Exercise: The Basic Solution

Return Address — 0xAABBCDA6

code

Data in this region are provided by users

AABBCDA6

AP → 0xAABBCCDD

28 bytes

AP →

fmt

to decimal 28...

0xAABBCCFF

$\frac{0}{0} \times \frac{0}{0} \times \frac{0}{0} \times \frac{0}{0} \times \frac{0}{0} \times \frac{0}{0} \times on$

$\frac{0}{0.8} \times \frac{0}{0.8} \times \quad \frac{0}{0.8} \times \frac{0}{0.} - \times \frac{0}{0n}$

$4 + (48)$

52

$z - 52$
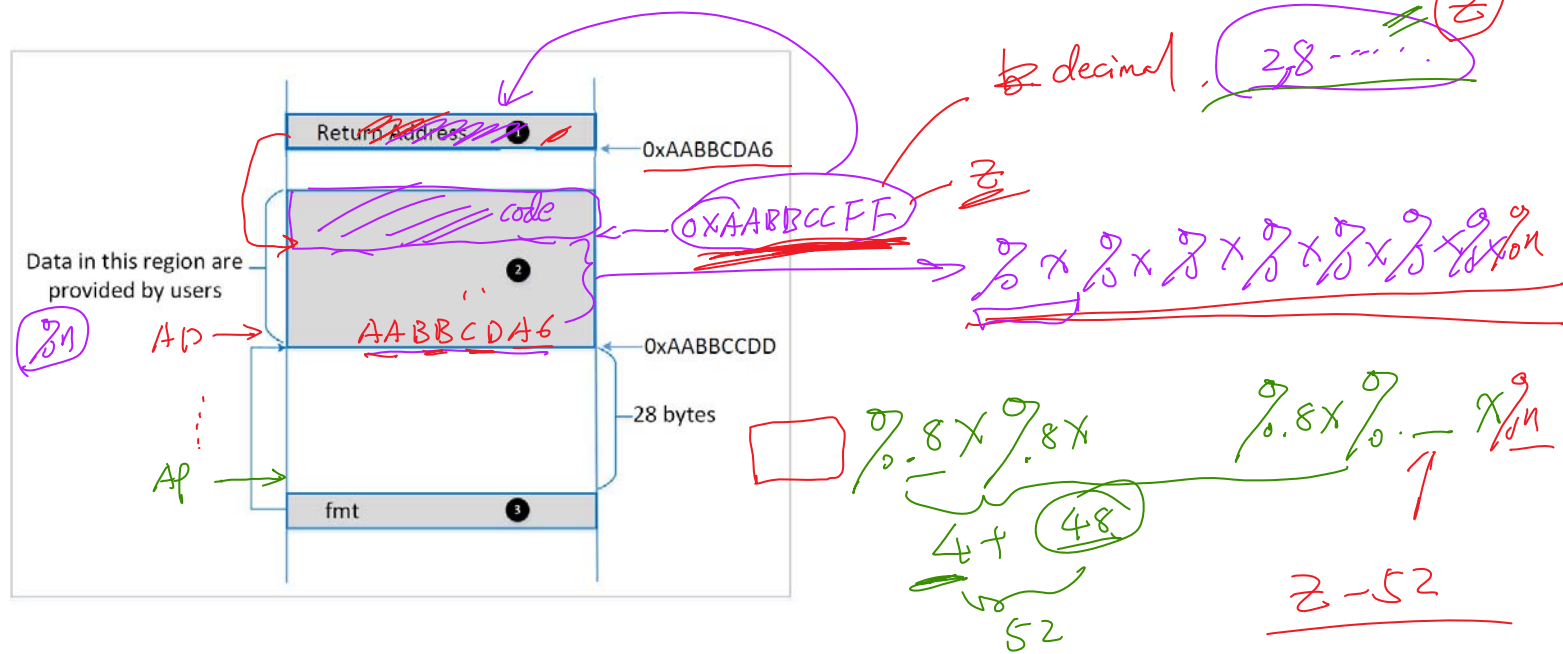
Exercise: An Improved Solution

Return Address ① ← 0xAABBCDA6

Data in this region are provided by users

AABBCDA6
:@@@@
AABBCDA8   ② ← AABBCCFF

← 0xAABBCCDD

28 bytes

fmt ③

%hn

① ← 0xAABBCDA8
← 0xAABBCDA6

High ← AA / BB / CC / FF ← Low
AABBCDA8
AABBCDA6
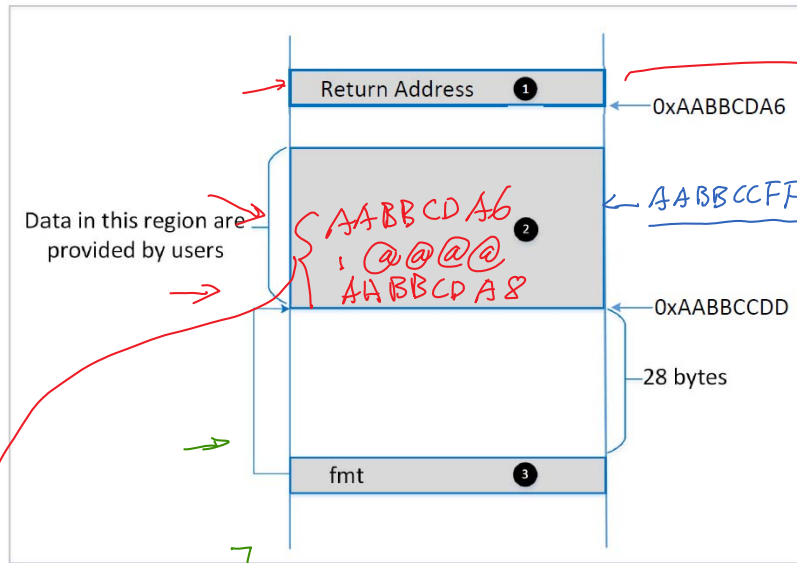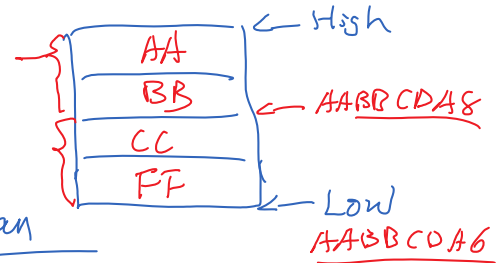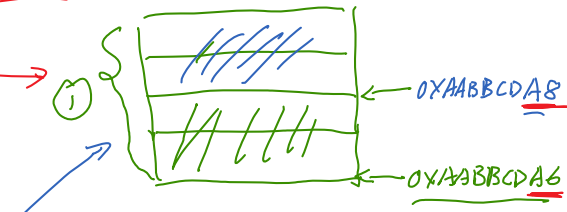
Big Endian

Little Endian

7
%x ···· %x %hn %.|x %hn

12   0XAABB − 12   0XCCFF − 0XAABB = T

Exercise: Return-to-libc Attack

"/bin/sh" : Address 0XAABBEGFF

0XAABBCDAA

| Return Address ① |
← 0xAABBCDA6

system( ) :

0X 99887766

Data in this region are
provided by users

AABBCCFF ←

0XAABBCDAA
@ @ @ @ —
0XAABBCDA6

← 0xAABBCCDD

28 bytes

| fmt ③ |