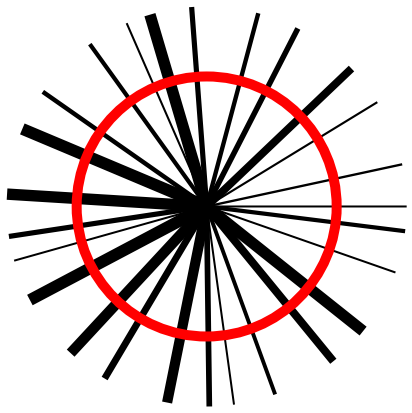
```
1000 fe,01,01,13 add sp,sp,-32
1004 00,11,2e,23 sw ra,28(sp)
1008 00,10,07,93 li a5,1
1012 00,f1,22,23 sw a5,4(sp)
1016 00,41,07,93 add a5,sp,4
1020 00,f1,26,23 sw a5,12(sp)
1024 ??,?0,07,93 li a5,✎
1028 00,f1,24,23 sw a5,8(sp)
1032 00,81,27,83 lw a5,8(sp)
1036 00,07,86,63 beqz a5,1048 # +12
1040 04,40,00,ef jal 1108 # +68
1044 00,80,00,6f j 1052 # +8
1048 c6,9f,f0,ef jal 128 # -920
1052 00,c1,27,83 lw a5,12(sp)
1056 00,07,a7,83 lw a5,0(a5)
1060 fc,07,9e,e3 bnez a5,1024 # -36
1064 00,00,07,93 li a5,0
1068 00,07,85,13 mv a0,a5
1072 01,c1,20,83 lw ra,28(sp)
1076 02,01,01,13 add sp,sp,32
1080 00,00,80,67 ret
1084 00,00,00,00
1088 00,00,00,00
1092 00,00,00,00
1096 00,00,00,00
1100 00,00,00,00
1104 00,00,00,00
1108 fe,01,01,13 add sp,sp,-32
1112 00,11,2e,23 sw ra,28(sp)
1116 00,c1,27,83 lw a5,12(sp)
1120 00,07,88,63 beqz a5,1136 # +16
1124 02,c0,00,ef jal 1168 # +44
1128 00,01,26,23 sw zero,12(sp)
1132 00,c0,00,6f j 1144 # +12
1136 c8,df,f0,ef jal 252 # -884
1140 c8,9f,f0,ef jal 252 # -888
1144 00,00,00,13 nop
1148 01,c1,20,83 lw ra,28(sp)
1152 02,01,01,13 add sp,sp,32
1156 00,00,80,67 ret
1160 00,00,00,00
1164 00,00,00,00
1168 ??,?0,07,13 li a4,✎
1172 30,57,10,73 csrw mtvec,a4
1176 00,00,00,13 nop
1180 00,00,80,67 ret
1184 00,00,00,00
1188 00,00,00,00
```

```c
int main(void) {
  // 4(sp)
  int run = 1;
  // 12(sp)
  int *prun = &run;
  do {
    // 8(sp)
    int choice = ✎;
    if (choice) {
      exploit();
    } else {
      bug();
    }
  } while(*prun);

  return 0;
}
```



PROJEKT: OVERFLOW

https://punkx.org/overflow
version: 0.0.6


```c
void exploit(void) {
  // 12(sp)
  int should_set_trap;
  if (should_set_trap) {
    set_trap();
    should_set_trap = 0;
  } else {
    copy();
    copy();
  }
}
```

```c
void set_trap(void) {
  asm("li a4, ✎");
  asm("csrw mtvec, a4");
}
```