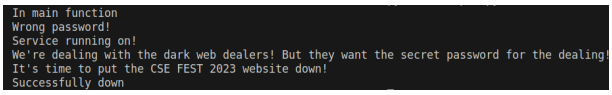
Online 1 - A1

Buffer Overflow Attack, CSE 406 July 12, 2023

You are given a vulnerable C program named A1.c. Replace ⟨**PARAM_1**⟩, ⟨**PARAM_2**⟩, ⟨**PARAM_3**⟩ in the source code with the corresponding values of Table-1.

Tasks

- First, you have to bypass the password check and get the service.
- Second, you have to shut the CSE FEST SERVER down! You can assume there is a folder named "CSEFESTSERVER" and you should simply remove the folder to shut down the server.
- Prepare payload(s) which will cause the program to run the above tasks.
- Expected Output:



- Make sure that you don't change the C program other than the macro parameters values as instructed.
- 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 18050xx.py and submit in Moodle.

Table 1: Parameters

ID	PARAM_1	PARAM_2	PARAM_3
1805001	30	50	400
1805002	45	70	435
1805003	60	90	470
1805004	75	110	505
1805005	90	130	540
1805006	105	150	575
1805007	120	170	610
1805008	135	190	645
1805009	150	210	680
1805010	165	230	715
1805011	180	250	750
1805012	195	270	785
1805013	210	290	820
1805014	225	310	855
1805015	240	330	890
1805016	255	350	925
1805017	270	370	960
1805018	285	390	995
1805019	300	410	1030
1805020	315	430	1065
1805021	330	450	1100
1805022	345	470	1135
1805023	360	490	1170
1805024	375	510	1205
1805025	390	530	1240
1805026	405	550	1275
1805027	420	570	1310
1805028	435	590	1345
1805029	450	610	1380
1805030	465	630	1415