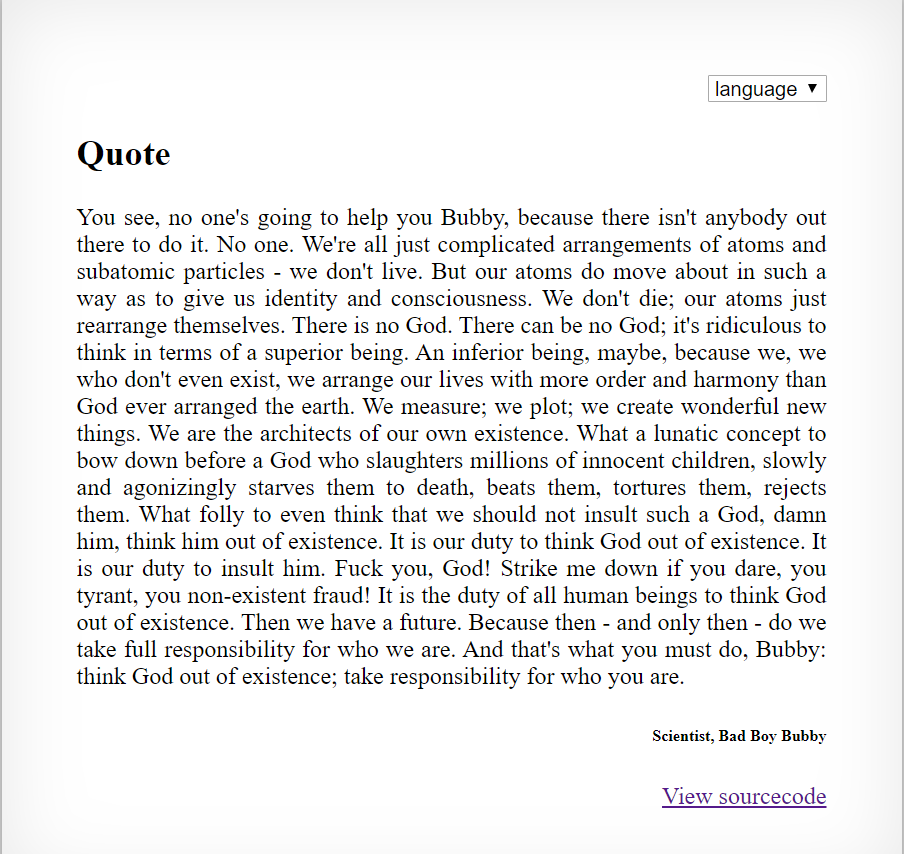
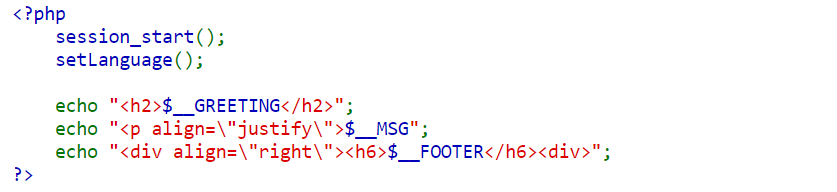
Pass for level 26: oGgWAJ7zcGT28vYazGo4rkhOPDhBu34T

Step 1:Login to natas 25



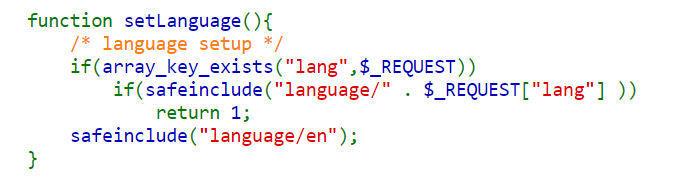
It seems that there is a secure option button that can change the language of the text but we need to look more inside the source code for more conclusions.

Step 2: View source code



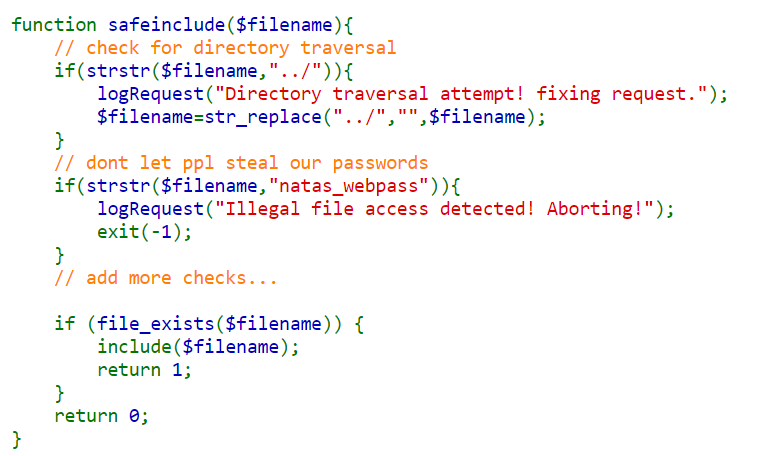
The php code that run in the website.

First it run the session and then run another build function called "setlanguage()"



Check if we post 'lang' : <value> we will do "safe input" to avoid injections.

In another function called "safeinclude()"



Checking weather the user input "../" for path traversal and "natas\_webpass" for print the code for the next level while injecting some code to the "lang" key.



Then we have the last functions, the FIRST will save array that represent list of all the files in some path and the SECOND function create log file with some message .

Step 3: Python program for post 'lang' with some value.

If we input …/./ it will become ../ due to "safeinclude()" function so we can traversal back in the tree of file system.

Now we cant just enter "…/./…/./…/./…/./…/./…/./…/.//etc/natas\_webpass/natas26" because it will block us, so we can find vulnerability in another location.

It can be lead us to the place where all the logs are.

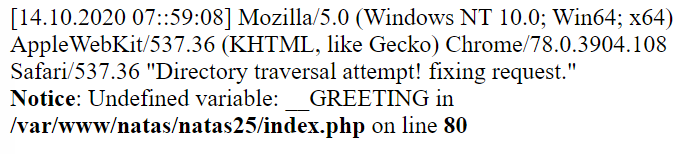
Let see what it will log out.



Note: $\_SERVER['HTTP\_USER\_AGENT']

The variable **$\_SERVER** store all the web server information.

The ['HTTP\_USER\_AGENT'] is from the header of out HTTP Request – who or what execute the request, in our case is python but if we choose to use CHROME for example it will output:



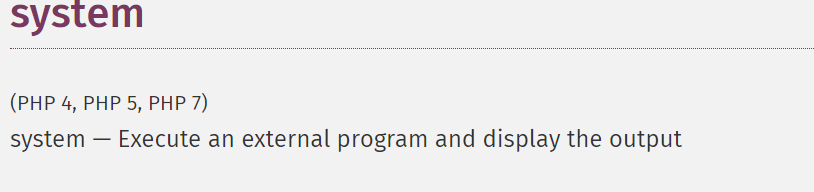
Step 4:

After some checks I get a conclusion, we can post any header we want in the post function,

So maby we can inject there php code that will run some code inside the website.

We can input php code inside the $message and it will execute it because it already in php format.

So I injected to the header "User-Agent" : "<?php system('cat /etc/natas\_webpass/natas26'); ?>"

Note: 

And hope to get the code for the next level.

