**Name**

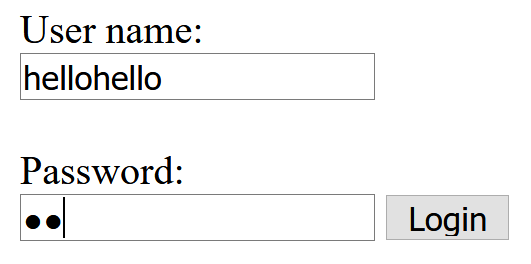
Lim Chun Yu (P1625273)

**Category**

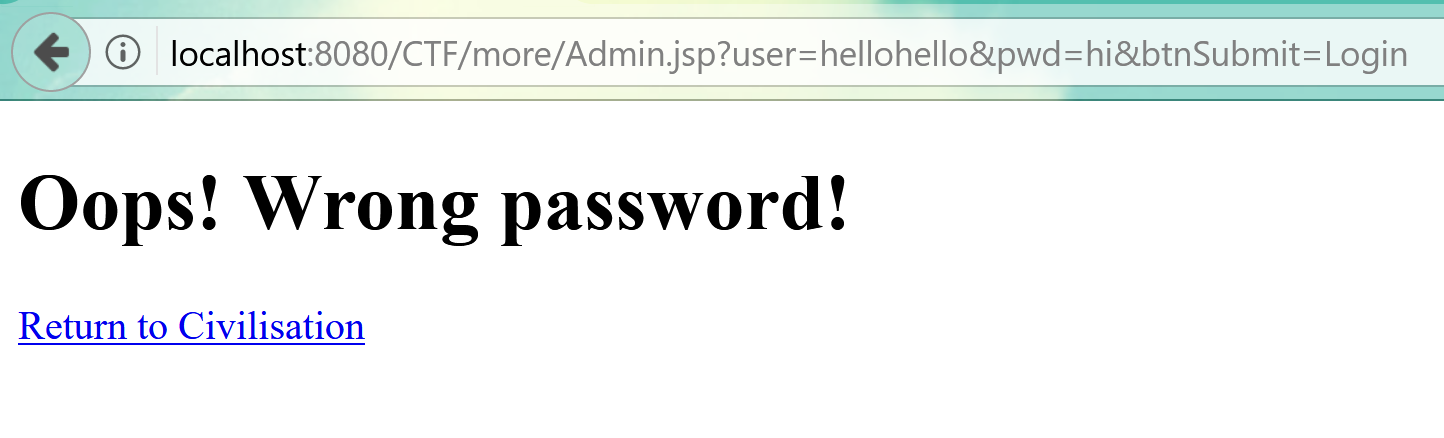
WEB/CRYPTOGRAPHY

**How to solve**

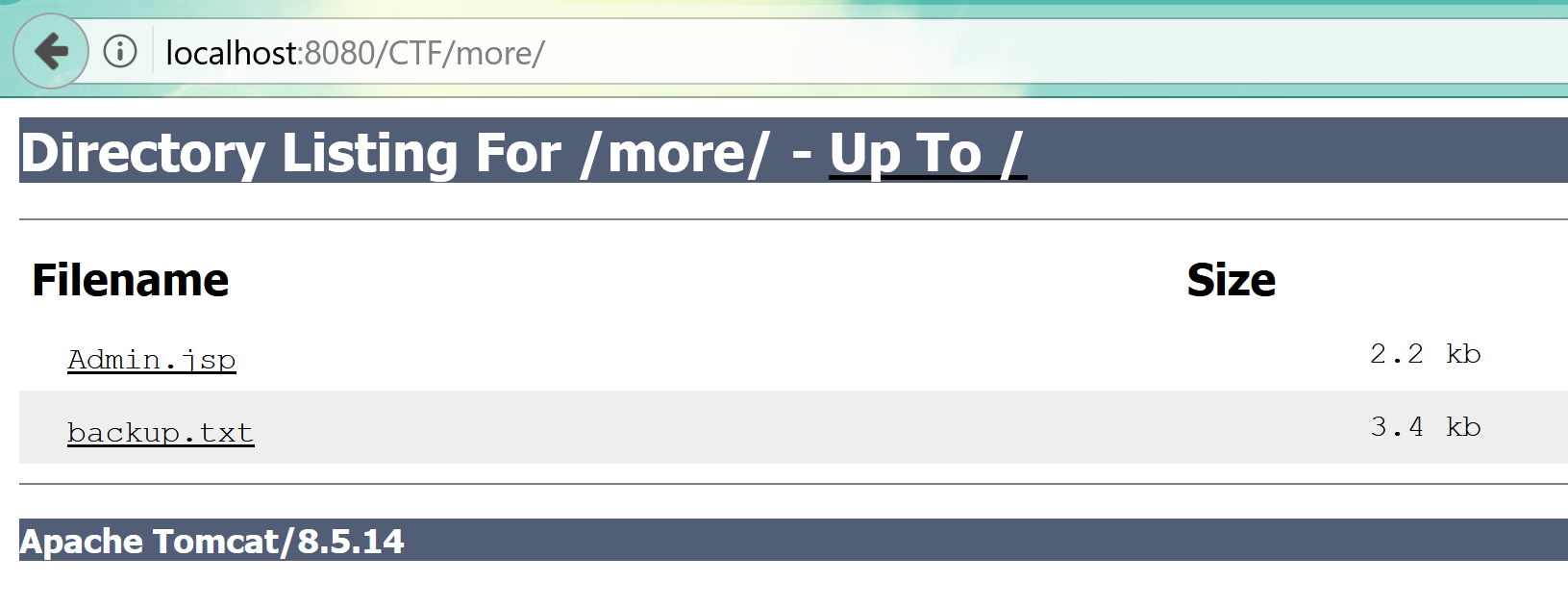
1. Login with wrong credentials

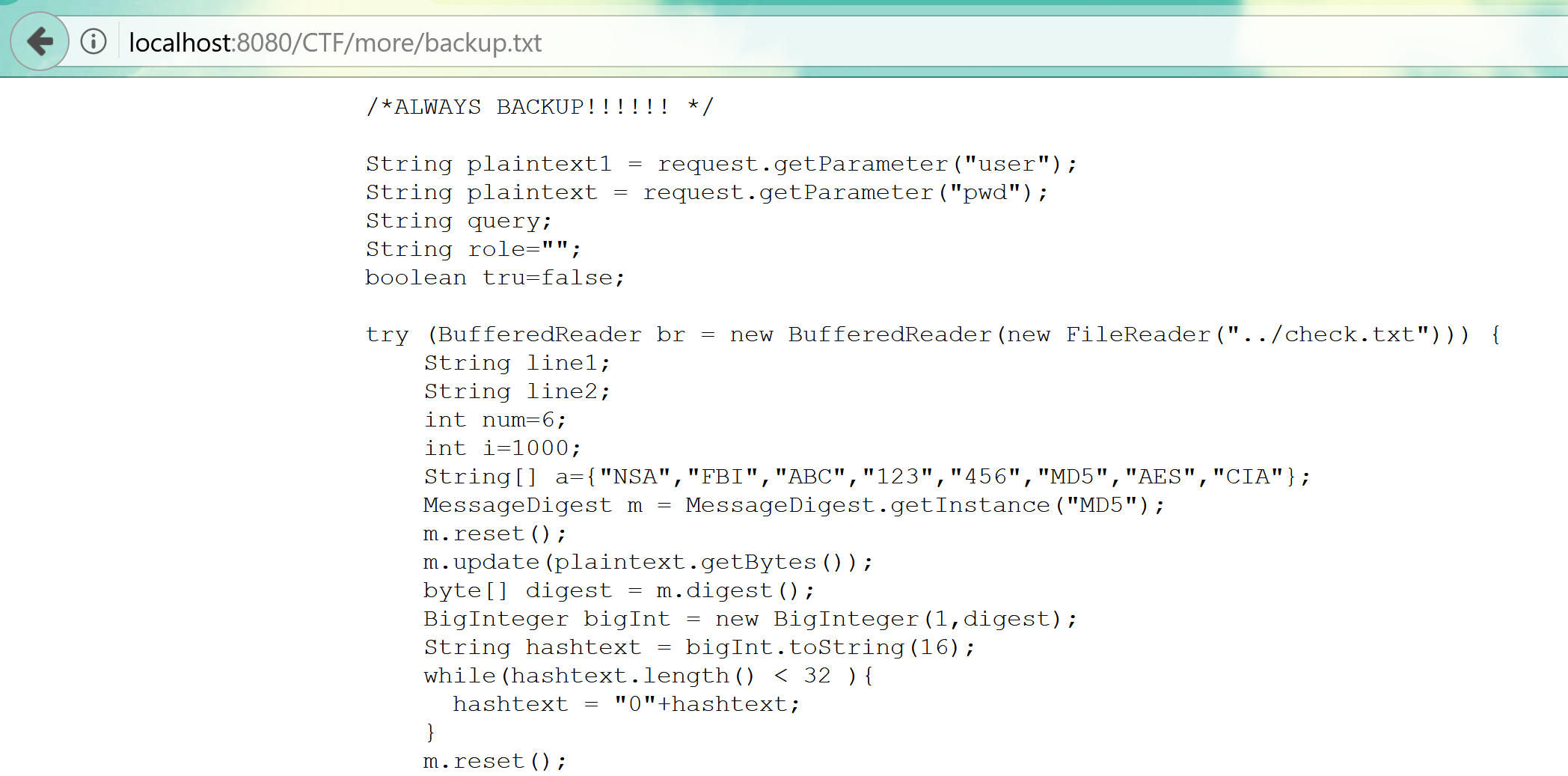


1. Realize the existence of folder called “more”



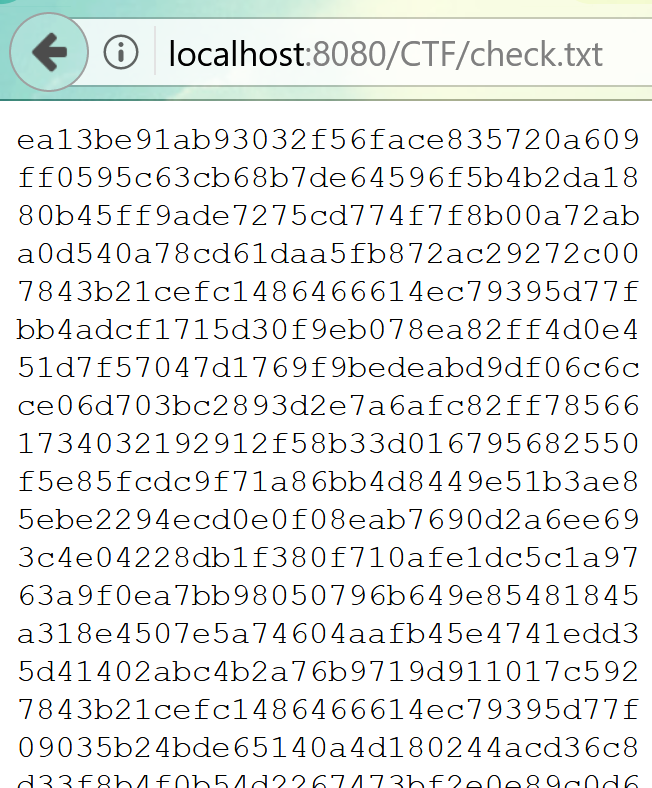
1. The folder has a directory listing you will discover backup.txt which shows the java code for admin.jsp



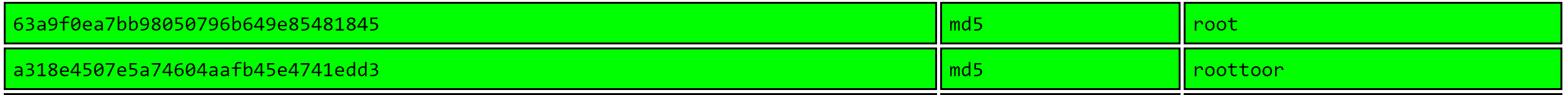


1. After understanding the program, you will realize it reads and validates passwords and usernames from a file named check.txt

Going to check.txt you will see a bunch of hashes from the program, you will understand that It reads in 2 lines at once, the first line being username and second line being password the user input is then hashed and compared.



1. After running the list of hashes against a program or website that will check the passwords against a list of known hashes, you will discover the account root,

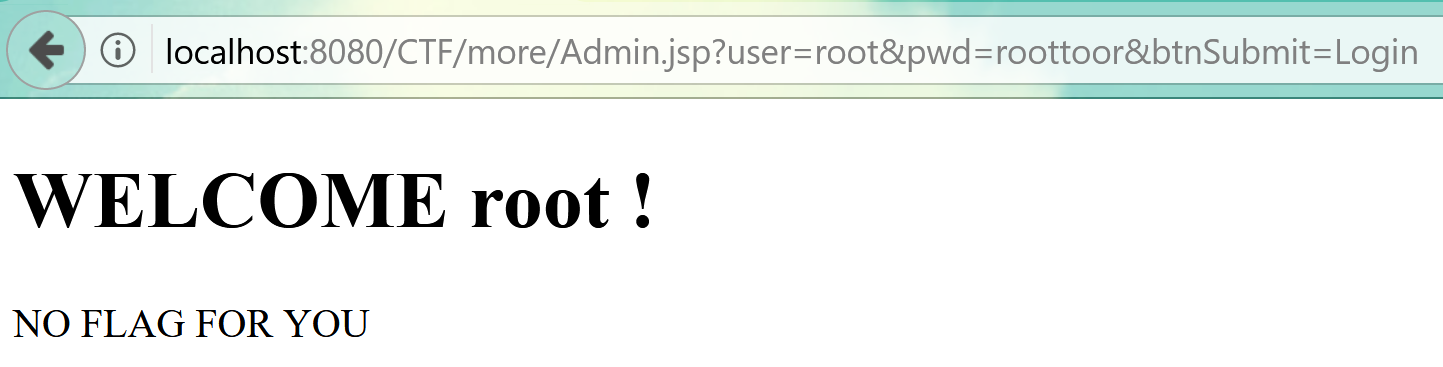


which has

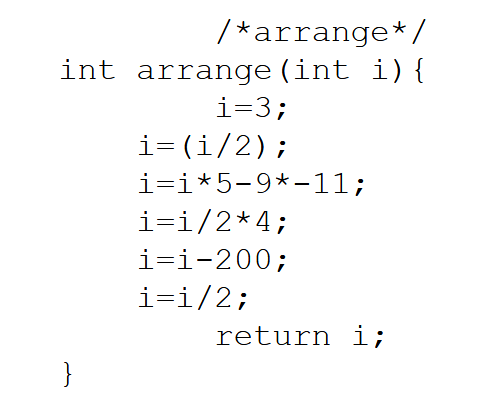
Username : root

Password : roottoor

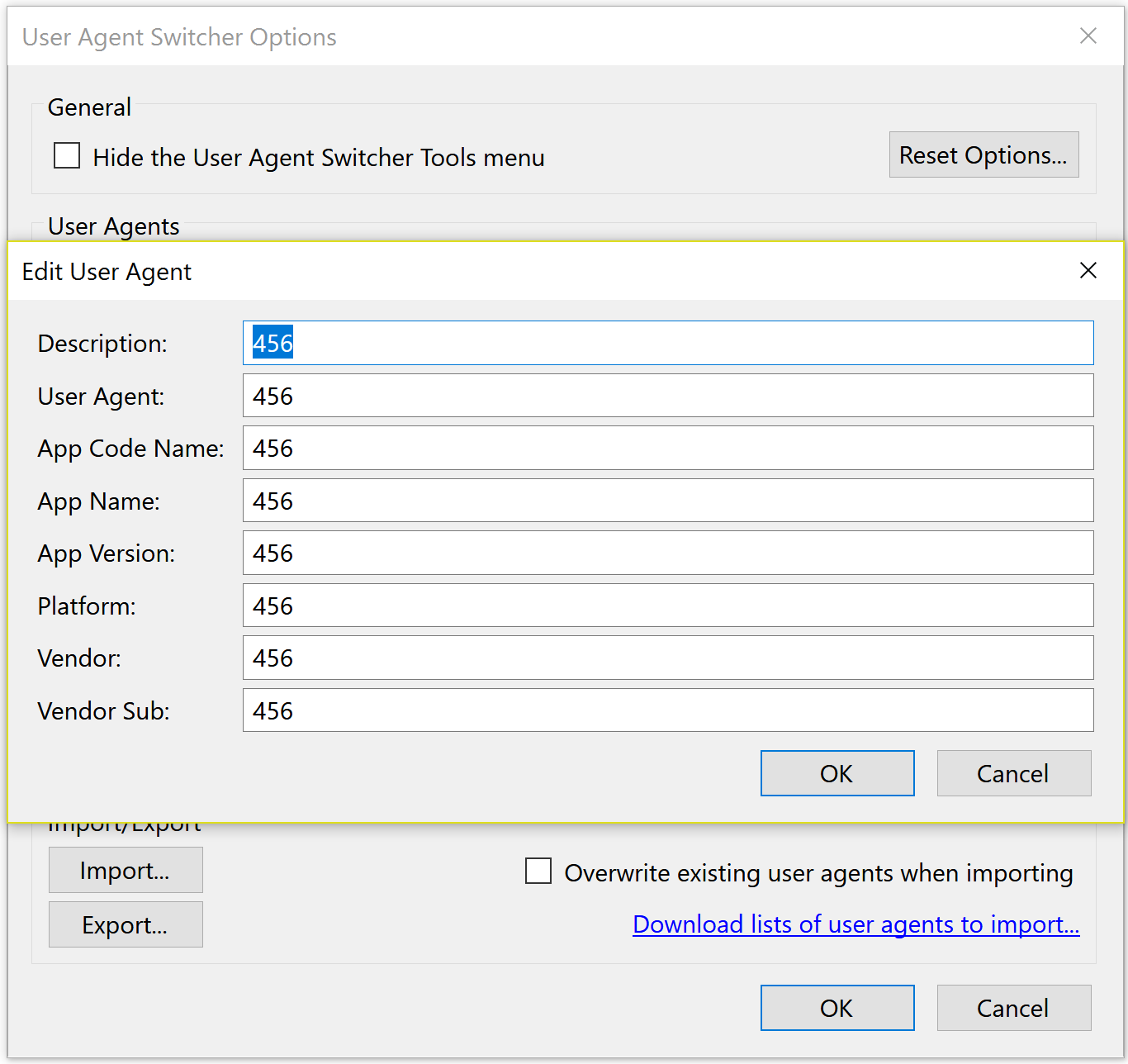
1. Inputting that will allow you access to the site admin.jsp
2. However, you will realize that no flag is printed



1. This is because program checks for user-agent and it references an array, there is also a simple class written that will always return the number 4 this is to confuse the user.



1. The user agent has to be “456”(fifth element in the array) in order for the flag to printed out.





**How to deploy**

1. deploy the file on a server, I used apache tomcat.
2. For apache tomcat, move the file to workspace
3. File -> Open Projects from File System
4. Select the file and press Finish
5. Refresh server
6. Run the file on the server
7. In the Admin.jsp file change the String “loc” to the location of the check.txt file on your computer.