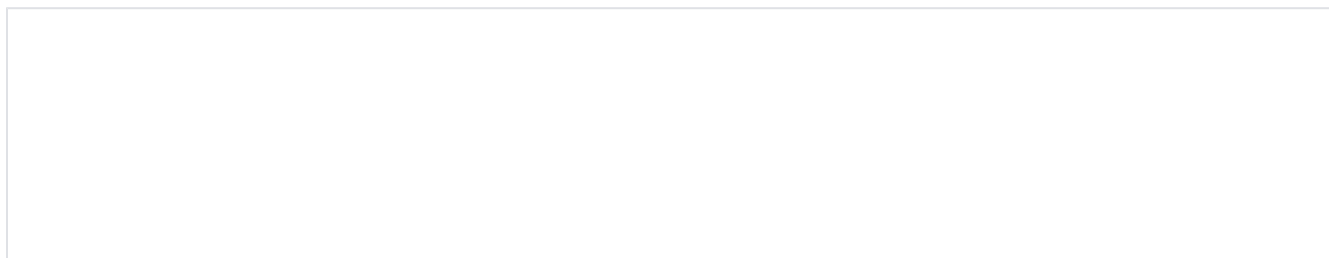


# TechNote

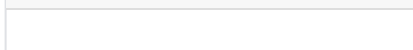
Lazenca.0x0



## Facebook Page

[Lazenca.0x0](#)

## Page tree



## Profile

- **Group**
  - [Twitter Profile](#)
  - [GitHub Profile](#)
  - [Facebook Profile](#)
- **Personal**
  - [Email](#)
  - [Linkedin](#)

## Tool

Title	Creator	Modified
<a href="#">Pwndbg(scwuaptx)</a>	<a href="#">Lazenca.0x0</a>	Jul 27, 2018
<a href="#">PWNTTOOLS</a>	<a href="#">Lazenca.0x0</a>	Jul 20, 2018
<a href="#">Clang Static Analyzer</a>	<a href="#">Lazenca.0x0</a>	Nov 30, 2017
<a href="#">Valgrind - Memcheck</a>	<a href="#">Lazenca.0x0</a>	Nov 28, 2017
<a href="#">ASAN - Address Sanitizer</a>	<a href="#">Lazenca.0x0</a>	Nov 28, 2017
<a href="#">Ponce</a>	<a href="#">Lazenca.0x0</a>	Sep 25, 2017
<a href="#">Triton</a>	<a href="#">Lazenca.0x0</a>	Sep 25, 2017
<a href="#">angr</a>	<a href="#">Lazenca.0x0</a>	Sep 20, 2017
<a href="#">qira</a>	<a href="#">Lazenca.0x0</a>	Jun 29, 2017
<a href="#">pwndbg</a>	<a href="#">Lazenca.0x0</a>	Jun 29, 2017
<a href="#">PEDA</a>	<a href="#">Lazenca.0x0</a>	Jun 29, 2017

Fuzzing		
Title	Creator	Modified
Wadi	Lazenc.a.0x0	Dec 13, 2017
libFuzzer	Lazenc.a.0x0	Dec 13, 2017
Honggfuzz	Lazenc.a.0x0	Dec 05, 2017
Boofuzz	Lazenc.a.0x0	Dec 04, 2017
Domato	Lazenc.a.0x0	Dec 04, 2017
AFL - American fuzzy lop	Lazenc.a.0x0	Nov 07, 2017
radamsa	Lazenc.a.0x0	Aug 20, 2017

Analysis		
Title	Creator	Modified
02.Dynamic program analysis	Lazenc.a.0x0	Nov 30, 2017
01.Static program analysis	Lazenc.a.0x0	Nov 30, 2017
Clang Static Analyzer	Lazenc.a.0x0	Nov 30, 2017
Valgrind - Memcheck	Lazenc.a.0x0	Nov 28, 2017
ASAN - Address Sanitizer	Lazenc.a.0x0	Nov 28, 2017
Valgrind	Lazenc.a.0x0	Nov 28, 2017
04.Concolic execution	Lazenc.a.0x0	Nov 28, 2017
06.DBI(Dynamic Binary Instrumentation)	Lazenc.a.0x0	Nov 28, 2017
05.Taint analysis	Lazenc.a.0x0	Nov 28, 2017
03.Symbolic execution(feat. Concrete execution)	Lazenc.a.0x0	Nov 28, 2017
DynamoRIO	Lazenc.a.0x0	Nov 17, 2017
Dyninst	Lazenc.a.0x0	Nov 17, 2017
PIN	Lazenc.a.0x0	Nov 17, 2017
IR(Intermediate Representation)	Lazenc.a.0x0	Sep 19, 2017

Heap exploits		
Title	Creator	Modified
fastbin_dup_into_stack [English]	Lazenc.a.0x0	Jan 03, 2021
fastbin_dup[English]	Lazenc.a.0x0	Jan 03, 2021
Double free[English]	Lazenc.a.0x0	Jan 03, 2021
Double free[Korean]	Lazenc.a.0x0	Jan 03, 2021
House of Orange[English]	Lazenc.a.0x0	Jan 03, 2021
House of einherjar[English]	Lazenc.a.0x0	Jan 03, 2021
The House of Lore[English]	Lazenc.a.0x0	Jan 03, 2021
The House of Spirit[English]	Lazenc.a.0x0	Jan 03, 2021
The House of Force[English]	Lazenc.a.0x0	Jan 03, 2021
Unsafe unlink[English]	Lazenc.a.0x0	Jan 03, 2021
Poison null byte[English]	Lazenc.a.0x0	Jan 03, 2021
Overlapping chunks[English]	Lazenc.a.0x0	Jan 03, 2021
unsorted bin attack[English]	Lazenc.a.0x0	Jan 03, 2021
first-fit(Use-After-Free) [English]	Lazenc.a.0x0	Jan 03, 2021
House of Orange[Korean]	Lazenc.a.0x0	Jan 03, 2021
House of einherjar[Korean]	Lazenc.a.0x0	Jan 03, 2021
The House of Lore[Korean]	Lazenc.a.0x0	Jan 03, 2021
The House of Spirit[Korean]	Lazenc.a.0x0	Jan 03, 2021
The House of Force[Korean]	Lazenc.a.0x0	Jan 03, 2021
Unsafe unlink[Korean]	Lazenc.a.0x0	Jan 03, 2021

Find more results

**Basic exploit technical**

Title	Creator	Modified
<a href="#">02.Heap Exploitation</a>	<a href="#">Lazenc.0x0</a>	Oct 13, 2019
<a href="#">12.Heap Feng Shui</a>	<a href="#">Lazenc.0x0</a>	Apr 19, 2019
<a href="#">11.Heap Spray</a>	<a href="#">Lazenc.0x0</a>	Apr 18, 2019
<a href="#">10.One-gadgets(feat. PLT/GOT overwrite)</a>	<a href="#">Lazenc.0x0</a>	Apr 17, 2019
<a href="#">09.Race condition</a>	<a href="#">Lazenc.0x0</a>	Apr 16, 2019
<a href="#">08.BROP(Blind Return Oriented Programming)</a>	<a href="#">Lazenc.0x0</a>	Apr 15, 2019
<a href="#">04.Frame faking(Fake ebp)</a>	<a href="#">Lazenc.0x0</a>	Apr 08, 2019
<a href="#">02.Return to Shellcode</a>	<a href="#">Lazenc.0x0</a>	Apr 04, 2019
<a href="#">16.Stack pivot</a>	<a href="#">Lazenc.0x0</a>	Nov 07, 2018
<a href="#">15.Return-to-dl-resolve</a>	<a href="#">Lazenc.0x0</a>	Oct 02, 2018
<a href="#">14.Return-to-csu(__libc_csu_init)</a>	<a href="#">Lazenc.0x0</a>	Sep 06, 2018
<a href="#">13.JOP(Jump-Oriented Programming)</a>	<a href="#">Lazenc.0x0</a>	Aug 27, 2018
<a href="#">06.ROP(Return Oriented Programming)</a>	<a href="#">Lazenc.0x0</a>	Aug 15, 2018
<a href="#">07.SROP(Sigreturn-oriented programming)</a>	<a href="#">Lazenc.0x0</a>	May 27, 2018
<a href="#">05.Frame Pointer Overwrite</a>	<a href="#">Lazenc.0x0</a>	Apr 22, 2018
<a href="#">03.RTL(Return to libc)</a>	<a href="#">Lazenc.0x0</a>	Apr 11, 2018
<a href="#">01.Shellcode</a>	<a href="#">Lazenc.0x0</a>	Feb 23, 2018

## Protection Tech

Title	Creator	Modified
<a href="#">06.PIE</a>	<a href="#">Lazenc.a.0x0</a>	Nov 28, 2018
<a href="#">05.PIC</a>	<a href="#">Lazenc.a.0x0</a>	Nov 28, 2018
<a href="#">01.NX Bit(MS : DEP)</a>	<a href="#">Lazenc.a.0x0</a>	Mar 18, 2018
<a href="#">04.RELRO</a>	<a href="#">Lazenc.a.0x0</a>	Sep 05, 2017
<a href="#">03.Canaries</a>	<a href="#">Lazenc.a.0x0</a>	Sep 05, 2017
<a href="#">02.ASLR</a>	<a href="#">Lazenc.a.0x0</a>	Sep 05, 2017

