# Buffer Overflow Online - A2

Buffer Overflow Attack, CSE 406 January 20, 2024

You are given a vulnerable C program named A2.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:

```
In main function
Wrong password!
Service running on!
We're deadling with the dark web dealers! But they want the secret password for the dealing!
It's time to put the CSE FEST 2024 webiste down!
Successfully down
```

- Make sure that you don't change the C program other than the macro parameters values as instructed.
- **You must compile the program for 64-bit machine**
- 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 in Moodle.

Table 1: Parameters

| ID | PARAM_1 | PARAM_2 | PARAM_3 |
|---|---|---|---|
| 1905031 | 510 | 690 | 1520 |
| 1905032 | 495 | 670 | 1485 |
| 1905033 | 480 | 650 | 1450 |
| 1905034 | 465 | 630 | 1415 |
| 1905035 | 450 | 610 | 1380 |
| 1905036 | 435 | 590 | 1345 |
| 1905037 | 420 | 570 | 1310 |
| 1905038 | 405 | 550 | 1275 |
| 1905039 | 390 | 530 | 1240 |
| 1905040 | 375 | 510 | 1205 |
| 1905041 | 360 | 490 | 1170 |
| 1905042 | 345 | 470 | 1135 |
| 1905043 | 330 | 450 | 1100 |
| 1905044 | 315 | 430 | 1065 |
| 1905045 | 300 | 410 | 1030 |
| 1905046 | 285 | 390 | 995 |
| 1905047 | 270 | 370 | 960 |
| 1905048 | 255 | 350 | 925 |
| 1905049 | 240 | 330 | 890 |
| 1905050 | 225 | 310 | 855 |
| 1905051 | 210 | 290 | 820 |
| 1905052 | 195 | 270 | 785 |
| 1905053 | 180 | 250 | 750 |
| 1905054 | 165 | 230 | 715 |
| 1905055 | 150 | 210 | 680 |
| 1905056 | 135 | 190 | 645 |
| 1905057 | 120 | 170 | 610 |
| 1905058 | 105 | 150 | 575 |
| 1905059 | 90 | 130 | 540 |
| 1905060 | 75 | 110 | 505 |
| Prev 1 | 60 | 90 | 470 |
| Prev 2 | 45 | 70 | 435 |
| Prev 3 | 30 | 50 | 400 |