درس ۷

ASM

stack

hello.asm

```
push rbp
mov rbp, rsp
...
pop rbp
ret
```

همه را یاد بگیرید @MyWebUniversity-Dari

یک کورس رایگان از MyWebUniversity

زبان Assembly

درس ۷

stack: push، pop، call و ret

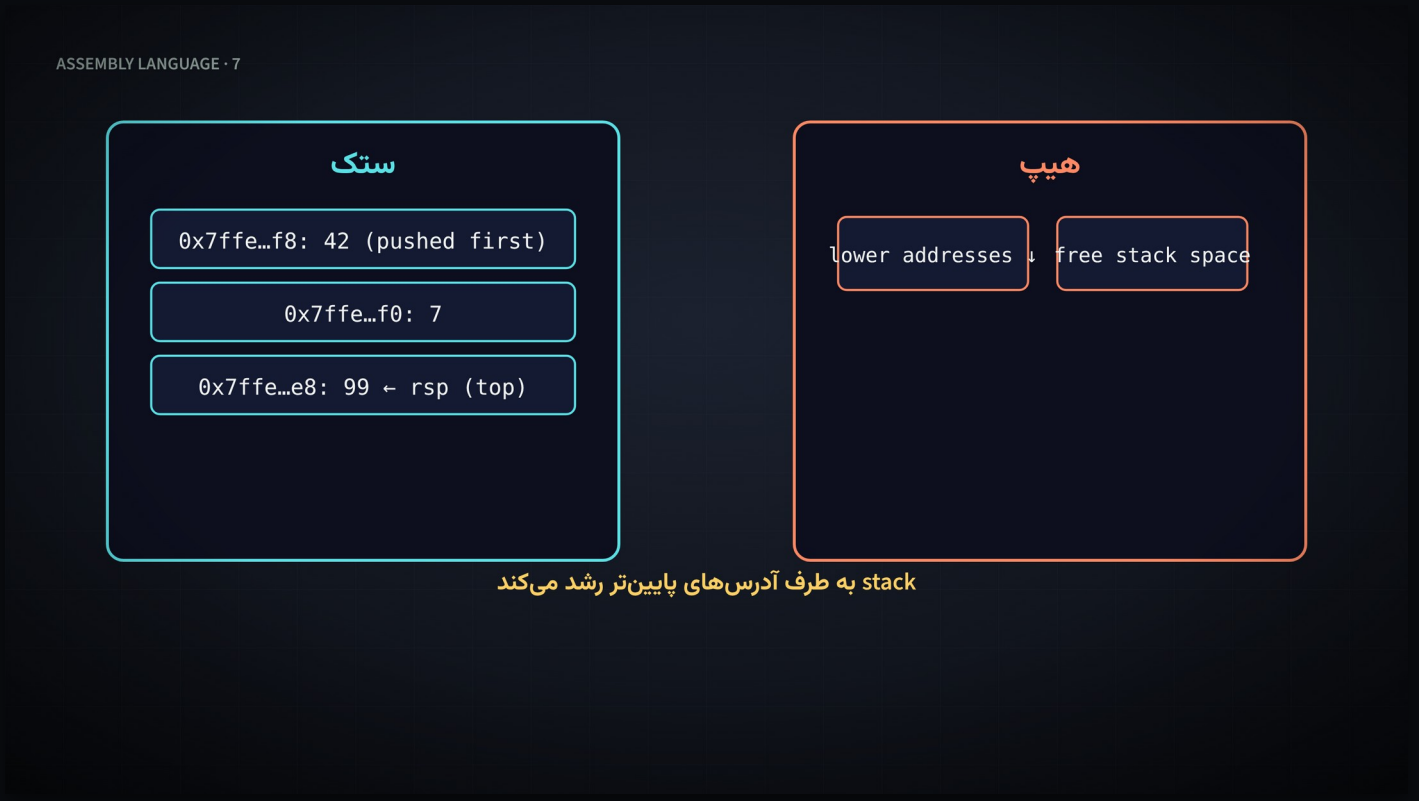
rsp، push و pop، call و ret، آدرس‌های برگشت و stack frame ها



stack چیست؟

stack یک ناحیهٔ حافظه است که به شکل آخر وارد، اول خارج استفاده می‌شود. rsp، یعنی stack ...

در stack، x86 به پایین رشد می‌کند: push کردن rsp را کوچک‌تر می‌کند، و pop کردن آن را بزرگ‌تر.



01

push و pop

push هشت را از rsp کم می‌کند و یک مقدار را آنجا می‌نویسد. pop مقدار در rsp را به یک ...

از آن‌ها برای ذخیرهٔ register هایی که باید نگه دارید استفاده کنید، و همیشه به ترتیب برعکس ...

ASSEMBLY LANGUAGE · 7

stack.asm

```
push rbx              ; save rbx
push r12              ; save r12
; ... use rbx and r12 freely ...
pop r12               ; restore in reverse order
pop rbx

; push rax  ==  sub rsp, 8 / mov [rsp], rax
; pop rax   ==  mov rax, [rsp] / add rsp, 8
```

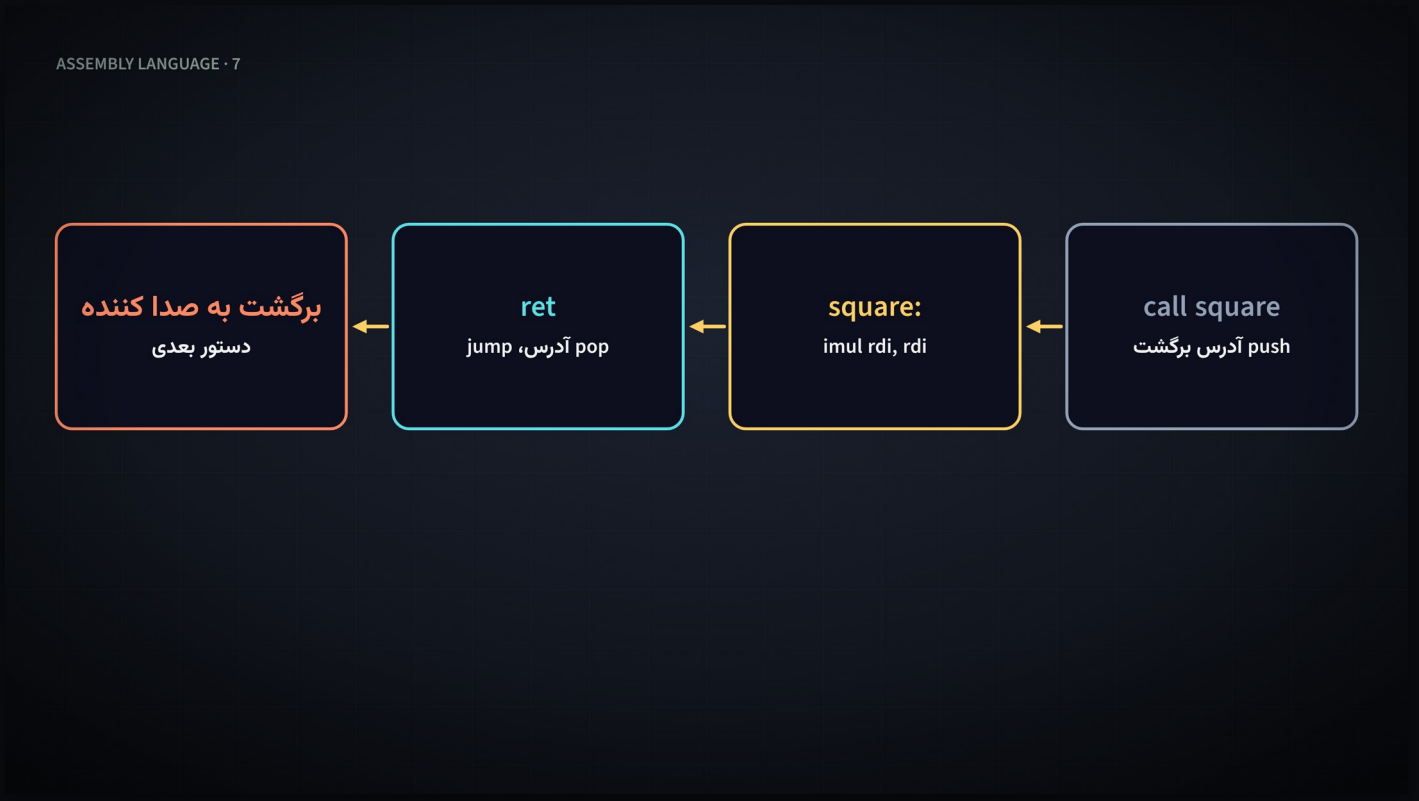
02

call و ret

call square — push آدرس برگشت

square: — imul rdi, rdi

ret — pop آدرس، jump



03

stack frame ها

هر صدا کردن تابع stack frame خودش را برای متغیرهای محلی و register های ذخیره‌شده می‌گیرد. ...

epilogue آن را برمی‌گرداند. متغیرهای محلی در offset های منفی از rbp زندگی می‌کنند.

ASSEMBLY LANGUAGE · 7

frame.asm

```
my_func:
    push rbp              ; prologue
    mov  rbp, rsp
    sub  rsp, 16          ; room for 2 locals
    mov  qword [rbp-8], 0     ; local a
    mov  qword [rbp-16], 5    ; local b
    ; ...
    mov  rsp, rbp         ; epilogue
    pop  rbp
    ret
```

04

باگ‌های stack

اگر push ها و pop ها جور نباشند، ret به آدرس غلط می‌پرد و پروگرام crash می‌کند. بازگشت ...

نوشتن بیرون از یک buffer محلی می‌تواند آدرس برگشت را بازنویسی کند. این حملهٔ کلاسیک buffer ...

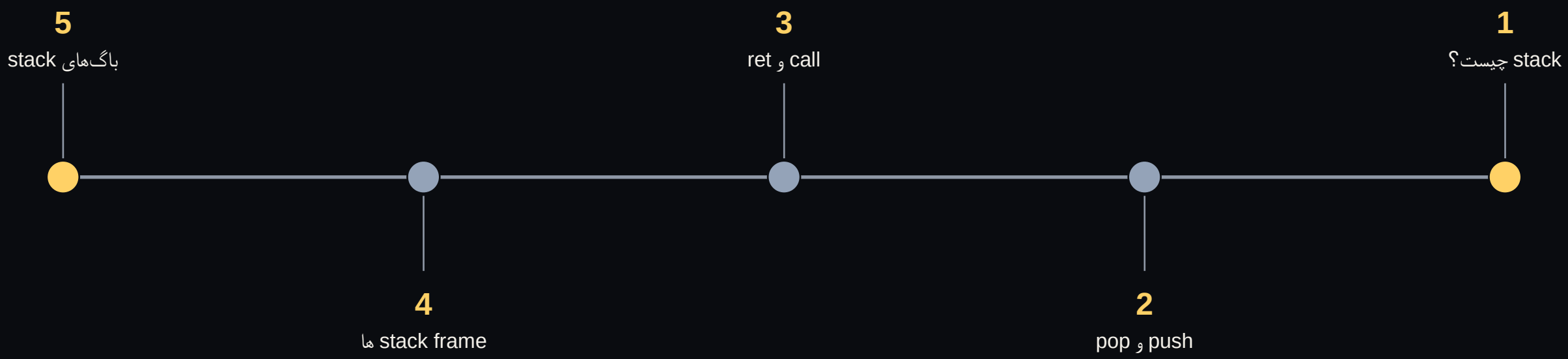
ASSEMBLY LANGUAGE · 7

terminal

```
$ ./broken
Segmentation fault (core dumped)
$ gdb ./broken
(gdb) run
Program received signal SIGSEGV
0x0000000000000000 in ?? ()    ← ret jumped to address 0
```

05

نقشهٔ درس


1
stack چیست؟
2
push و pop
3
call و ret
4
stack frame ها
5
stack باگ‌های

منابع و مطالعهٔ بیشتر





تشکر از تماشای شما

MyWebUniversity.com

آموزش رایگان تکنالوژی از سال ۲۰۰۰ — انگلیسی و دری

@MyWebUniversity-Dari · @MyWebUniversity