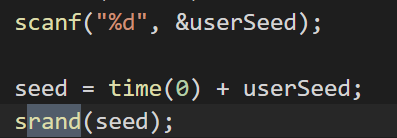
Discovery

1:

Using the time in the seed makes the ‘calculated’ seed discoverable by iteration. Rather than using time(0) we could read 4 bytes from /dev/urandom.  
Also on the same snippet: The user having a hand in seeding seems questionable. I’m not a mathematician so I can’t say for certain, I don’t think it would give them any information if we pulled from /dev/urandom and they incremented that number, but we could just as well skip taking their input and remove that risk entirely.



2: