[j00ru] Night Sky

Initial recon

```
$ file night_sky
night_sky: ELF 64-bit LSB  shared object, x86-64, version 1 (SYSV), dynamically linked (uses
shared libs), for GNU/Linux 2.6.24, BuildID[sha1]=b8f46988ccb50aea56107807b4d9ef3191d4a717,
stripped

$ ./checksec.sh --file night_sky
RELRO           STACK CANARY      NX            PIE             RPATH      RUNPATH      FILE
Full RELRO      Canary found      NX enabled    PIE enabled     No RPATH   No RUNPATH   night_sky
```

Night Sky

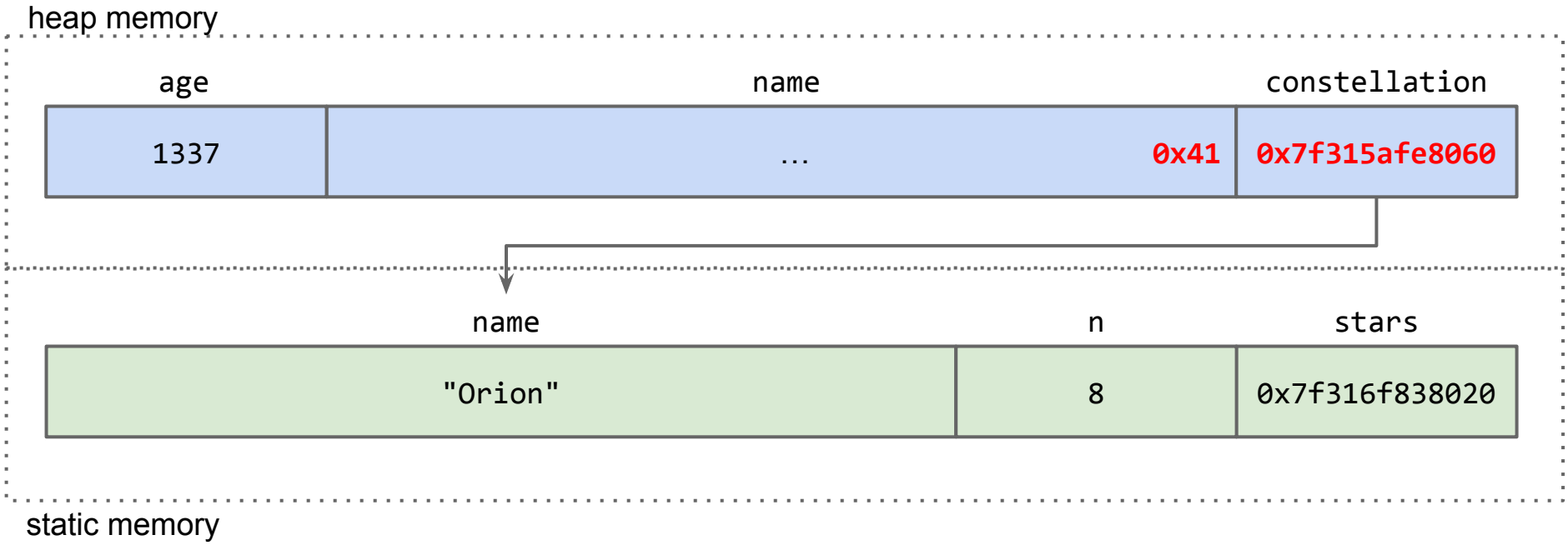
```
$ ./night_sky
Welcome to the Night Sky Creater, version alpha-0.0.1
Select an operation.
```

Available operations

```
add_star    remove_star    edit_star  list_stars
create_constellation       remove_constellation
edit_constellation         list_constellations
register_program           save_to_file
```

Night Sky

First bug: `edit_star` + `list_stars`



Night Sky

1. AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA`P

(1337 years old)
Select an operation.

Night Sky

Second bug: `register_program`

```
uint16_t n;
ASSERT(read_all(STDIN_FILENO, &n, sizeof(n)));
ASSERT(n <= globals::kMaxSerialLength);

char buffer[globals::kMaxSerialLength + 1];
ssize_t bytes_read = read(STDIN_FILENO, buffer, n - 1);
```

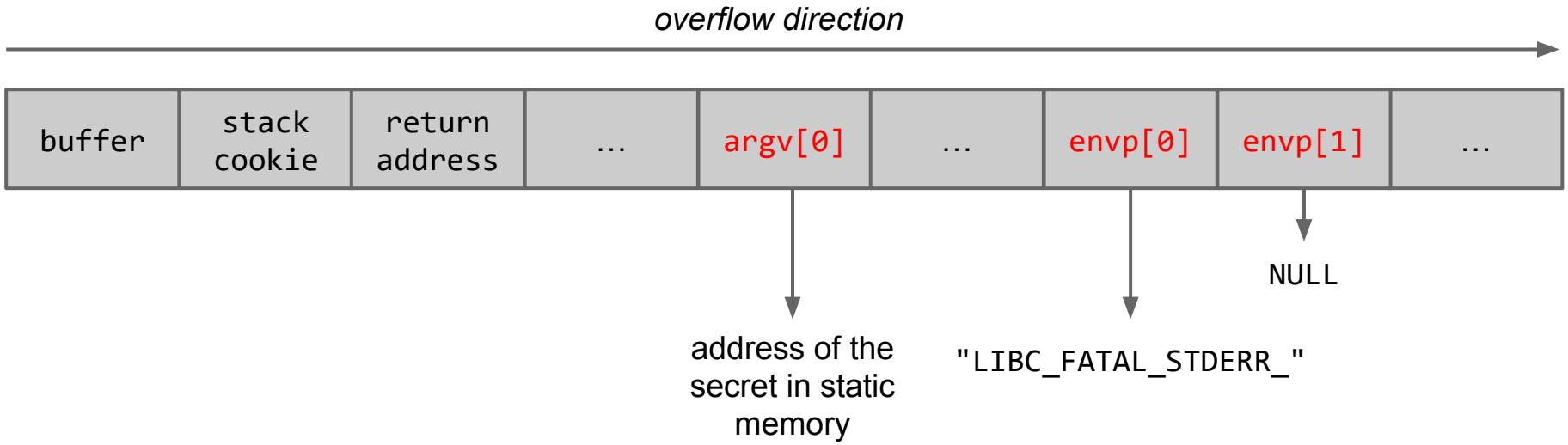
65535

Night Sky

1. It is possible to trash the stack with 64kB of controlled data.
2. The stack protector is enabled, so code execution is not possible.
3. The `LIBC_FATAL_STDERR_` variable is not set, so we can't even use the SSP memory disclosure trick… or can we?

Night Sky

- Well, we know a pointer to controlled memory, and have full control over `envp[]`.



Night Sky

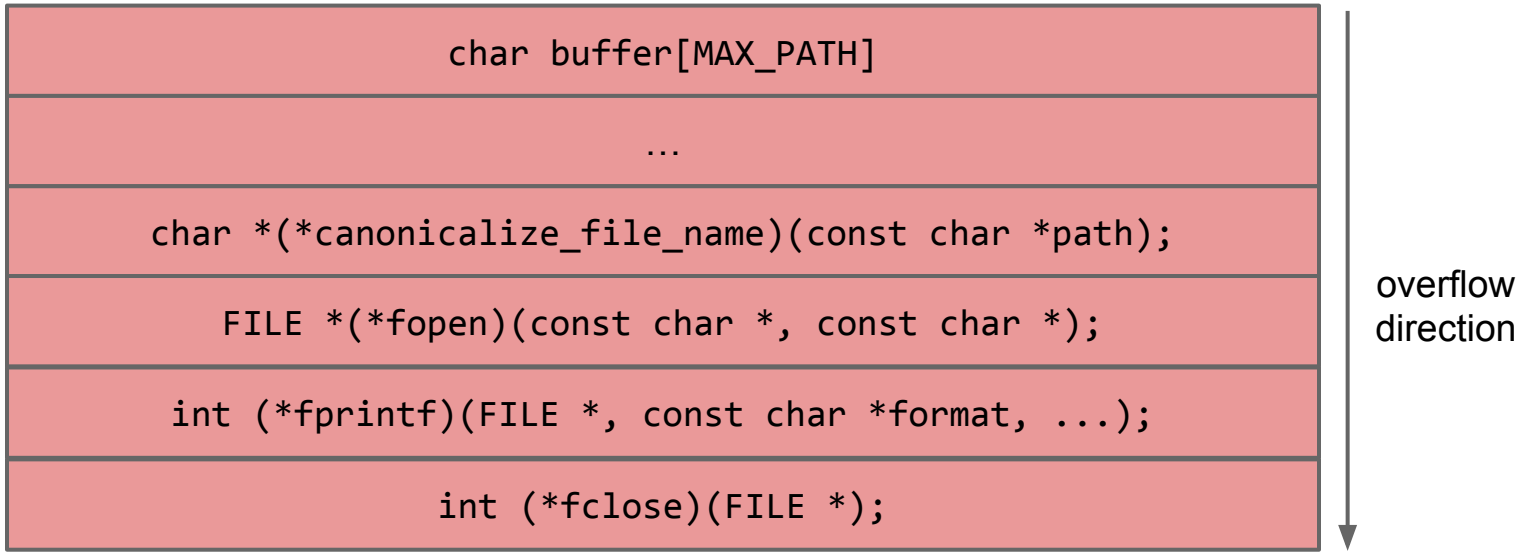
Serial number leaked:

```
*** stack smashing detected ***:
7fcc3-3e62a-ef5bc-e89c9-c44ad-d303b terminated
/bin/bash: line 1:     2 Aborted                 (core dumped)
./night_sky
```

Night Sky

Third bug: `save_to_file`

- Stack-based buffer overflow with controlled size.



Night Sky

- Controlled EIP via overwritten function pointer.
- Since the base address of the challenge is known and there is controlled data in static memory, you could probably use a stack pivot + ROP chain.
- However, there is an easier solution.

Night Sky

`canonicalize_file_name()` and `system()` are in the same memory page in libc!

```
.text:0000000000046640                 public system ; weak
.text:0000000000046640 system          proc near
.text:0000000000046640                 test    rdi, rdi
.text:0000000000046643                 jz      short loc_46650
.text:0000000000046645                 jmp     sub_46170

.text:0000000000046D20 ; =============== S U B R O U T I N E =======================================
.text:0000000000046D20
.text:0000000000046D20
.text:0000000000046D20                 public canonicalize_file_name ; weak
.text:0000000000046D20 canonicalize_file_name proc near
.text:0000000000046D20                 xor     esi, esi
.text:0000000000046D22                 jmp     realpath_0
.text:0000000000046D22 canonicalize_file_name endp
.text:0000000000046D22
```

Night Sky

You can do a 2-byte partial overwrite of `canonicalize_file_name`, and brute-force 4 bits of ASLR.

Night Sky

```
$ python exploit.py
[+] Static address leaked: 7fd96ca18060
[+] Leaked serial number: 7fcc3-3e62a-ef5bc-e89c9-c44ad-d303b
Trying....

[-] Failed.
Trying....

[-] Failed.
Trying....

[+] Got flag: "DrgnS{55P_M3m0ry_d15c105ur3_4nd_part141_0v3rwr1t35_FTW!}"
```