Jsclean

JavaScript Cleaning Service: Transform ugly JavaScript files to pretty clean JavaScript files!

nc cha.hackpack.club:41718

ANALYSIS:

We are given a python file. The challenge description says that the python script cleans our javascript code. So we take a look at the python script that is provided.

jsclean.py:

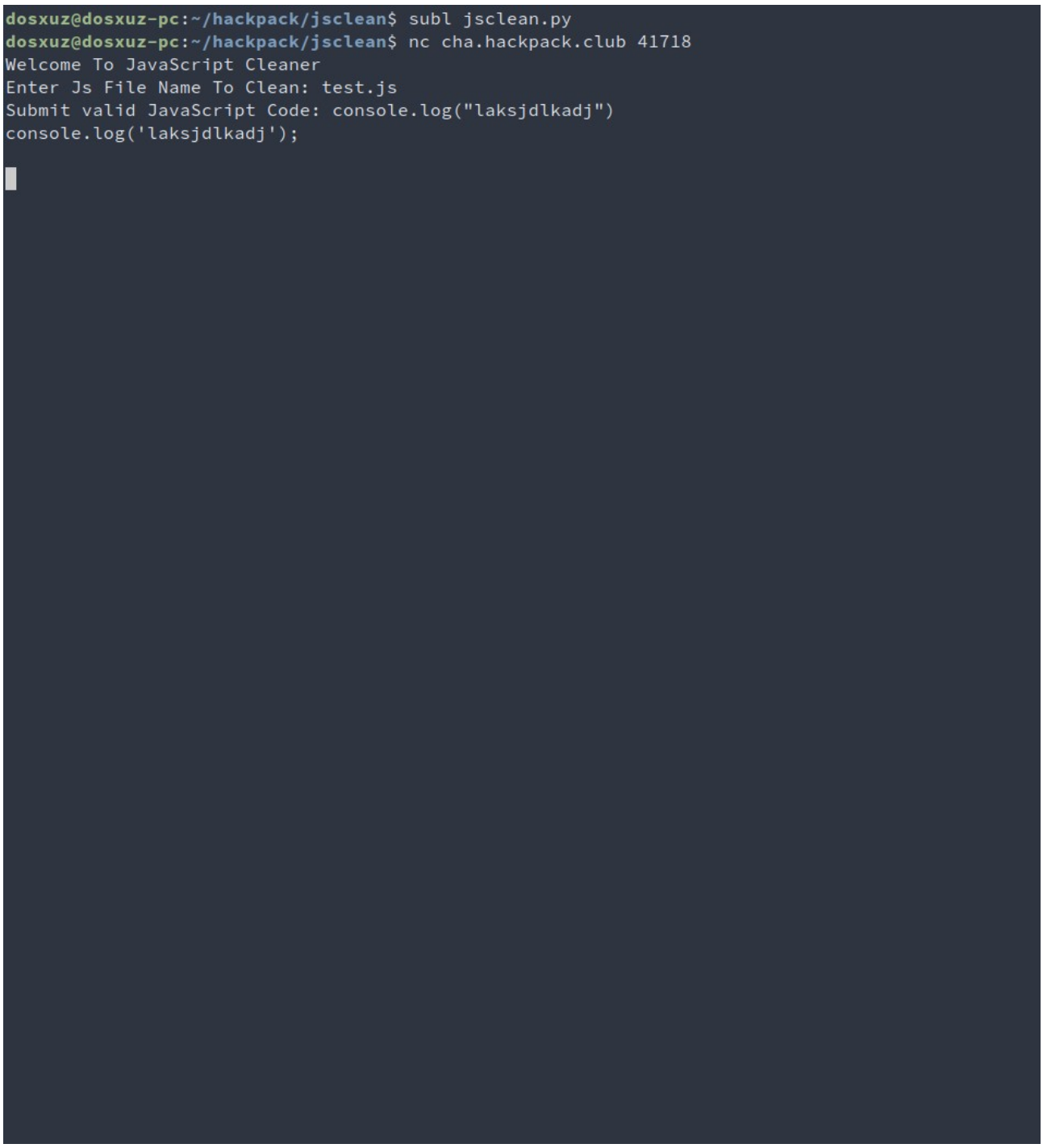
```
import os
import sys
import subprocess


def main(argv):
    print("Welcome To JavaScript Cleaner")
    js_name = input("Enter Js File Name To Clean: ")
    code = input("Submit valid JavaScript Code: ")

    js_name = os.path.basename(js_name) # No Directory Traversal for you

    if not ".js" in js_name:
        print("No a Js File")
        return

    with open(js_name,'w') as fin:
        fin.write(code)

    p = subprocess.run(['/usr/local/bin/node','index.js','-f',js_name],stdout=subprocess.PIPE);
    print(p.stdout.decode('utf-8'))

main(sys.argv)
```

So, we see that there is a node command executed with the use of index.js and the -f flag. We have to give a proper js file name as the script checks if our filename has the extension of ‘.js’ or not.

Since I don’t have the index.js on my local computer, I connect to the host and port they’ve provided.

After connecting, this is what we get:

We know that the script checks for proper filename. So we enter ‘test.js’ as out filename and we give the command as ‘console.log(“lkasjdlakjdlk”);’ as follows:



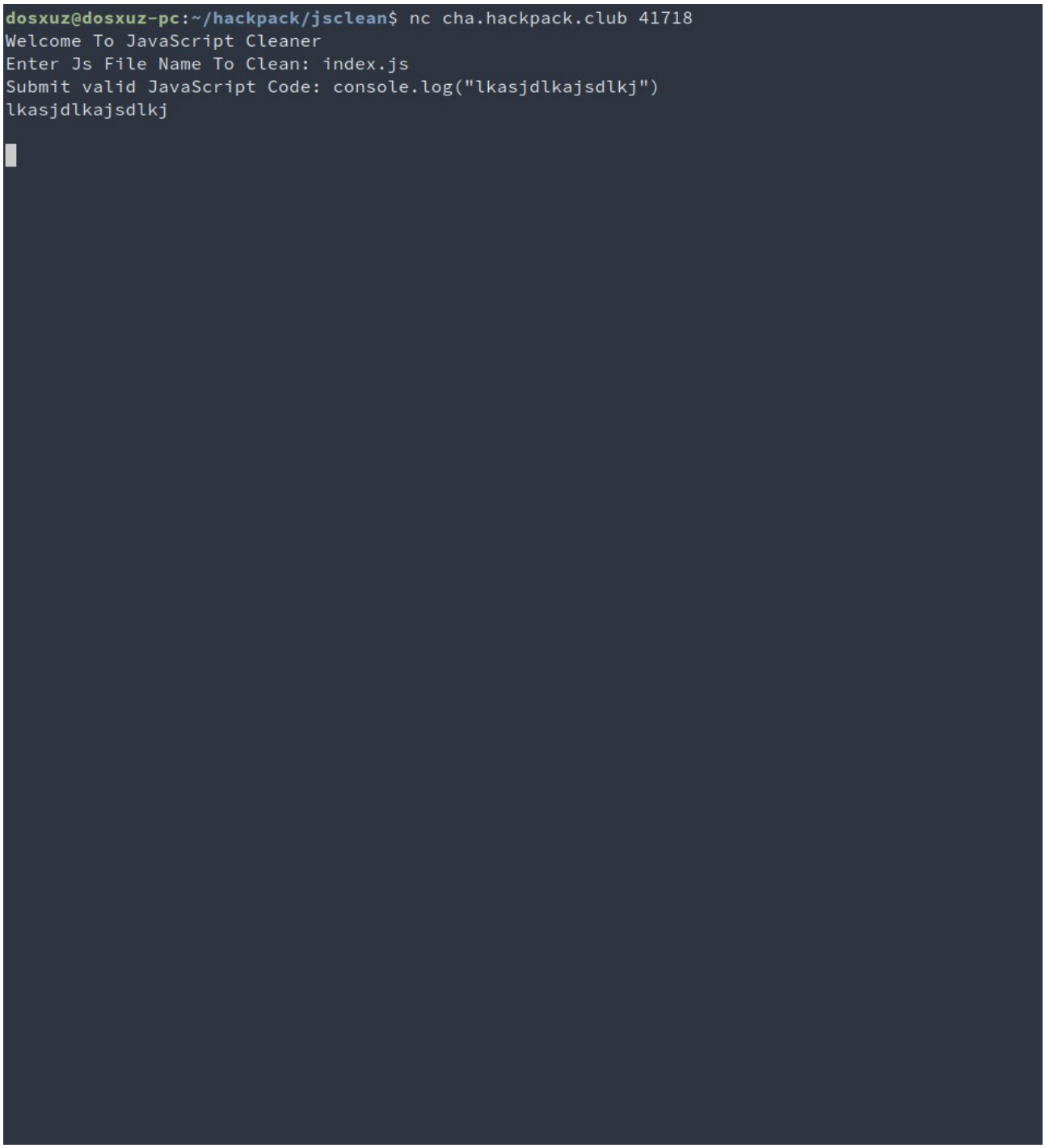
We can see that the script gives the output by placing the given code in a new line and adding a semicolon at the end.

Also, if we give multiline code on a single line separated by semicolos (;), we get the commands as our output.

FINDING OUT THE BUG:

So, we need to look for the bug in the code. I noticed the ‘index.js’ file present in the code. What if I give the name of the file as ‘index.js’ rather than something else? What do we get?

Upon doing the same I get the conde being executed as follows:



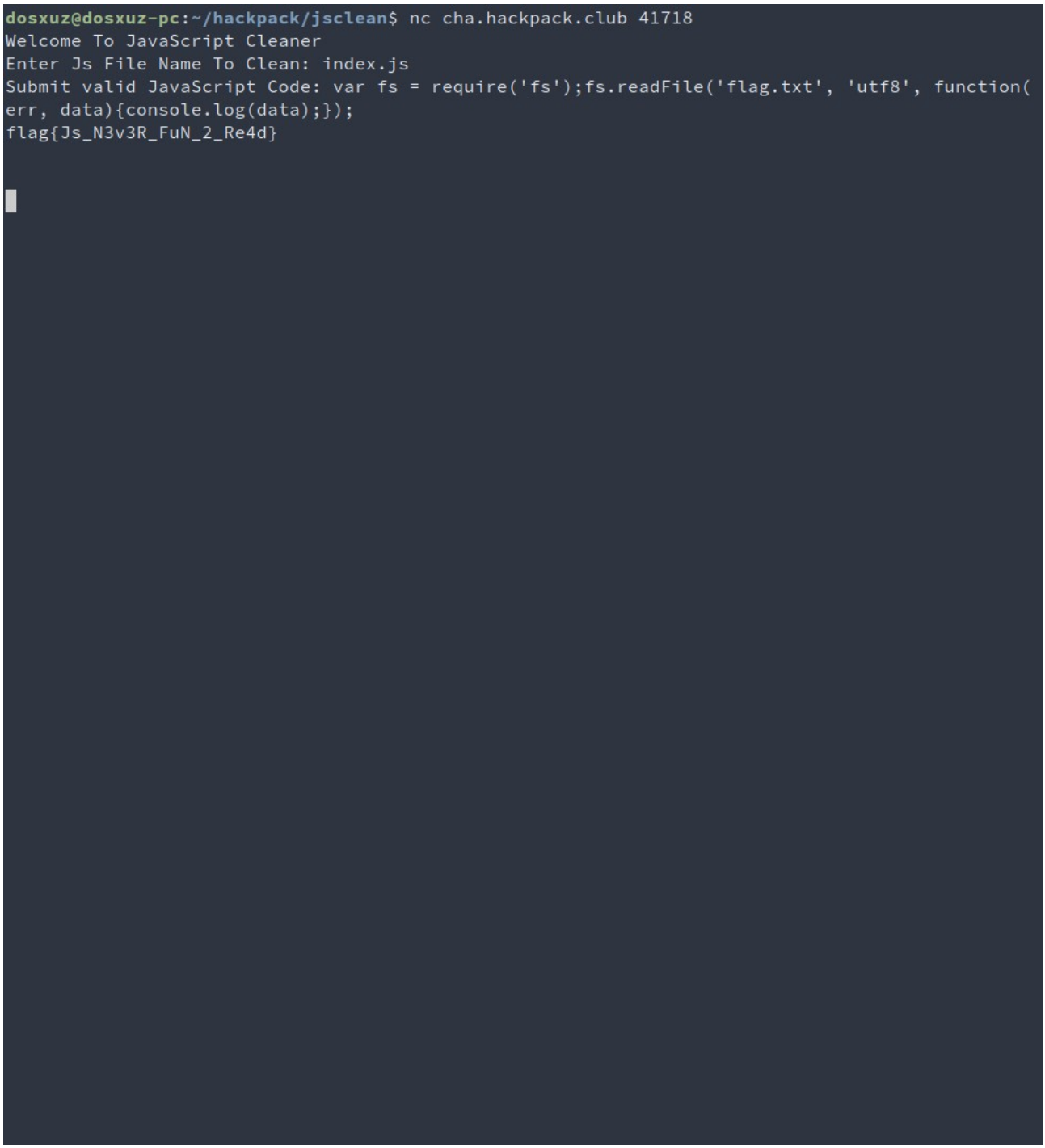
Okay so we have code execution. We now just need to read the flag file using javascript code.

EXPLOITING THE BUG:

So we use the following code written in one line, seperated by semicolon (;) so separate the different lines in order to read the flag :

var fs = require('fs');fs.readFile('flag.txt', 'utf8', function(err, data){console.log(data);});

This gives us the following output:



That’s how we get the flag.