There are two cookies:

1. FLAG: which contains an incomplete flag;

2. UID: user ID

What we can think is that by giving the correct user-ID, the page will return the flag.

The value contained in UID “f899139df5e1059396431415e770c6dd” seems a hashed value.

By using a password cracker we can see that the value is an MD5 hash, where the ciphertext is

100.

This means that the UID= MD5(100) is a wrong UID (since we don’t have a correct flag). UID

seems the MD5 of an integer: what if we bruteforce them? We can start from 1 to 100.