Analysis of the bug

The seed read from the unitialized variable is not really random: it is determined by the functions that have been called before `do_exec()`. If the attacker can control the contents of the stack frame of a function called immediately before `do_exec()`, it can set the seed to a known value, essentially fixing the value of the canary.

We run `server` in a debugger and send the `le\n` string, to cause a call to `do_login()` immediately followed by a call do `do_exec()`. We set a breakpoint in `do_exec()` and send send 79 `A`s of input. These will satisfy the `fgets()` in `do_login()`; then, the program will move to `do_exec()`. We can now verify that `canary_seed` is set to 0x41414141 and we can take note of the contents of the `canary` array after the call to `setup_canary()` (e.g., with `x/xg canary`). If we repeat these steps on the actual server, the same canary will be generated.