Deneb (Launched 2000)

- *Username:* `deneb`
- ▼ *Click to reveal password:*
  `neveruse`
- *Points:* 10 for code, 5 for writeup

Relevant lectures: 1 - Security Principles

> **STORY**
> EvanBot's message is alarming. Could the Caltopian Jupiter exploration project have some secondary evil purpose? Following Bot's advice, you decide to hack into the Deneb satellite to investigate further. The fear of the Y2K bug at the turn of the century drove Gobian engineers to conduct a sweeping evaluation of its systems and correct any deficiencies. Deneb, the first Gobian satellite launched in the 21st century, features a more secure version of the original Spica file viewing utility.

Consider what security vulnerabilities occur during error checking. Which security principles are involved in correctly implementing error checking?

The exploit for this question uses an `interact` file, and the example code also provides an example of how to overwrite files. You may find this useful while looking at the behavior of the vulnerable program!

Tips

- You might find it helpful to use two terminals to debug this question. We recommend learning how to use `tmux`. Alternatively, you can open multiple terminals on your computer and connect using two separate SSH connections.

Deliverables

- A script `interact`
- A writeup.
