Binary Patch Practice
Eliza

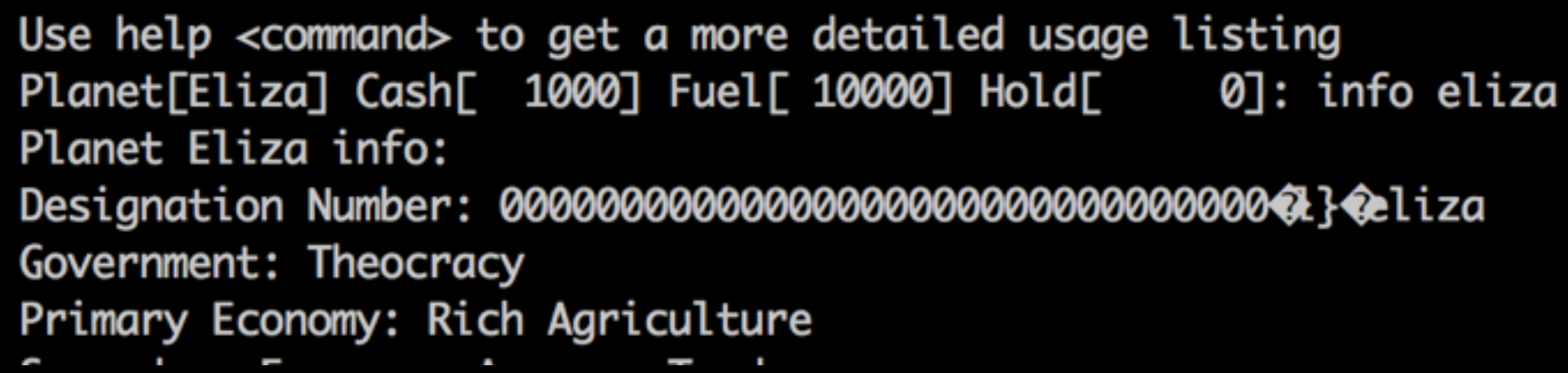
http://secprog.cs.nctu.edu.tw/files/eliza

Vulnerabilities

- Information Leak
  - doinfo - uninitialized variable
- Stack overflow
  - my_printf() - copy from big size to small size
  - dobuy() - no boundary check

Information Leak

- help
- info

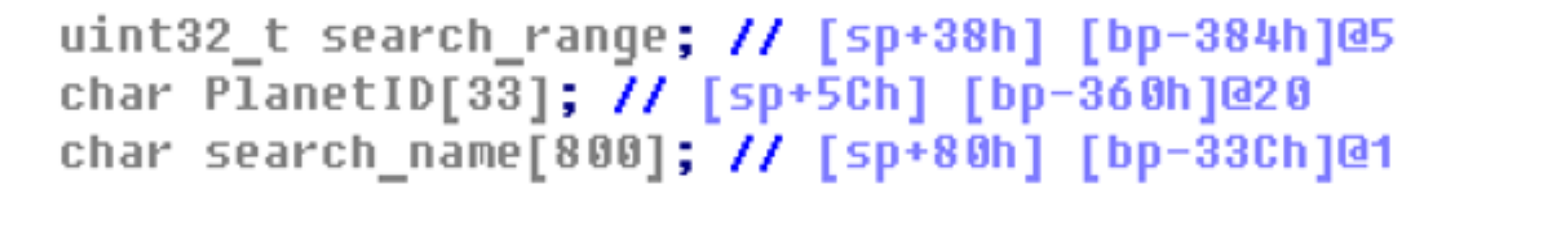


```
Use help <command> to get a more detailed usage listing
Planet[Eliza] Cash[  1000] Fuel[ 10000] Hold[     0]: info eliza
Planet Eliza info:
Designation Number: 00000000000000000000000000000000�t}�eliza
Government: Theocracy
Primary Economy: Rich Agriculture
```

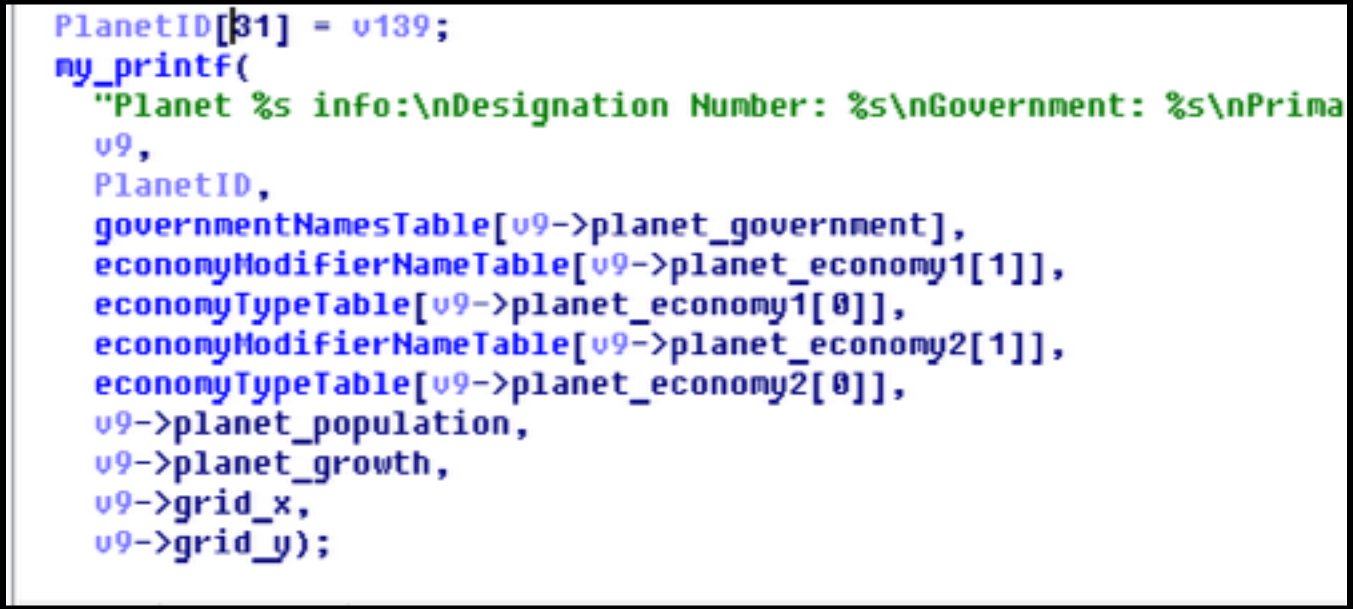
doinfo()

- PlanetID uninitialized & print as string

  -> leak previous function stack bp-360h



```
uint32_t search_range; // [sp+38h] [bp-384h]@5
char PlanetID[33]; // [sp+5Ch] [bp-360h]@20
char search_name[800]; // [sp+80h] [bp-33Ch]@1
```



```
PlanetID[31] = v139;
my_printf(
  "Planet %s info:\nDesignation Number: %s\nGovernment: %s\nPrima
  v9,
  PlanetID,
  governmentNamesTable[v9->planet_government],
  economyModifierNameTable[v9->planet_economy1[1]],
  economyTypeTable[v9->planet_economy1[0]],
  economyModifierNameTable[v9->planet_economy2[1]],
  economyTypeTable[v9->planet_economy2[0]],
  v9->planet_population,
  v9->planet_growth,
  v9->grid_x,
  v9->grid_y);
```

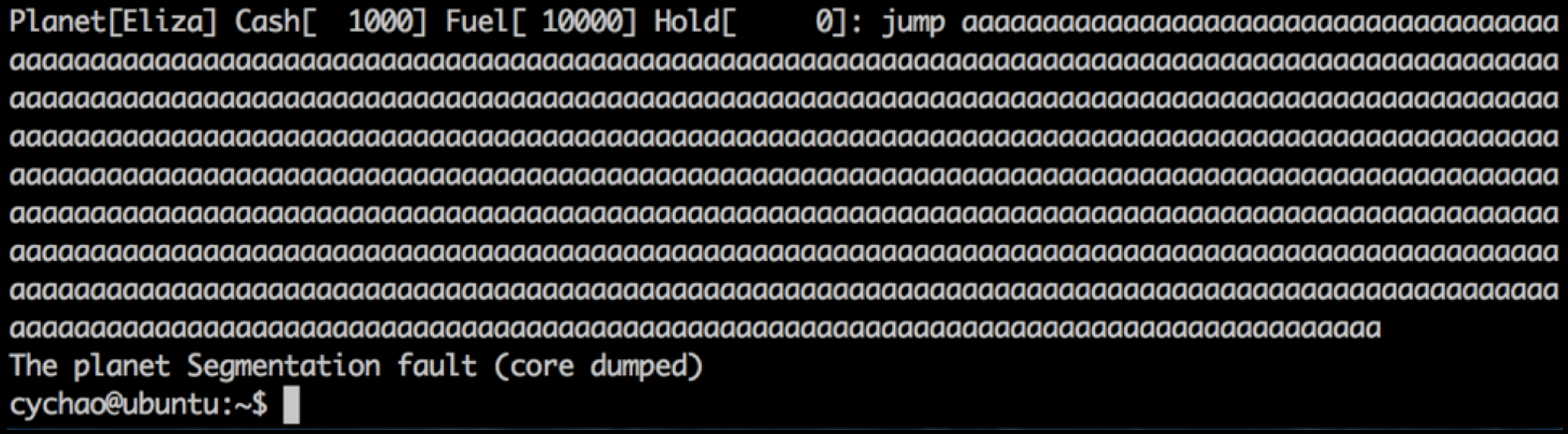
How to Patch?

- my_printf? argument?
- PlanetID[32]=0 ?
- doinfo() stack size? layout?

Try it!

Stack overflow (1)

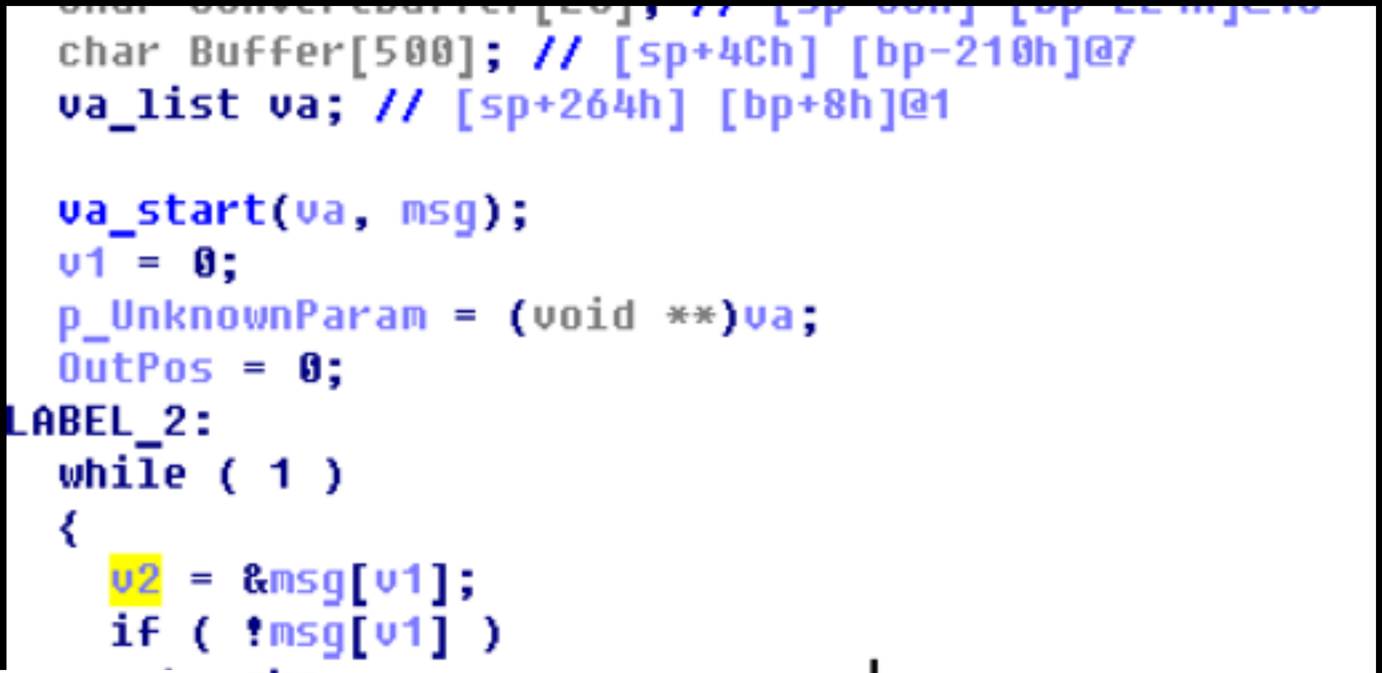
- “jump “+“a”*796



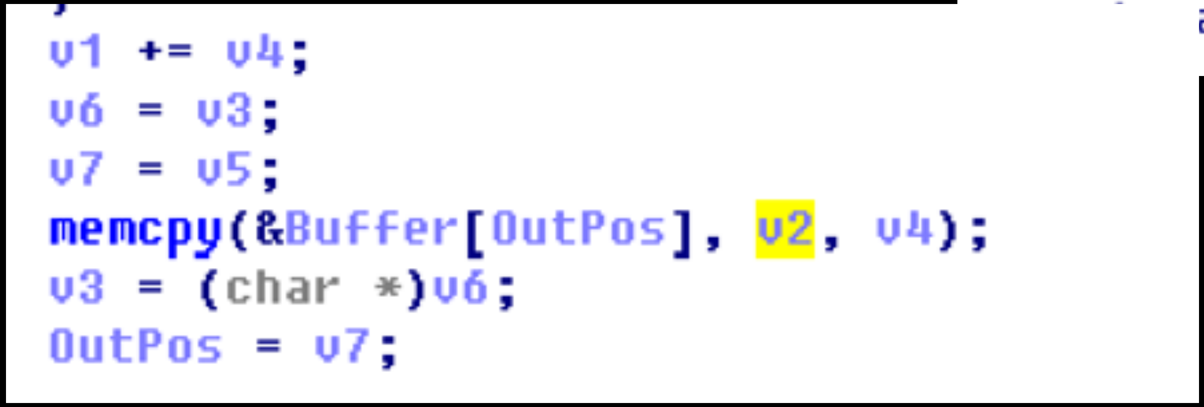
```
Planet[Eliza] Cash[  1000] Fuel[ 10000] Hold[     0]: jump aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
The planet Segmentation fault (core dumped)
cychao@ubuntu:~$ 
```

my_printf()

- msg = function argument
- Buffer[500]
- memcpy



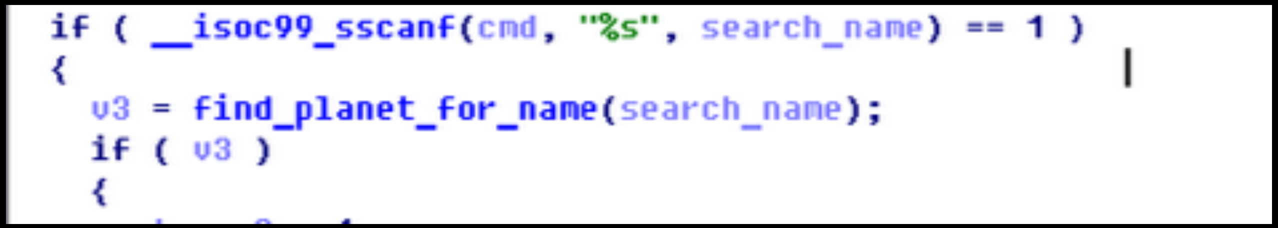
```
char Buffer[500]; // [sp+4Ch] [bp-210h]@7
va_list va; // [sp+264h] [bp+8h]@1

va_start(va, msg);
v1 = 0;
p_UnknownParam = (void **)va;
OutPos = 0;
LABEL_2:
while ( 1 )
{
  v2 = &msg[v1];
  if ( !msg[v1] )
        ak;
```



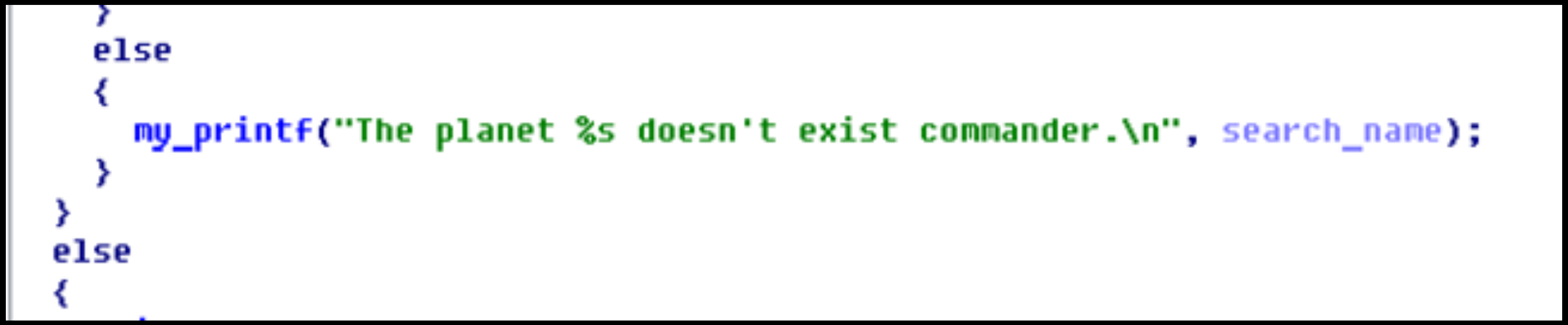
```
v1 += v4;
v6 = v3;
v7 = v5;
memcpy(&Buffer[OutPos], v2, v4);
v3 = (char *)v6;
OutPos = v7;
```

dojump()

- Search_name = sizeof(cmd) - sizeof(“jump “)



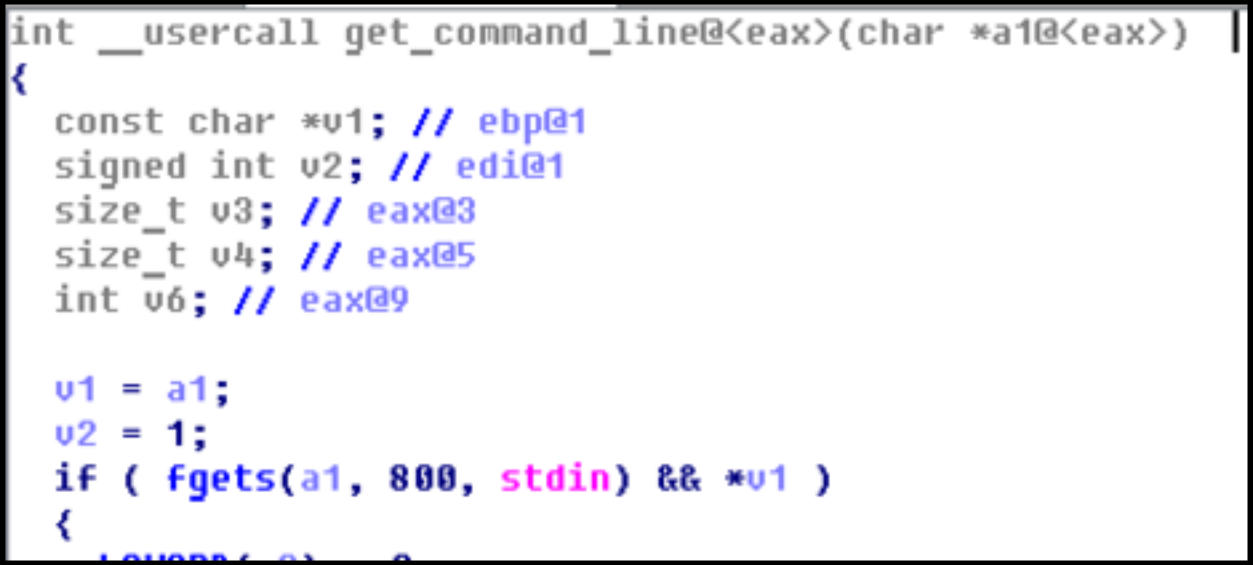
```
if ( __isoc99_sscanf(cmd, "%s", search_name) == 1 )
{
  v3 = find_planet_for_name(search_name);
  if ( v3 )
  {
```



```
  }
  else
  {
    my_printf("The planet %s doesn't exist commander.\n", search_name);
  }
}
else
{
```

get_command_line

- fgets(cmd,800,stdin)



```
int __usercall get_command_line@<eax>(char *a1@<eax>)
{
  const char *v1; // ebp@1
  signed int v2; // edi@1
  size_t v3; // eax@3
  size_t v4; // eax@5
  int v6; // eax@9

  v1 = a1;
  v2 = 1;
  if ( fgets(a1, 800, stdin) && *v1 )
  {
```

How to Patch?

- Command length?
- dojump error handling?
- my_printf?