

# Buffer Overflow

---

Stefan Mangard

Computer Organization and Networks  
Graz University of Technology

## **Buffer overflow**

---

# Buffer overflow

```
_start:  
ADDI sp,zero,0x700  
ADDI fp,zero,0x700  
JAL ra,main  
EBREAK  
main:  
ADDI sp,sp,-8  
SW ra,4(sp)  
SW fp,0(sp)  
ADDI fp,sp,8  
JAL ra,vuln  
LW fp,0(sp)  
LW ra,4(sp)  
ADDI sp,sp,8  
JALR zero,0(ra)
```



# Buffer overflow

```
_start:  
ADDI sp,zero,0x700  
ADDI fp,zero,0x700  
JAL ra,main  
EBREAK  
main:  
ADDI sp,sp,-8  
SW ra,4(sp)  
SW fp,0(sp)  
ADDI fp,sp,8  
JAL ra,vuln  
LW fp,0(sp)  
LW ra,4(sp)  
ADDI sp,sp,8  
JALR zero,0(ra)
```



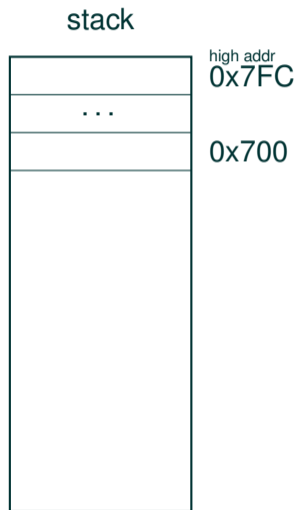
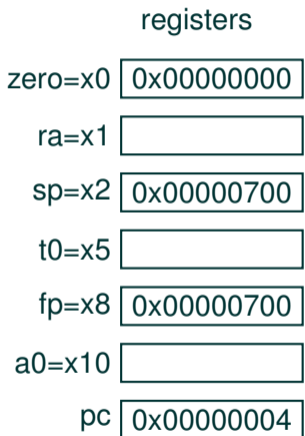
# Buffer overflow

```
_start:  
  ADDI sp,zero,0x700  
  ADDI fp,zero,0x700  
  JAL ra,main  
  EBREAK  
main:  
  ADDI sp,sp,-8  
  SW ra,4(sp)  
  SW fp,0(sp)  
  ADDI fp,sp,8  
  JAL ra,vuln  
  LW fp,0(sp)  
  LW ra,4(sp)  
  ADDI sp,sp,8  
  JALR zero,0(ra)
```



# Buffer overflow

```
_start:  
  ADDI sp,zero,0x700  
  ADDI fp,zero,0x700  
  JAL ra,main  
  EBREAK  
main:  
  ADDI sp,sp,-8  
  SW ra,4(sp)  
  SW fp,0(sp)  
  ADDI fp,sp,8  
  JAL ra,vuln  
  LW fp,0(sp)  
  LW ra,4(sp)  
  ADDI sp,sp,8  
  JALR zero,0(ra)
```



# Buffer overflow

```
_start:  
  ADDI sp,zero,0x700  
  ADDI fp,zero,0x700  
  JAL ra,main  
  EBREAK  
main:  
  ADDI sp,sp,-8  
  SW ra,4(sp)  
  SW fp,0(sp)  
  ADDI fp,sp,8  
  JAL ra,vuln  
  LW fp,0(sp)  
  LW ra,4(sp)  
  ADDI sp,sp,8  
  JALR zero,0(ra)
```



# Buffer overflow

```
_start:  
  ADDI sp,zero,0x700  
  ADDI fp,zero,0x700  
  JAL ra,main  
  EBREAK  
main:  
  ADDI sp,sp,-8  
  SW ra,4(sp)  
  SW fp,0(sp)  
  ADDI fp,sp,8  
  JAL ra,vuln  
  LW fp,0(sp)  
  LW ra,4(sp)  
  ADDI sp,sp,8  
  JALR zero,0(ra)
```





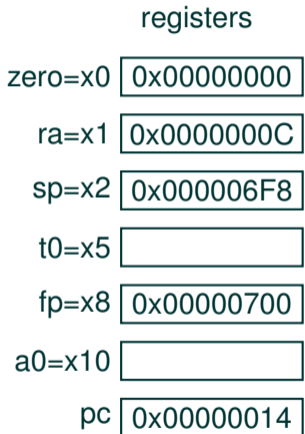
# Buffer overflow

```
_start:  
  ADDI sp,zero,0x700  
  ADDI fp,zero,0x700  
  JAL ra,main  
  EBREAK  
main:  
  ADDI sp,sp,-8  
  SW ra,4(sp)  
  SW fp,0(sp)  
  ADDI fp,sp,8  
  JAL ra,vuln  
  LW fp,0(sp)  
  LW ra,4(sp)  
  ADDI sp,sp,8  
  JALR zero,0(ra)
```



# Buffer overflow

```
_start:  
  ADDI sp,zero,0x700  
  ADDI fp,zero,0x700  
  JAL ra,main  
  EBREAK  
main:  
  ADDI sp,sp,-8  
  SW ra,4(sp)  
  SW fp,0(sp)  
  ADDI fp,sp,8  
  JAL ra,vuln  
  LW fp,0(sp)  
  LW ra,4(sp)  
  ADDI sp,sp,8  
  JALR zero,0(ra)
```



# Buffer overflow

```
_start:  
  ADDI sp,zero,0x700  
  ADDI fp,zero,0x700  
  JAL ra,main  
  EBREAK  
main:  
  ADDI sp,sp,-8  
  SW ra,4(sp)  
  SW fp,0(sp)  
  ADDI fp,sp,8  
  JAL ra,vuln  
  LW fp,0(sp)  
  LW ra,4(sp)  
  ADDI sp,sp,8  
  JALR zero,0(ra)
```





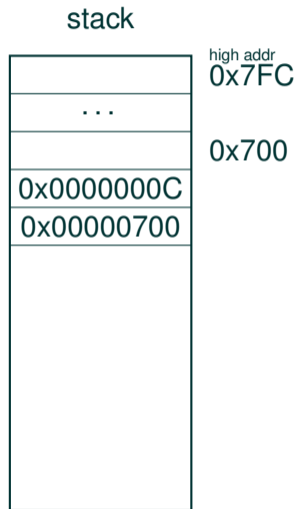
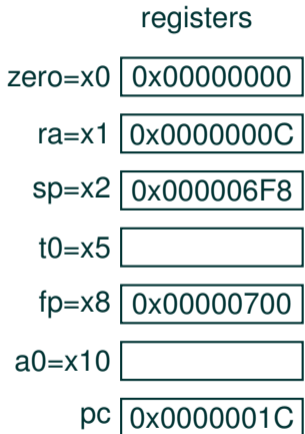
# Buffer overflow

```
_start:  
  ADDI sp,zero,0x700  
  ADDI fp,zero,0x700  
  JAL ra,main  
  EBREAK  
main:  
  ADDI sp,sp,-8  
  SW ra,4(sp)  
  SW fp,0(sp)  
  ADDI fp,sp,8  
  JAL ra,vuln  
  LW fp,0(sp)  
  LW ra,4(sp)  
  ADDI sp,sp,8  
  JALR zero,0(ra)
```



# Buffer overflow

```
_start:  
  ADDI sp,zero,0x700  
  ADDI fp,zero,0x700  
  JAL ra,main  
  EBREAK  
main:  
  ADDI sp,sp,-8  
  SW ra,4(sp)  
  SW fp,0(sp)  
  ADDI fp,sp,0  
  JAL ra,vuln  
  LW fp,0(sp)  
  LW ra,4(sp)  
  ADDI sp,sp,8  
  JALR zero,0(ra)
```



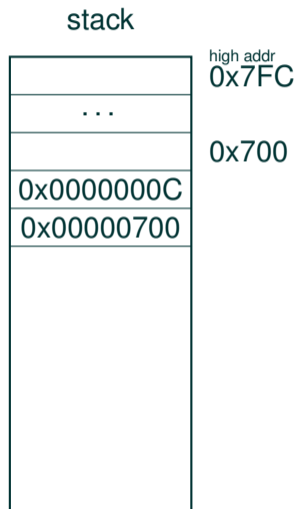
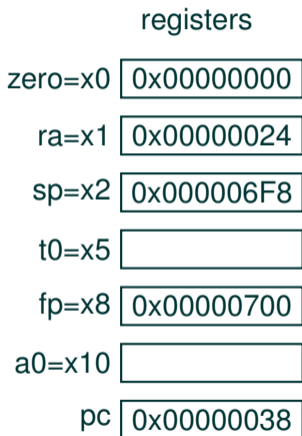
# Buffer overflow

```
_start:  
  ADDI sp,zero,0x700  
  ADDI fp,zero,0x700  
  JAL ra,main  
  EBREAK  
main:  
  ADDI sp,sp,-8  
  SW ra,4(sp)  
  SW fp,0(sp)  
  ADDI fp,sp,8  
  JAL ra,vuln  
  LW fp,0(sp)  
  LW ra,4(sp)  
  ADDI sp,sp,8  
  JALR zero,0(ra)
```



# Buffer overflow

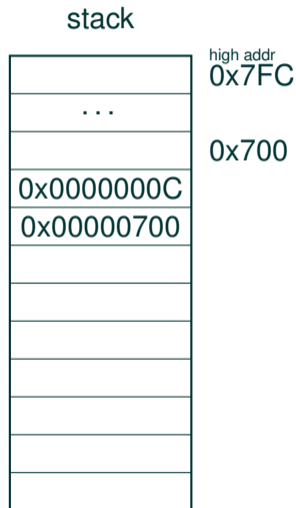
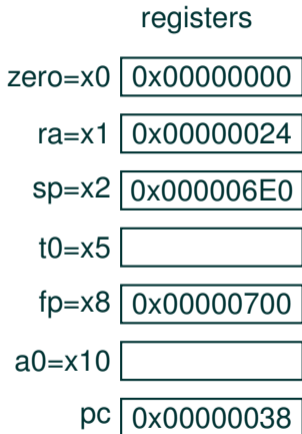
```
vuln:  
ADDI sp,sp,-24  
SW ra,20(sp)  
SW fp,16(sp)  
ADDI fp,sp,24  
ADDI a0,fp,-24  
JAL ra,gets  
LW ra,20(sp)  
LW fp,16(sp)  
ADDI sp,sp,24  
JALR zero,0(ra)  
gets:  
LW t0,0x7FC(zero)  
SW t0,0(a0)  
ADDI a0,a0,4  
BNE t0,zero,gets  
JALR zero,0(ra)  
secret:  
SW zero,0x7FC(zero)  
EBREAK
```





# Buffer overflow

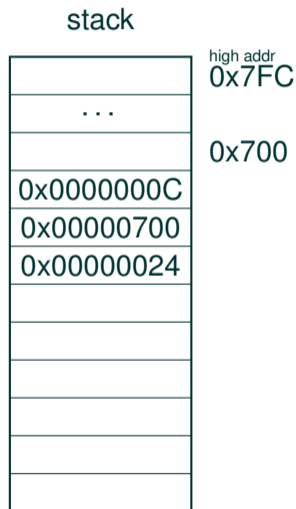
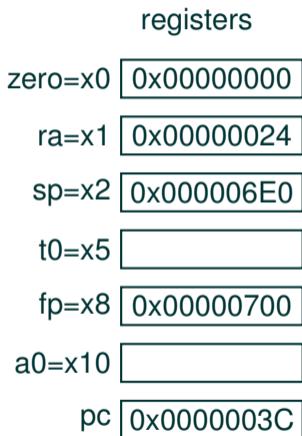
```
vuln:  
ADDI sp,sp,-24  
SW ra,20(sp)  
SW fp,16(sp)  
ADDI fp,sp,24  
ADDI a0,fp,-24  
JAL ra,gets  
LW ra,20(sp)  
LW fp,16(sp)  
ADDI sp,sp,24  
JALR zero,0(ra)  
gets:  
LW t0,0x7FC(zero)  
SW t0,0(a0)  
ADDI a0,a0,4  
BNE t0,zero,gets  
JALR zero,0(ra)  
secret:  
SW zero,0x7FC(zero)  
EBREAK
```





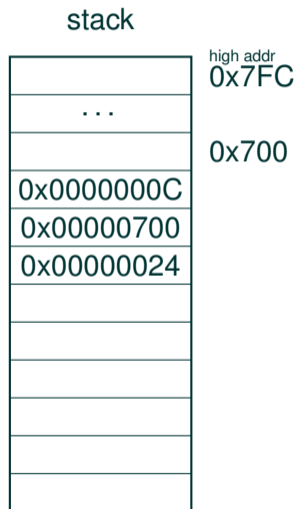
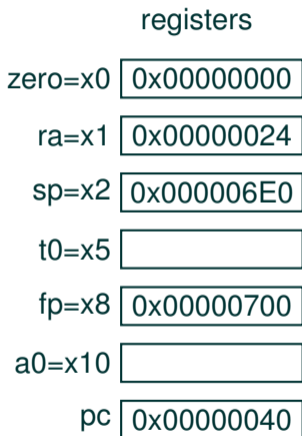
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW ra,20(sp)  
  SW fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL ra,gets  
  LW ra,20(sp)  
  LW fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW t0,0x7FC(zero)  
  SW t0,0(a0)  
  ADDI a0,a0,4  
  BNE t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW zero,0x7FC(zero)  
  EBREAK
```



# Buffer overflow

```
vuln:
  ADDI sp,sp,-24
  SW ra,20(sp)
  SW fp,16(sp)
  ADDI fp,sp,24
  ADDI a0,fp,-24
  JAL ra,gets
  LW ra,20(sp)
  LW fp,16(sp)
  ADDI sp,sp,24
  JALR zero,0(ra)
gets:
  LW t0,0x7FC(zero)
  SW t0,0(a0)
  ADDI a0,a0,4
  BNE t0,zero,gets
  JALR zero,0(ra)
secret:
  SW zero,0x7FC(zero)
  EBREAK
```



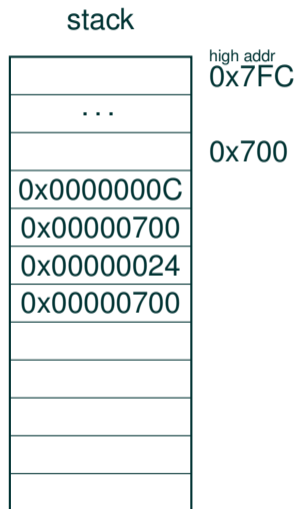
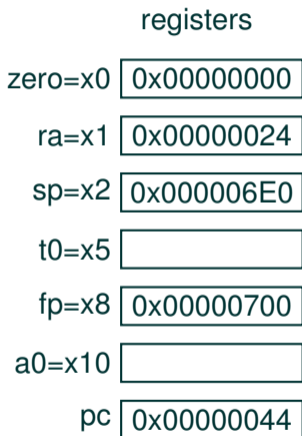
# Buffer overflow

```
vuln:
  ADDI sp,sp,-24
  SW ra,20(sp)
  SW fp,16(sp)
  ADDI fp,sp,24
  ADDI a0,fp,-24
  JAL ra,gets
  LW ra,20(sp)
  LW fp,16(sp)
  ADDI sp,sp,24
  JALR zero,0(ra)
gets:
  LW t0,0x7FC(zero)
  SW t0,0(a0)
  ADDI a0,a0,4
  BNE t0,zero,gets
  JALR zero,0(ra)
secret:
  SW zero,0x7FC(zero)
  EBREAK
```



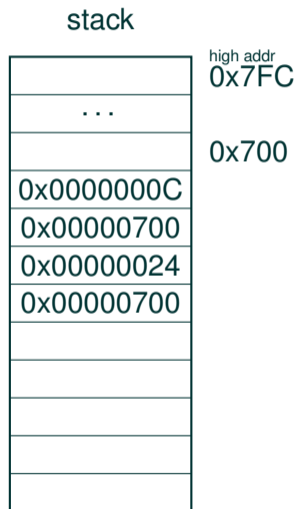
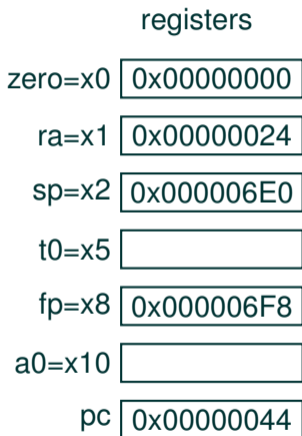
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



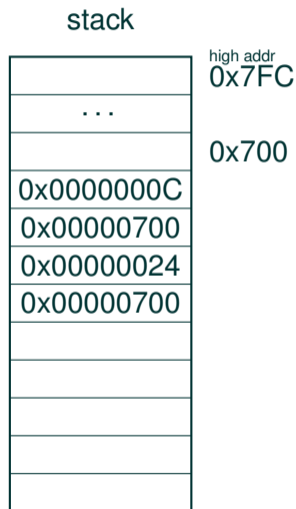
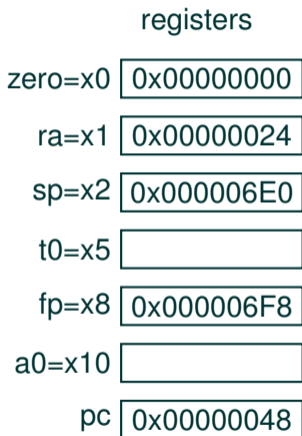
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



# Buffer overflow

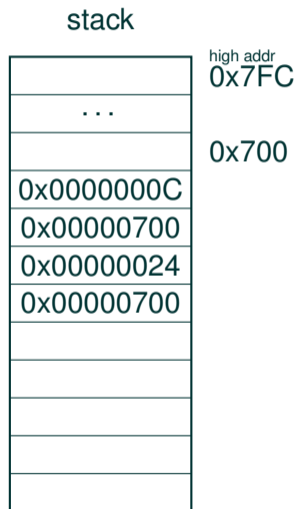
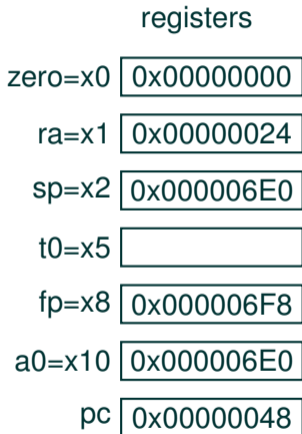
```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```





# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW ra,20(sp)  
  SW fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL ra,gets  
  LW ra,20(sp)  
  LW fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW t0,0x7FC(zero)  
  SW t0,0(a0)  
  ADDI a0,a0,4  
  BNE t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW zero,0x7FC(zero)  
  EBREAK
```



# Buffer overflow

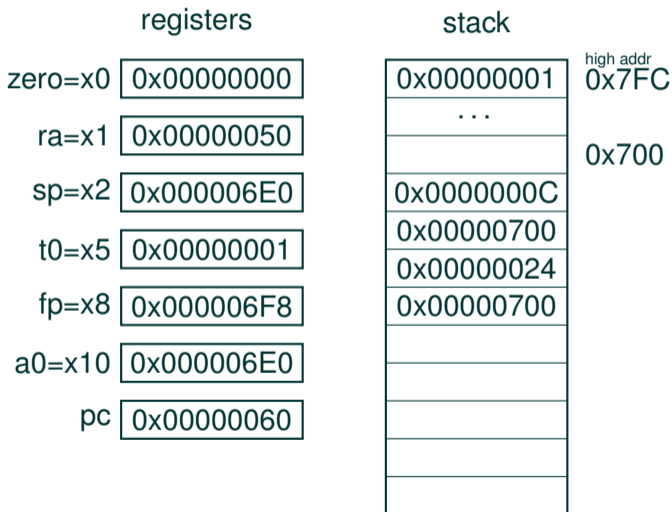
```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```





# Buffer overflow

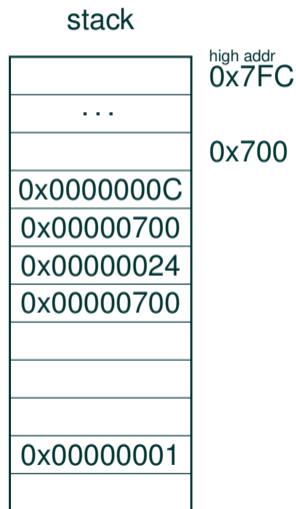
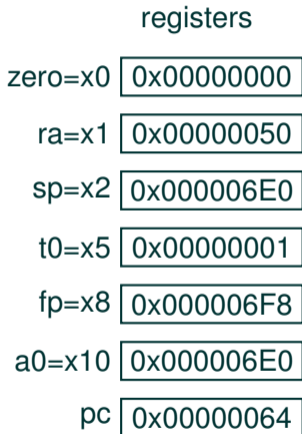
```
vuln:
  ADDI sp,sp,-24
  SW ra,20(sp)
  SW fp,16(sp)
  ADDI fp,sp,24
  ADDI a0,fp,-24
  JAL ra,gets
  LW ra,20(sp)
  LW fp,16(sp)
  ADDI sp,sp,24
  JALR zero,0(ra)
gets:
  LW t0,0x7FC(zero)
  SW t0,0(a0)
  ADDI a0,a0,4
  BNE t0,zero,gets
  JALR zero,0(ra)
secret:
  SW zero,0x7FC(zero)
  EBREAK
```





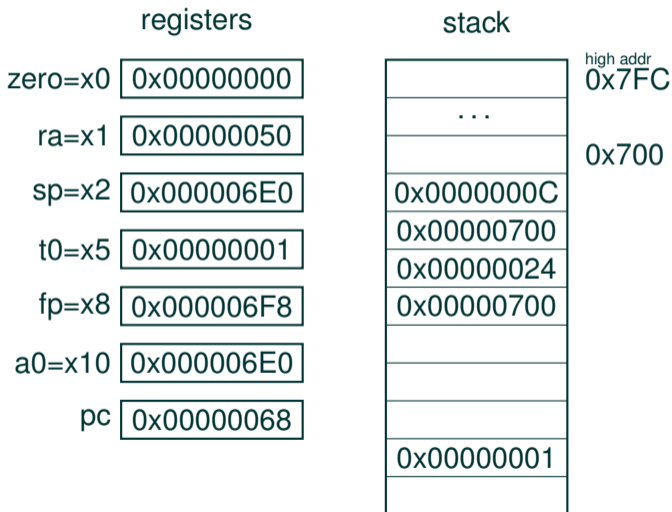
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



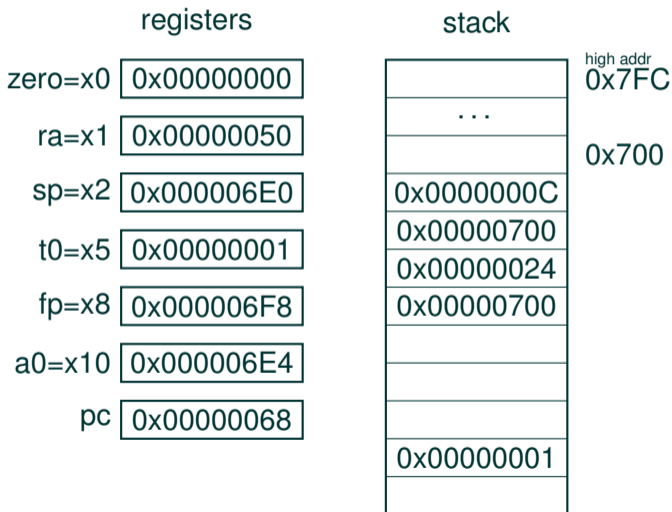
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



# Buffer overflow

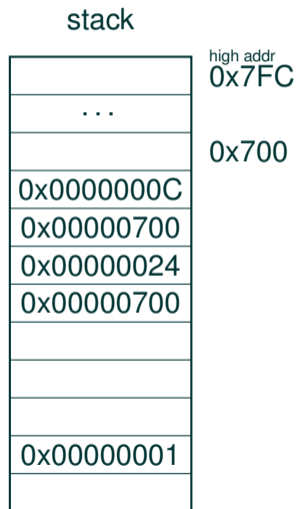
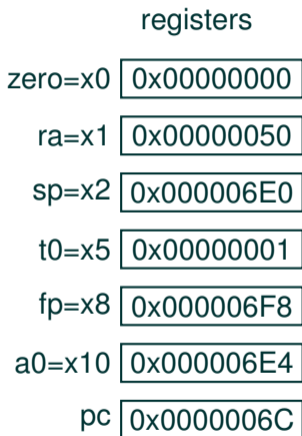
```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```





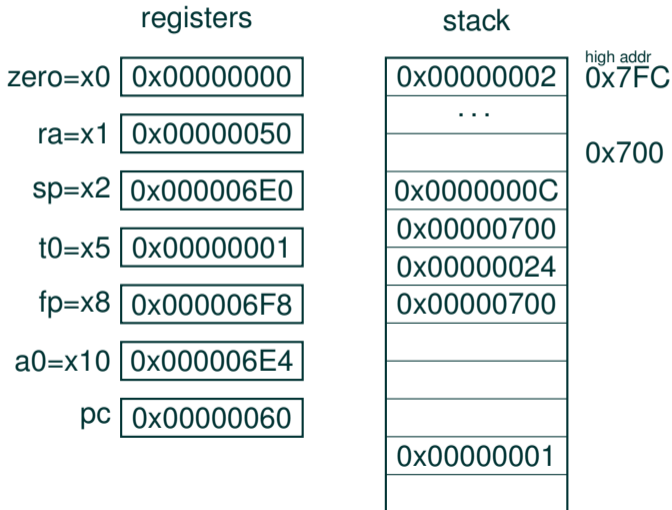
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



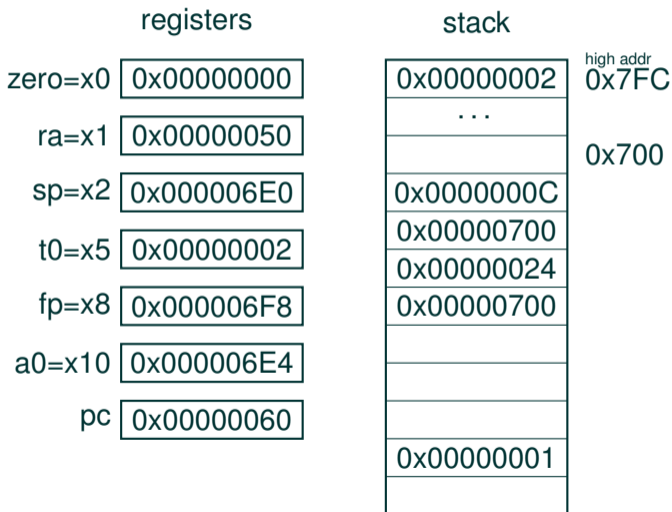
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



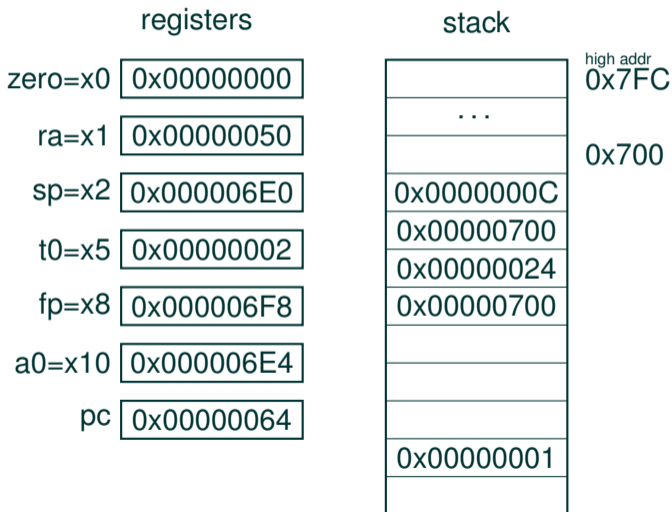
# Buffer overflow

```
vuln:
  ADDI sp,sp,-24
  SW   ra,20(sp)
  SW   fp,16(sp)
  ADDI fp,sp,24
  ADDI a0,fp,-24
  JAL  ra,gets
  LW   ra,20(sp)
  LW   fp,16(sp)
  ADDI sp,sp,24
  JALR zero,0(ra)
gets:
  LW   t0,0x7FC(zero)
  SW   t0,0(a0)
  ADDI a0,a0,4
  BNE  t0,zero,gets
  JALR zero,0(ra)
secret:
  SW   zero,0x7FC(zero)
  EBREAK
```



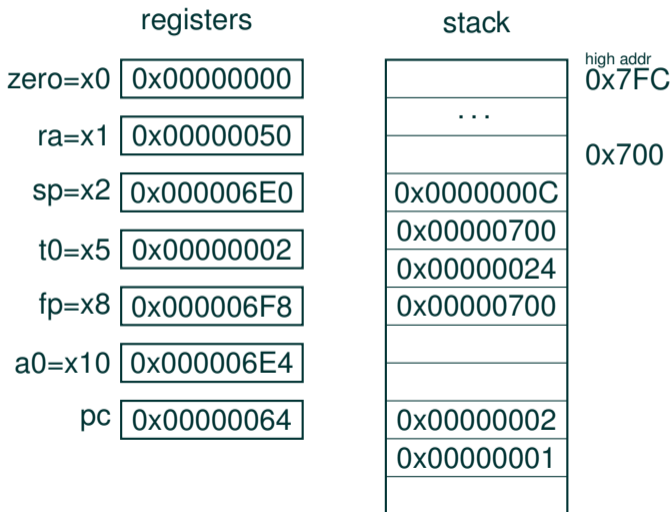
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



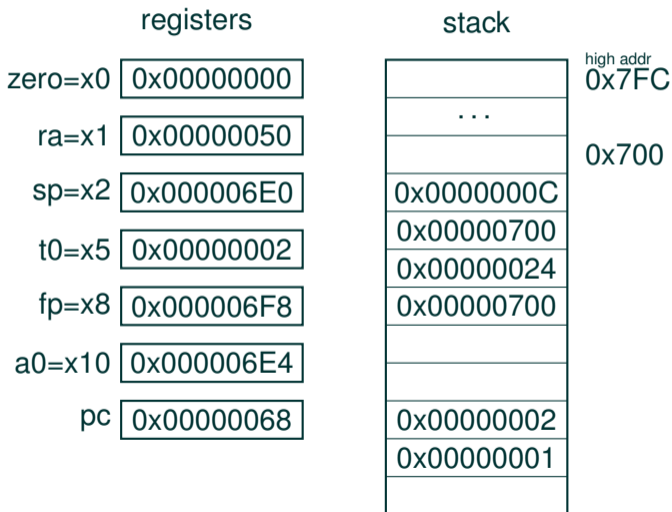
# Buffer overflow

```
vuln:
  ADDI sp,sp,-24
  SW ra,20(sp)
  SW fp,16(sp)
  ADDI fp,sp,24
  ADDI a0,fp,-24
  JAL ra,gets
  LW ra,20(sp)
  LW fp,16(sp)
  ADDI sp,sp,24
  JALR zero,0(ra)
gets:
  LW t0,0x7FC(zero)
  SW t0,0(a0)
  ADDI a0,a0,4
  BNE t0,zero,gets
  JALR zero,0(ra)
secret:
  SW zero,0x7FC(zero)
  EBREAK
```



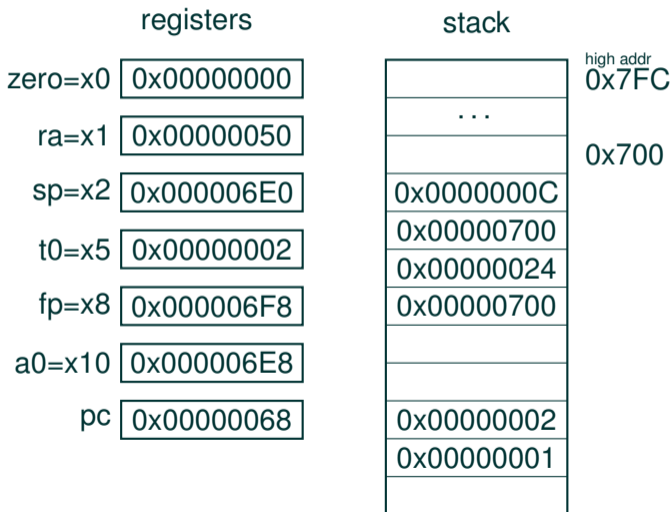
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



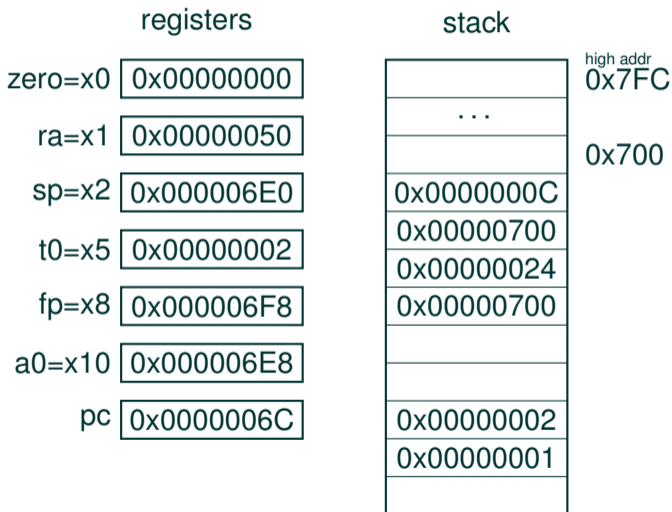
# Buffer overflow

```
vuln:
  ADDI sp,sp,-24
  SW ra,20(sp)
  SW fp,16(sp)
  ADDI fp,sp,24
  ADDI a0,fp,-24
  JAL ra,gets
  LW ra,20(sp)
  LW fp,16(sp)
  ADDI sp,sp,24
  JALR zero,0(ra)
gets:
  LW t0,0x7FC(zero)
  SW t0,0(a0)
  ADDI a0,a0,4
  BNE t0,zero,gets
  JALR zero,0(ra)
secret:
  SW zero,0x7FC(zero)
  EBREAK
```



# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```





# Buffer overflow

```
vuln:
  ADDI sp,sp,-24
  SW   ra,20(sp)
  SW   fp,16(sp)
  ADDI fp,sp,24
  ADDI a0,fp,-24
  JAL  ra,gets
  LW   ra,20(sp)
  LW   fp,16(sp)
  ADDI sp,sp,24
  JALR zero,0(ra)
gets:
  LW   t0,0x7FC(zero)
  SW   t0,0(a0)
  ADDI a0,a0,4
  BNE  t0,zero,gets
  JALR zero,0(ra)
secret:
  SW   zero,0x7FC(zero)
  EBREAK
```



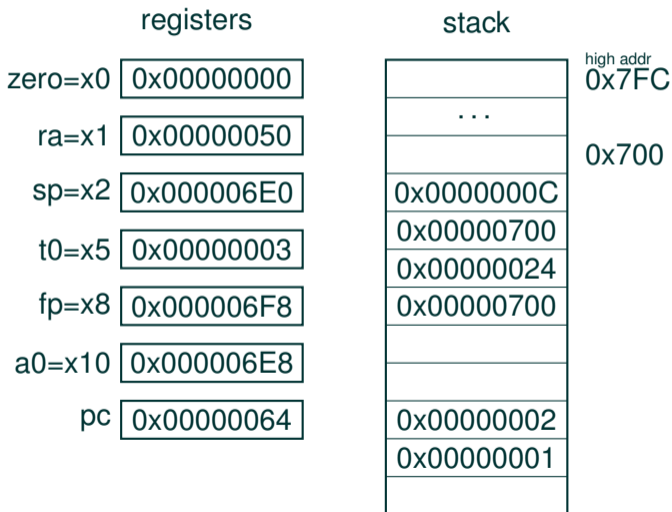
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



# Buffer overflow

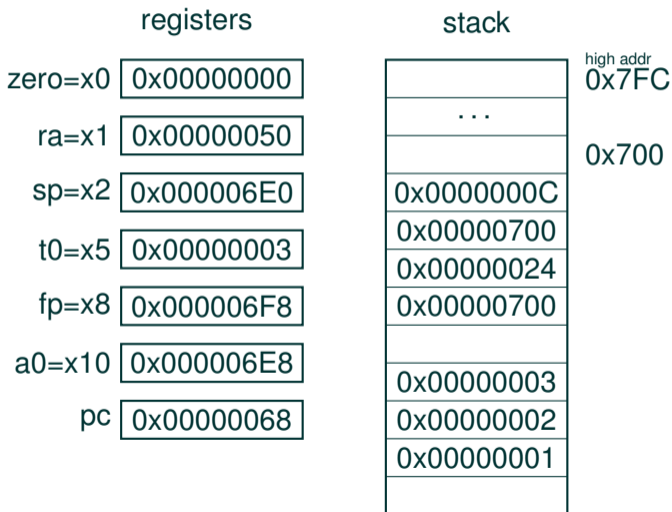
```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```

	registers
zero=x0	0x00000000
ra=x1	0x00000050
sp=x2	0x000006E0
t0=x5	0x00000003
fp=x8	0x000006F8
a0=x10	0x000006E8
pc	0x00000064

	stack	high addr
		0x7FC
	...	
		0x700
	0x0000000C	
	0x00000700	
	0x00000024	
	0x00000700	
	0x00000003	
	0x00000002	
	0x00000001	
		low addr

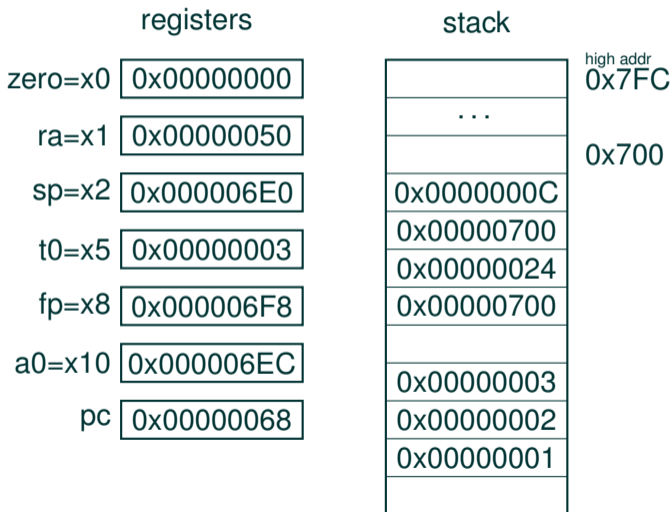
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



# Buffer overflow

```
vuln:
  ADDI sp,sp,-24
  SW ra,20(sp)
  SW fp,16(sp)
  ADDI fp,sp,24
  ADDI a0,fp,-24
  JAL ra,gets
  LW ra,20(sp)
  LW fp,16(sp)
  ADDI sp,sp,24
  JALR zero,0(ra)
gets:
  LW t0,0x7FC(zero)
  SW t0,0(a0)
  ADDI a0,a0,4
  BNE t0,zero,gets
  JALR zero,0(ra)
secret:
  SW zero,0x7FC(zero)
  EBREAK
```

	registers
zero=x0	0x00000000
ra=x1	0x00000050
sp=x2	0x000006E0
t0=x5	0x00000003
fp=x8	0x000006F8
a0=x10	0x000006EC
pc	0x0000006C

	stack
high addr	0x7FC
	...
	0x700
	0x0000000C
	0x00000700
	0x00000024
	0x00000700
	0x00000003
	0x00000002
	0x00000001
low addr	1/1

# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```





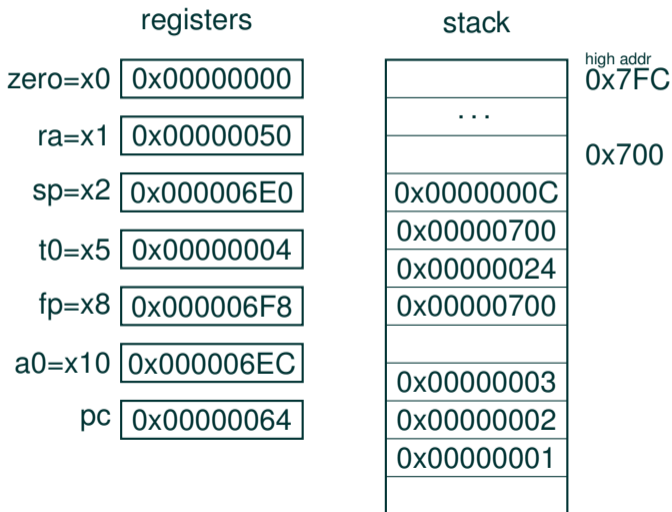
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



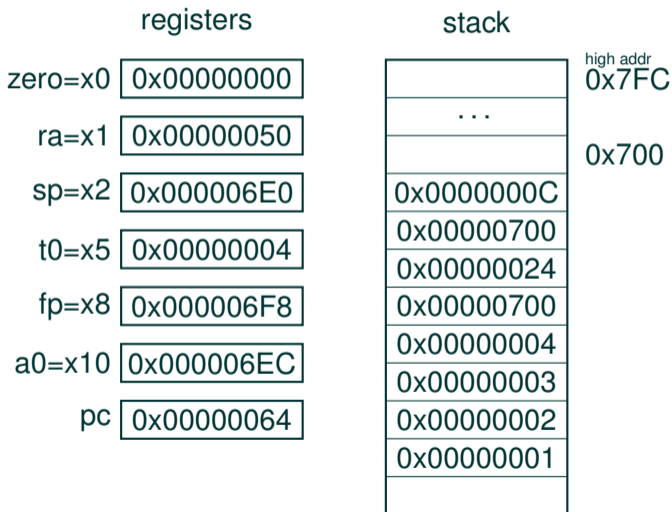
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



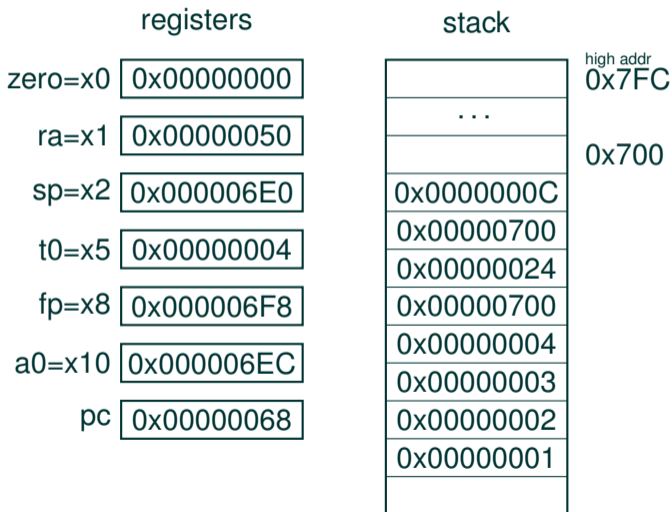
# Buffer overflow

```
vuln:
  ADDI sp,sp,-24
  SW ra,20(sp)
  SW fp,16(sp)
  ADDI fp,sp,24
  ADDI a0,fp,-24
  JAL ra,gets
  LW ra,20(sp)
  LW fp,16(sp)
  ADDI sp,sp,24
  JALR zero,0(ra)
gets:
  LW t0,0x7FC(zero)
  SW t0,0(a0)
  ADDI a0,a0,4
  BNE t0,zero,gets
  JALR zero,0(ra)
secret:
  SW zero,0x7FC(zero)
  EBREAK
```



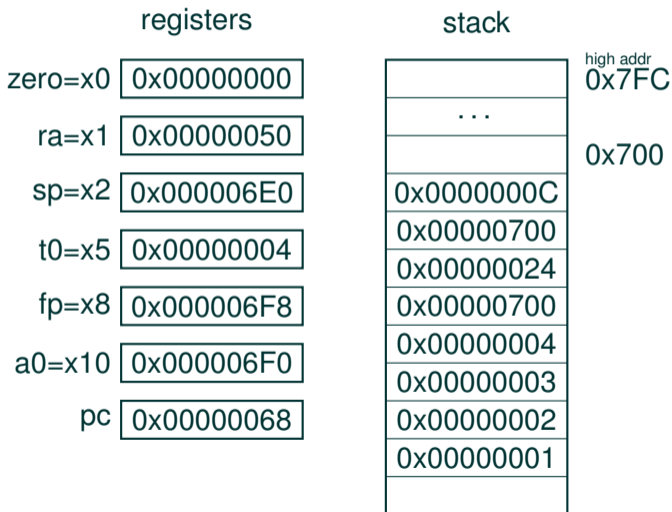
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



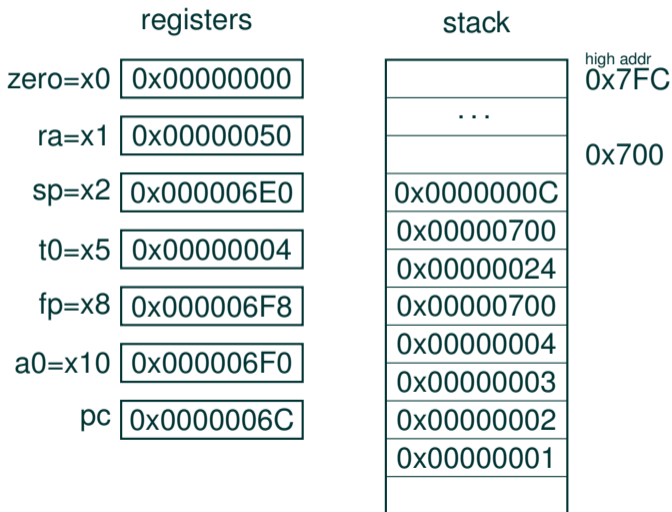
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



# Buffer overflow

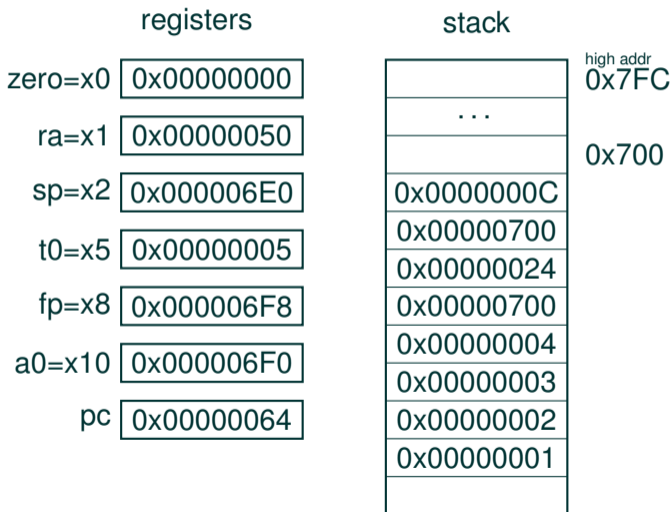
```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```





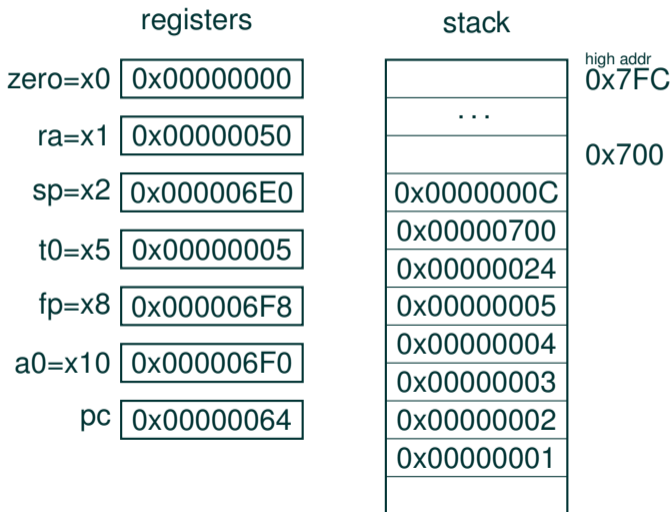
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



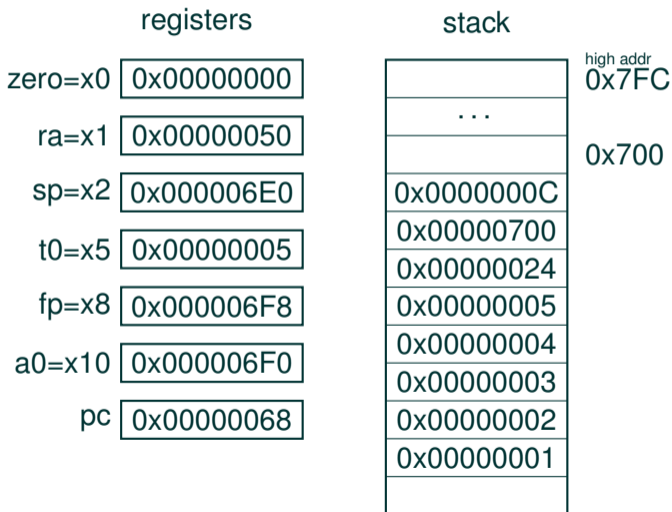
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



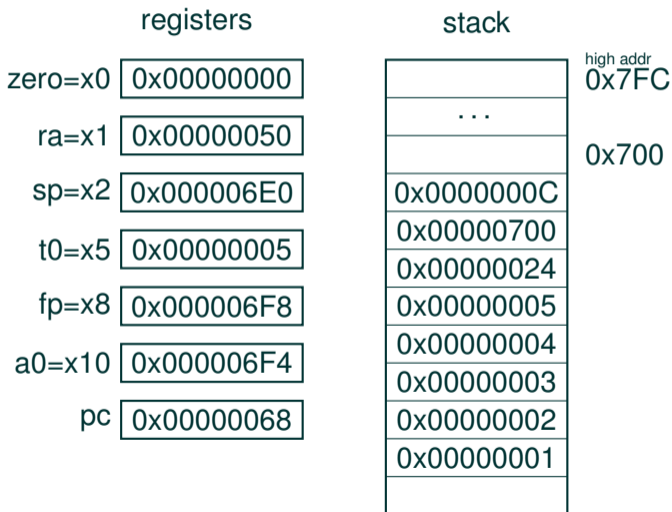
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



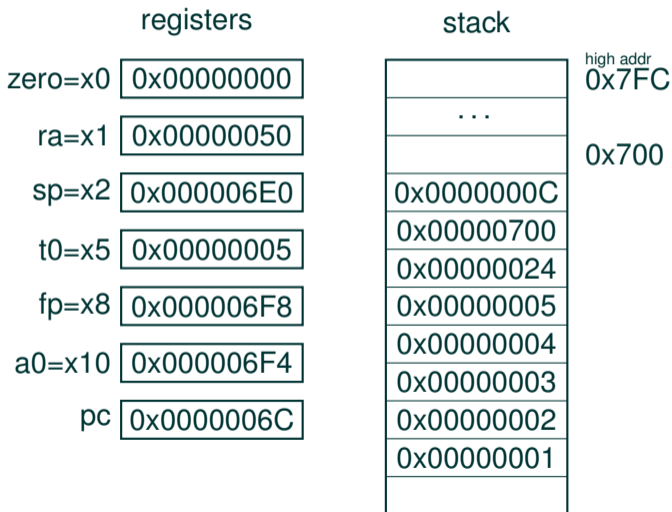
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



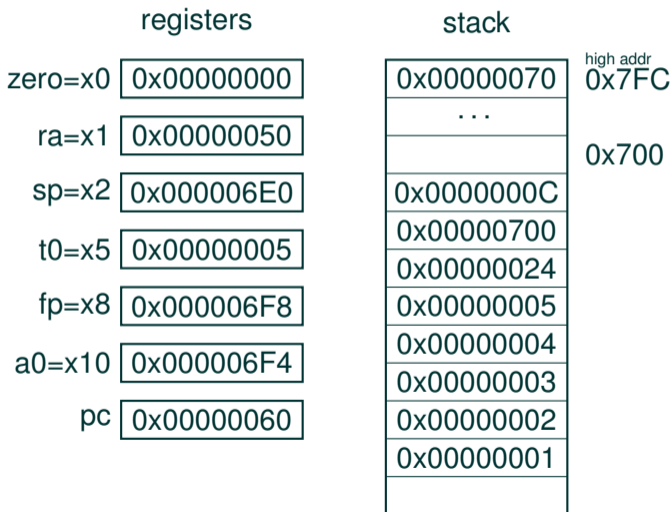
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



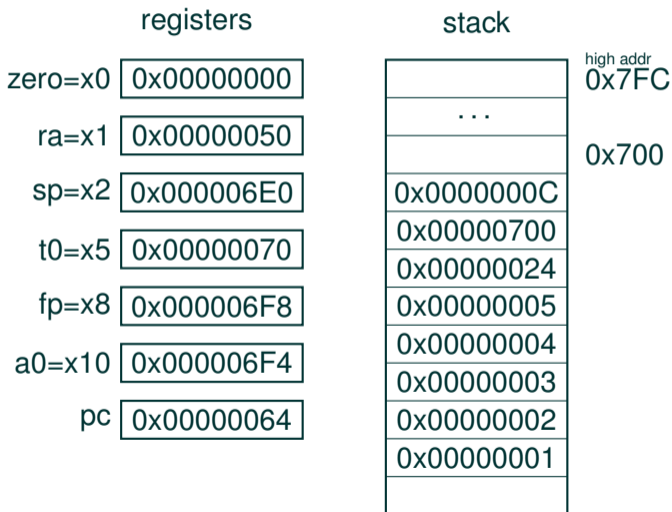
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



# Buffer overflow

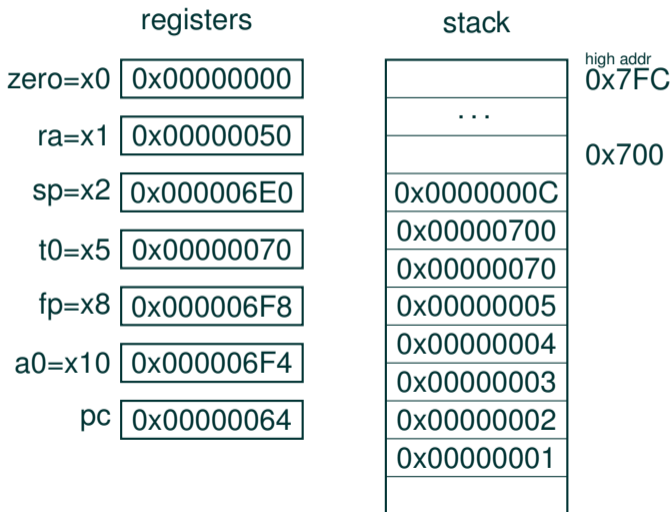
```
vuln:
  ADDI sp,sp,-24
  SW ra,20(sp)
  SW fp,16(sp)
  ADDI fp,sp,24
  ADDI a0,fp,-24
  JAL ra,gets
  LW ra,20(sp)
  LW fp,16(sp)
  ADDI sp,sp,24
  JALR zero,0(ra)
gets:
  LW t0,0x7FC(zero)
  SW t0,0(a0)
  ADDI a0,a0,4
  BNE t0,zero,gets
  JALR zero,0(ra)
secret:
  SW zero,0x7FC(zero)
  EBREAK
```





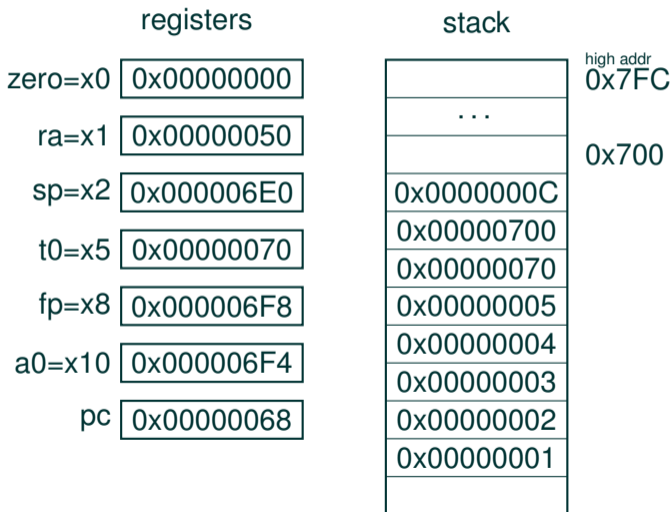
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



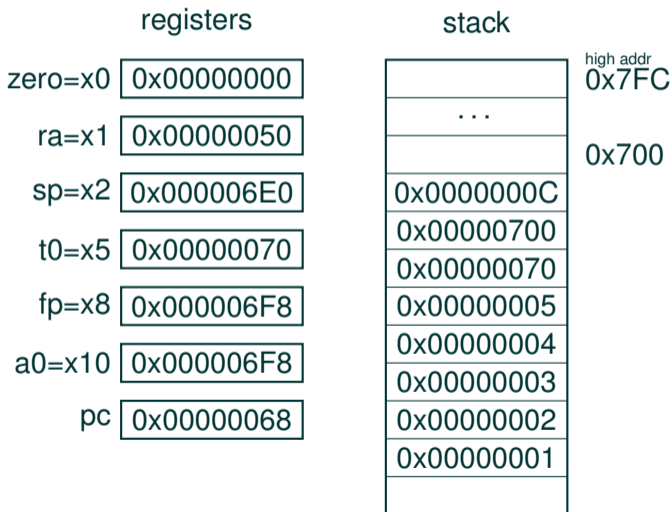
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



# Buffer overflow

```
vuln:
  ADDI sp,sp,-24
  SW ra,20(sp)
  SW fp,16(sp)
  ADDI fp,sp,24
  ADDI a0,fp,-24
  JAL ra,gets
  LW ra,20(sp)
  LW fp,16(sp)
  ADDI sp,sp,24
  JALR zero,0(ra)
gets:
  LW t0,0x7FC(zero)
  SW t0,0(a0)
  ADDI a0,a0,4
  BNE t0,zero,gets
  JALR zero,0(ra)
secret:
  SW zero,0x7FC(zero)
  EBREAK
```



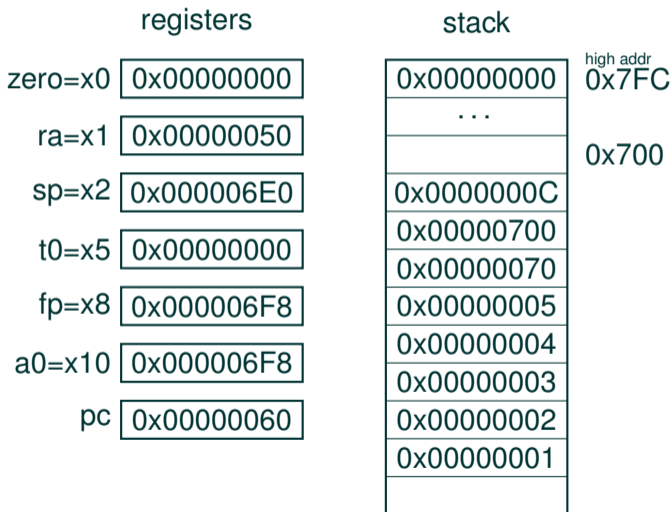
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



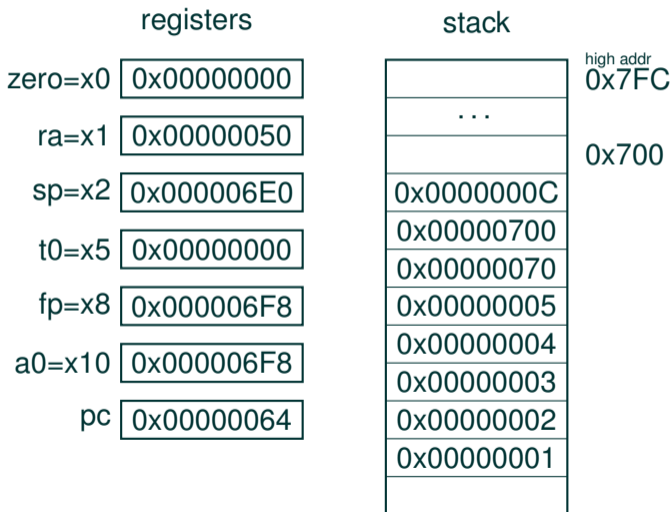
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



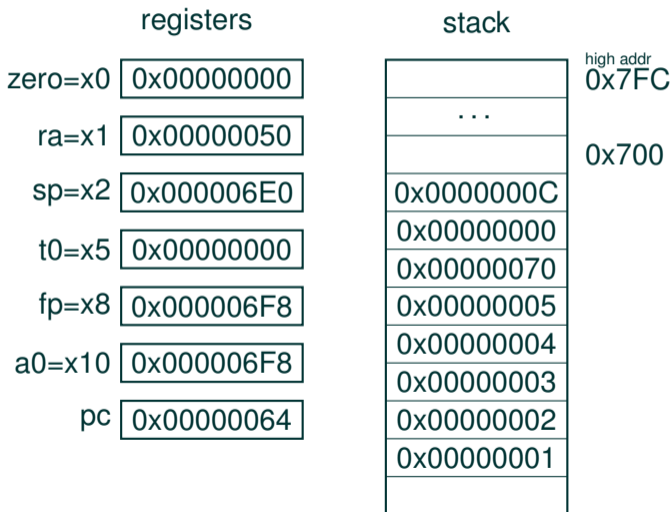
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



# Buffer overflow

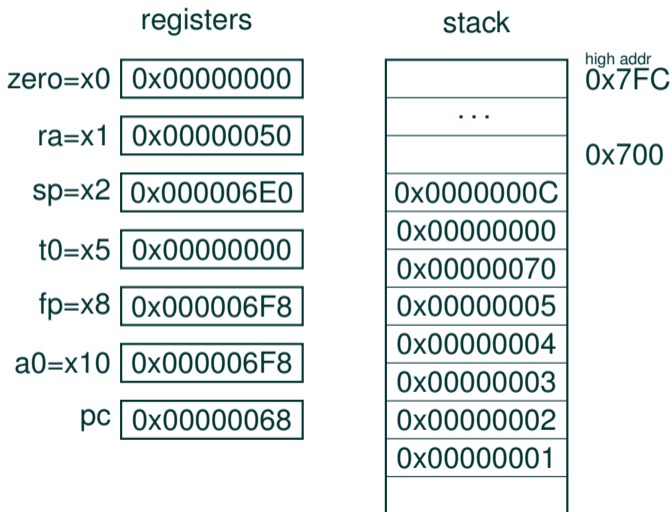
```
vuln:
  ADDI sp,sp,-24
  SW ra,20(sp)
  SW fp,16(sp)
  ADDI fp,sp,24
  ADDI a0,fp,-24
  JAL ra,gets
  LW ra,20(sp)
  LW fp,16(sp)
  ADDI sp,sp,24
  JALR zero,0(ra)
gets:
  LW t0,0x7FC(zero)
  SW t0,0(a0)
  ADDI a0,a0,4
  BNE t0,zero,gets
  JALR zero,0(ra)
secret:
  SW zero,0x7FC(zero)
  EBREAK
```





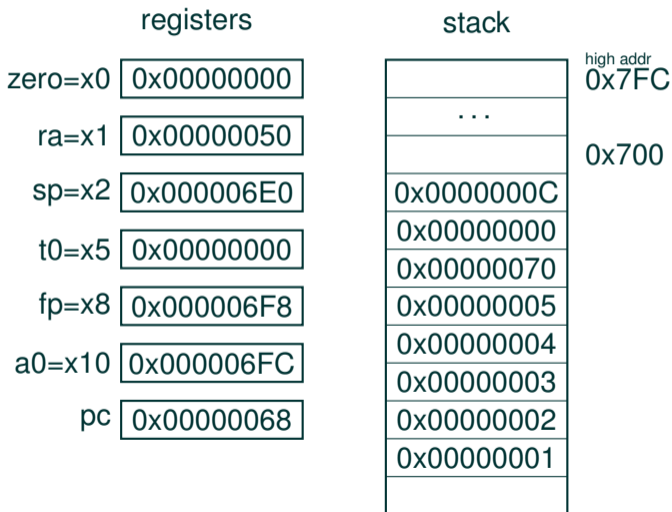
# Buffer overflow

```
vuln:
  ADDI sp,sp,-24
  SW ra,20(sp)
  SW fp,16(sp)
  ADDI fp,sp,24
  ADDI a0,fp,-24
  JAL ra,gets
  LW ra,20(sp)
  LW fp,16(sp)
  ADDI sp,sp,24
  JALR zero,0(ra)
gets:
  LW t0,0x7FC(zero)
  SW t0,0(a0)
  ADDI a0,a0,4
  BNE t0,zero,gets
  JALR zero,0(ra)
secret:
  SW zero,0x7FC(zero)
  EBREAK
```



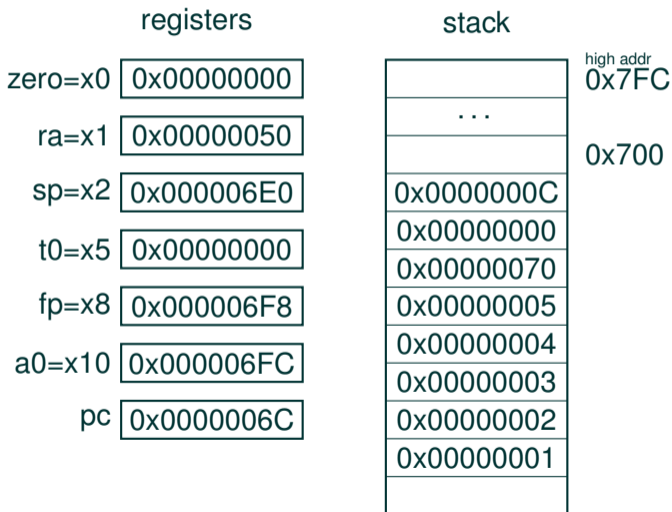
# Buffer overflow

```
vuln:
  ADDI sp,sp,-24
  SW ra,20(sp)
  SW fp,16(sp)
  ADDI fp,sp,24
  ADDI a0,fp,-24
  JAL ra,gets
  LW ra,20(sp)
  LW fp,16(sp)
  ADDI sp,sp,24
  JALR zero,0(ra)
gets:
  LW t0,0x7FC(zero)
  SW t0,0(a0)
  ADDI a0,a0,4
  BNE t0,zero,gets
  JALR zero,0(ra)
secret:
  SW zero,0x7FC(zero)
  EBREAK
```



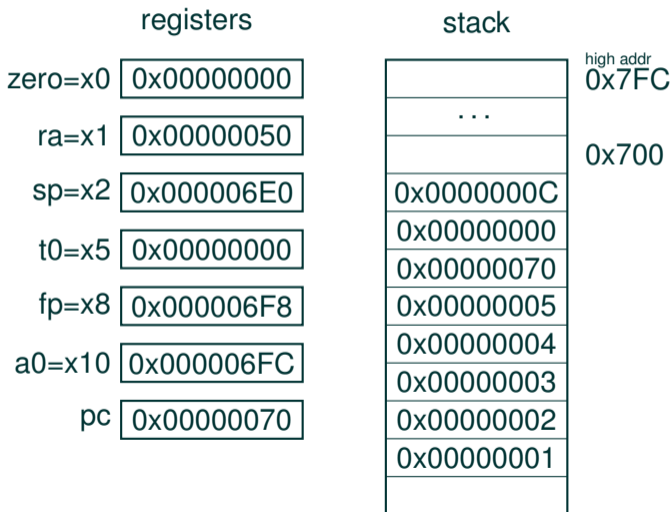
# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



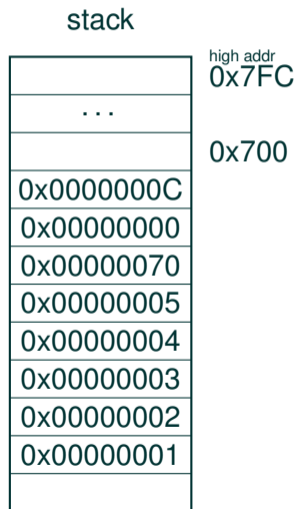
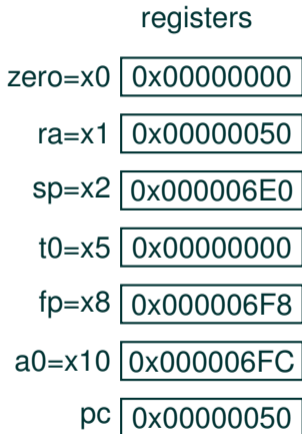
# Buffer overflow

```
vuln:
  ADDI sp,sp,-24
  SW ra,20(sp)
  SW fp,16(sp)
  ADDI fp,sp,24
  ADDI a0,fp,-24
  JAL ra,gets
  LW ra,20(sp)
  LW fp,16(sp)
  ADDI sp,sp,24
  JALR zero,0(ra)
gets:
  LW t0,0x7FC(zero)
  SW t0,0(a0)
  ADDI a0,a0,4
  BNE t0,zero,gets
  JALR zero,(ra)
secret:
  SW zero,0x7FC(zero)
  EBREAK
```



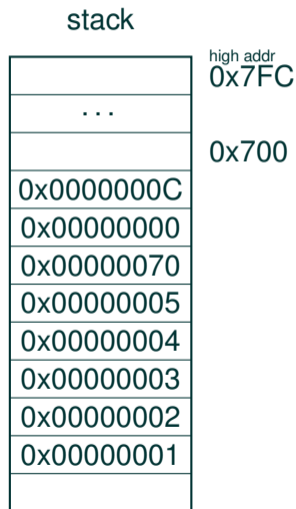
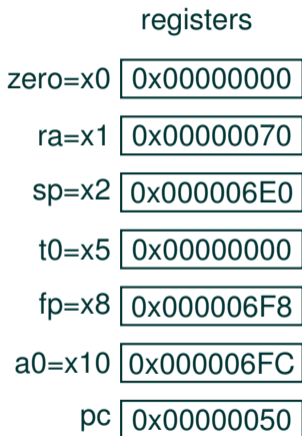
# Buffer overflow

```
vuln:  
ADDI sp,sp,-24  
SW ra,20(sp)  
SW fp,16(sp)  
ADDI fp,sp,24  
ADDI a0,fp,-24  
JAL ra,gets  
LW ra,20(sp)  
LW fp,16(sp)  
ADDI sp,sp,24  
JALR zero,0(ra)  
gets:  
LW t0,0x7FC(zero)  
SW t0,0(a0)  
ADDI a0,a0,4  
BNE t0,zero,gets  
JALR zero,0(ra)  
secret:  
SW zero,0x7FC(zero)  
EBREAK
```



# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```



# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```

	registers
zero=x0	0x00000000
ra=x1	0x00000070
sp=x2	0x000006E0
t0=x5	0x00000000
fp=x8	0x000006F8
a0=x10	0x000006FC
pc	0x00000054

	stack	high addr
		0x7FC
	...	
		0x700
	0x0000000C	
	0x00000000	
	0x00000070	
	0x00000005	
	0x00000004	
	0x00000003	
	0x00000002	
	0x00000001	

# Buffer overflow

```
vuln:  
  ADDI sp,sp,-24  
  SW   ra,20(sp)  
  SW   fp,16(sp)  
  ADDI fp,sp,24  
  ADDI a0,fp,-24  
  JAL  ra,gets  
  LW   ra,20(sp)  
  LW   fp,16(sp)  
  ADDI sp,sp,24  
  JALR zero,0(ra)  
gets:  
  LW   t0,0x7FC(zero)  
  SW   t0,0(a0)  
  ADDI a0,a0,4  
  BNE  t0,zero,gets  
  JALR zero,0(ra)  
secret:  
  SW   zero,0x7FC(zero)  
  EBREAK
```

	registers
zero=x0	0x00000000
ra=x1	0x00000070
sp=x2	0x000006E0
t0=x5	0x00000000
fp=x8	0x00000005
a0=x10	0x000006FC
pc	0x00000054

	stack	high addr
		0x7FC
	...	
		0x700
	0x0000000C	
	0x00000000	
	0x00000070	
	0x00000005	
	0x00000004	
	0x00000003	
	0x00000002	
	0x00000001	



# Buffer overflow

```
vuln:
  ADDI sp,sp,-24
  SW ra,20(sp)
  SW fp,16(sp)
  ADDI fp,sp,24
  ADDI a0,fp,-24
  JAL ra,gets
  LW ra,20(sp)
  LW fp,16(sp)
  ADDI sp,sp,24
  JALR zero,0(ra)
gets:
  LW t0,0x7FC(zero)
  SW t0,0(a0)
  ADDI a0,a0,4
  BNE t0,zero,gets
  JALR zero,0(ra)
secret:
  SW zero,0x7FC(zero)
  EBREAK
```

	registers
zero=x0	0x00000000
ra=x1	0x00000070
sp=x2	0x000006E0
t0=x5	0x00000000
fp=x8	0x00000005
a0=x10	0x000006FC
pc	0x00000058

	stack	high addr
		0x7FC
	...	
		0x700
	0x0000000C	
	0x00000000	
	0x00000070	
	0x00000005	
	0x00000004	
	0x00000003	
	0x00000002	
	0x00000001	













# Buffer Overflow

---

Stefan Mangard

Computer Organization and Networks  
Graz University of Technology