

Lec10: Heap Exploitation

Taesoo Kim

NSA Codebreaker Challenges

Carnegie Mellon University	11	5	5	2	2	2	2
Lafayette College	3	2	2	1	1	1	1
Georgia Institute of Technology	32	19	16	8	5	3	0
Pennsylvania State University	55	14	11	6	3	3	0
University of Hawaii	21	10	8	4	3	2	0
University of Tulsa	14	6	6	5	2	1	0
Purdue University	12	7	7	1	1	1	0
Virginia Community College System	15	2	1	1	1	1	0
Lesley University	1	1	1	1	1	1	0
Technical University of Munich	1	1	1	1	1	1	0

Administrivia

- Just **one** more lab after this week!
- Last lab (Lab11) includes alternative **Web exploitation** (e.g., xss/sqlinj)
- Due: **Lab10** is out and its due on **Nov 16**
- [NSA Codebreaker Challenge](#) → Due: **Nov 30**

Grading

- In the last lecture (Dec 1), we will let you know your grade
- If that's not the grade that you wanted, you have two more weeks for additional work (let's discuss in person)
- Dec 1 : Real world exploitation
 - Exploiting JS engine vuln.
 - Exploiting Linux kernel heap vuln.

Best Write-ups for Lab09

- 2048-int: brian_edmonds, shudak3
- intq: brian_edmonds, N/A
- race: carterchen, shudak3
- urandom: brian_edmonds, mansourah
- concat: carterchen, jallen309
- type: rohandvora, nagendra
- django: jallen309, carterchen
- tictou: markwis, carterche
- srop: sralhan6, rohandvora/jallen309
- simple-aeg: dhaval, jallen309

Discussion: Lab09

- What's the most “annoying” bug or challenge?
- What's the most “interesting” bug or challenge?
- or .. just exhausted?

Discussion: 2048-int

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

Discussion: intq

- (in 64-bit) what does the expression, $1 > 0$, evaluate to?
 - ? (a) == 0, (b) == 1, (c) == NaN, (d) == -1
- (unsigned short) $1 > -1$?
 - ? (a) == 1, (b) == 0, (c) == -1, (d) undefined
- $-1U > 0$?
 - ? (a) == 1, (b) == 0, (c) == -1, (d) undefined

Discussion: intq

- $-1L > 1U$? on x86-64 and x86
 - ? (a) 0 on both platforms, (b) 1 on both platforms, (c) 0 on x86-64, 1 on x86, (d) 1 on x86-64, 0 on x86
- `UINT_MAX + 1`?
 - ? (a) 0, (b) 1, (c) `INT_MAX`, (d) `UINT_MAX`, (e) undefined
- (in 32-bit) what's `abs(-2147483648)`?
 - ? (a) `== 0`, (b) `< 0`, (c) `> 0`, (d) `== NaN`

Discussion: intq

- $-1 \ll 2$?
 - ? (a) 0, (b) 4, (c) INT_MAX, (d) INT_MIN, (e) undefined
- $\text{INT_MAX} + 1$?
 - ? (a) 0, (b) 1, (c) INT_MAX, (d) UINT_MAX, (e) undefined
- $-\text{INT_MIN}$?
 - ? (a) 0, (b) 1, (c) INT_MAX, (d) UINT_MAX, (e) INT_MIN, (f) undefined

Discussion: race

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

Discussion: urandom

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

Discussion: type

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

Discussion: django

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

Discussion: tictou

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

Discussion: SROP

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

```
mov    rax, 0xf  
syscall
```

Lab10: Heap Exploitation

- various malloc implementation (e.g., dlmalloc, ptmalloc)
- use-after-free
- double-free techniques

Today's Tutorial

- In-class tutorial:
 - Your first heap exploitation
 - Exploring heap memory structure in G

In-class Tutorial

```
$ ssh YOURID@cyclonus.gtisc.gatech.edu -p 2023
$ ssh YOURID@cyclonus.gtisc.gatech.edu -p 2022
$ ssh YOURID@computron.gtisc.gatech.edu -p 2023
$ ssh YOURID@computron.gtisc.gatech.edu -p 2022

$ cd tut/lab10
$ cat README
```