

CS2506 C05: Heap Spraying

2017 Nov.17-Dec.11

17FALL CS 2506: C05 Heap Spraying

CS 2506 Computer Organization II

[Staff](#)

[Course Syllabus](#)

[Calendar](#)

[Assignments](#)

[Resources](#)

[Forum](#)

MIPS4	Cache Memory	N/A	here	23:59 Dec 1	5%	Nov 13
-------	------------------------------	-----	----------------------	-------------	----	--------

	C/x86 Assignments	Associated Files	Due	Weight	Last Modified
x86	Attack Lab Warmup session: pptx pdf	N/A	23:59 Oct 25	8%	Aug 31
C01	Set Type in C	C01 Test Harness	23:59 Sept 18	5%	Sept 3
C02	Parsing MIPS32 Instructions	C02 Test Harness (see README)	23:59 Oct 20	6%	Sept 25
C03	MIPS32 Disassembler Warmup Session pptx pdf	C03 Test Harness Unpack, read header comment in gradeC03.sh	Milestone: 23:59 Nov 13 Final: 23:59 Dec 6	1.4% 12.6%	Aug 28
C04	Hamming Codes Submit a .c file, not a tar file	C04 Test Harness	23:59 Dec 13	5%	Dec 12
C05	Heap Spraying	N/A	23:59 Dec 11	3%	Nov 17

stewes36@vt.edu,

**“This assignment was very challenging,
but a lot of fun too!”**

Step 1. Payload to execute './success' in the victim server

construct the necessary assembly code to perform a system call to start executing the “./**success**” program.

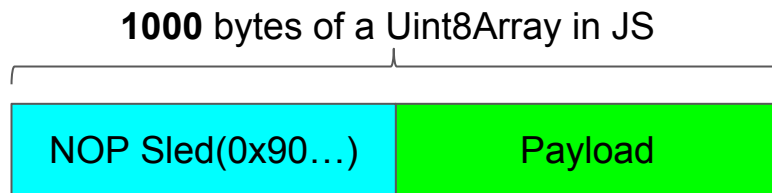
```
0000000000400078 <start>:
400078: 48 c7 c0 3b 00 00 00    mov     $0x3b,%rax
40007f: 48 8d 3d 10 00 00 00    lea     0x10(%rip),%rdi    # 400096
<hello>
400086: 48 c7 c6 00 00 00 00    mov     $0x0,%rsi
40008d: 48 c7 c2 00 00 00 00    mov     $0x0,%rdx
400094: 0f 05                  syscall
```

```
0000000000400096 <hello>:
400096: 2e 2f                  cs (bad)
400098: 73 75                  jae     40010f <hello+0x79>
40009a: 63 63 65              movslq  0x65(%rbx),%esp
40009d: 73 73                  jae     400112 <hello+0x7c>
```

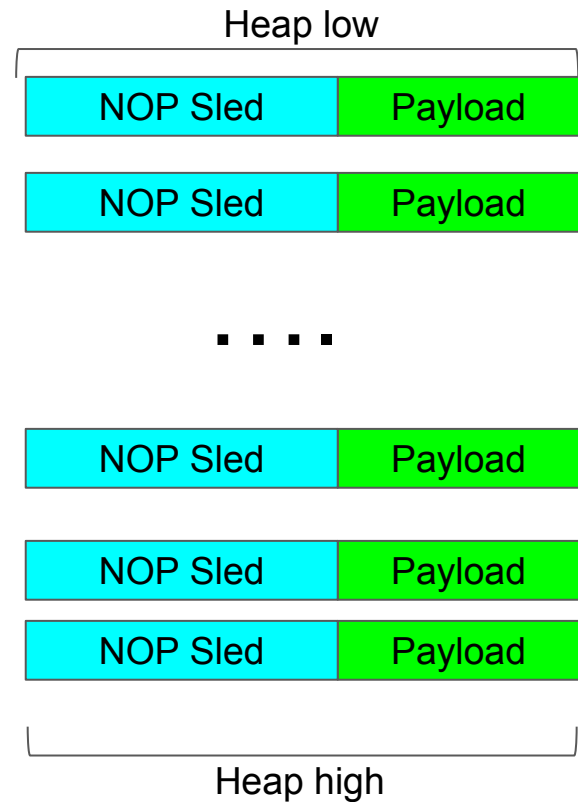
Payload

Step 2. Nop sled

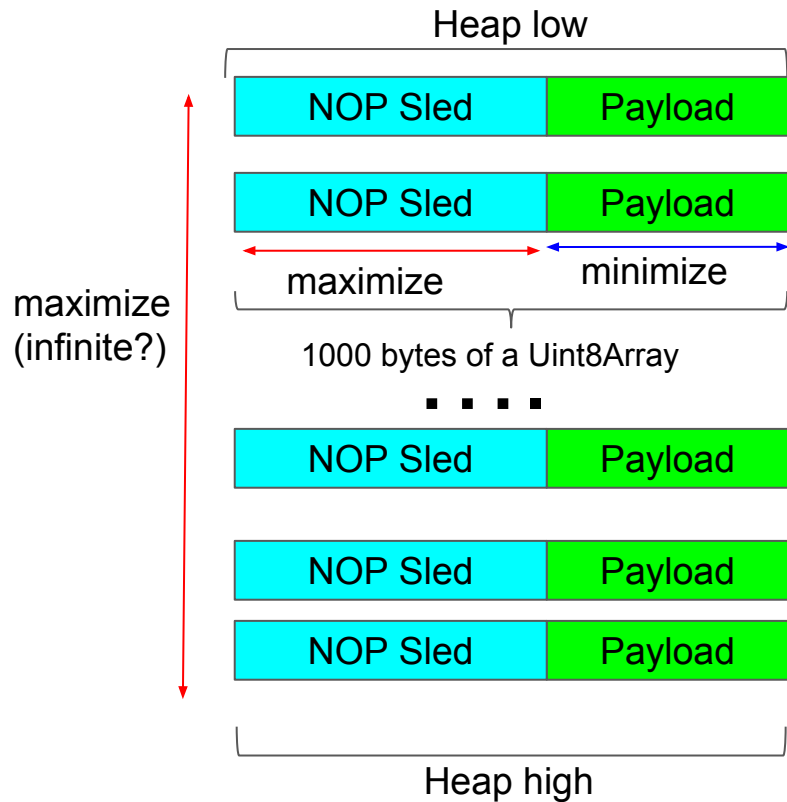
```
var obj =  
new Uint8Array(1000);
```



Step 3. Heap spraying



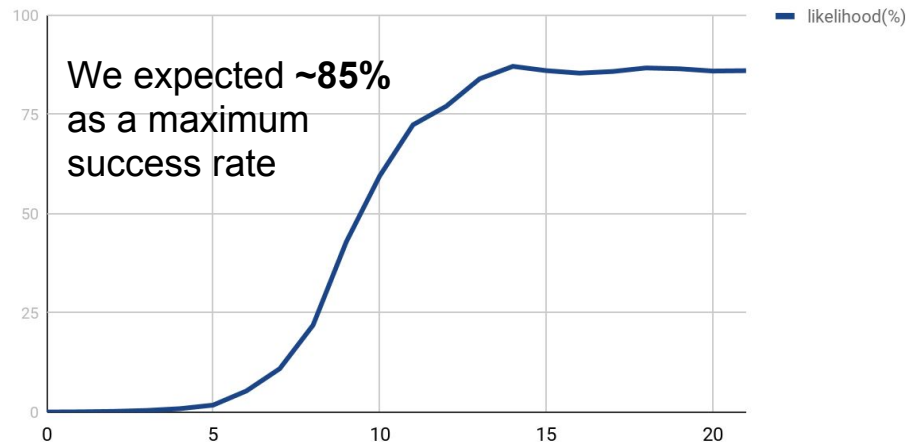
Maximizing the Likelihood of attack



gadgets#	allocated Heapsize	gadgets span	Likelihood(%)
2 ⁰	1.66MB	1000B	0.06
2 ¹	1.66MB	290.6KB	0.11
2 ²	1.66MB	292.7KB	0.22
2 ³	1.66MB	312.76KB	0.45
2 ⁴	1.66MB	319.18KB	0.90
2 ⁵	1.66MB	319.18KB	1.80
2 ⁶	1.11MB	319.18KB	5.37
2 ⁷	1.09MB	483.99KB	10.97
2 ⁸	1.09MB	514.29KB	21.94
2 ⁹	1.09MB	704.95KB	42.96
2 ¹⁰	1.6MB	1.22MB	59.51
2 ¹¹	2.63MB	2.26MB	72.40
2 ¹²	4.95MB	4.61MB	77.09
2 ¹³	9.08MB	8.73MB	83.99
2 ¹⁴	17.5MB	17.13MB	87.14
2 ¹⁵	35.45MB	35.18MB	86.06
2 ¹⁶	71.55MB	71.14MB	85.43
2 ¹⁷	142MB	141.75MB	85.85
2 ¹⁸	283.3MB	280.95MB	86.74
2 ¹⁹	563.65MB	561.85MB	86.53
2 ²⁰	1.11GB	1.11GB	85.96
2 ²¹	2.22GB	2.21GB	86.05

Expectation

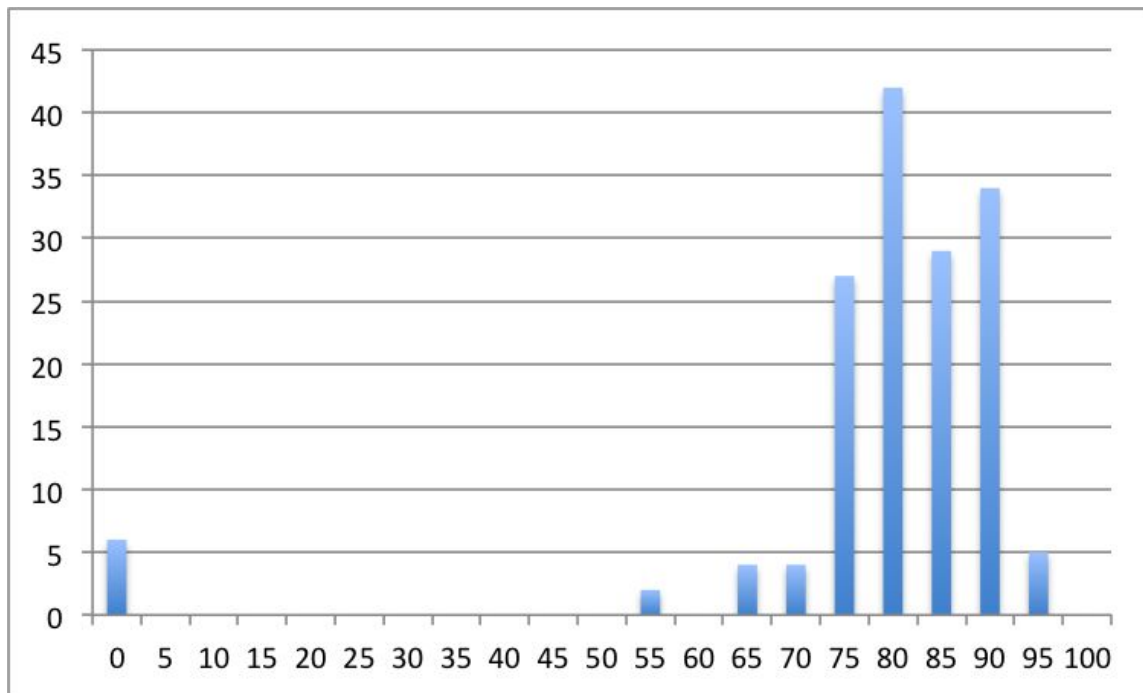
2^N gadgets versus Likelihood(%) of attack with 1000 bytes
Uint8Array



Study Result

105 teams (**153** students)
in cs2506 class

Most of students achieved the
attacks and knew the way to
increase the
Likelihood.



forum.cs.vt.edu



A screenshot of a web browser displaying a forum page. The address bar shows the URL https://forum.cs.vt.edu/board_show.pl?bid=346. The page contains a list of forum topics, each with a checkbox, a title, an author, and a count. The topics are related to a course, likely C04, and include discussions about grading, submission, and office hours.

Topic	Author	Count
<input type="checkbox"/> C04 Overview Entry Definition	glio07	9
<input type="checkbox"/> File Requirement for C04	kkc6	2
<input checked="" type="checkbox"/> Heap Spraying Grading	dallada1	6
<input checked="" type="checkbox"/> heap spray error message	yibing1	2
<input checked="" type="checkbox"/> C04 Curator	jdm2980	1
<input checked="" type="checkbox"/> C03 Scores Updated	wmcquain	1
<input checked="" type="checkbox"/> For hamming code, why the parameter pBits are uint8_t	gli007	3
<input checked="" type="checkbox"/> Is Heap Spraying a team work?	gli007	2
<input checked="" type="checkbox"/> Office Hours changes	akpaul	1
<input checked="" type="checkbox"/> Heap Spraying submission	joo918	2
<input checked="" type="checkbox"/> Heap Spraying Final Submission Portal	m4i6r1o	12
<input type="checkbox"/> C03 Scores	wmcquain	1
<input checked="" type="checkbox"/> File Format Reminder	wmcquain	1
<input checked="" type="checkbox"/> Grade Updates	wmcquain	1
<input type="checkbox"/> C03 Scores	wmcquain	1
<input type="checkbox"/> Valgrind Results for C04	vtodd15	2
<input checked="" type="checkbox"/> Heap Spraying Q&A	ankijin	9
<input checked="" type="checkbox"/> Nick Office Hours Canceled 12/7	nickhrdy	1
<input checked="" type="checkbox"/> No successes in heap spraying	m4i6r1o	14
<input type="checkbox"/> Office hours update	bharti	1
<input checked="" type="checkbox"/> Can't find makefile	ankitd20	3
<input checked="" type="checkbox"/> C03 Disassembler on Curator	m4i6r1o	2
<input type="checkbox"/> Disassembler input/output files?	yevhenp	2
<input checked="" type="checkbox"/> HW MIPS4	gli007	1
<input checked="" type="checkbox"/> Heap Spraying Help	vtodd15	3
<input checked="" type="checkbox"/> Heap Spraying	stewes36	3
<input type="checkbox"/> Alex Office Hours Moved 12/1/17	alexs9	1
<input checked="" type="checkbox"/> Final Exam Time and Location	wmcquain	1
<input type="checkbox"/> Updated office hours for 12/01	bharti	1
<input type="checkbox"/> Sukrit - Office Hours 11/27 - 12/01	sukrit	2
<input type="checkbox"/> No Office Hours Today (Nov 28) and Thursday (Nov 30)	wmcquain	1
<input checked="" type="checkbox"/> Lawrence Office Hours Moved 11/28	lawps7	1
<input checked="" type="checkbox"/> MIPS04 AMAT unit	gli007	1
<input checked="" type="checkbox"/> Heap Spraying	wmcquain	5

We mainly discussed the following issues in the cs forum.

- **Assembly codes**
 - Some students didn't add an ending '\0' to the shellcode
- **How to spray out the codes**
 - They didn't know how many NOP+SHELLCODE instances can touch the ./success (over 30,000)
- **Team works or not?**
- **Submission portal issues**
 - Some assembly codes made zombie process in the server
- **Javascript codes issues**
 - Most of them were unfamiliar with JS
- **Grading issues**

Submission

Submission Instructions for CS2506 CyberSecurity Lab Fall 2017

File Edit View Insert Format Tools Table Add-ons Help See new changes

75% - Heading 2 - Trebuchet ... - 13 - B I U A - CD 19 total viewers

Submitting attacker's files

- Move to submission portal of cs2506 and log in with PID and SLO password
 - <https://courses.cs.vt.edu/cs2506/autograder/#/login>
- Move to autograder tab or move to here by:
 - <https://courses.cs.vt.edu/cs2506/autograder/#/autograder/submissions>
 - switch submission_id either "cs2506test" or "cs2506final"
- Upload attacker's javascript file and wait for the result
 - Choose a javascript(*.js) file from your computer and submit it.
 - Waiting for the Status COMPLETE
 - You can see the updated Status by refreshing your browser

ID	Submission	Created	Last Modified	Status
id220968e	c9947c08-6564-4317-8659-8ea7930240c5	2017-11-15 15:08:04	2017-11-15 15:08:04	NEW
id220968e	c9947c08-6564-4317-8659-8ea7930240c5	2017-11-15 15:08:04	2017-11-15 15:08:04	PROCESSING
id220968e	c9947c08-6564-4317-8659-8ea7930240c5	2017-11-15 15:08:04	2017-11-15 15:08:04	COMPLETE

Status: **NEW**

your javascript file is just submitted.

Status: **PROCESSING**

Your javascript file is loaded and is running on the browser. You should not be able to see the result yet.

Status: **COMPLETE**

You can see the result as below by expanding tabs

> COMPLETE > grade

Kijin An
6:47 PM Dec 8
Resolve

chrome browser recommended

Kijin An
8:35 PM Yesterday
Send me email if you have questions.
(ankijin.vt.edu)

Submission Instructions for CS2506 CyberSecurity Lab Fall 2017

File Edit View Insert Format Tools Table Add-ons Help See new changes

75% - Heading 2 - Trebuchet ... - 13 - B I U A - CD More -

```
Result for TEST Submission: 4716a05-499c-4d32-af6b-62b495205d6
number of success: 4 / 5

trial # 1
trying to run maliciouspage.html
Loaded page: A malicious page
triggerOverflow
upgrading segment 0x2505000-0x3350000
jumping to 0x2505000
success: true

trial # 2
trying to run maliciouspage.html
Loaded page: A malicious page
triggerOverflow
upgrading segment 0x2505000-0x3350000
jumping to 0x2505000
SLOM Segmentation Fault (core dumped)
```

Final Submission and partnership

You should submit a version of "cs2506final" before the deadline. Please specify your partnership in your submission version of javascript file. A team can submit it once and you can check PIDs in the final result.

```
var obj = new Uint8Array(1000); //maximum size of Uint8Array is 1000
var info = {};
triggerOverflow(obj, info);
if (info.error) {
    console.log(info.error);
} //error if obj is not a Uint8Array
```

Kijin An
6:10 PM Dec 7
Resolve

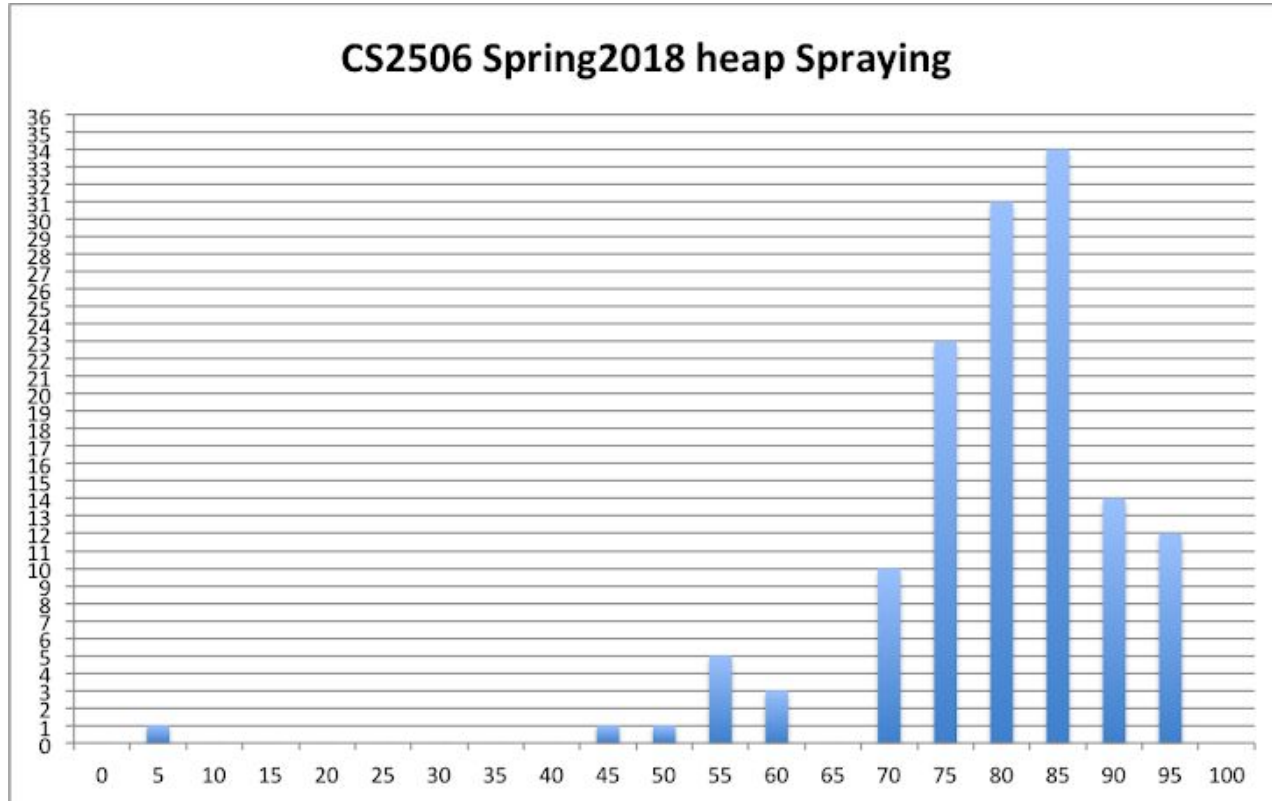
specify your PID if you don't have a partner.

Gene Kim
3:34 AM Dec 9
Resolve

if anyone would like to partner for this lab, txt me at 5712056543

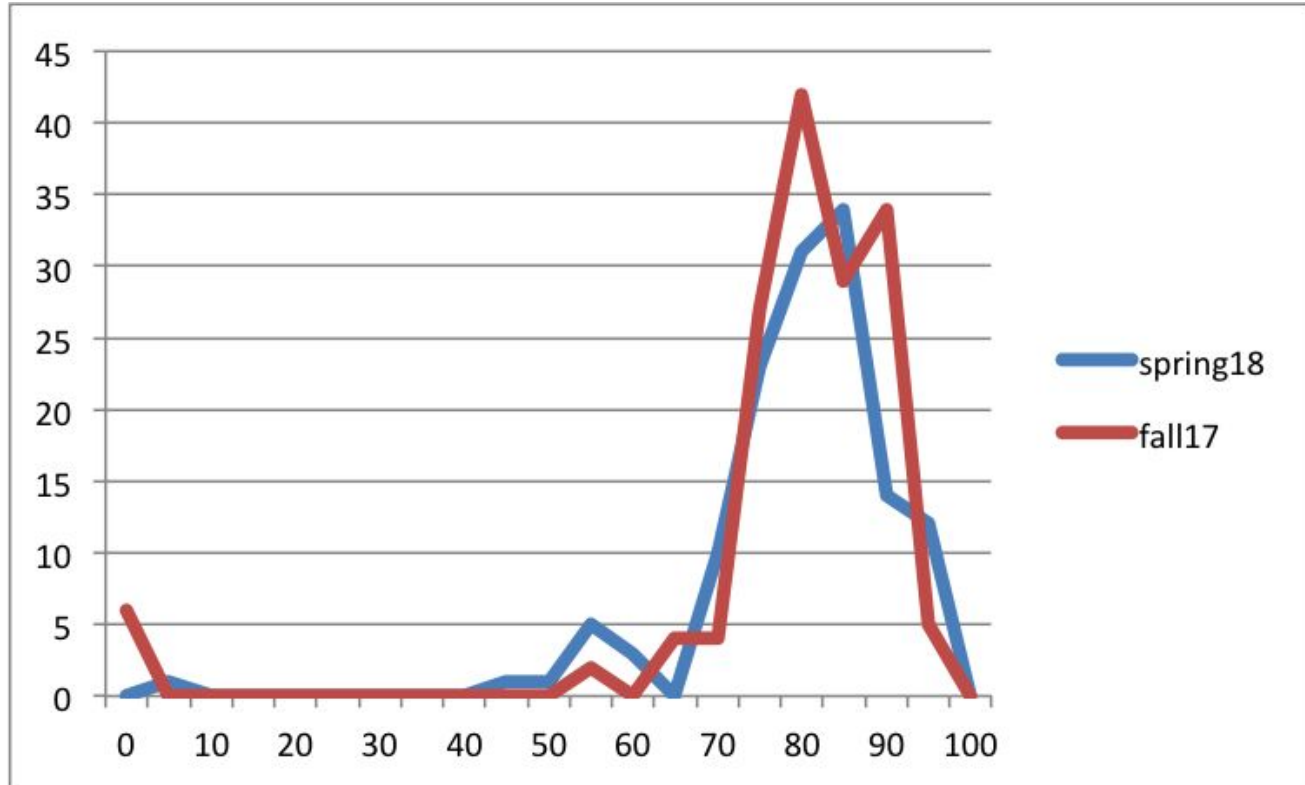
CS2506 Spring 2018

Spring 2018



Over 160 students, 135 students (97 teams) submitted the final versions within the due date. The following graph show their best success rates in this term.

Comparison



Grading policy

- Success rate 50/100 - 100%
- Success rate 20-50 - 90%
- Success rate $0 < 20$ - 80 %
- Success rate 0 - partial credit not to exceed 40%. (The last category would require a code review by the responsible TA.)