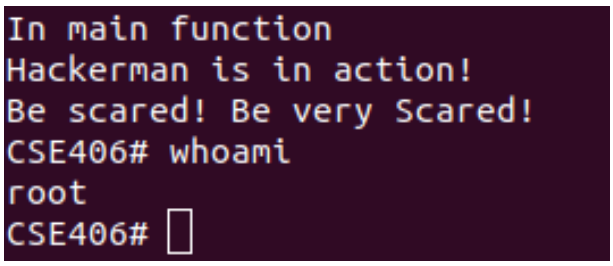
Online 1 - B1

Buffer Overflow Attack, CSE 406 July 8, 2023

You are given a vulnerable C program named B1.c. Replace ⟨**PARAM_1**⟩, ⟨**PARAM_2**⟩, ⟨**PARAM_3**⟩ in the source code with the corresponding values of Table-1.

Tasks

- First, compile the program from the root's privilege and set its UID as shown in the lab. Do not forget to turn off address space randomization and stack protection. Also, make sure that the stack is executable while compiling the program.
- Prepare a payload (e.g. badfile) which will cause the program to open a shell with root's privilege when executed by other users (seed).
- Expected Output:



- Make sure that you don't change the C program other than the macro parameters values as instructed.
- If you have used cloud VM, make to sure to write the public ip of the vm as a comment in the exploit py file.
- Rename your exploit.py file with 18050xx.py and submit in moodle.

Table 1: Parameters

ID	PARAM_1	PARAM_2	PARAM_3
1805061	33	77	377
1805062	49	109	416
1805063	65	141	455
1805064	81	173	494
1805065	97	205	533
1805066	113	237	572
1805067	129	269	611
1805068	145	301	650
1805069	161	333	689
1805070	177	365	728
1805071	193	397	767
1805072	209	429	806
1805073	225	461	845
1805074	241	493	884
1805075	257	525	923
1805076	273	557	962
1805077	289	589	1001
1805078	305	621	1040
1805079	321	653	1079
1805080	337	685	1118
1805081	353	717	1157
1805082	369	749	1196
1805083	385	781	1235
1805084	401	813	1274
1805085	417	845	1313
1805086	433	877	1352
1805087	449	909	1391
1805088	465	941	1430
1805089	481	973	1469
1805090	497	1005	1508