Tiffany Nguyen, Giselle Hernandez
Professor Samuel Addington
CECS 478 Sec01
07 December 2025

Format String Guardian

GitHub Repo Link: https://github.com/tifftknguyen/Final-Project-478.git

What Didn't Work

We needed to add this section because our original proposal was overly ambitious. This was mainly due to the misunderstanding of our project assignment instructions. Our original proposal was to create a Format String Guardian that includes an AST-scanner with 25 test cases and a Tamper Evident Log system. This was far too ambitious. We narrowed this down to just a lightweight scanner with 26 test cases to create an even environment 13 safe and 13 unsafe. When it came to the troubleshooting stage after creating the files, we ran into issues with just trying to run the docker image and all test cases at once instead of 1 by 1 because that would take far too long to run all 26. Then the next HUGE issue we ran into was our compose file and just ensuring everything was running smoothly.

What Works

What worked were our test cases, both safe and unsafe. Our main format string guardian was able to capture unsafe string formatting functions, such as printf() and strcpy(), that don't do bound checking, which can easily lead to buffer overflow and create unpredictable, risky behavior. We also noticed the small number of false positives that our program captures, but it's more crucial to flag potential risky flags than to miss any critical vulnerability code practices. We were also able to automatically run all 26 test cases, removing the tedious work of running the 26 files individually.

What's Next

We will work to further refine everything once comments are given. If time permits, we will attempt to improve the scanner from lightweight to AST. Test cases are good for the time given. However, a good addition is to see whether or not other test cases can be more suitable for a real life world environment. Sometimes finding a safe integer is less efficient compared to another user inputting their username. Another thing we need to consider next is how to make sure our test cases print concisely and are more legible to read and analyze. We would also want to have peer feedback to better improve and enhance our format string guardian.

Demo Video

Tiffany uploaded on Canvas.