PROGETTO SETTIMANALE

EXPLOITARE LE VULNERABILITÀ:
-SQL INJECTION (BLIND).
-XSS STORED.

SCOPO DELL'ESERCIZIO:

-RECUPERARE LE PASSWORD DEGLI UTENTI PRESENTI SUL DB (SFRUTTANDO LA SQLI).

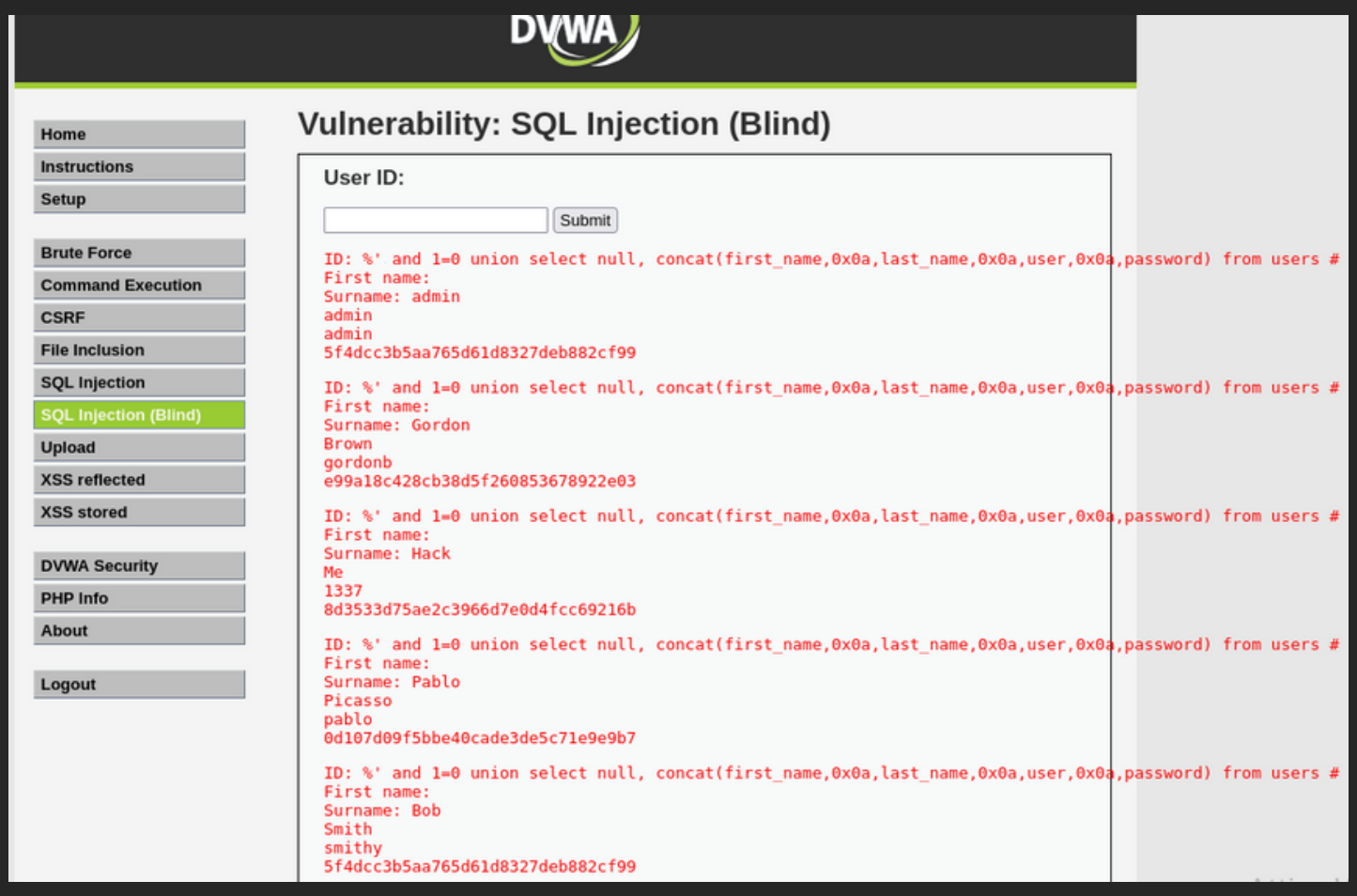
-RECUPERARE I COOKIE DI SESSIONE DELLE VITTIME DEL XSS STORED ED INVIARLI AD UN SERVER SOTTO IL CONTROLLO DELL'ATTACCANTE

BENEDETTA FORESTIERI

RECUPERO PASSWORD DAL DB

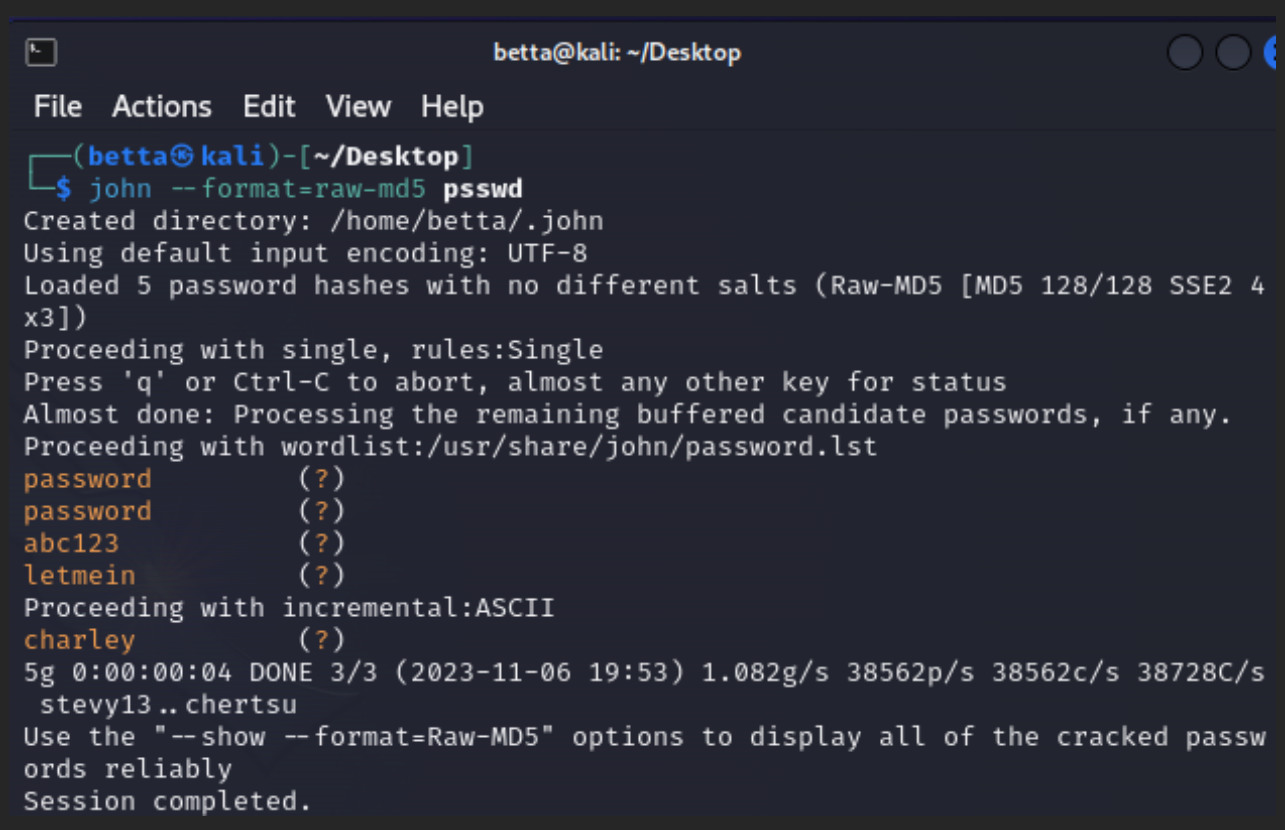
L'attacco SQL injection sfrutta il linguaggio SQL per manipolare il database.

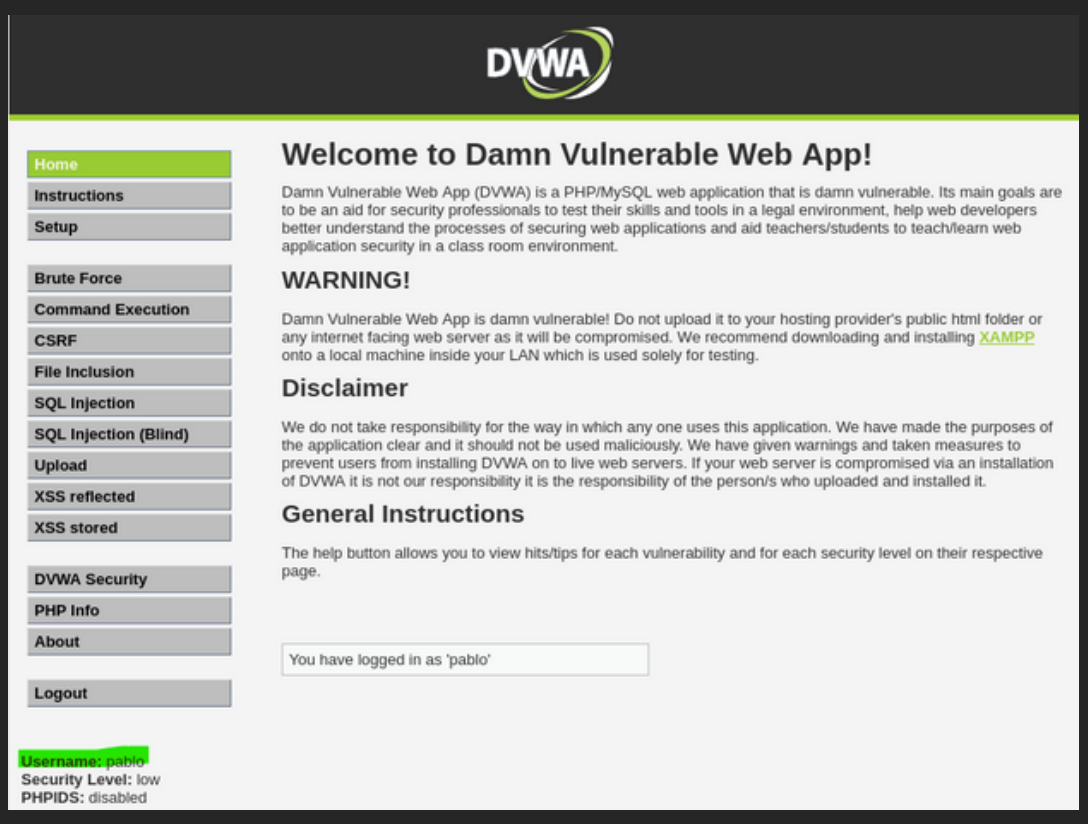
Avvio DVWA su Kali Linux, setto la sicurezza a “Low” ed inserisco una query SQRL.
Quest’ultima mi permette di vedere nomi utenti e password degli utenti nel database.



Apro Kali, creo un file contenente gli hash delle password e lancio il comando a John, software per il cracking delle password.

Le password sono state craccate con successo.
Eseguo una verifica inserendo su DVWA la password “letmein” e user “pablo”.





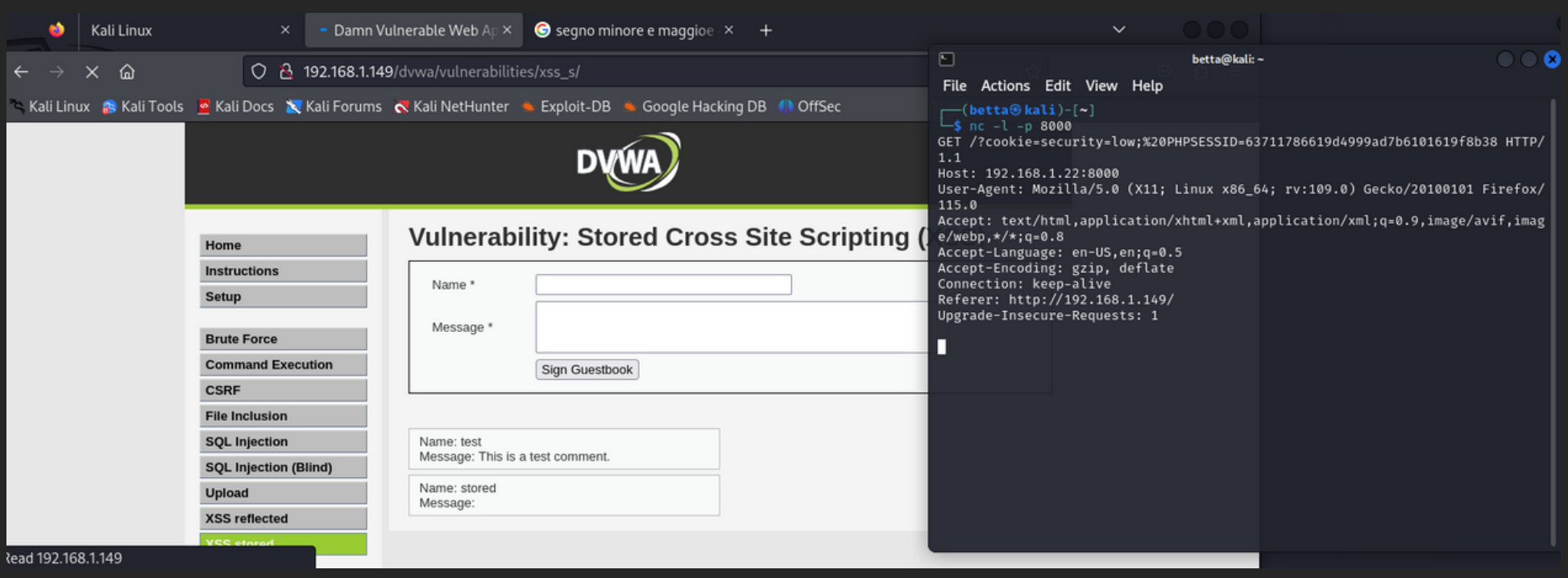
Come mostrato in figura, il Login è avvenuto con successo.
Le credenziali sono corrette.

RECUPERO COOKIE DI SESSIONE

L’attacco XSS **Stored** è un attacco in cui un aggressore inserisce un codice malevolo in un sito web o un'applicazione web. Questo codice dannoso viene memorizzato sul server e poi restituito agli utenti quando visitano la pagina, eseguendo il codice nel loro browser.

A differenza dell’attacco XSS Reflected, dove il payload viene riflesso immediatamente e influisce solo sugli utenti che accedono a un link o una richiesta contenente il payload, in un attacco XSS Stored, il codice malevolo viene conservato sul server e può interessare tutti gli utenti che visitano la pagina infetta.

Per recuperare i cookie di sessione e inviarli a un server locale, inserisco nel messaggio un payload XSS.



Utilizzo Netcat per ascoltare sul server locale i cookie “rubati” e per ricevere ulteriori dati inviati dallo script.

Netcat è un servizio a riga di comando che offre una vasta gamma di funzionalità, tra cui la capacità di eseguire scansioni delle porte di un computer remoto, funzionare come un server locale, facilitare il trasferimento di file, consentire la comunicazione in stile chat e addirittura agevolare la creazione di un'entrata segreta (backdoor) in un sistema.