# SERVE MY SAUCE

The giant finale in the sauce trilogy we have again a saucy webpage. But this time reading the sauce code isn’t going to help us.

Navigating to different pages in the top navbar we notice that there is a page parameter in the URL:



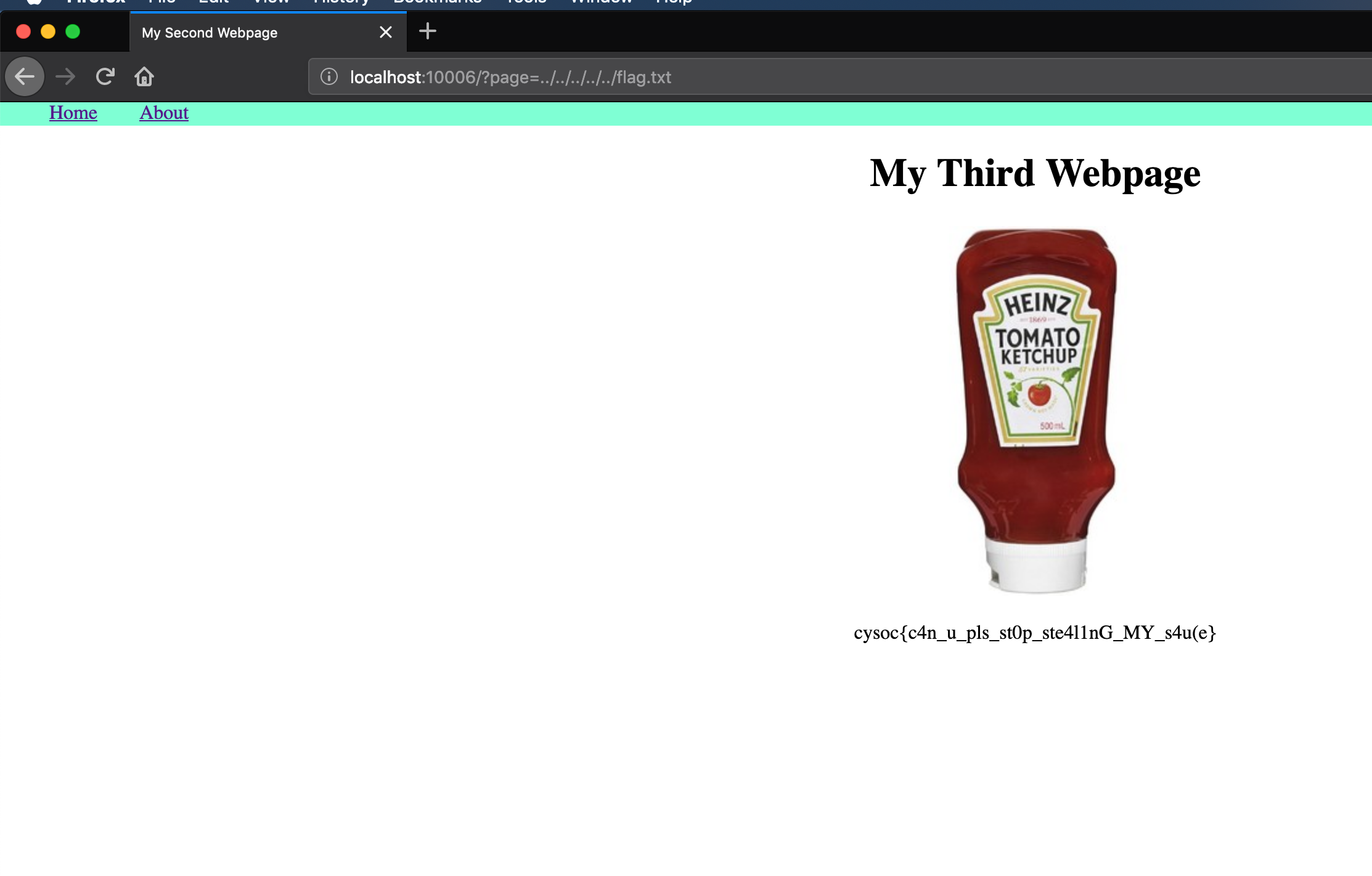
The home page also hints at a Local File Inclusion with 3 sentences all starting with local file and including.

Changing the page param to something else results in an empty webpage.





We are also told from the challenge description that the flag is stored in /flag.txt on the server. Trying page=/flag.txt also results in nothing as this is an absolute path and will not work in the command. So trying putting a relative path in the command with page=../../../../../../../flag.txt reveals the flag.



This gives the flag:

**cysoc{c4n\_u\_pls\_st0p\_ste4l1nG\_MY\_s4u(e}**

As this is a command injection it is also possible to perform remote code execution. It is left to the reader to try and see if you can pop a shell on the box ;)