Buffer Overflow

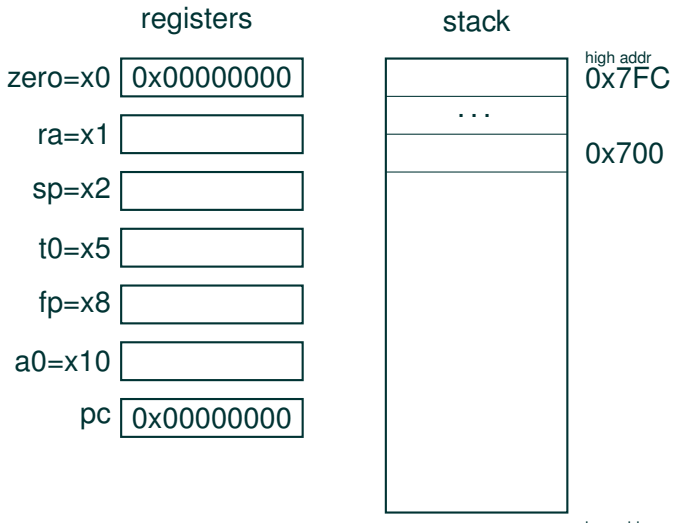
Stefan Mangard

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)
```

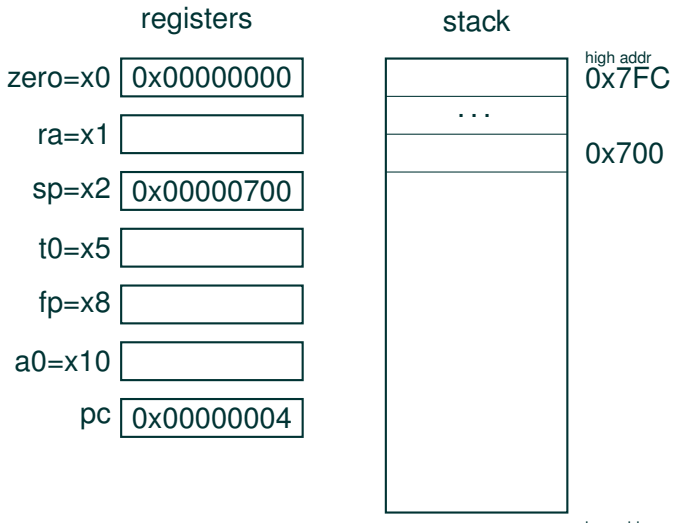


Buffer overflow

```
_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

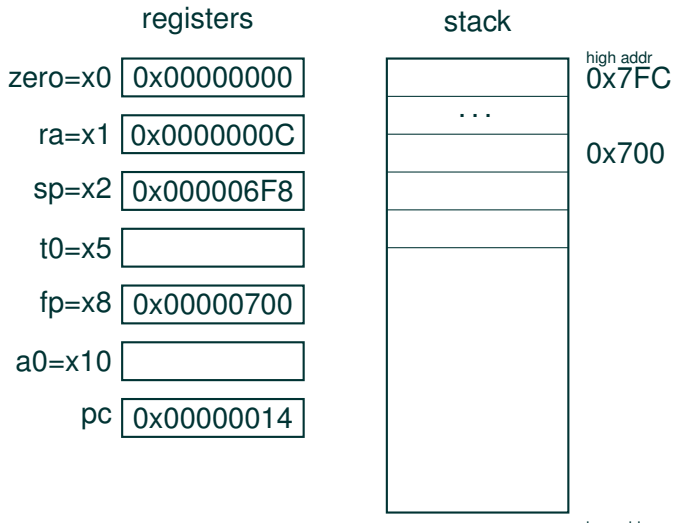
```
_start:
 ADDI sp,zero,0x700
 ADDI fp,zero,0x700
 JAL ra,main
 EBREAK
main:
 ADDI sp,sp,-8
 SW   ra,4(sp)
 SW   fp,0(sp)
 ADDI fp,sp,8
 JAL  ra,vuln
 LW   fp,0(sp)
 LW   ra,4(sp)
 ADDI sp,sp,8
 JALR zero,0(ra)
```

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)
```

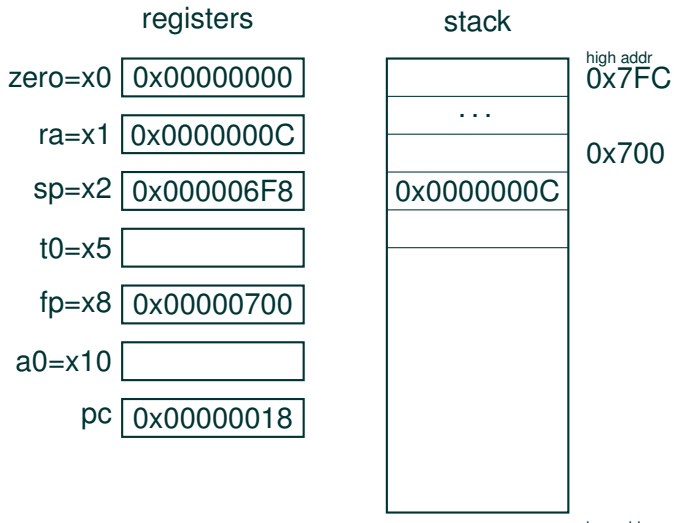


Buffer overflow

```
_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)
```

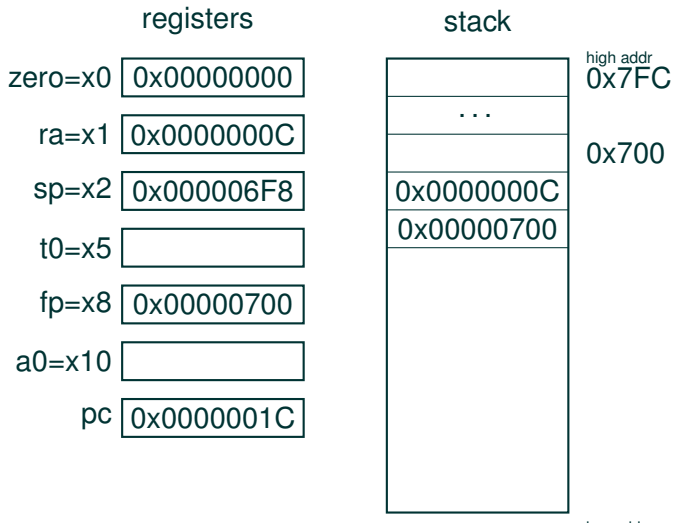


Buffer overflow

```
_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,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)
```

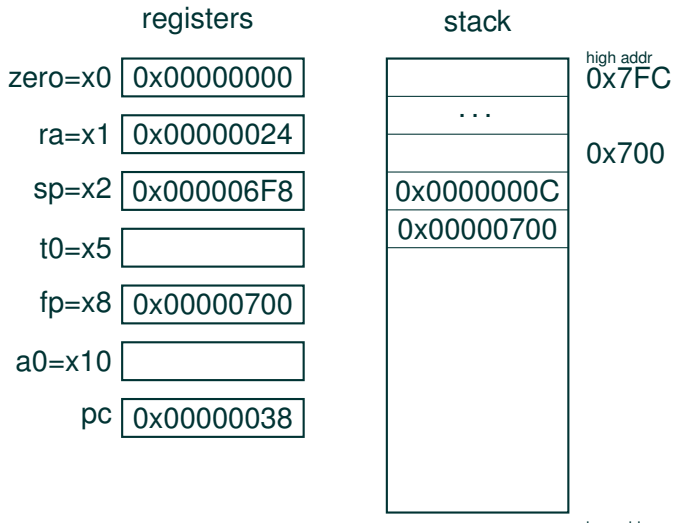


Buffer overflow

```
_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)
```

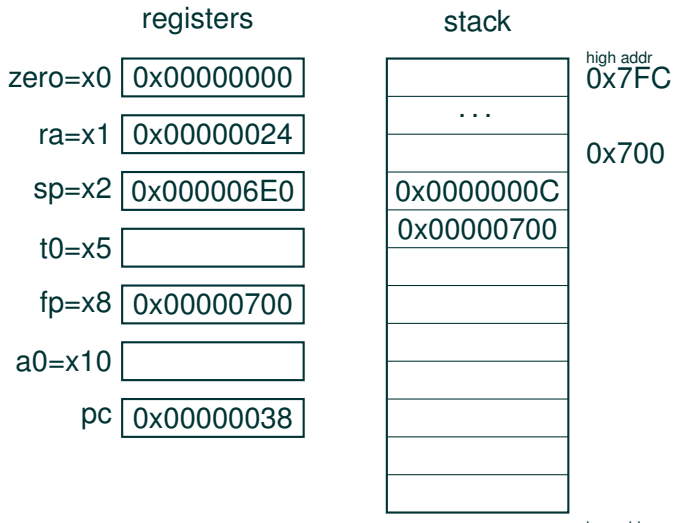
Buffer overflow

```
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
```



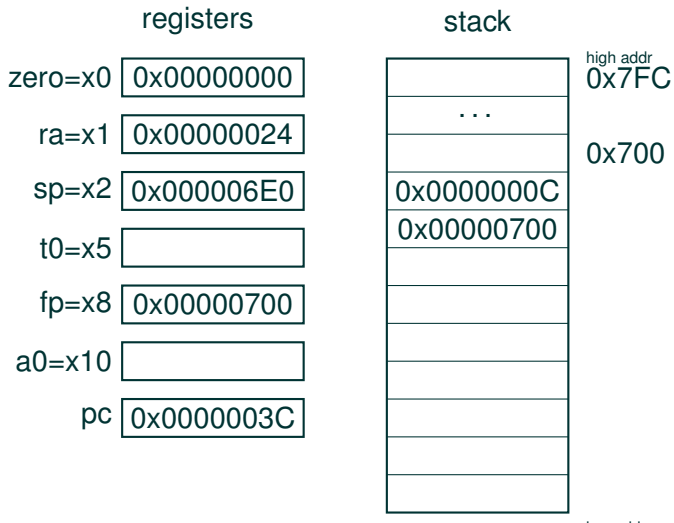
Buffer overflow

```
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
```



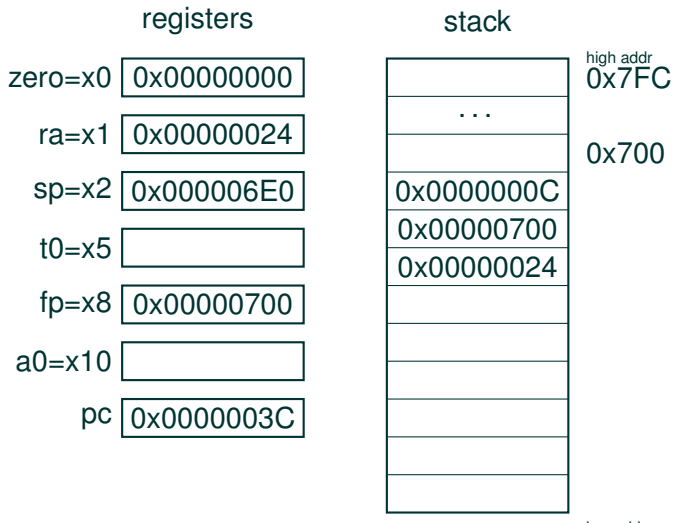
Buffer overflow

```
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
```



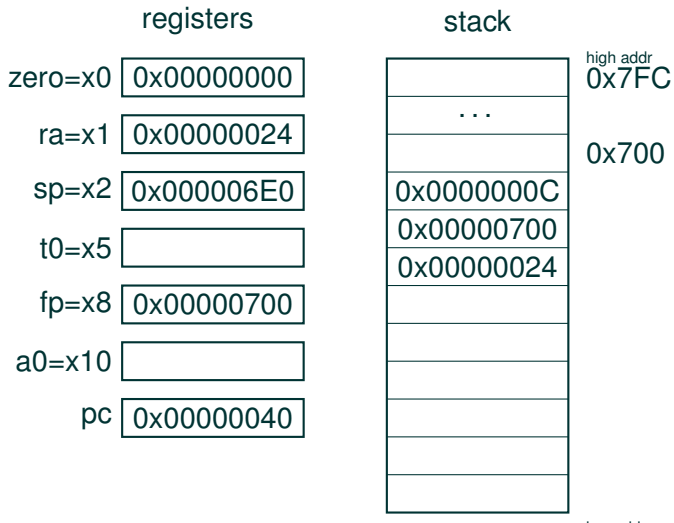
Buffer overflow

```
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
```



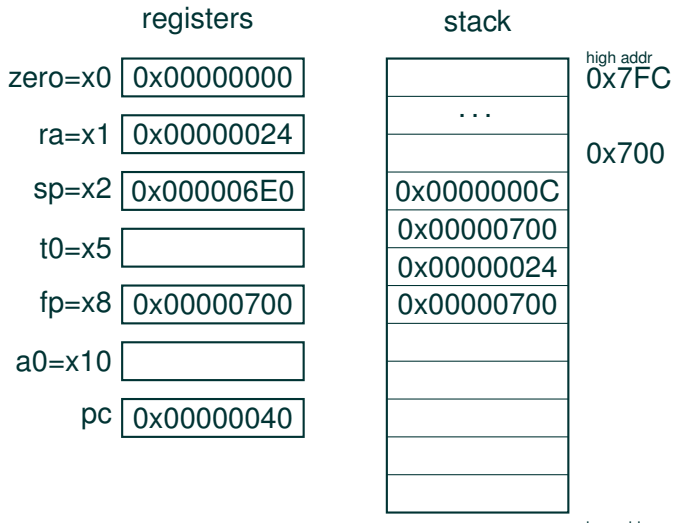
Buffer overflow

```
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
```



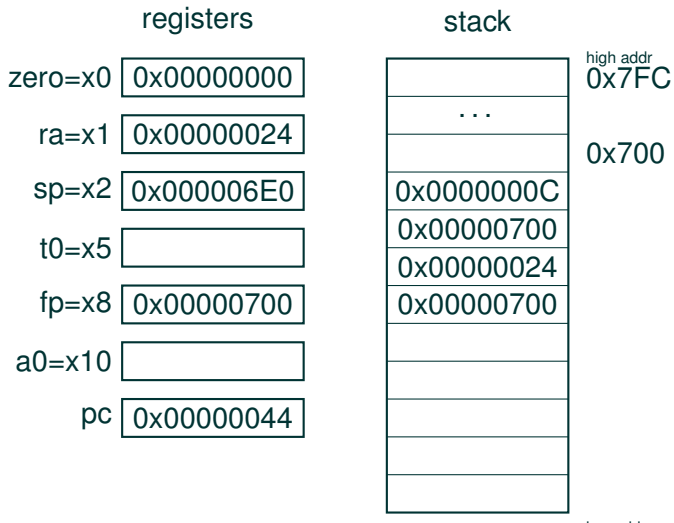
Buffer overflow

```
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
```



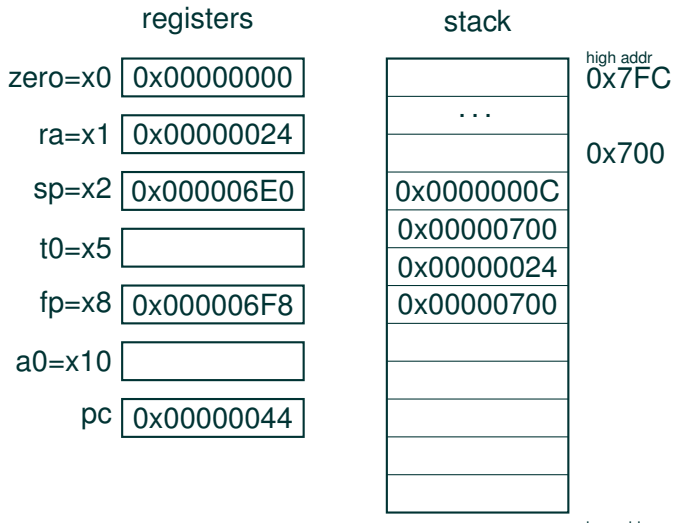
Buffer overflow

```
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
```



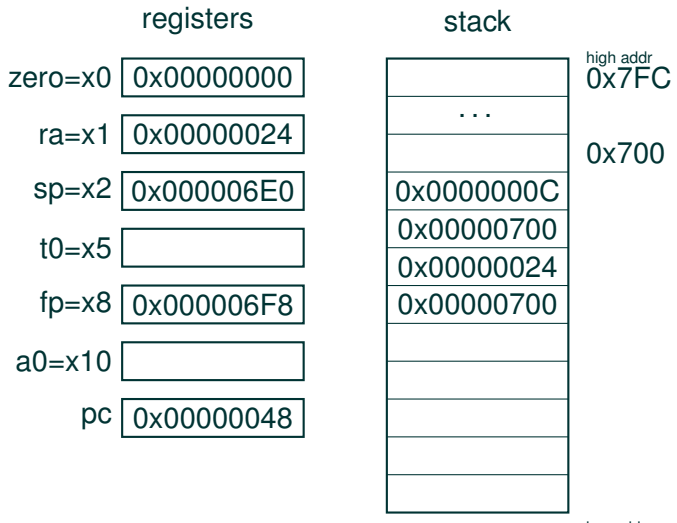
Buffer overflow

```
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
```



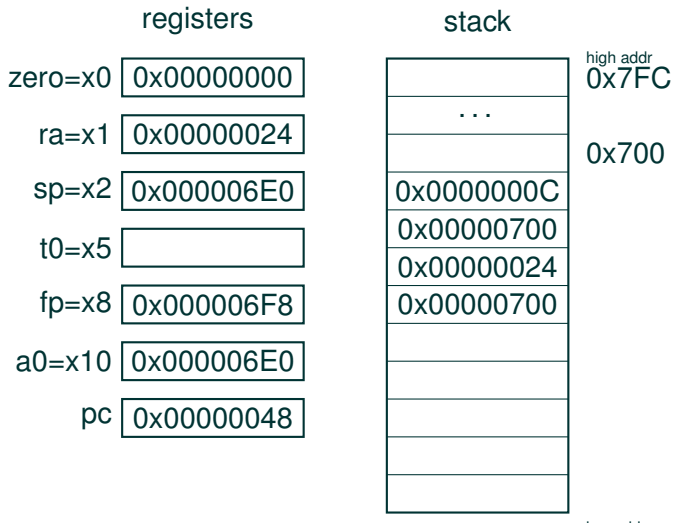
Buffer overflow

```
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
```



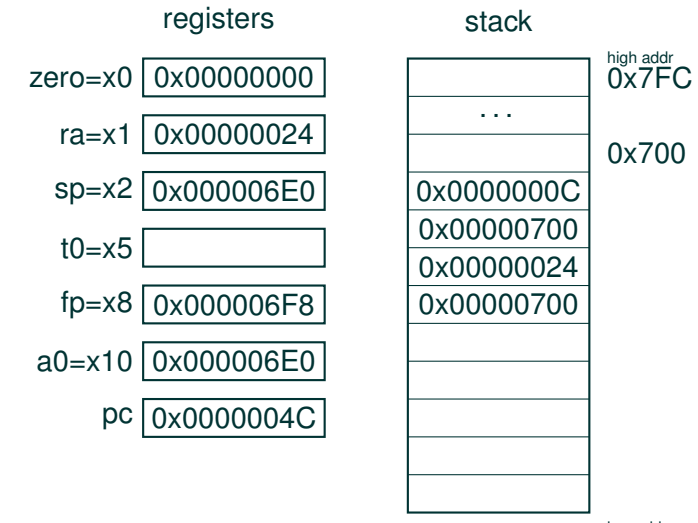
Buffer overflow

```
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
```



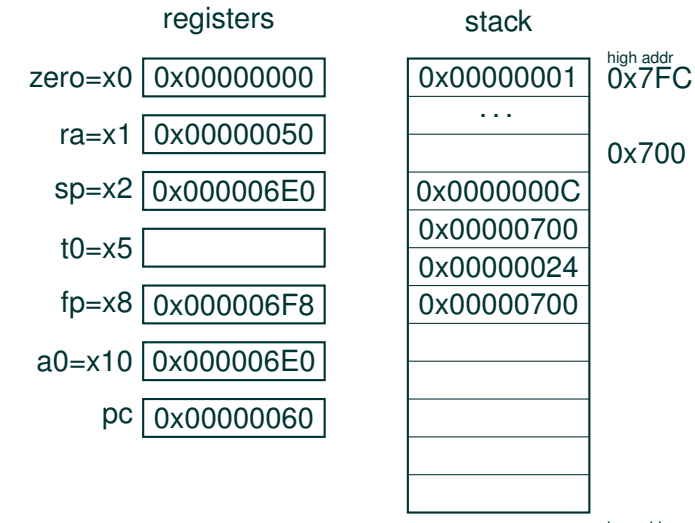
Buffer overflow

```
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
```



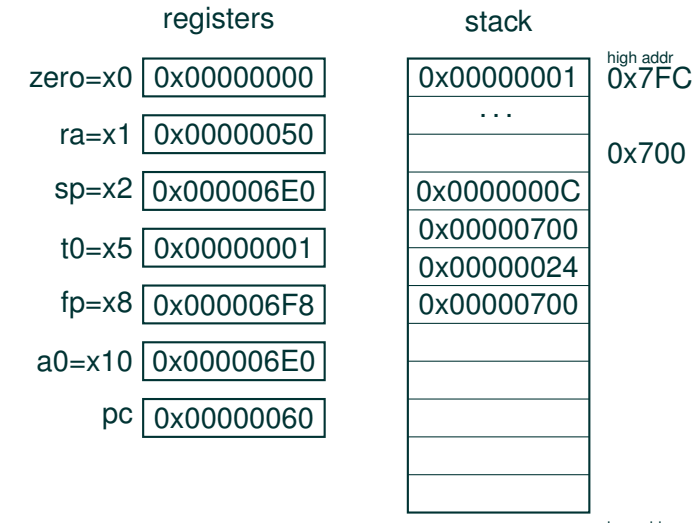
Buffer overflow

```
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
```



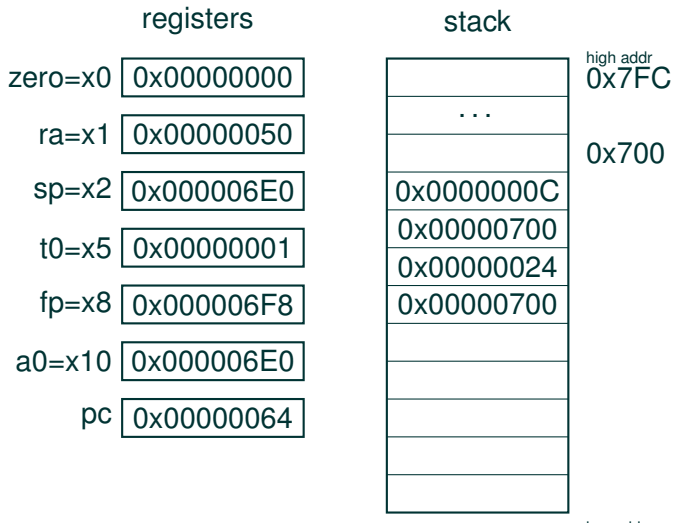
Buffer overflow

```
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
```



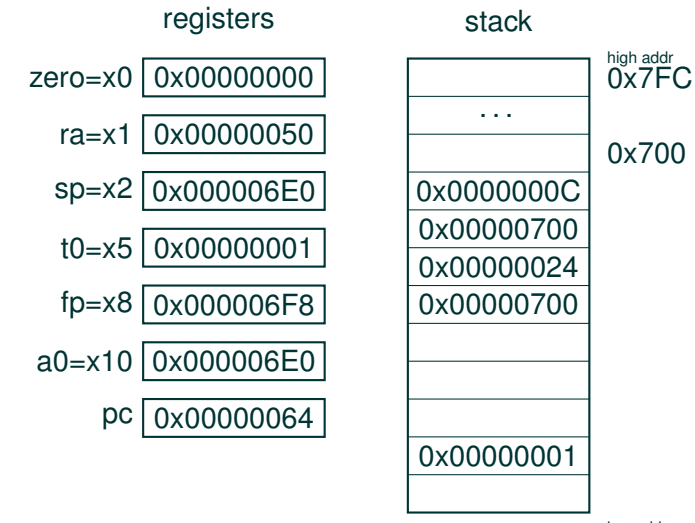
Buffer overflow

```
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
```



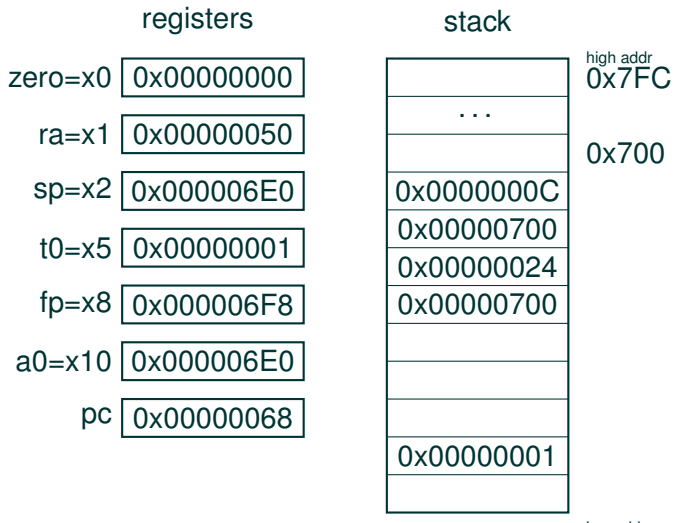
Buffer overflow

```
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
```



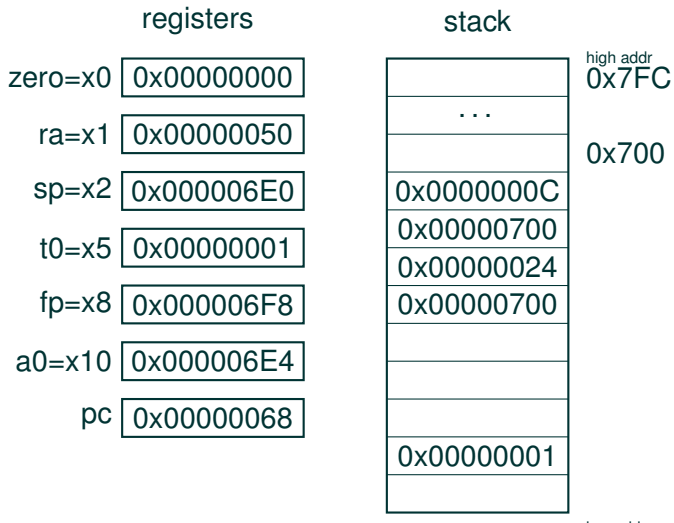
Buffer overflow

```
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
```



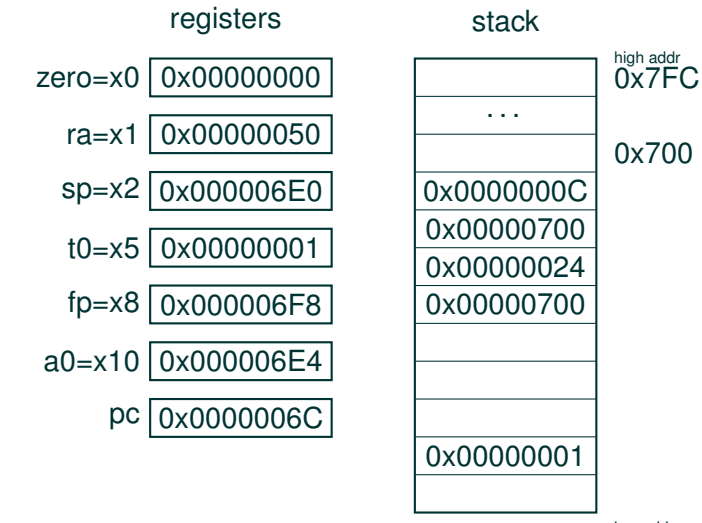
Buffer overflow

```
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
```



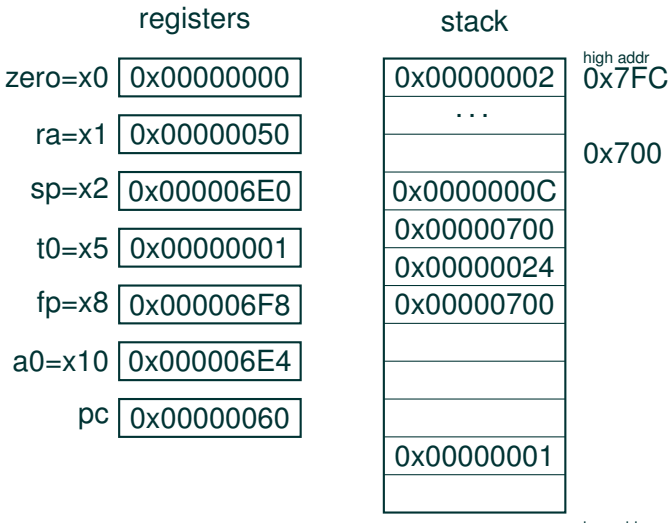
Buffer overflow

```
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
```

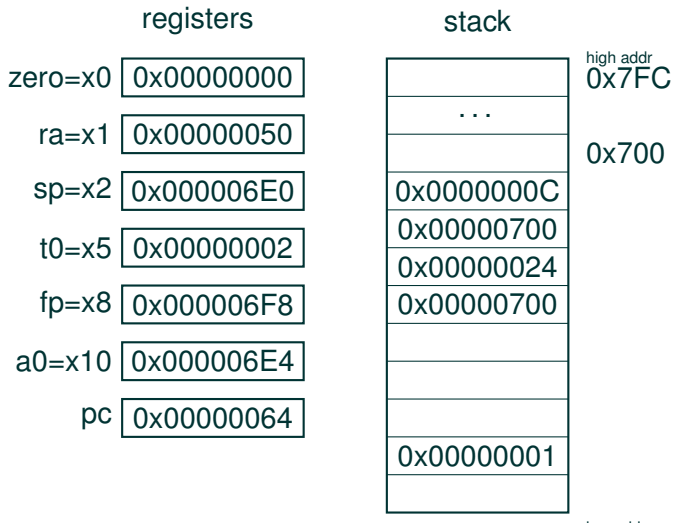


Buffer overflow

```
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
```

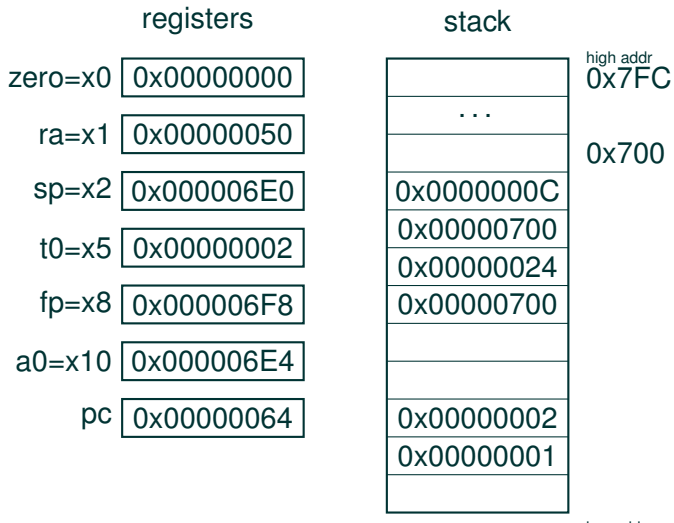
Buffer overflow

```
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
```



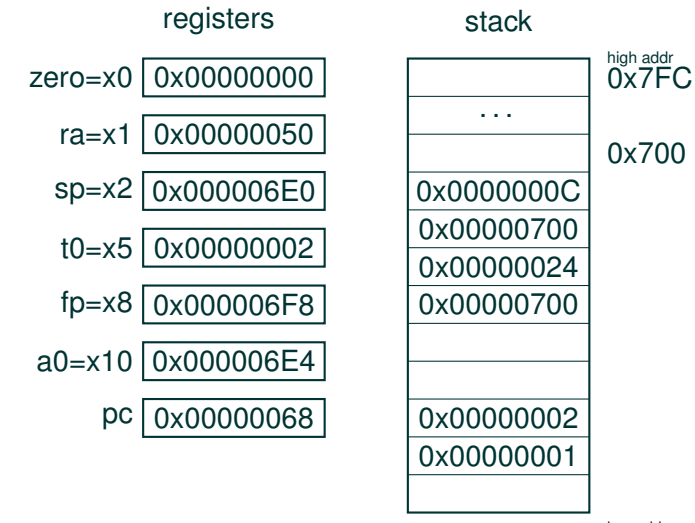
Buffer overflow

```
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
```



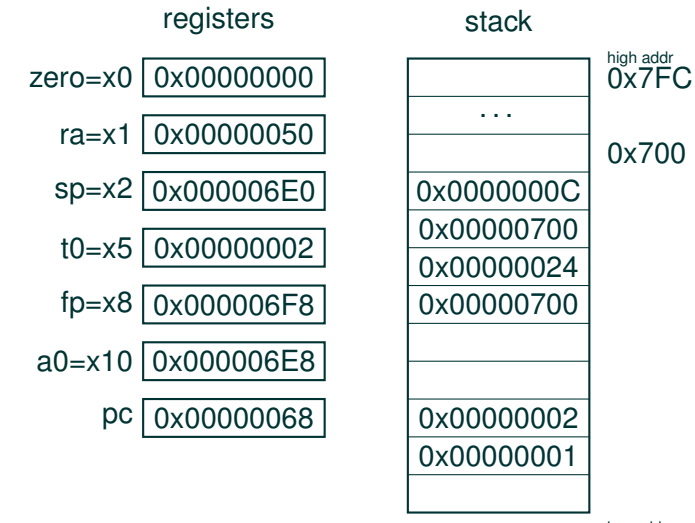
Buffer overflow

```
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
```



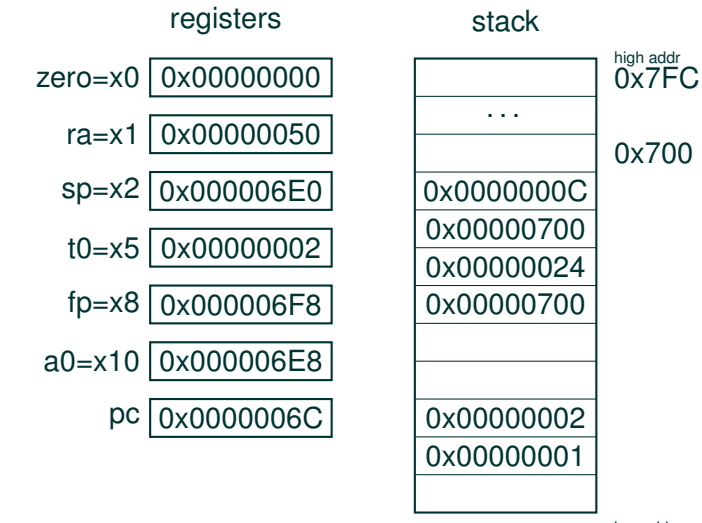
Buffer overflow

```
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
```



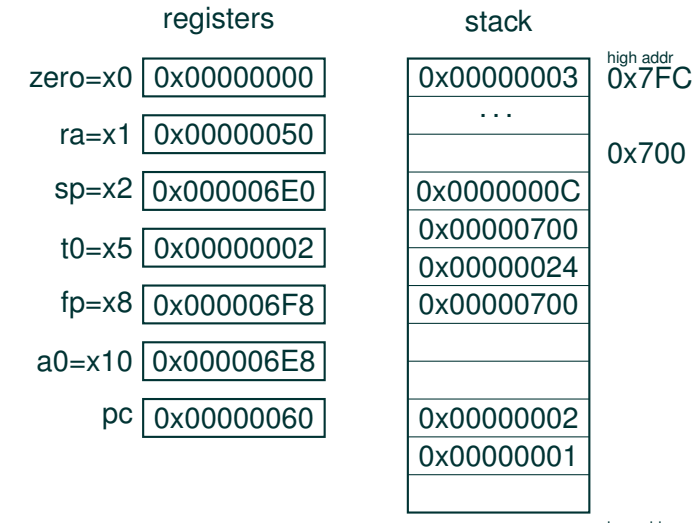
Buffer overflow

```
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
```



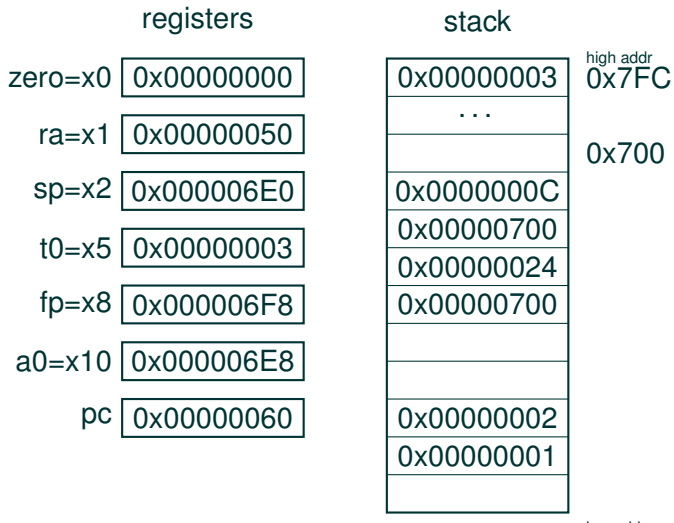
Buffer overflow

```
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
```



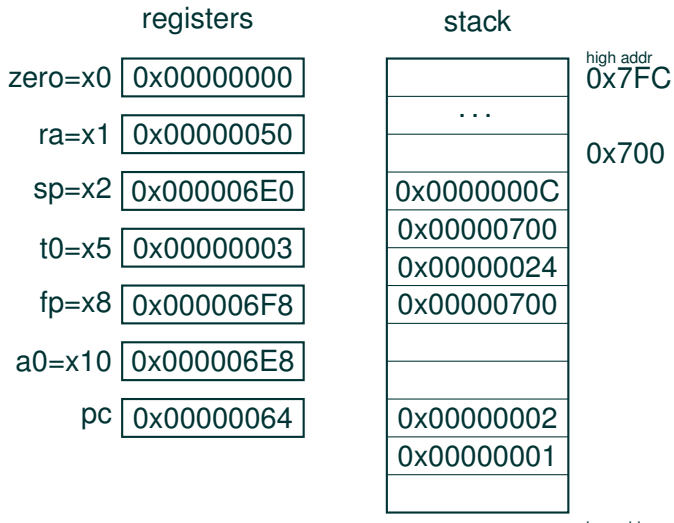
Buffer overflow

```
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
```



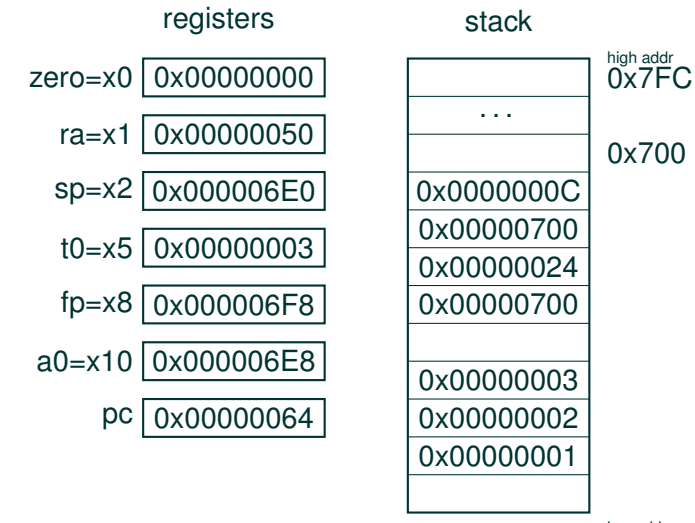
Buffer overflow

```
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
```



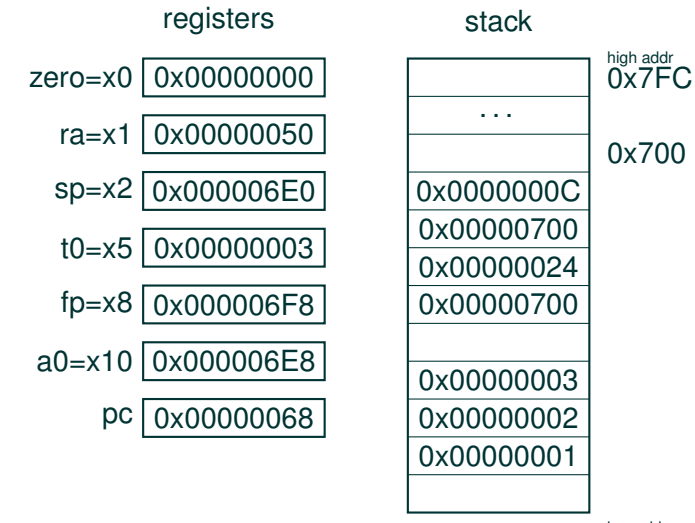
Buffer overflow

```
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,0(ra)
secret:
 SW   zero,0x7FC(zero)
 EBREAK
```



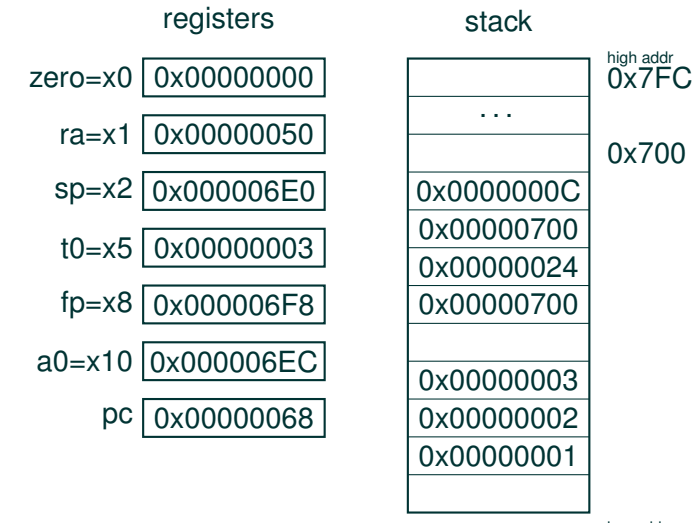
Buffer overflow

```
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
```



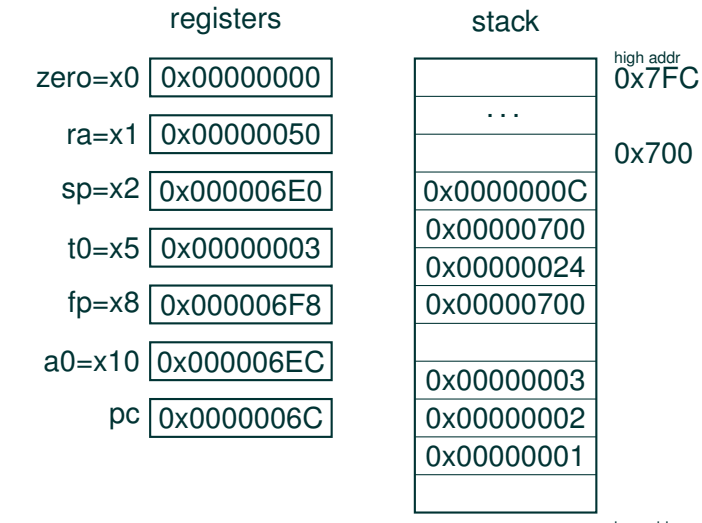
Buffer overflow

```
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
```



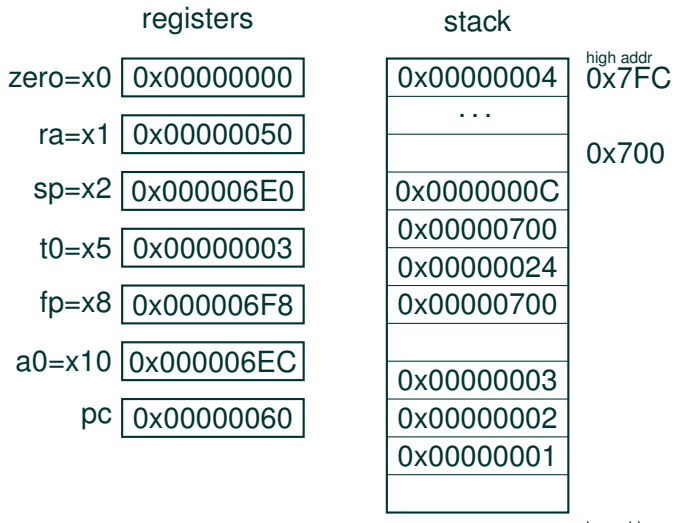
Buffer overflow

```
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
```



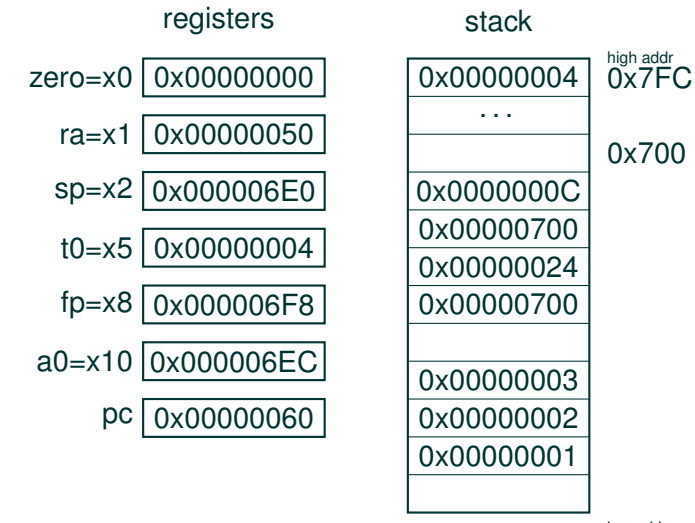
Buffer overflow

```
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
```



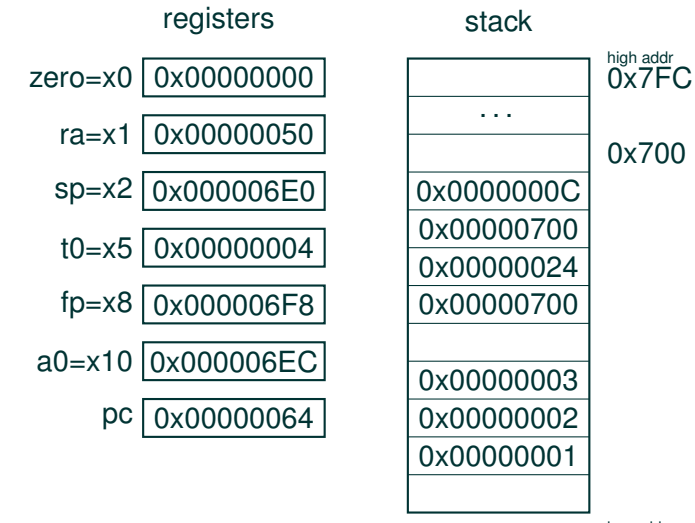
Buffer overflow

```
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
```



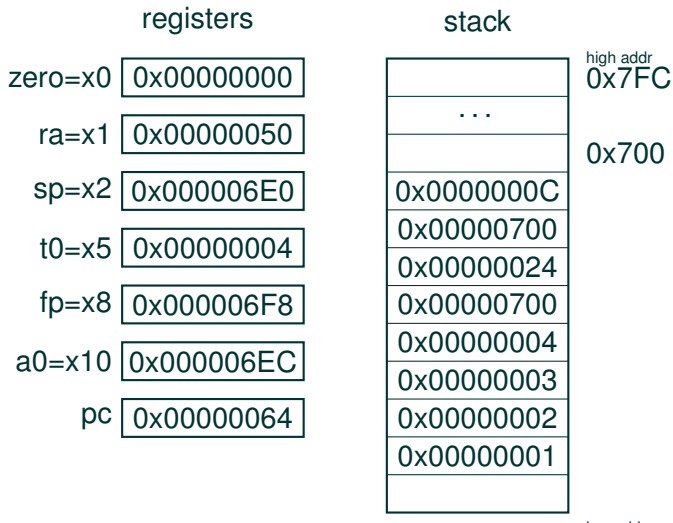
Buffer overflow

```
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
```



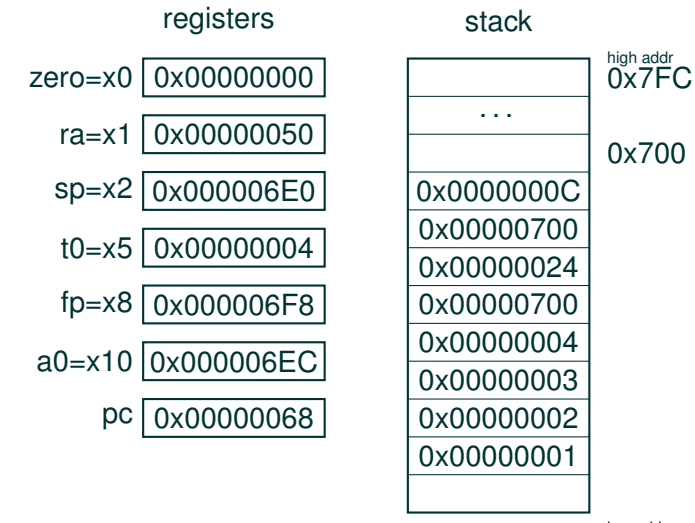
Buffer overflow

```
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
```



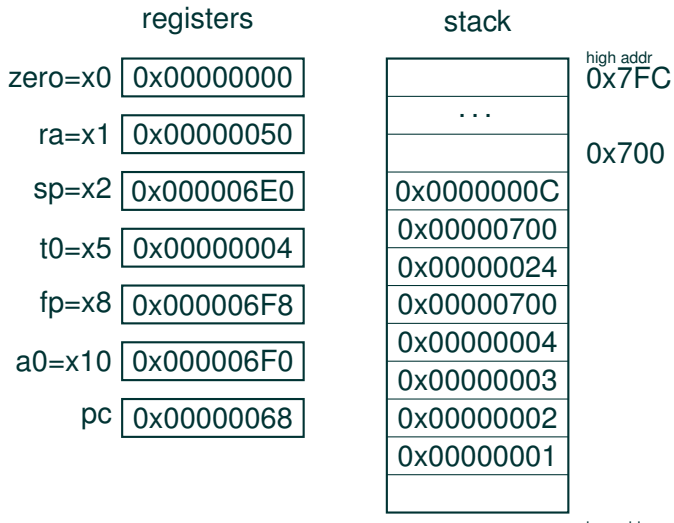
Buffer overflow

```
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
```



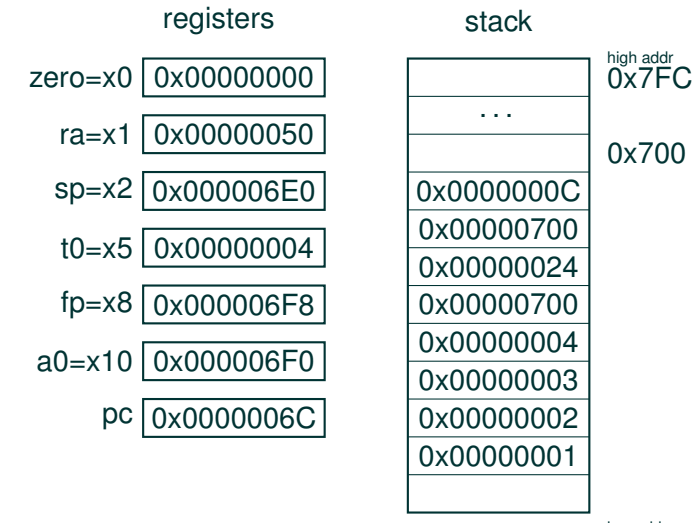
Buffer overflow

```
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
```



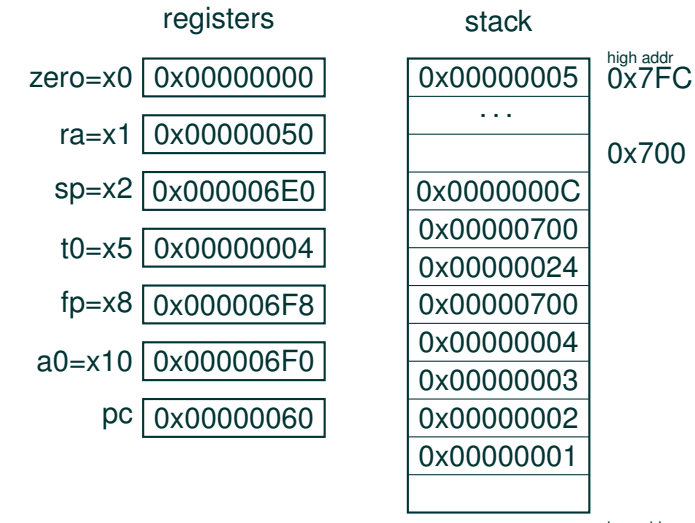
Buffer overflow

```
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
```



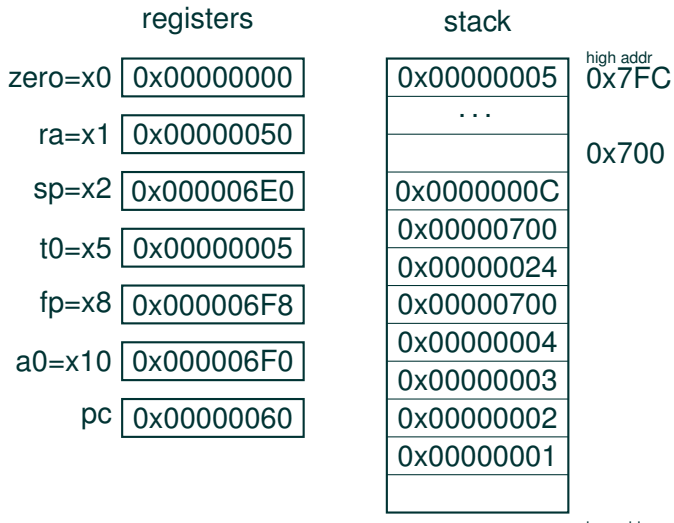
Buffer overflow

```
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
```



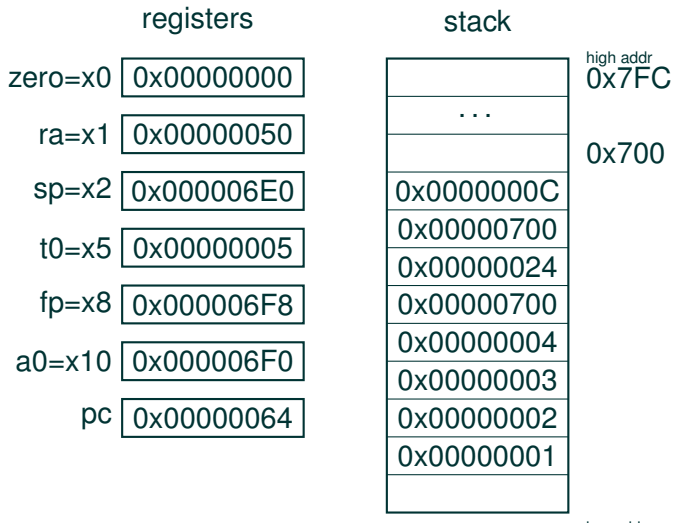
Buffer overflow

```
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
```



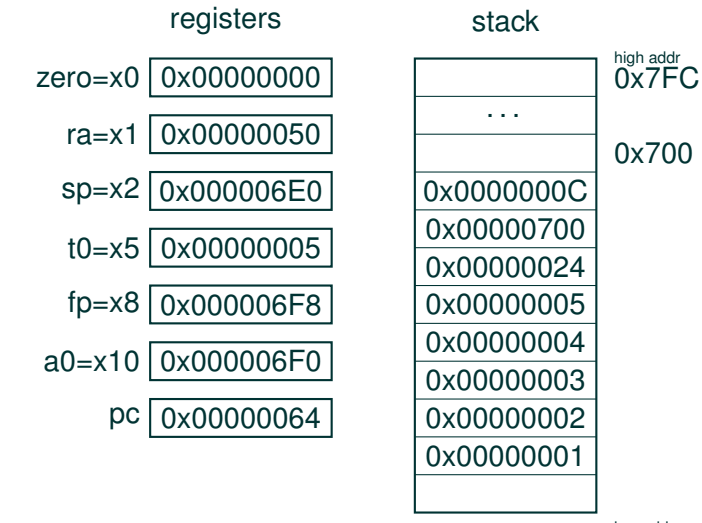
Buffer overflow

```
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
```



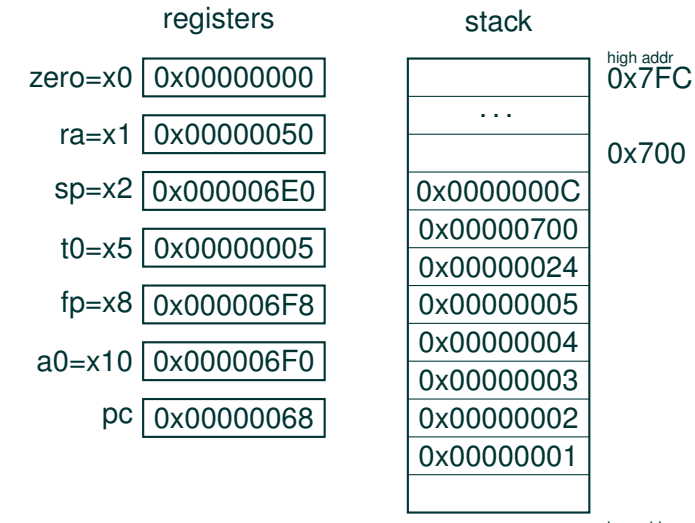
Buffer overflow

```
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
```



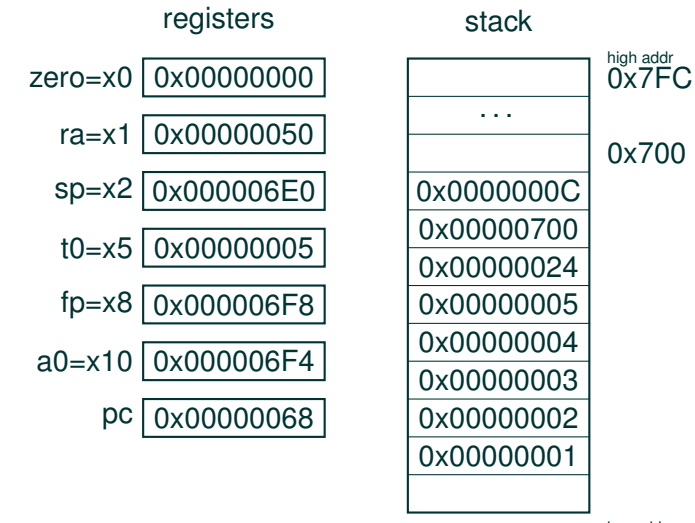
Buffer overflow

```
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
```



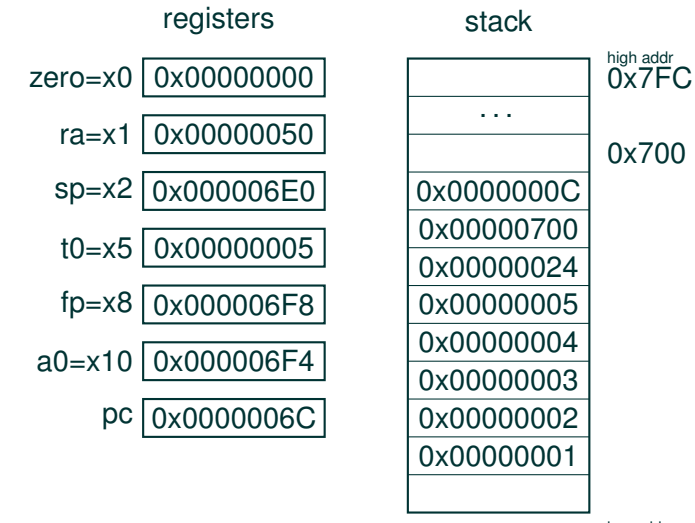
Buffer overflow

```
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
```



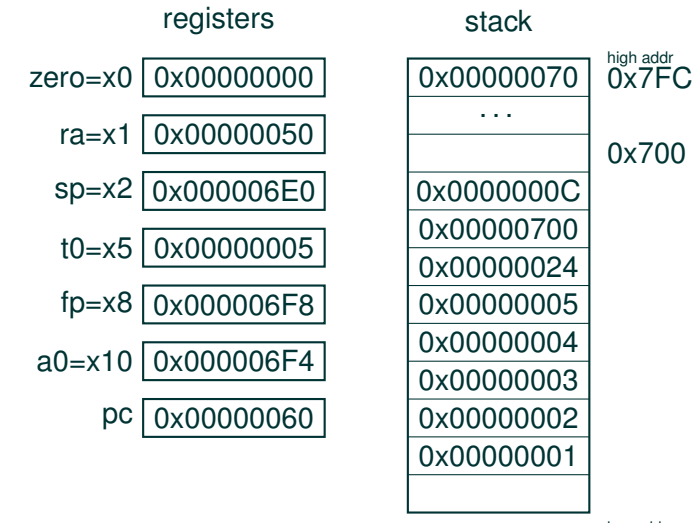
Buffer overflow

```
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
```



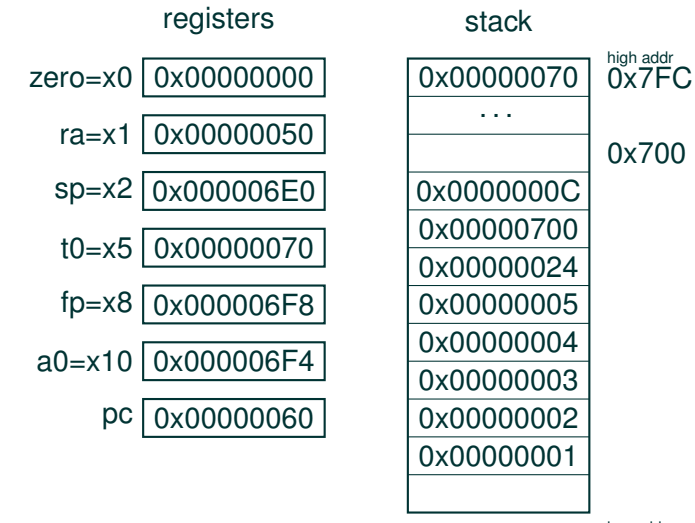
Buffer overflow

```
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
```



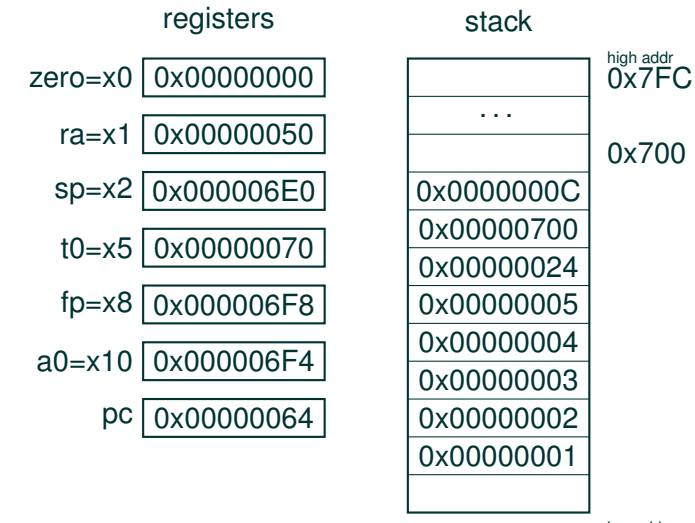
Buffer overflow

```
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
```



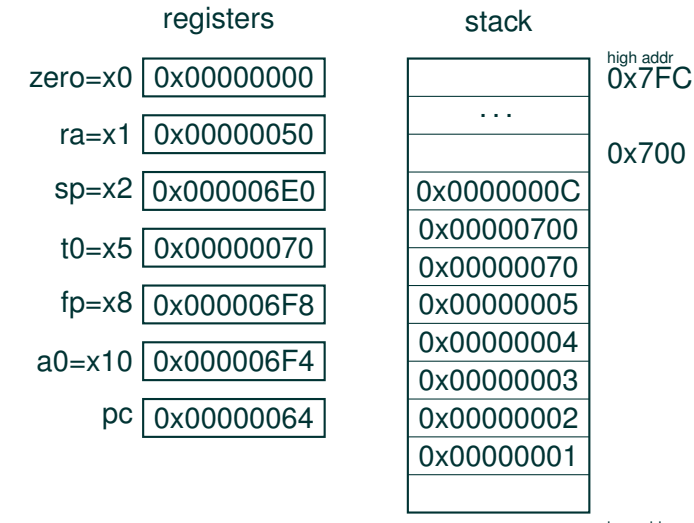
Buffer overflow

```
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
```



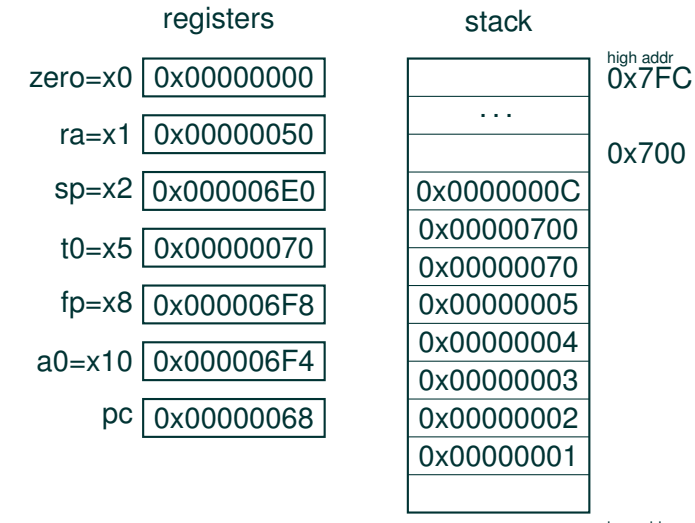
Buffer overflow

```
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
```



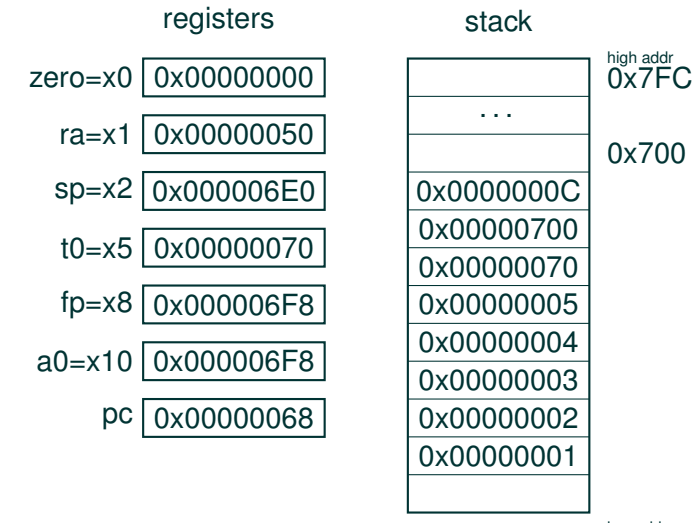
Buffer overflow

```
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
```



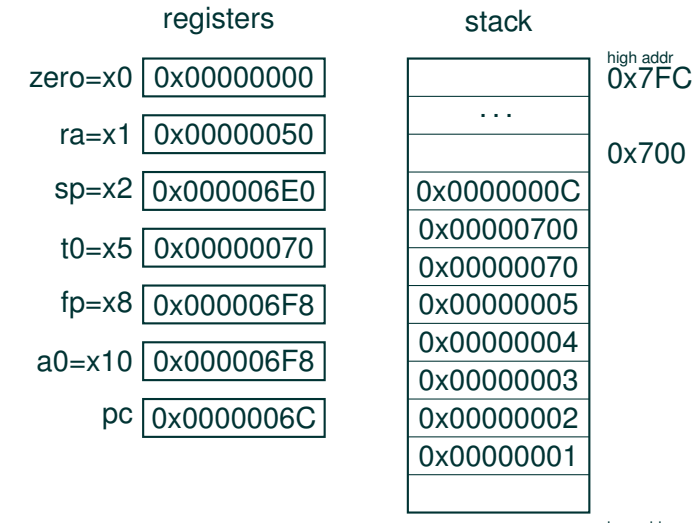
Buffer overflow

```
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
```



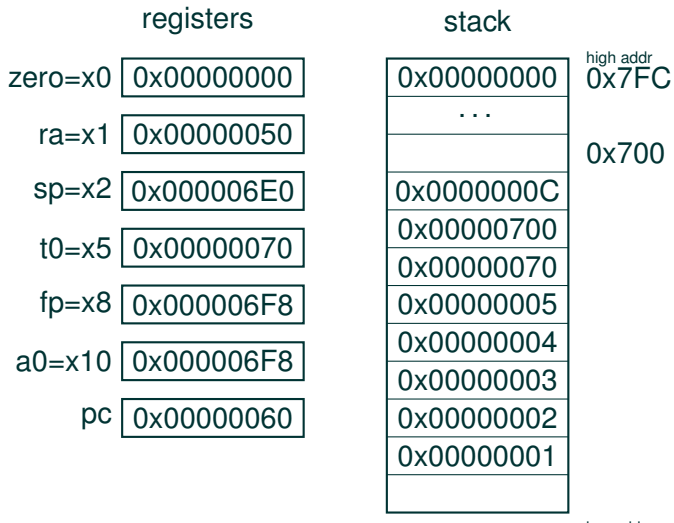
Buffer overflow

```
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
```



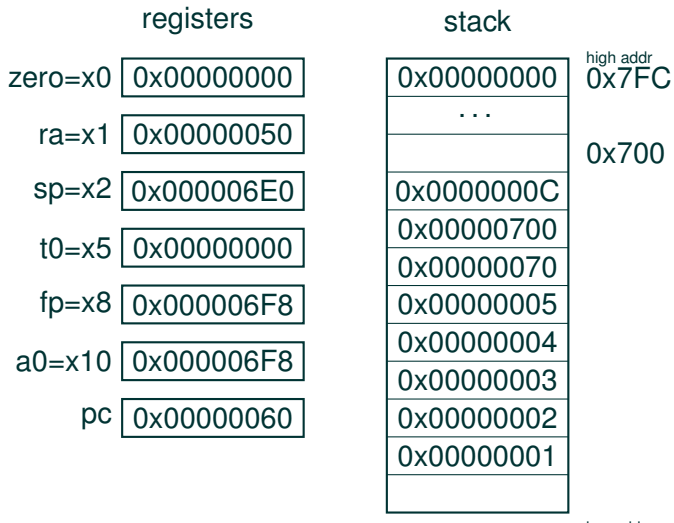
Buffer overflow

```
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
```



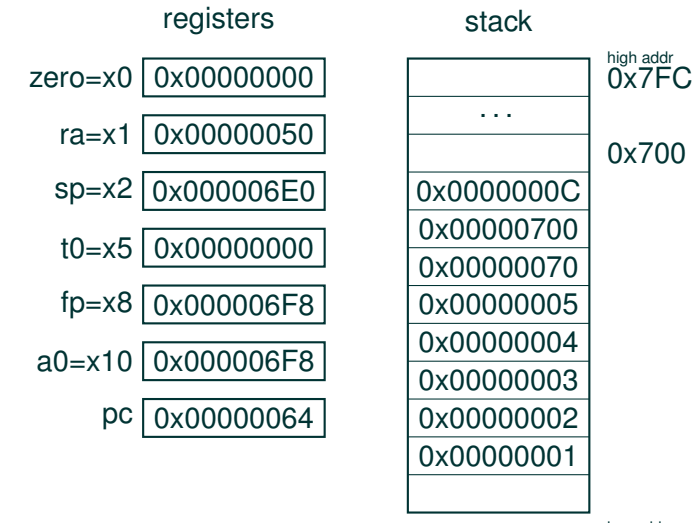
Buffer overflow

```
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
```



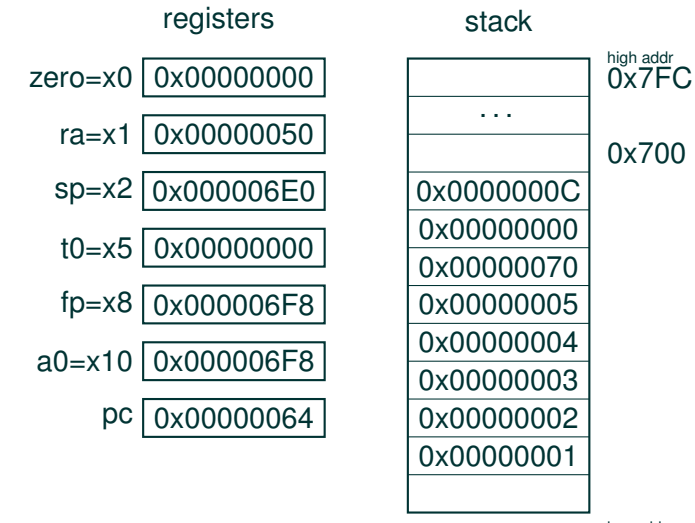
Buffer overflow

```
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
```



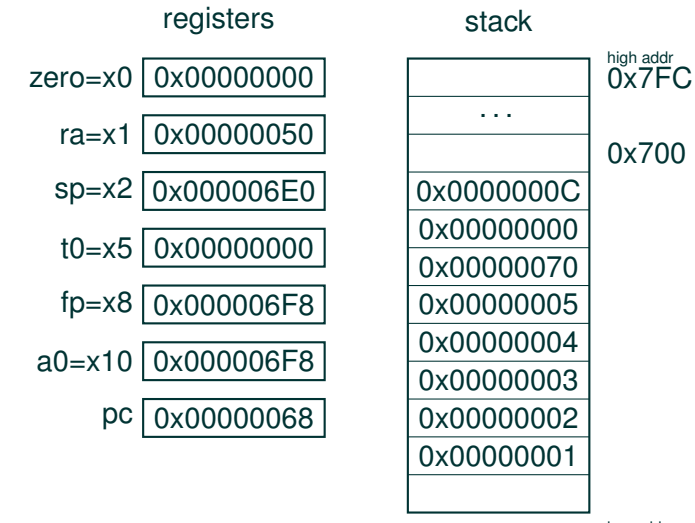
Buffer overflow

```
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,0(ra)
secret:
 SW   zero,0x7FC(zero)
 EBREAK
```



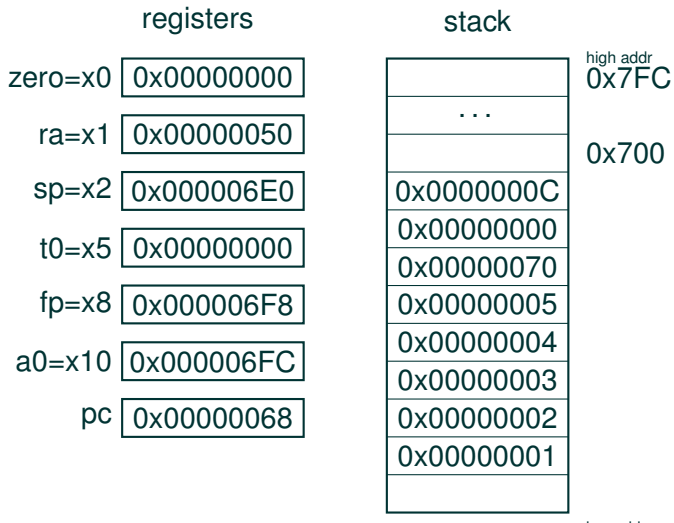
Buffer overflow

```
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
```



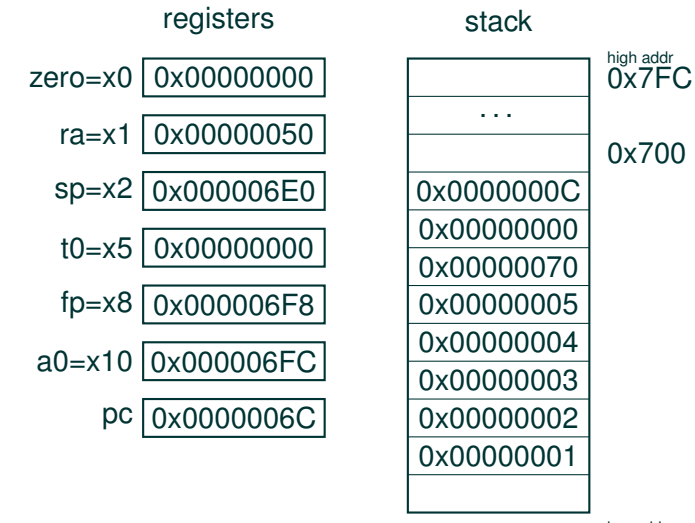
Buffer overflow

```
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
```



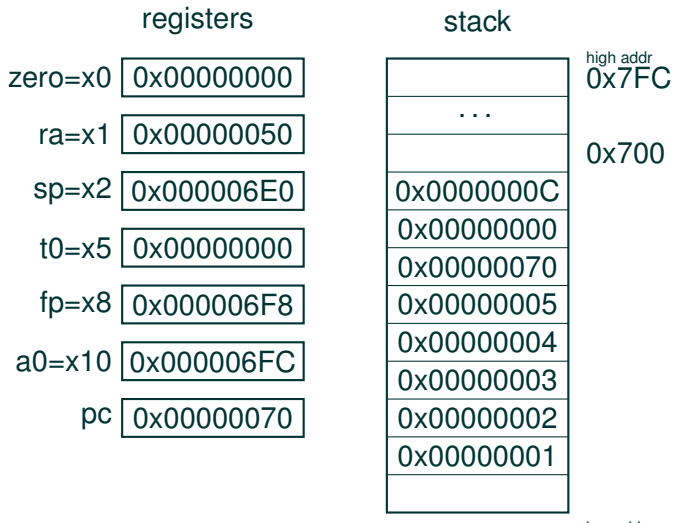
Buffer overflow

```
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
```



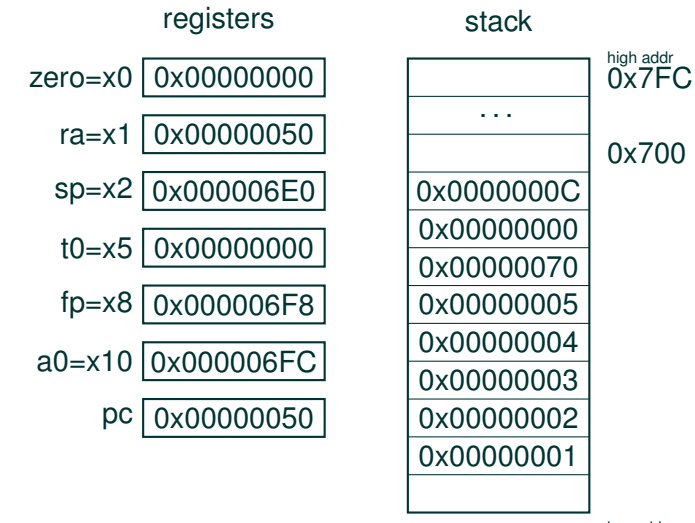
Buffer overflow

```
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
```



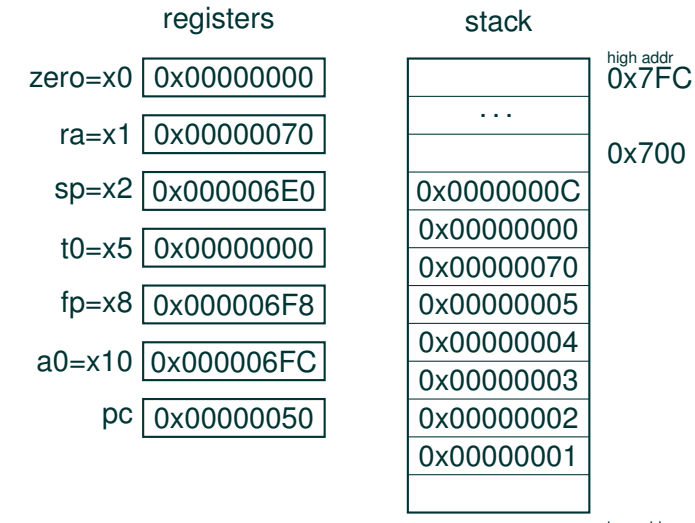
Buffer overflow

```
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
```



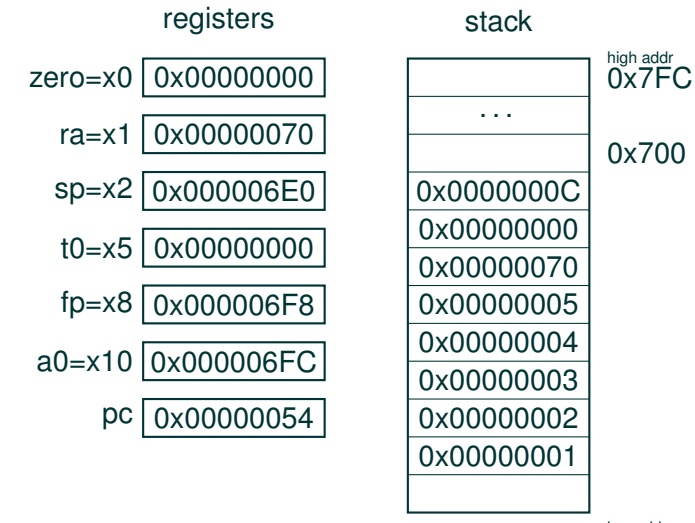
Buffer overflow

```
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
```



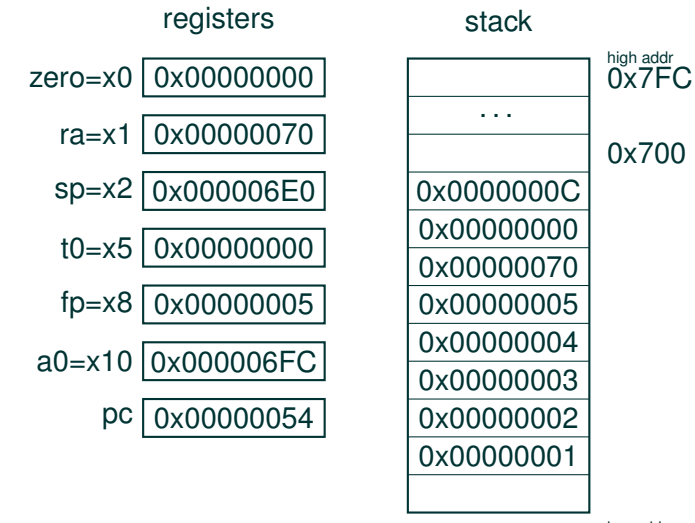
Buffer overflow

```
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
```



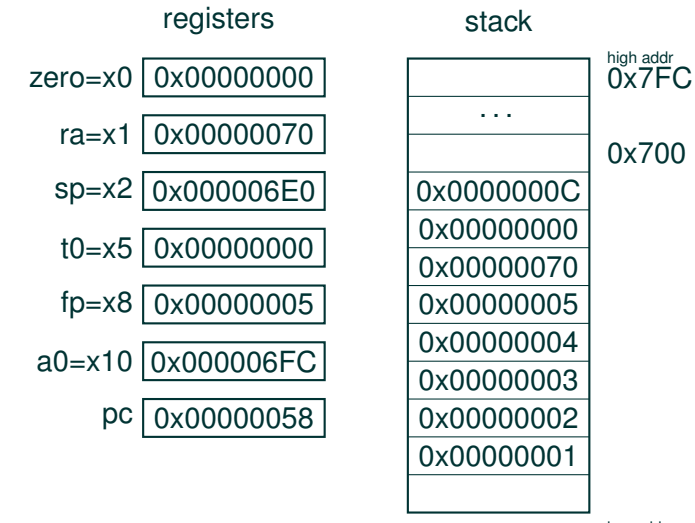
Buffer overflow

```
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
```



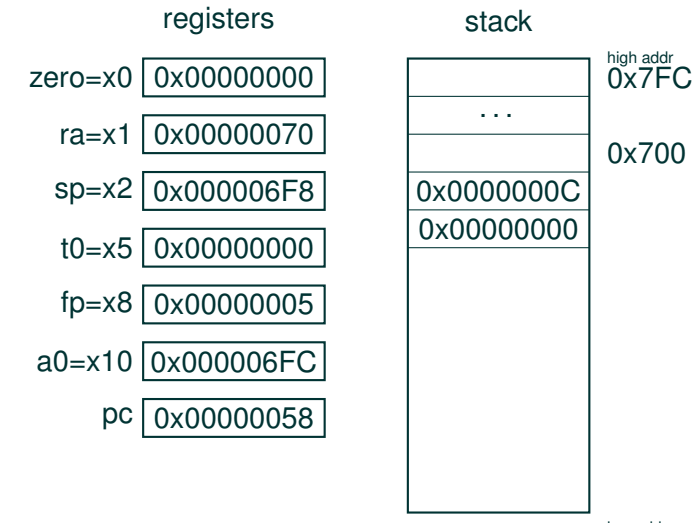
Buffer overflow

```
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
```



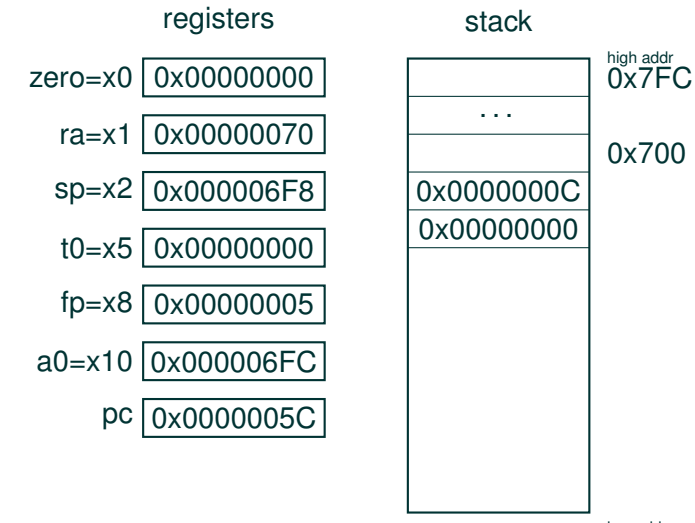
Buffer overflow

```
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
```



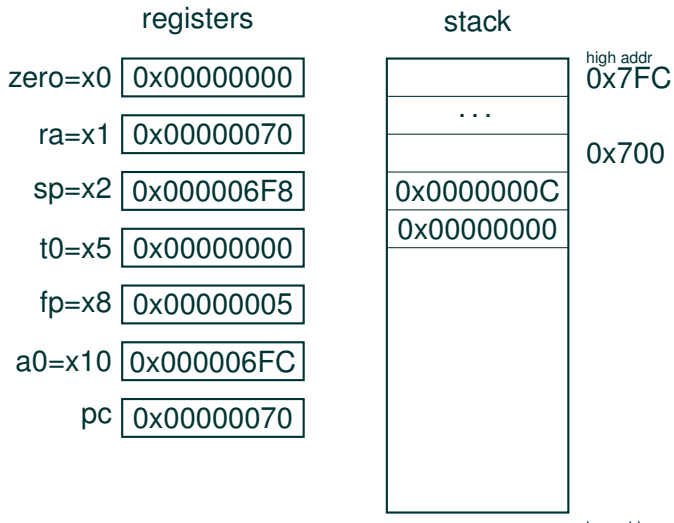
Buffer overflow

```
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
```



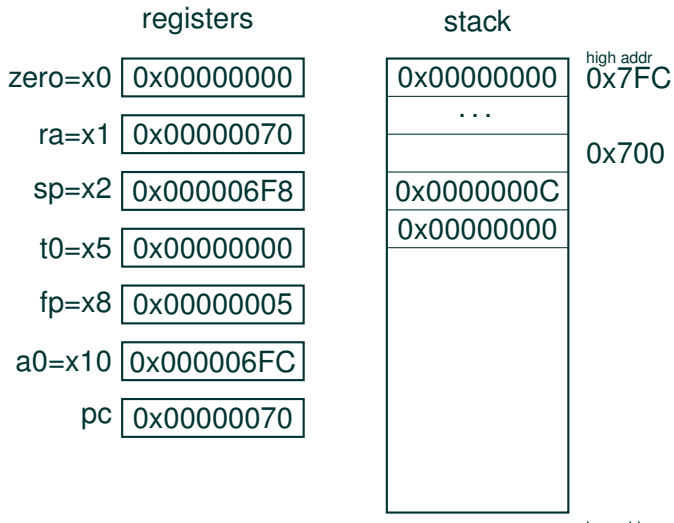
Buffer overflow

```
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
```



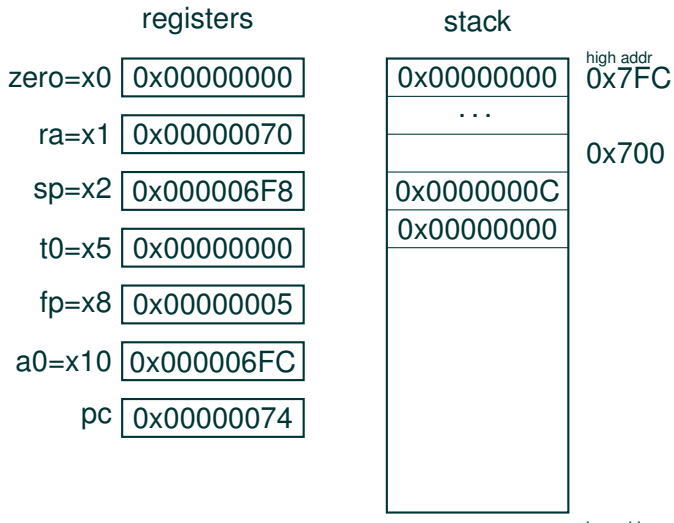
Buffer overflow

```
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

Stefan Mangard

Computer Organization and Networks
Graz University of Technology