For this flag we saw that it was dependent on flag 3, so we tried using sqlmap again.
We first tried to see if the database contained anything new, but it didn't seem to be the case when listing tables, columns etc.

Then we saw that we could do –os-shell with sqlmap, and when trying this we managed to get an os-shell where we could run commands.

Command:

```
sqlmap -u http://10.162.2.83/php/recherche_old.php --forms
--cookie="PHPSESSID=svtfg83fvil5v3b6rt21jv0b74" --os-shell --batch
```

Now when we have a shell, it seems to be a non-interactive shell, which means for example it does not update file path if we try cd and such. But we could do ls and when doing ls /var/www/html we saw the flag:

flag{3b2000a12a0b465d721592f1575cb07039f6e466f95ce5}.jpg

The reason we knew to look in /var/www/html is because if we run whoami the user is www-data which is a “web user”.