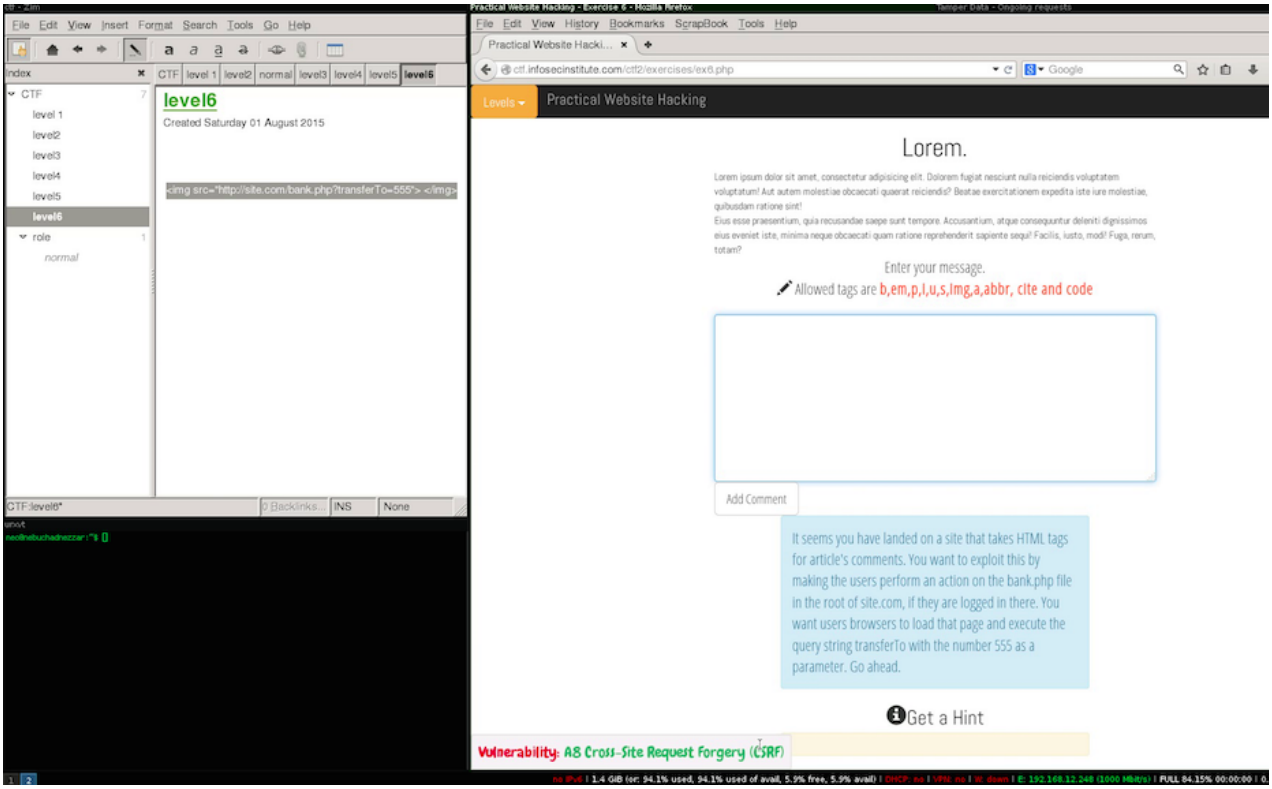
Infosecinstitute CTF 2 - LEVEL 6

In this level we have a simple comment application Cross-Site Request Forgery.



In this level the objective is to create a payload to be added as a comment in a way that when other users visit the page a request is executed when the page loads, in this scenario we have to exploit the vulnerabilities:

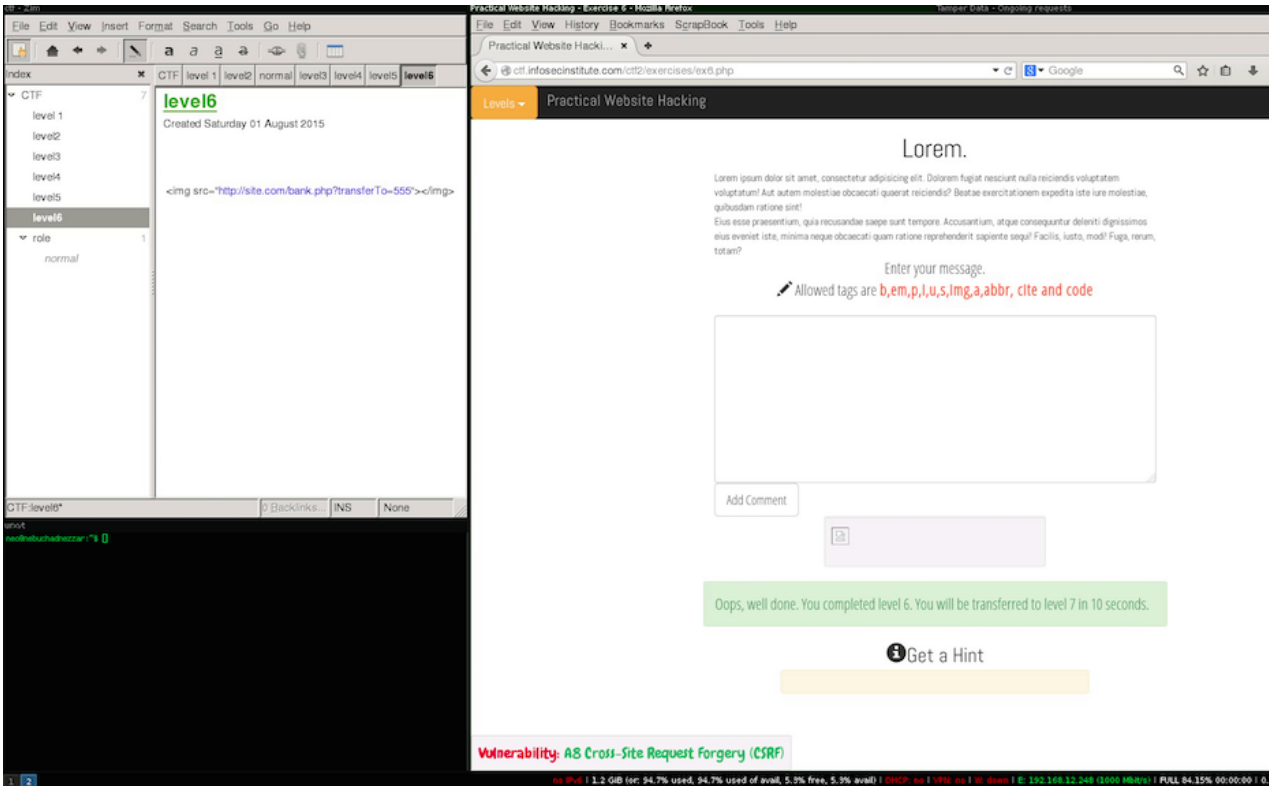
1. Cross site scripting.
2. Cross-Site Request Forgery.

The second vulnerability is not actually on the level it self, the objective is to emulate a second website that is vulnerable to Cross-Site Request Forgery, and the current level would be what the attacker would use to launch its attack.

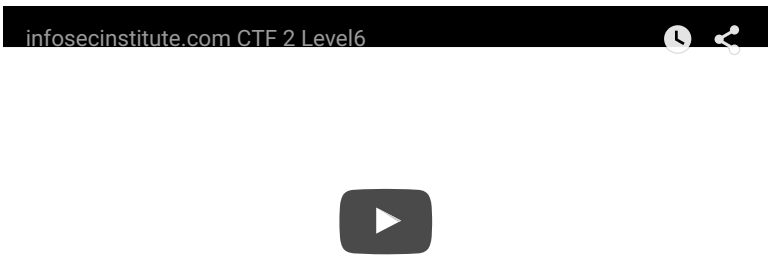
This types of vulnerabilities are very common and used to deliver many types of payloads that might include the exploitation of vulnerabilities on the users browsers leading to remote code execution in the user's system, so try to remember the next time you visit an wordpress blog ;)

In our case we need to verify if their are any allowed tags that we could use.

One of the allowed tags is the img tag even when the source provided to the tag is not an actual image the browser makes the request, since the input doesn't have any type of validation this level is quite simple.



Video



0x4E0x650x6F
0x4E0x650x6F