BLOCK2

Here it’s a bit more complex and we need to understand what’s going on.

Two variables are involved:

* $\_, the password that we provided;
* $ua: it is given by the parameter HTTP\_USER\_AGENT through the global variable

$\_SERVER.

For example, let’s see how an md5 looks like (I use an online PHP tester); for example, given

the following code:

$tmp = MD5("a");

echo $tmp;

The result is:

0cc175b9c0f1b6a831c399e269772661

If we try to do the sum with a character, like with the following code:

$tmp2 = $tmp + "a";

echo $tmp2;

The result is:

0

Ok, that’s suspicious: this code is full of those things called type juggling.

The comparison is between the addition of the md5 of the password and the first letter of the

password with the md5 of the field contained in the user agent. Here we are exploiting odd

PHP’s behaviours, and this comparison returns True on several conditions, e.g., MD5(“a”) + “a”

== Md5(“a”) is True.