Pseudo-random fsb

Deskripsi soal : Memasukkan nilai yang sesuai dengan nilai yang disediakan melalui format string bug

Writeup:

Soal ini mempunyai 2 kelemahan, yang pertama adalah pada random srand(time(NULL)), yang dapat dibypass dengan mengimitasi randomnya dan memasukan hasil randomnya langsung tanpa menggunakan FSB, dan bisa juga menggunakan FSB.

Jika menggunakan format string, variable randomnya ada di argument ke 9, dengan menginput %p sebanyak 9 kali, maka nilai hex di argument ke 9 dapat dimasukkan. Ketika sudah dimasukkan maka flag akan keluar.