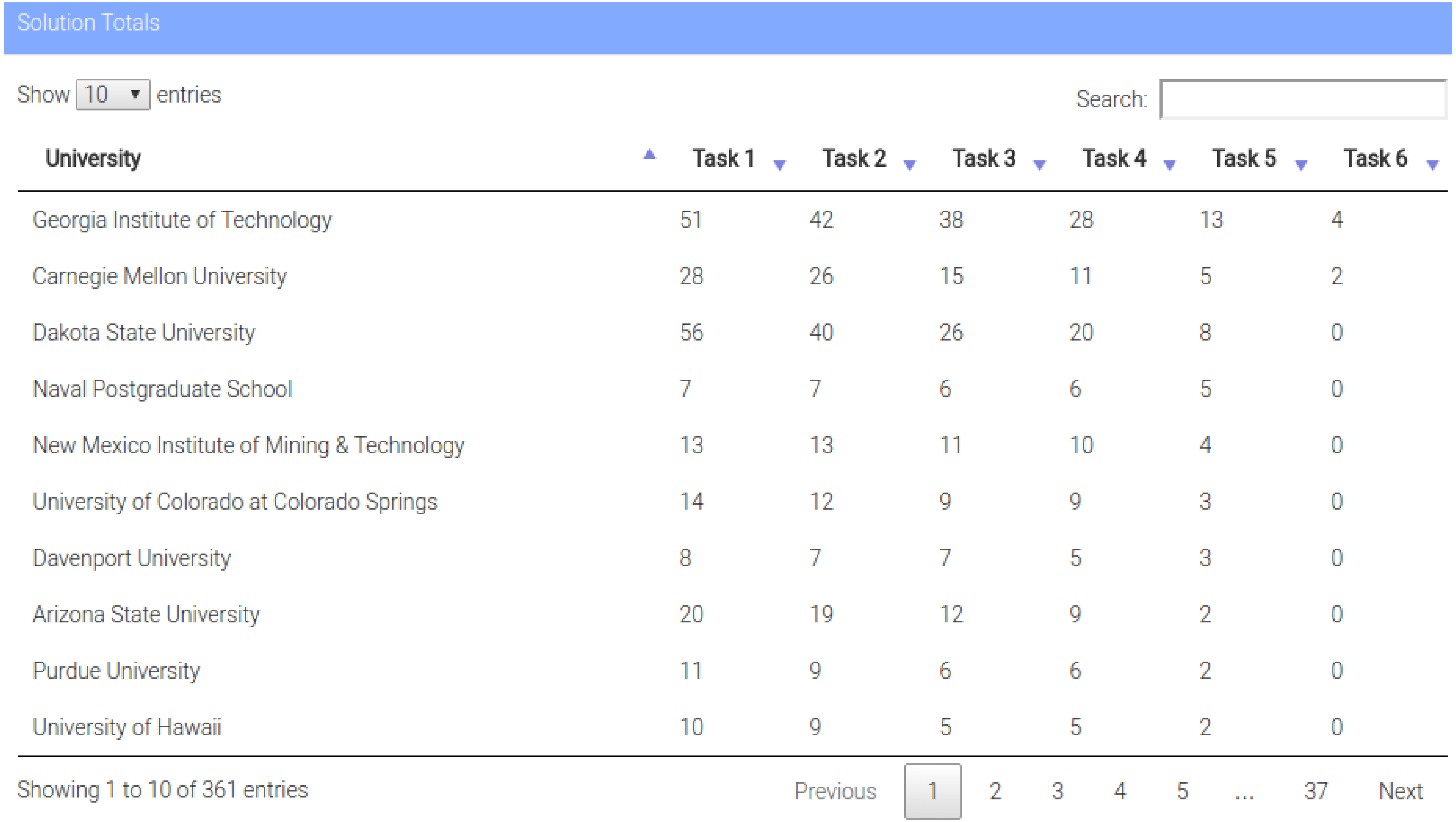
Lec09: Miscellaneous

Insu Yun

Scoreboard

NSA Codebreaker Challenges



Solution Totals

Show 10 entries

Search:

University	Task 1	Task 2	Task 3	Task 4	Task 5	Task 6
Georgia Institute of Technology	51	42	38	28	13	4
Carnegie Mellon University	28	26	15	11	5	2
Dakota State University	56	40	26	20	8	0
Naval Postgraduate School	7	7	6	6	5	0
New Mexico Institute of Mining & Technology	13	13	11	10	4	0
University of Colorado at Colorado Springs	14	12	9	9	3	0
Davenport University	8	7	7	5	3	0
Arizona State University	20	19	12	9	2	0
Purdue University	11	9	6	6	2	0
University of Hawaii	10	9	5	5	2	0

Showing 1 to 10 of 361 entries

Administrivia

- Due: Lab09 is out and its due on Nov 10
- NSA Codebreaker Challenge → Due: Dec 1

Discussion: Lab08

- What's the most "annoying" bug or challenge?
- What's the most "interesting" bug or challenge?
- What's different between remote & local?

Discussion: passwd

- What was the problem?
- How did you solve?

Discussion: mini-shellshock

- What was the problem?
- How did you solve?

Discussion: mini-shellshock

- CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, and CVE-2014-7187
-

specially crafted environment variable # Discussion: mini-shellshock CGI

(Common Gateway Interface)

- HTTP headers → Environment variable
-

If script is a *bash* script?

Discussion: obscure

- What was the problem?
- How did you solve?

Discussion: obscure

- ARM
  - different calling convention
  - r0: first argument

Discussion: obscure

```
__libc_csu_init (int argc, char **argv, char **envp)
 {
   const size_t size = __init_array_end - __init_array_start;
   for (size_t i = 0; i < size; i++)
       (*__init_array_start [i]) (argc, argv, envp);
}
```

Disscussion: obscure

```
.text:00008610          ADD     R4, R4, #1
.text:00008614          LDR     R3, [R5,#4]!
.text:00008618          MOV     R0, R7          // R0 = R7
.text:0000861C          MOV     R1, R8
.text:00008620          MOV     R2, R9
.text:00008624          BLX     R3              // EIP = R3
.text:00008628          CMP     R4, R6
.text:0000862C          BNE     loc_8610
.text:00008630          LDMFD   SP!, {R3-R9,PC} // R3...R9 & PC
```

Discussion: ieee754

- What was the problem?
- How did you solve?

Discussion: diehard

- What was the problem?
- How did you solve?

Discussion: array

- What was the problem?
- How did you solve?

2kills

- What was the problem?
- How did you solve?

jmp-to-where2

- What was the problem?
- How did you solve?

return-to-dl

- What was the problem?
- How did you solve?

return-to-dl

- How GOT works?
- make fake SYMTAB, STRTAB ...

2048_game

- What was the problem?
- How did you solve?

2048_game

- How to calculate address?

2048_game

- Using format string, arbitrary read!
- Extract binary is also possible

Lab09: Miscellaneous

- integer overflow
- web
- race condition
- interesting exploit techniques

Today's Tutorial

- In-class tutorial:
  - One shot exploit

Today's Totorial

```c
int main() {
    char buf[0x100];
    printf("Give me something...");
    fgets(buf, 2 * sizeof(buf), stdin);
}
```

Today's Totorial

- [...][printf plt][pop ret][__libc_start_main GOT][main]

Today's Totorial

- calculate system based on leaked address
- [...][system][XXXX][/bin/sh addr]

In-class Tutorial

```
$ git git@clone tc.gtisc.gatech.edu:seclab-pub cs6265
or
$ git pull
$ cd cs6265/lab08
$ ./init.sh

$ cd tut
$ cat README
```

Lec09: Miscellaneous

Insu Yun