Ryan Schanzenbacher
12/1/23
Vulnerability Technical Details

The vulnerability I am going to write about was actually found by a friend of mine while trying to break the server. It is a version of directory traversal (...again) that I hadn't thought of, but this time I'm going to talk about why it really isn't that terrible. In this case, symlinks are improperly handled for one specific file: `index.html`

Steps to Reproduce:

1. Create a file named `index.html` that is a symlink to a secret file.
2. Launch the server either using root permissions or using the docker container (since this runs as root by default).
3. Navigate to the directory that contains the file. When you navigate into it, the symlink will be followed and data can be leaked.

Alternate steps:

1. Run the python script provided to create a file outside the directory and spin up the server, launch firefox and verify that data has been leaked.