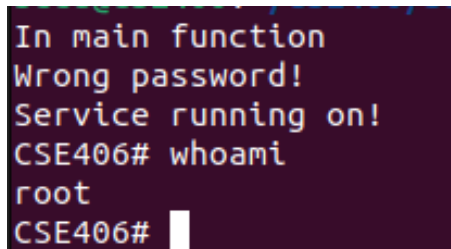


BUFFER OVERFLOW ONLINE - B1

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, you must get the service even though you don't know the password.
- Second, you have to open the shell having root access.
- Prepare payload(s) which will cause the program to run the above tasks.
- Expected Output:



```
In main function
Wrong password!
Service running on!
CSE406# whoami
root
CSE406#
```

- Ensure you don't change the C program other than the macro parameters values as instructed.
- **You cannot use assembly codes in the exploit py file.**
- **You must compile the program for 64-bit machine**
- **10%** bonus marks if you do the tasks using only the terminal.
- If you have used a cloud VM, make sure to write the public IP of the VM as a comment in the exploit py file.
- Rename your exploit.py file with 19050xx.py and submit it in Moodle.

Table 1: Parameters

ID	PARAM_1	PARAM_2	PARAM_3
1905061	30	50	400
1905062	45	70	435
1905063	60	90	470
1905064	75	110	505
1905065	90	130	540
1905066	105	150	575
1905067	120	170	610
1905068	135	190	645
1905069	150	210	680
1905070	165	230	715
1905071	180	250	750
1905072	195	270	785
1905073	210	290	820
1905074	225	310	855
1905075	240	330	890
1905076	255	350	925
1905077	270	370	960
1905078	285	390	995
1905079	300	410	1030
1905080	315	430	1065
1905081	330	450	1100
1905082	345	470	1135
1905083	360	490	1170
1905084	375	510	1205
1905085	390	530	1240
1905086	405	550	1275
1905087	420	570	1310
1905088	435	590	1345
1905089	450	610	1380
1905090	465	630	1415
Prev 1	480	650	1450
Prev 2	495	670	1485
Prev 3	510	690	1520