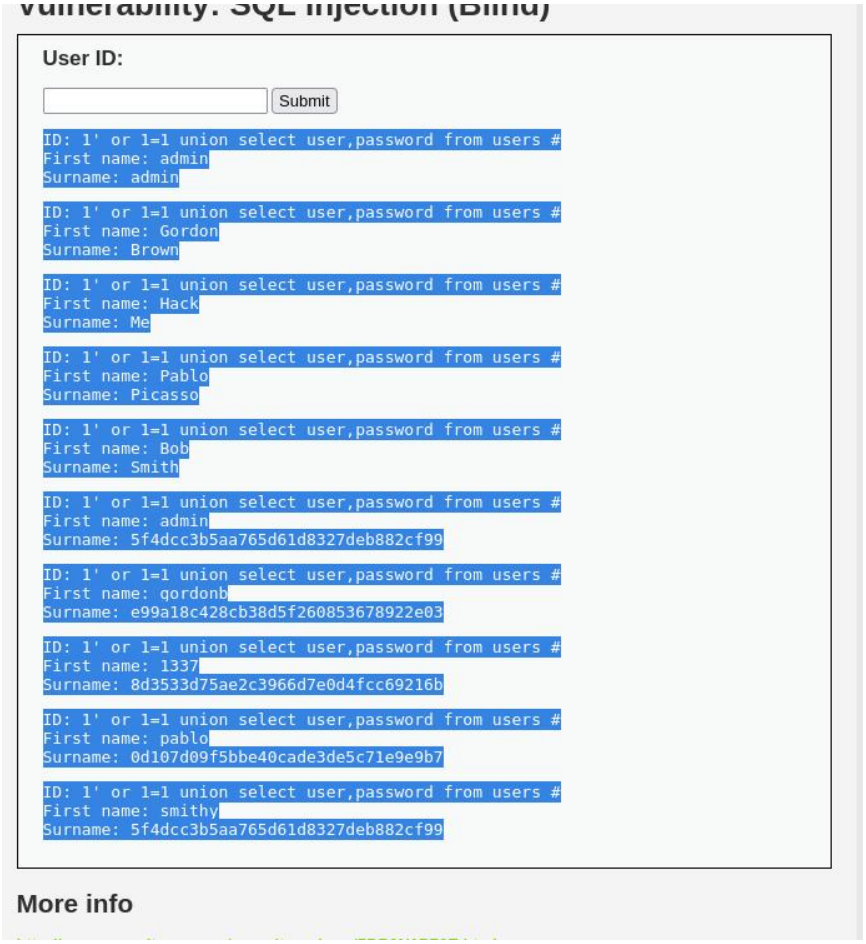
PROGETTO S6/L5

In questo report dimostriamo che la pagina è vulnerabile tramite attacchi SQLi e SSX

ATTACCO SQLi

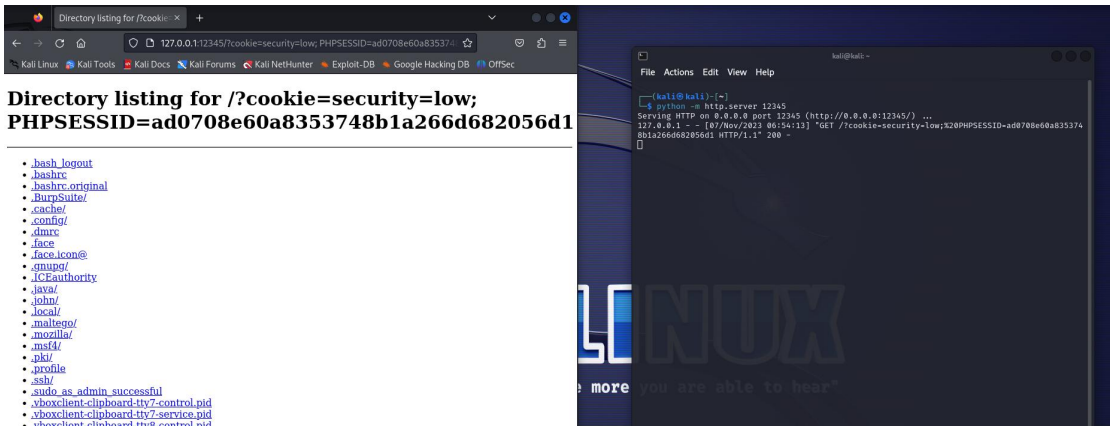
Questo è un attacco di tipo SQLi, attraverso il quale usiamo un comando sql nella txt box che poi è eseguito dal url.



Questo codice ci permette estrapolare username e psw degli utenti registrati, persino quelli criptati.

ATTACCO XXS

CROSS-SITE SCRIPTING: è un attacco dove si sfrutta la vulnerabilità del sito web, il quale permette a un utente mal intenzionato di inserire script.
In questo attacco usiamo uno script attraverso il quale richiediamo i cookies, faremo in modo che lo script sia collegato alla pagina cosi da rimandarci i cookies, useremo un server creato da noi por poter ricevere questi dati.
Cosi a ogni persona che accede alla pagina gli vengono intercettati i cookie e veniamo a conoscienza di questi dati.



In questo caso ho usato un server creato con python attraverso il quale non solo otteniemo i cookies di sessione ma abbiamo anche la possibilita di navigare attraverso il server.