**20**