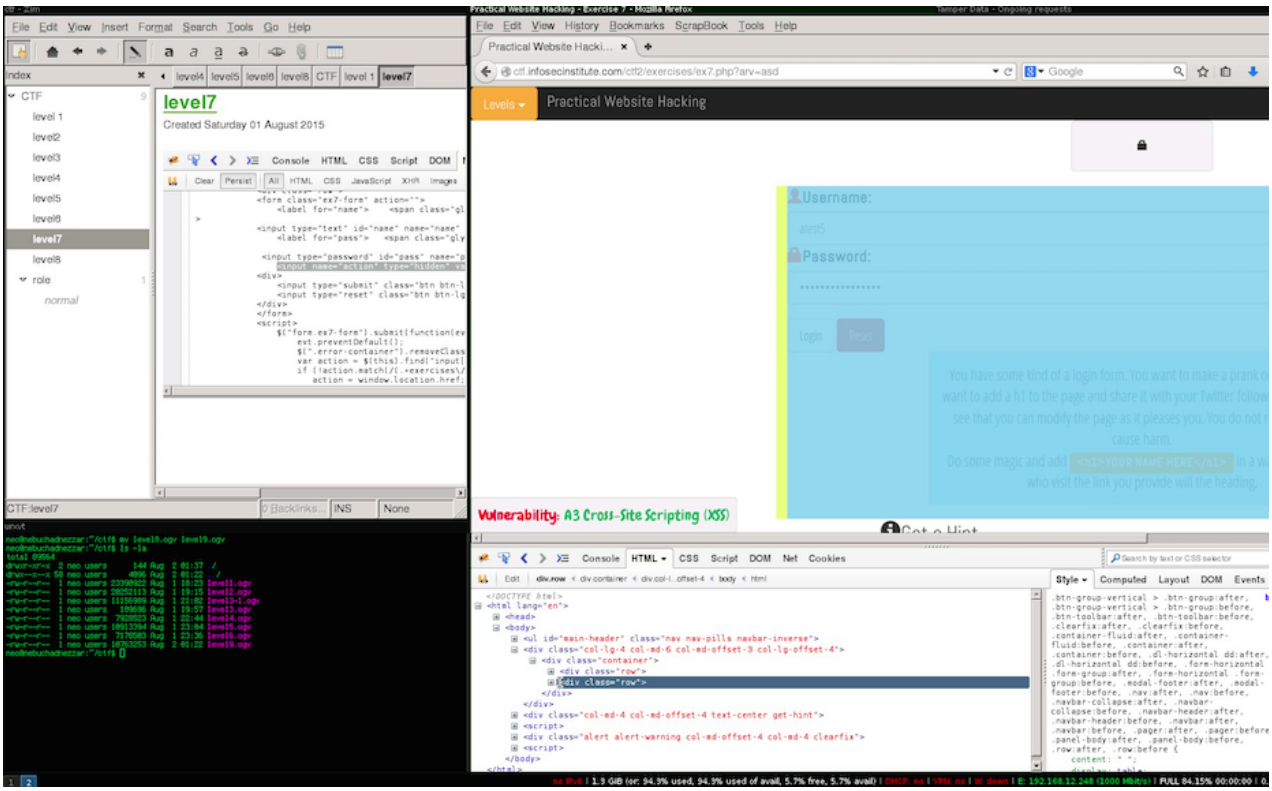
Infosecinstitute CTF 2 - LEVEL 7

This will be solution for Level 7 Practical Web Hacking CTF #2.

This level we have a simple login screen, the objective is to exploit a A3 Cross-Site_Scripting, this types of vulnerabilities exploit the interpreter in the browser to achieve client site code execution (Javascript).

1. session hijacking
2. Cross-Site Request Forgery

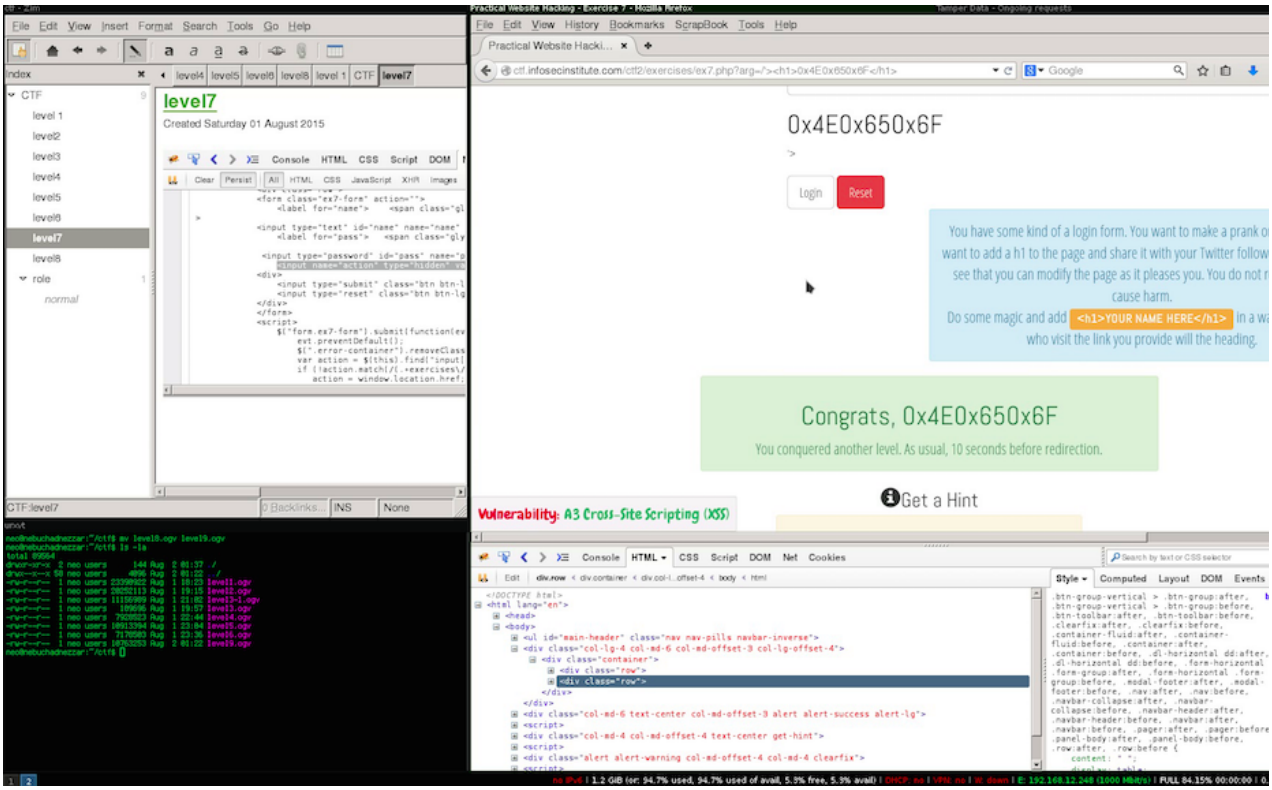
The objective is to inset a html tag with our name in it, for that we need to see some details about the implementation.



After close inspection of the url we noticed that a script uses the **window.location.href**, this lead to the idea that some of that information might be sent to server, for later use, in the attempt to verify this i noticed that a hidden input field with the value of arguments sent in the query string.

Tasks:

1. break\ end the hidden tag.
2. Create tag with the required string.
3. Enjoy level 8 :)



Infosecinstitute CTF 2 - Level 7

0x4E0x650x6F
0x4E0x650x6F