# Spica (Launched 1977)

- *Username:* `spica`
- ▶ *Click to reveal password:*
- *Points:* 5 for checkpoint, 5 for code, 5 for writeup

*Relevant lectures: 3 - Memory Safety Vulnerabilities*

> **STORY**
> The logs inside the Remus satellite contain a cryptic reference to a highly intelligent bot. Of course, you had heard of the urban legend of EvanBot, the top-secret genius AI that single-handedly developed Caltopian space travel technology, but the message in Remus suggests that it may be more than a legend. You decide to investigate further and follow the hint to Spica. Spica is an old Gobian Union geolocation satellite with a utility for viewing telemetry log files. Exploit this utility and hack into Spica to see what secrets it holds about the mysterious EvanBot.

`telemetry` is the vulnerable C program in this question. It takes a file and prints out its contents, but it expects the file to be specially formatted: The first byte of the file specifies its length, followed by the actual file.

The program also implements a check to make sure the buffer isn't too large. Can you see a way to get around this check?

The output of `egg` is forwarded to the input file, so `print` statements in `egg` will be written to the file.

---

## Deliverables

- A script `egg`
- A writeup.

---