nullhat 2025: Tart m3za

@elesquina

The target accepts a tar archive and extracts it server-side. The extraction follows symlinks inside the archive, so a crafted archive can redirect a path that looks harmless into a sensitive location. The intended primitive is to place a symlink entry first and later place a regular file entry that writes through that symlink during extraction. On its own, the server tries to clean up symlinks, but there is a race condition before the cleanup happens.

To make the race practical, I include a very large padding file in the archive so extraction takes longer and the timing window is wider. Then I repeatedly trigger extraction until I win the race and the symlink remains active long enough for the following file entry to be written through it. When the race is won, the extraction step yields the content I want, and I save that recovered content as `filler.bin`.

Finally, I search the recovered file for the flag string. Grepping for the usual prefix gives `ELITESEC{race4syml1nk_expl0its_r_4_real}`.