

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 usually means we have a broken session id, and the usual flaws are:

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

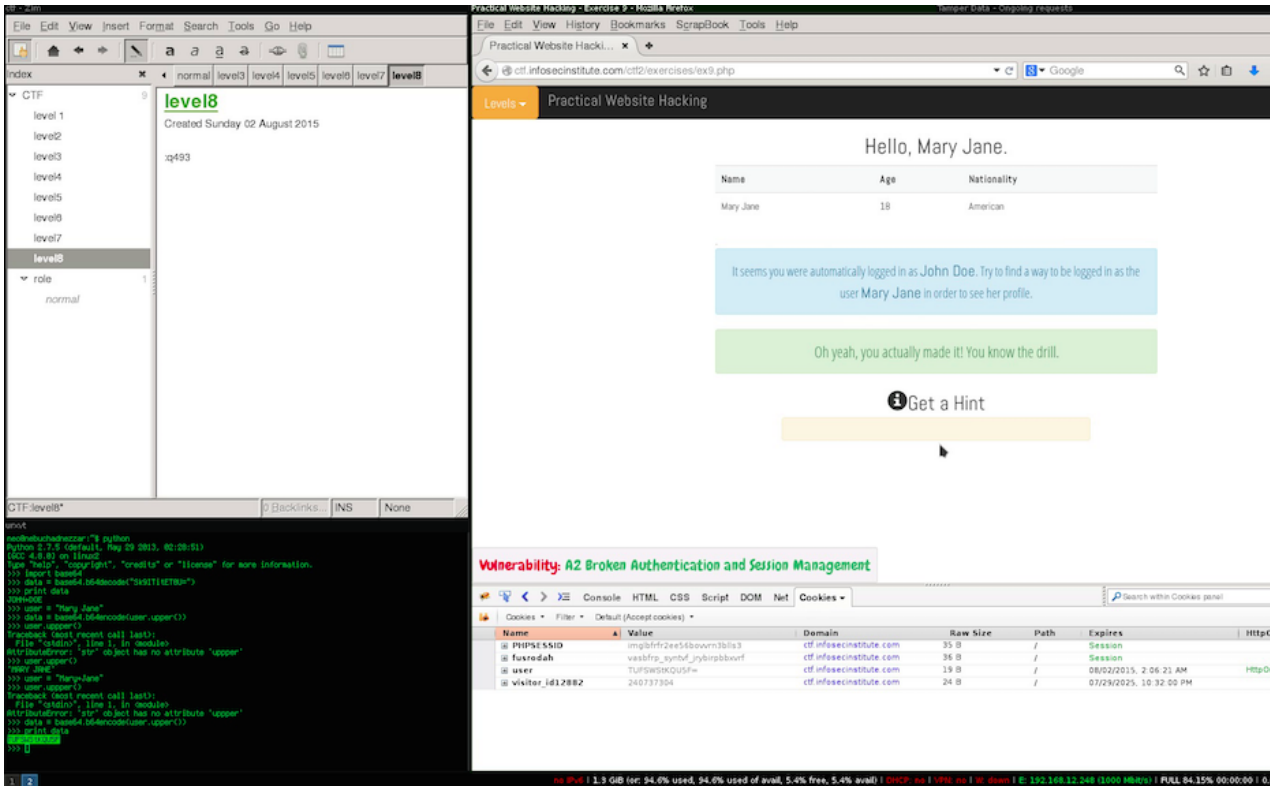
The screenshot shows a web browser window displaying a user profile for "John Doe" with age 84 and nationality Indian. A message indicates automatic login and suggests logging in as user "Mary Jane". Below the profile is a "Get a Hint" button. The browser's developer tools show a "Vulnerability: A2 Broken Authentication and Session Management". The Cookies panel lists several cookies, including a session cookie with a base64-encoded value.

The terminal window shows a Python script that decodes the base64 string from the session ID. The script output is:

```
level8
Created Sunday 02 August 2015
12493
role
normal
```

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 encoded 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