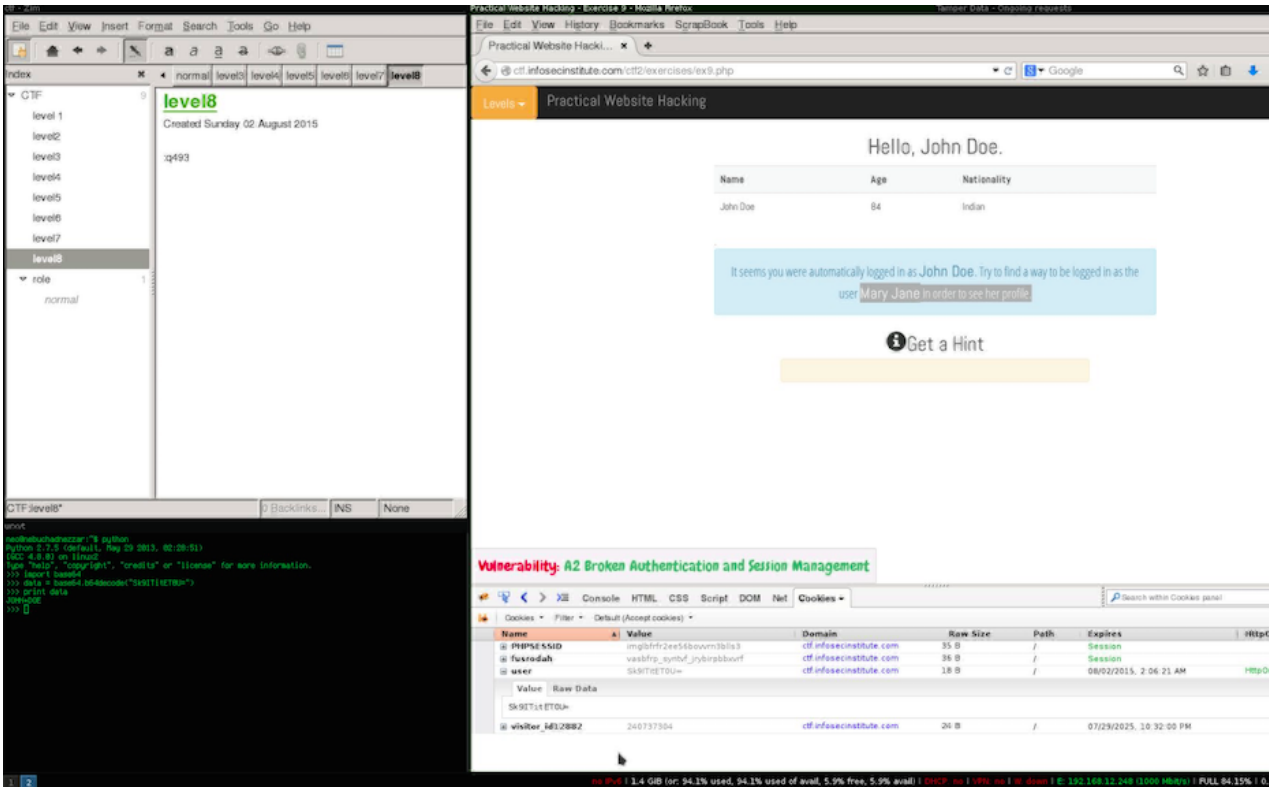
Infosecinstitute CTF 2 - LEVEL 9

This will be solution for Level 9 Practical Web Hacking CTF #2.

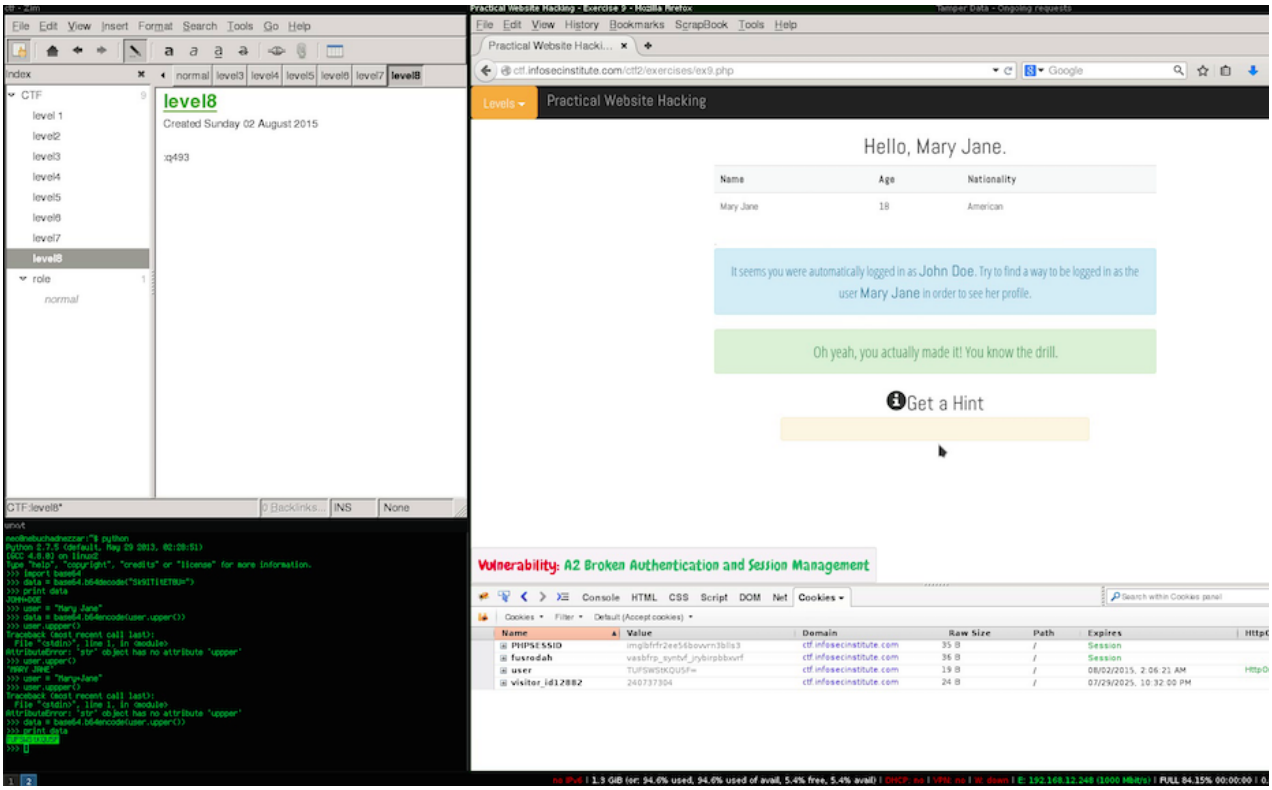
This level we are told that we have a broken Session management, as i explained in level 5 this usualy means we have a broken session id, and the usual flaws are:

1. Depercated hashing algorithm like md5,md4 sha1 etc.
2. Unsafe session ids based on time or user imput.

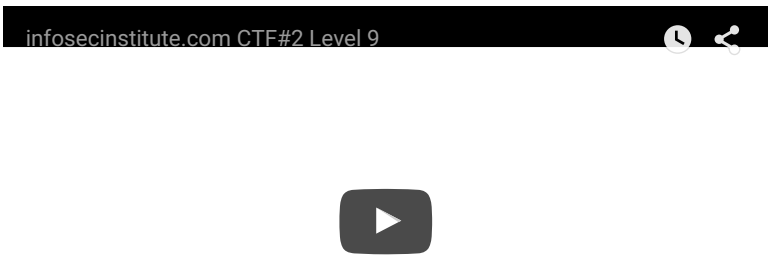


After looking at the session id i noticed what might be familiar encoding style, to test it out we open our python shell and decoded the base64 string in the session id.

This allows us to see what was enconded in the token and how we can reproduce it for the other user, in this case its the name of the user and the space replaced by **"+"** easy.



Video



0x4E0x650x6F
0x4E0x650x6F