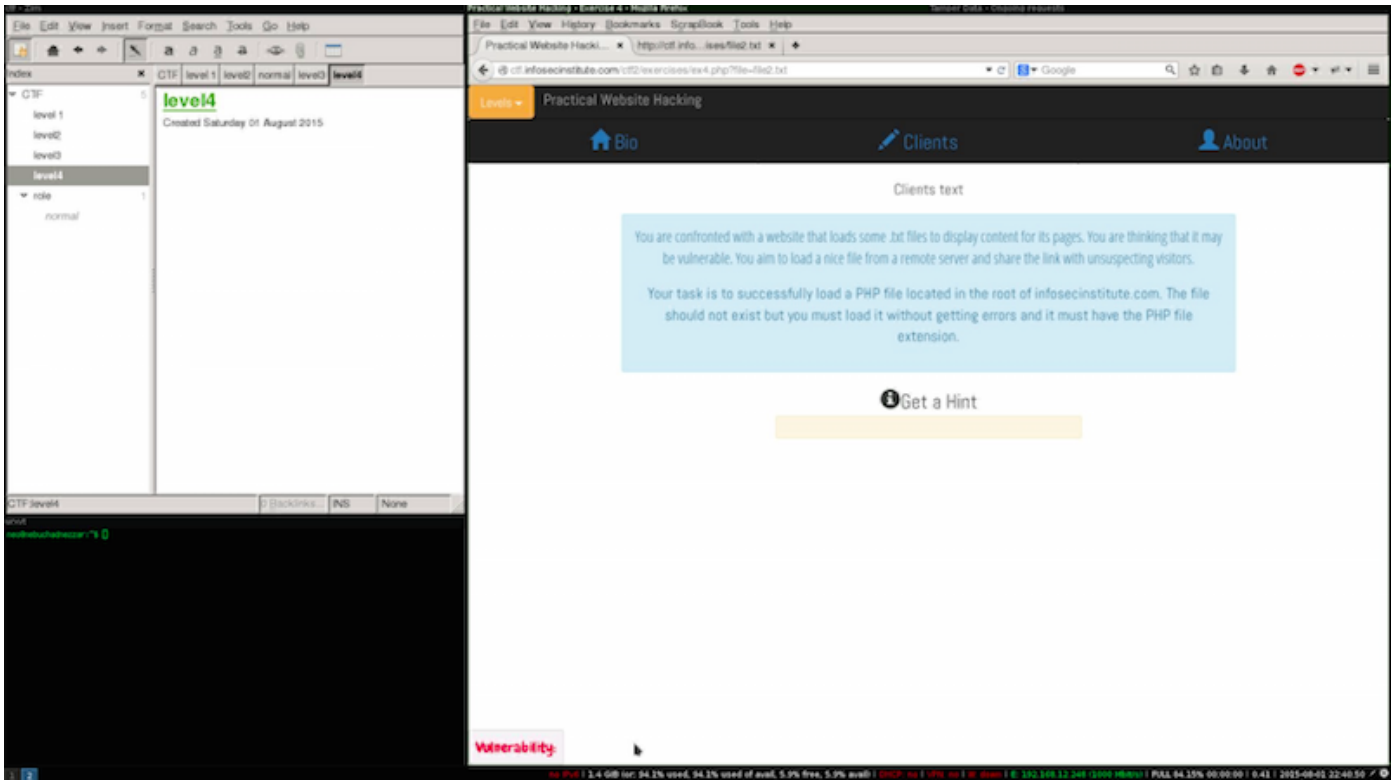
Infosecinstitute CTF 2 - LEVEL 4

This will be solution for Level 4 Practical Web Hacking CTF #2.

In this Level is about file inclusion vulnerabilities File include.

The objective is to inject a php file, that we are told that it should be included form the root of a given domain (infosecinstitute.com), it also says that it should include the file even if it doen't exist, as you will se from the description this types of bugs are very easy to exploit.

File inclusion vulnerabilities in php happened when developers attempt to implement dynamic functionalities using the inputs of the users without proper validation, their are as many ways to implement this as there are for exploiting them.



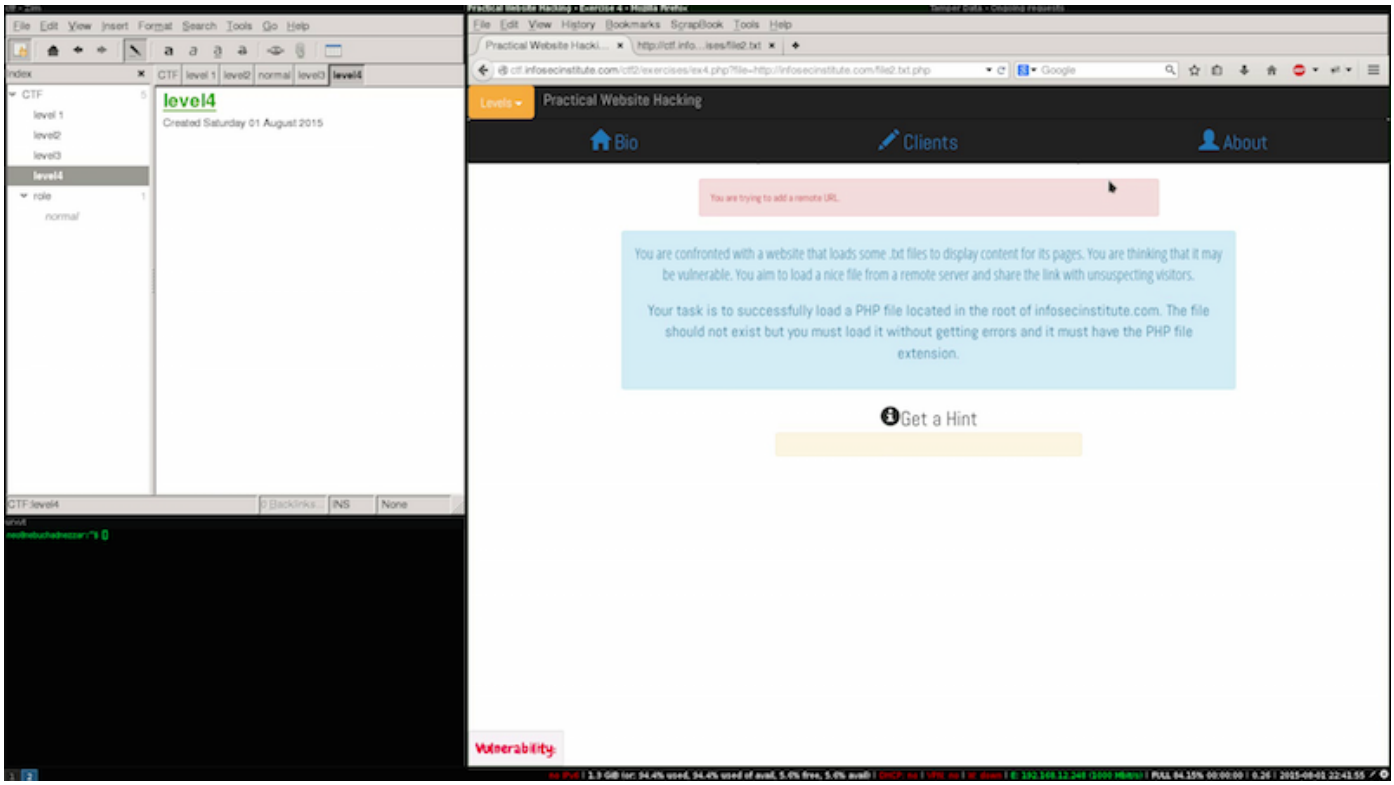
The most used ones are:

1. Null byte injection.
2. Bypass the protection and use the inplementation to load a local or remotefile.

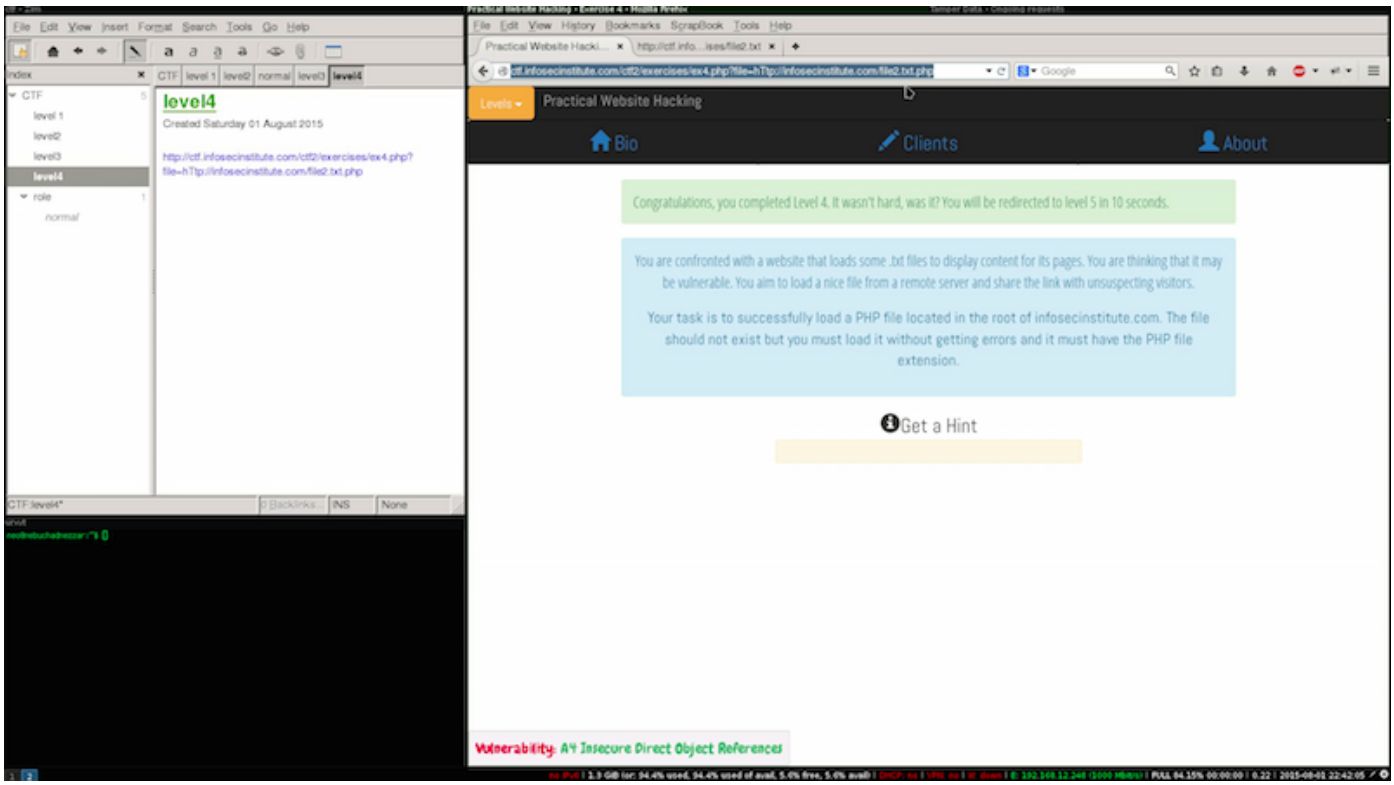
The null byte injection method cannot be used on the latest versions of PHP from the HTTP headers we can see that the version might be one that released after this fix, so we are left with the second option.

To exploit this we need to understand the limitations of the implementation and potential flaws, that we could use, having this in mind we can try to execute a direct remote file include with the information

available.

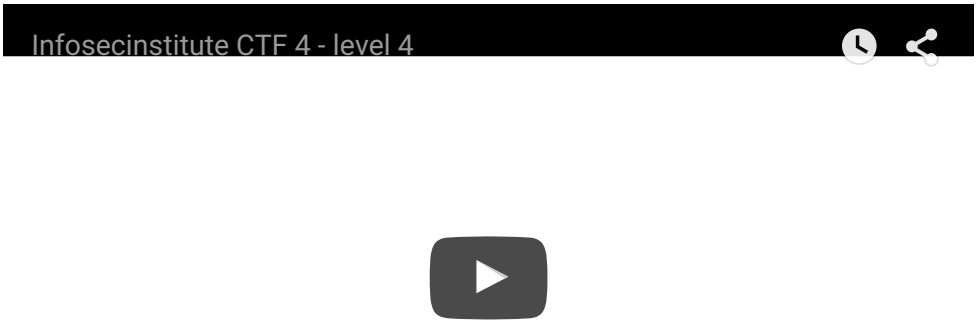


By the error we can see a message from the protection, a very frequent implementation mistaque around regular expression usage is the CASING, to test this we can change the case of one char and submit.



And we are off to level 5 :)

Video



0x4E0x650x6F
0x4E0x650x6F