Notices

- HW1 was released (deadline 4.27 Wed)
  - No intermediate feedback session
  - Please use piazza (or email) if you have any questions
  - Considering midterm, please start HW1 as soon as possible.

HW1 hints

- [1] Unchecked system call returning code – 1 bug
- [2] Stack buffer overflow/underflow – 1 bug
- [3] Command injection – 1 bug
- [4] Arithmetic overflow/underflow – 7 bugs
- [5] Heap overflow/underflow – 2 bugs
- [6] Temporal memory safety violation 1 bug
- [7] Local persisting pointers – 1 bug
- [8] String vulnerability – 1 bugs
- [9] Iteration errors – 3 bugs
- [10] Wrong operators – 2 bugs
- [11] Type error – 1 bug

HW1 hints

Total 21 bugs (except example bugs)

- Checkerboard.c (4 bugs)
  - [5] - 1, [6] - 1, [4] – 2
- Circle.c (2 bugs)
  - [5] - 1, [10] - 1
- Filter.c (3 bugs)
  - [7] – 1, [8] – 1, [9] – 1
- Rect.c (3 bugs)
  - [9] – 2, [11] – 1
- resize.c (4 bugs)
  - [4] – 3, [10] – 1
- solid.c (5 bugs)
  - [1] – 1, [2] – 1 , [3]- 1, [4] – 2

How to read [x]-y? → there are y type-x bugs

[5]-1 → There is one type-5 bug

[9]-2 → There are two type-9 bugs

HW1 hints

- [1] Unchecked system call returning code
  - Add proper check function (e.g., malloc)
- [2] Stack buffer overflow/underflow
- [3] Command injection
  - Remove “system” call, if available
- [4] Arithmetic overflow/underflow
- [5] Heap overflow/underflow
- [6] Temporal memory safety violation
- [7] Local persisting pointers
  - Please check piazza example

HW1 hints

- [8] String vulnerability
  - Omitted null terminator in string
- [9] Iteration errors
  - Off-by-one error

```
char exampleArray[] = { 'H', 'e', 'l', 'l', 'o', ' ', 'W', 'o', 'r', 'l', 'd' };

for(int i = 0; i <= 11; i++)
{
  print(exampleArray[i])
}
```

- [10] Wrong operators
  - `==` instead of `=`
- [11] Type error
  - Foo(char**)
  - Char *test; Foo(test);