LEVEL06:

```
level06@OverRide:~$ ./level06
***********************************
*               level06          *
***********************************
-> Enter Login: coucou
***********************************
***** NEW ACCOUNT DETECTED ********
***********************************
-> Enter Serial: 1234
level06@OverRide:~$ ./level06
***********************************
*               level06          *
***********************************
-> Enter Login: eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
eeeeeeeeeeeeeeeeeeeeee
***********************************
***** NEW ACCOUNT DETECTED ********
***********************************
-> Enter Serial: level06@OverRide:~$
```

Strings:

```
➜  ex06 strings ../Debug_files/level06
/lib/ld-linux.so.2
__gmon_start__
libc.so.6
_IO_stdin_used
fflush
__isoc99_scanf
signal
puts
__stack_chk_fail
stdin
printf
fgets
getchar
strcspn
stdout
strnlen
alarm
system
ptrace
__libc_start_main
GLIBC_2.7
GLIBC_2.4
GLIBC_2.0
PTRh
QVhy
E
 ;E
D$L1
T$Le3
UWVS
[^_]
[32m.---------------------------.
[31m| !! TAMPERING DETECTED !!  |
[32m'---------------------------'
********************************
level06
-> Enter Login:
***** NEW ACCOUNT DETECTED ********
-> Enter Serial:
Authenticated!
/bin/sh
;*2$"
```

Objdump:

```
08048748 <auth>:
 8048748:       55                      push   %ebp
 8048749:       89 e5                   mov    %esp,%ebp
 804874b:       83 ec 28                sub    $0x28,%esp
 804874e:       c7 44 24 04 63 8a 04    movl   $0x8048a63,0x4(%esp)
 8048755:       08
 8048756:       8b 45 08                mov    0x8(%ebp),%eax
 8048759:       89 04 24                mov    %eax,(%esp)
 804875c:       e8 bf fd ff ff          call   8048520 <strcspn@plt>
 8048761:       03 45 08                add    0x8(%ebp),%eax
 8048764:       c6 00 00                movb   $0x0,(%eax)
 8048767:       c7 44 24 04 20 00 00    movl   $0x20,0x4(%esp)
 804876e:       00
 804876f:       8b 45 08                mov    0x8(%ebp),%eax
 8048772:       89 04 24                mov    %eax,(%esp)
 8048775:       e8 56 fe ff ff          call   80485d0 <strnlen@plt>
 804877a:       89 45 f4                mov    %eax,-0xc(%ebp)
 804877d:       50                      push   %eax
 804877e:       31 c0                   xor    %eax,%eax
 8048780:       74 03                   je     8048785 <auth+0x3d>
 8048782:       83 c4 04                add    $0x4,%esp
 8048785:       58                      pop    %eax
 8048786:       83 7d f4 05             cmpl   $0x5,-0xc(%ebp)
 804878a:       7f 0a                   jg     8048796 <auth+0x4e>
 804878c:       b8 01 00 00 00          mov    $0x1,%eax
 8048791:       e9 e1 00 00 00          jmp    8048877 <auth+0x12f>
 8048796:       c7 44 24 0c 00 00 00    movl   $0x0,0xc(%esp)
 804879d:       00
 804879e:       c7 44 24 08 01 00 00    movl   $0x1,0x8(%esp)
 80487a5:       00
 80487a6:       c7 44 24 04 00 00 00    movl   $0x0,0x4(%esp)
 80487ad:       00
```

```
80487ae:       c7 04 24 00 00 00 00    movl   $0x0,(%esp)
80487b5:       e8 36 fe ff ff          call   80485f0 <ptrace@plt>
80487ba:       83 f8 ff                cmp    $0xffffffff,%eax
80487bd:       75 2e                   jne    80487ed <auth+0xa5>
80487bf:       c7 04 24 68 8a 04 08    movl   $0x8048a68,(%esp)
80487c6:       e8 c5 fd ff ff          call   8048590 <puts@plt>
80487cb:       c7 04 24 8c 8a 04 08    movl   $0x8048a8c,(%esp)
80487d2:       e8 b9 fd ff ff          call   8048590 <puts@plt>
80487d7:       c7 04 24 b0 8a 04 08    movl   $0x8048ab0,(%esp)
80487de:       e8 ad fd ff ff          call   8048590 <puts@plt>
80487e3:       b8 01 00 00 00          mov    $0x1,%eax
80487e8:       e9 8a 00 00 00          jmp    8048877 <auth+0x12f>
80487ed:       8b 45 08                mov    0x8(%ebp),%eax
80487f0:       83 c0 03                add    $0x3,%eax
80487f3:       0f b6 00                movzbl (%eax),%eax
80487f6:       0f be c0                movsbl %al,%eax
80487f9:       35 37 13 00 00          xor    $0x1337,%eax
80487fe:       05 ed ed 5e 00          add    $0x5eeded,%eax
8048803:       89 45 f0                mov    %eax,-0x10(%ebp)
8048806:       c7 45 ec 00 00 00 00    movl   $0x0,-0x14(%ebp)
804880d:       eb 4c                   jmp    804885b <auth+0x113>
804880f:       8b 45 ec                mov    -0x14(%ebp),%eax
8048812:       03 45 08                add    0x8(%ebp),%eax
8048815:       0f b6 00                movzbl (%eax),%eax
8048818:       3c 1f                   cmp    $0x1f,%al
804881a:       7f 07                   jg     8048823 <auth+0xdb>
804881c:       b8 01 00 00 00          mov    $0x1,%eax
8048821:       eb 54                   jmp    8048877 <auth+0x12f>
8048823:       8b 45 ec                mov    -0x14(%ebp),%eax
8048826:       03 45 08                add    0x8(%ebp),%eax
8048829:       0f b6 00                movzbl (%eax),%eax
804882c:       0f be c0                movsbl %al,%eax
804882f:       89 c1                   mov    %eax,%ecx
8048831:       33 4d f0                xor    -0x10(%ebp),%ecx
8048834:       ba 2b 3b 23 88          mov    $0x88233b2b,%edx
8048839:       89 c8                   mov    %ecx,%eax
804883b:       f7 e2                   mul    %edx
804883d:       89 c8                   mov    %ecx,%eax
804883f:       29 d0                   sub    %edx,%eax
8048841:       d1 e8                   shr    %eax
8048843:       01 d0                   add    %edx,%eax
8048845:       c1 e8 0a                shr    $0xa,%eax
8048848:       69 c0 39 05 00 00       imul   $0x539,%eax,%eax
804884e:       89 ca                   mov    %ecx,%edx
8048850:       29 c2                   sub    %eax,%edx
8048852:       89 d0                   mov    %edx,%eax
```

```
 8048854:       01 45 f0                add    %eax,-0x10(%ebp)
 8048857:       83 45 ec 01             addl   $0x1,-0x14(%ebp)
 804885b:       8b 45 ec                mov    -0x14(%ebp),%eax
 804885e:       3b 45 f4                cmp    -0xc(%ebp),%eax
 8048861:       7c ac                   jl     804880f <auth+0xc7>
 8048863:       8b 45 0c                mov    0xc(%ebp),%eax
 8048866:       3b 45 f0                cmp    -0x10(%ebp),%eax
 8048869:       74 07                   je     8048872 <auth+0x12a>
 804886b:       b8 01 00 00 00          mov    $0x1,%eax
 8048870:       eb 05                   jmp    8048877 <auth+0x12f>
 8048872:       b8 00 00 00 00          mov    $0x0,%eax
 8048877:       c9                      leave
 8048878:       c3                      ret
```

```
08048879 <main>:
 8048879:       55                      push   %ebp
 804887a:       89 e5                   mov    %esp,%ebp
 804887c:       83 e4 f0                and    $0xfffffff0,%esp
 804887f:       83 ec 50                sub    $0x50,%esp
 8048882:       8b 45 0c                mov    0xc(%ebp),%eax
 8048885:       89 44 24 1c             mov    %eax,0x1c(%esp)
 8048889:       65 a1 14 00 00 00       mov    %gs:0x14,%eax
 804888f:       89 44 24 4c             mov    %eax,0x4c(%esp)
 8048893:       31 c0                   xor    %eax,%eax
 8048895:       50                      push   %eax
 8048896:       31 c0                   xor    %eax,%eax
 8048898:       74 03                   je     804889d <main+0x24>
 804889a:       83 c4 04                add    $0x4,%esp
 804889d:       58                      pop    %eax
 804889e:       c7 04 24 d4 8a 04 08    movl   $0x8048ad4,(%esp)
 80488a5:       e8 e6 fc ff ff          call   8048590 <puts@plt>
 80488aa:       c7 04 24 f8 8a 04 08    movl   $0x8048af8,(%esp)
 80488b1:       e8 da fc ff ff          call   8048590 <puts@plt>
 80488b6:       c7 04 24 d4 8a 04 08    movl   $0x8048ad4,(%esp)
 80488bd:       e8 ce fc ff ff          call   8048590 <puts@plt>
 80488c2:       b8 08 8b 04 08          mov    $0x8048b08,%eax
 80488c7:       89 04 24                mov    %eax,(%esp)
 80488ca:       e8 41 fc ff ff          call   8048510 <printf@plt>
 80488cf:       a1 60 a0 04 08          mov    0x804a060,%eax
 80488d4:       89 44 24 08             mov    %eax,0x8(%esp)
 80488d8:       c7 44 24 04 20 00 00    movl   $0x20,0x4(%esp)
 80488df:       00
```

```
80488e0:       8d 44 24 2c             lea    0x2c(%esp),%eax
80488e4:       89 04 24                mov    %eax,(%esp)
80488e7:       e8 64 fc ff ff          call   8048550 <fgets@plt>
80488ec:       c7 04 24 d4 8a 04 08    movl   $0x8048ad4,(%esp)
80488f3:       e8 98 fc ff ff          call   8048590 <puts@plt>
80488f8:       c7 04 24 1c 8b 04 08    movl   $0x8048b1c,(%esp)
80488ff:       e8 8c fc ff ff          call   8048590 <puts@plt>
8048904:       c7 04 24 d4 8a 04 08    movl   $0x8048ad4,(%esp)
804890b:       e8 80 fc ff ff          call   8048590 <puts@plt>
8048910:       b8 40 8b 04 08          mov    $0x8048b40,%eax
8048915:       89 04 24                mov    %eax,(%esp)
8048918:       e8 f3 fb ff ff          call   8048510 <printf@plt>
804891d:       b8 60 8a 04 08          mov    $0x8048a60,%eax
8048922:       8d 54 24 28             lea    0x28(%esp),%edx
8048926:       89 54 24 04             mov    %edx,0x4(%esp)
804892a:       89 04 24                mov    %eax,(%esp)
804892d:       e8 ae fc ff ff          call   80485e0 <__isoc99_scanf@plt>
8048932:       8b 44 24 28             mov    0x28(%esp),%eax
8048936:       89 44 24 04             mov    %eax,0x4(%esp)
804893a:       8d 44 24 2c             lea    0x2c(%esp),%eax
804893e:       89 04 24                mov    %eax,(%esp)
8048941:       e8 02 fe ff ff          call   8048748 <auth>
8048946:       85 c0                   test   %eax,%eax
8048948:       75 1f                   jne    8048969 <main+0xf0>
804894a:       c7 04 24 52 8b 04 08    movl   $0x8048b52,(%esp)
8048951:       e8 3a fc ff ff          call   8048590 <puts@plt>
8048956:       c7 04 24 61 8b 04 08    movl   $0x8048b61,(%esp)
804895d:       e8 3e fc ff ff          call   80485a0 <system@plt>
8048962:       b8 00 00 00 00          mov    $0x0,%eax
8048967:       eb 05                   jmp    804896e <main+0xf5>
8048969:       b8 01 00 00 00          mov    $0x1,%eax
804896e:       8b 54 24 4c             mov    0x4c(%esp),%edx
8048972:       65 33 15 14 00 00 00    xor    %gs:0x14,%edx
8048979:       74 05                   je     8048980 <main+0x107>
804897b:       e8 00 fc ff ff          call   8048580 <__stack_chk_fail@plt>
8048980:       c9                      leave
8048981:       c3                      ret
8048982:       90                      nop
```

Reversed source:

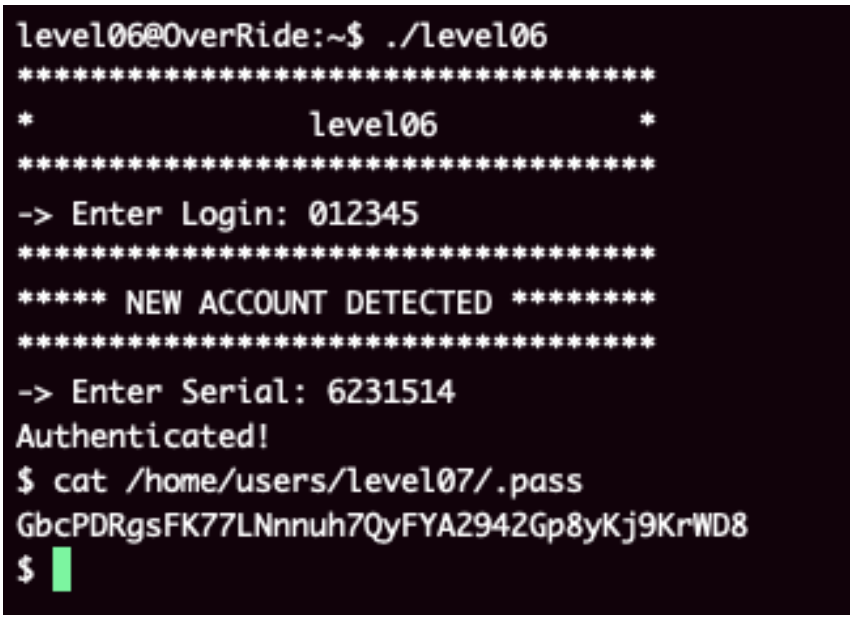
```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int auth(char *log, int serial)
{
// ebp = 0xffffd6a8
    int i;          // 0xffffd69c   -0x0c (ebp)
    int key;        // 0xffffd698   -0x10 (ebp)
    int j;          // 0xffffd694   -0x14 (ebp)
    char s1[0x14];  // 0xffffd680   (esp)
```

```
    *(log + strcspn(log, "\n")) = '\0';
    i = strnlen(log, 0x20);
    if (i <= 5)
        return 1;
    if (ptrace(PT_TRACEME, 0, 1, 0) == -1)
    {
        puts("\x1b[32m.-------------------------.");
        puts("\x1b[31m| !! TAMPERING DETECTED !!  |");
        puts("\x1b[32m\'-------------------------\'");
        return 1;
    }
// exemple: log = 012345
    key = (int)((log[3]) ^ 0x1337) + 0x5eeded;
// exemple: key = 0x33 ^ 0x1337 = 0x1304 + 0x5eeded = 0x5F00F1
    j = 0;
    while (j < i)
    {
        if (log[j] < ' ')
            return 1;
/*      Real op
        ecx = log[j] ^ key;
        edx = (0x88233b2b * ecx) >> 32;
        eax = ((((ecx - edx) >> 1) + edx) >> 10) * 0x539;
        eax = edx - eax;
*/

//      Ghidra simplification
        key = key + ((log[j] ^ key) % 0x539) ;
//      Exemple
// 0 0x5F00F1 + (0x30 ^ 0x5F00F1)0x5F00C1 % 0x539 = + 0x411 = 0x5F0502
// 1 0x5F0502 + (0x31 ^ 0x5F0502)0x5F0533 % 0x539 = + 0x34a = 0x5F084C
// 2 0x5F084C + (0x32 ^ 0x5F084C)0x5F087E % 0x539 = + 0x15c = 0x5F09A8
// 3 0x5F09A8 + (0x33 ^ 0x5F09A8)0x5F099B % 0x539 = + 0x279 = 0x5F0C21
// 4 0x5F0C21 + (0x34 ^ 0x5F0C21)0x5F0C15 % 0x539 = + 0x4f3 = 0x5F1114
// 5 0x5F1114 + (0x35 ^ 0x5F1114)0x5F1121 % 0x539 = + 0x4c6 = 0x5F15DA
        j++;
    }
```

```
    if (serial != key)
        return 1;
    return 0;
}

int main(int ac, char **av)
{
//ebp = 0xffffd708
//esp = 0xffffd700
    int stack_protect;      // 0xffffd6fc   0x4c (esp)
    char log[0x10];         // 0xffffd6dc   0x2c (esp)
    int  serial;            // 0xffffd6d8   0x28 (esp)
    char *save = (char*)av; // 0xffffd6cc   0x1c (esp)
    char s2[0x1c];          // 0xffffd6b0   (esp)

    puts("***********************************");
    puts("*\t\tlevel06\t\t  *");
    puts("***********************************");
    printf("-> Enter Login: ");

    fgets(log, 0x20, stdin);

    puts("***********************************");
    puts("***** NEW ACCOUNT DETECTED ********");
    puts("***********************************");
    printf("-> Enter Serial: ");
    scanf("%u", serial);
    if (auth(log, serial) == 0)
    {
        puts("Authenticated!");
        system("/bin/sh");
        return 0;
    }
    return 1;
}
```

Ghidra simplification:

```
  local_14 = local_14 + ((int)param_1[local_18] ^ local_14) % 0x539;
}
```



Flag : GbcPDRgsFK77LNnnuh7QyFYA2942Gp8yKj9KrWD8