Online 1 - B2

You are given a vulnerable C program named **stack-B2.c**. Replace ⟨PARAM_1⟩, ⟨PARAM_2⟩, ⟨PARAM_3⟩ in the source code with the corresponding values of the table.

Tasks

- First, compile the program **for 64 bit** 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:

```
In main function
Welcome to trial session…
SEED-VM#
```

- 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.

	PARAM_1	**PARAM_2**	**PARAM_3**
1805091	145	301	650
1805092	158	318	669
1805093	171	335	688
1805094	184	352	707
1805095	197	369	726
1805096	210	386	745
1805097	223	403	764
1805098	236	420	783
1805099	249	437	802
1805100	262	454	821
1805101	275	471	840
1805102	288	488	859
1805103	301	505	878
1805104	314	522	897
1805105	327	539	916
1805106	340	556	935
1805107	353	573	954
1805108	366	590	973

1805109	379	607	992
1805110	392	624	1011
1805111	405	641	1030
1805112	418	658	1049
1805113	431	675	1068
1805114	444	692	1087
1805115	457	709	1106
1805116	470	726	1125
1805117	483	743	1144
1805118	496	760	1163
1805119	509	777	1182
1805120	522	794	1201