# 02.Heap Exploitation

## List



### Heap Exploit

Description of Heap Exploitation.

| Title | Creator | Modified |
|---|---|---|
| House of Orange | Lazenca.0x0 | Feb 04, 2020 |
| Overlapping chunks | Lazenca.0x0 | Jan 25, 2020 |
| Poison null byte | Lazenca.0x0 | Jan 25, 2020 |
| unsorted bin attack | Lazenca.0x0 | Jan 23, 2020 |
| unsafe unlink | Lazenca.0x0 | Oct 13, 2017 |
| Overlapping chunks 2 | Lazenca.0x0 | Aug 09, 2017 |
| House of einherjar | Lazenca.0x0 | Aug 04, 2017 |
| fastbin_dup_into_stack | Lazenca.0x0 | Aug 04, 2017 |
| fastbin_dup | Lazenca.0x0 | Aug 04, 2017 |
| first-fit(Use-After-Free) | Lazenca.0x0 | Aug 04, 2017 |
| The House of Lore | Lazenca.0x0 | Aug 04, 2017 |
| The House of Spirit | Lazenca.0x0 | Aug 03, 2017 |
| The House of Force | Lazenca.0x0 | Aug 03, 2017 |

## Exploit table

## Exploit table

| Exploits | Access area | | Overwrite area | | | | | Free | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Stack | Heap | Top chunk | F - size | F - bk | A - prev_size | A - size | Double Free | Free (Stack area) | |
| First fit | | O | | | | | | | | |
| Fastbin dup | | O | | | | | | O | | |
| Fastbindupinto stack | O | | | | | O | | O | | |
| Poison null byte | | O | | O (1byte) | | | | | | |
| Overlapping chunks | | O | | O | | | | | | |
| Overlapping chunks 2 | | O | | O | | | | | | |
| House of einherjar | O | | | | | O | O | | | |
| The House of Force | O | | O | | | | | | | |
| The House of Lore | O | | | | O | | | | | |
| The House of Spirit | O | | | | | | | | O | |
| Unsorted bin attack | O | | | | O | | | | | |
| Unsafe unlink | O | | | | | O | O | | | |