Exploits

```
#define MAX_PASSLEN 10
#define PASSWORD_OK 1
#define PASSWORD_FAIL 2

void set_password(char *pass) {
    FILE *f = get_password_file();
    fprintf(f, pass);
}
int authenticate() {
    FILE *f = get_password_file();
    char userpass[MAX_PASSLEN];
    char secret[MAX_PASSLEN];
    fscanf(f, "%s", secret);
    fprintf(stdout, "Password:");
    fscanf(stdin, "%s", userpass);
    if (strncmp(secret, userpass, MAX_PASSLEN) == 0)
        return PASSWORD_OK;
    else
        return PASSWORD_FAIL;
}
__start() {
    if (authenticate() == PASSWORD_OK) {
        char newpass[MAX_PASSLEN];
        fprintf(stdout, "New password:");
        fscanf(stdin, "%s", newpass);
        set_password(newpass);
    } else {
        fprintf(stdout, "Sorry, wrong password\n");
    }
}
```

```
00400300 <authenticate>:
  400300       addiu   sp,sp,-72
  400304       sw      ra,68(sp)
  400308       sw      fp,64(sp)
  40030c       move    fp,sp
  400310       li      t9, get_password_file
  400314       nop
  400318       jalr    t9
  40031c       nop
  400320       sw      v0,16(fp)
  400324       addiu   v1,fp,40
  400328       lw      a0,16(fp)
  40032c       lui     v0,0x40
  400330       addiu   a1,v0,1184
  400334       move    a2,v1
  400338       li      t9, fscanf
  40033c       nop
  400340       jalr    t9
  400344       nop
  400348       li      a0,1
  40034c       lui     v0,0x40
  400350       addiu   a1,v0,1188
  400354       li      t9,fprintf
  400358       nop
  40035c       jalr    t9
  400360       nop
  400364       addiu   v1,fp,24
  400368       move    a0,zero
  40036c       lui     v0,0x40
  400370       addiu   a1,v0,1184
  400374       move    a2,v1
  400378       li      t9, fscanf
  40037c       nop
  400380       jalr    t9
  400384       nop
  400388       addiu   v0,fp,40
  40038c       addiu   v1,fp,24
  400390       move    a0,v0
  400394       move    a1,v1
  400398       li      t9, strncmp
  40039c       nop
  4003a0       jalr    t9
  4003a4       nop
  4003a8       bnez    v0,4003c0
  4003ac       nop
  4003b0       li      v0,1
  4003b4       sw      v0,56(fp)
  4003b8       b       4003c8
  4003bc       nop
  4003c0       li      v0,2
  4003c4       sw      v0,56(fp)
  4003c8       lw      v0,56(fp)
  4003cc       move    sp,fp
  4003d0       lw      ra,68(sp)
  4003d4       lw      fp,64(sp)
  4003d8       addiu   sp,sp,72
  4003dc       jr      ra
  4003e0       nop
```

parent:

…

arg4

arg3

arg2

arg1

child:

ra

fp

result_tmp

secretpass

userpass

f

…