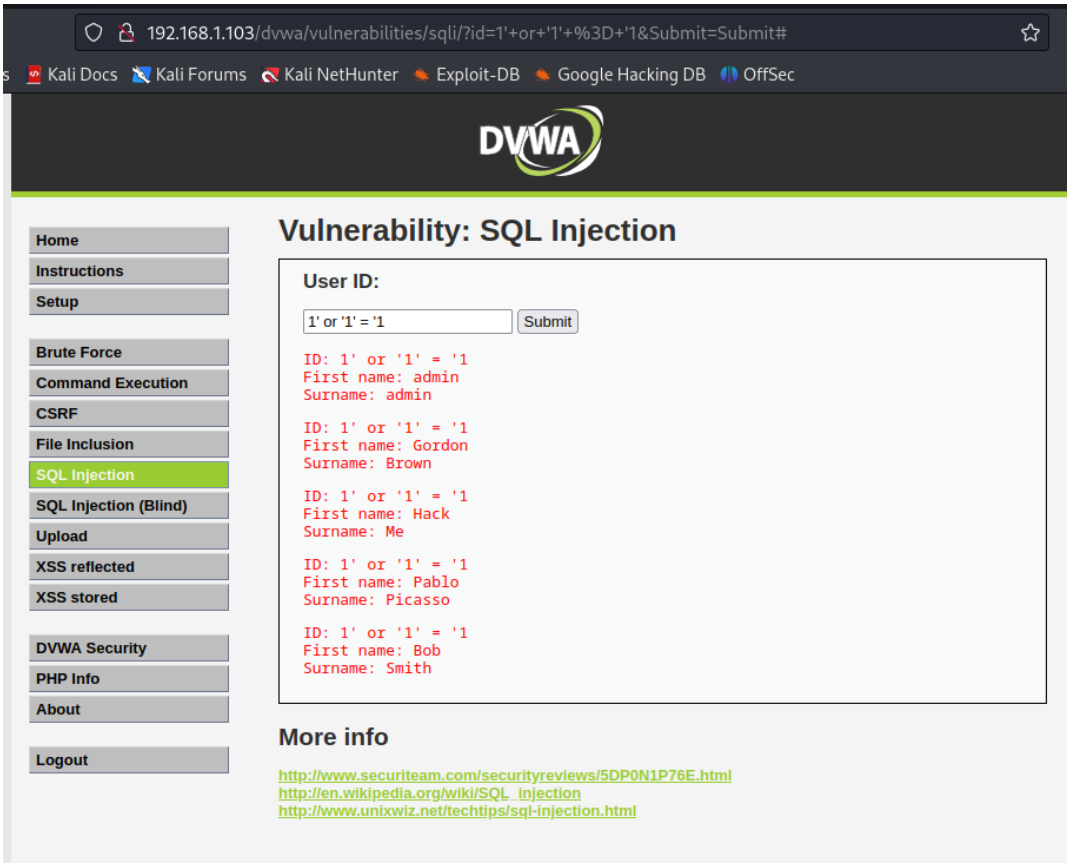
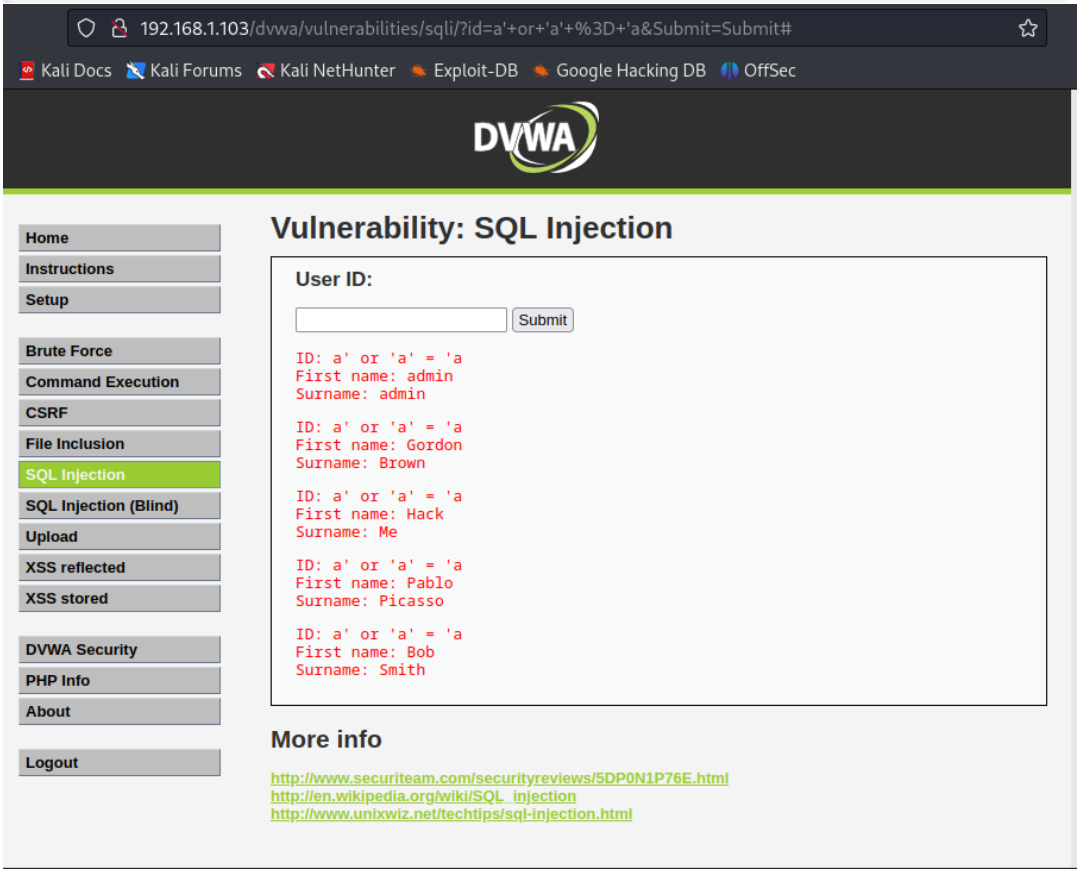
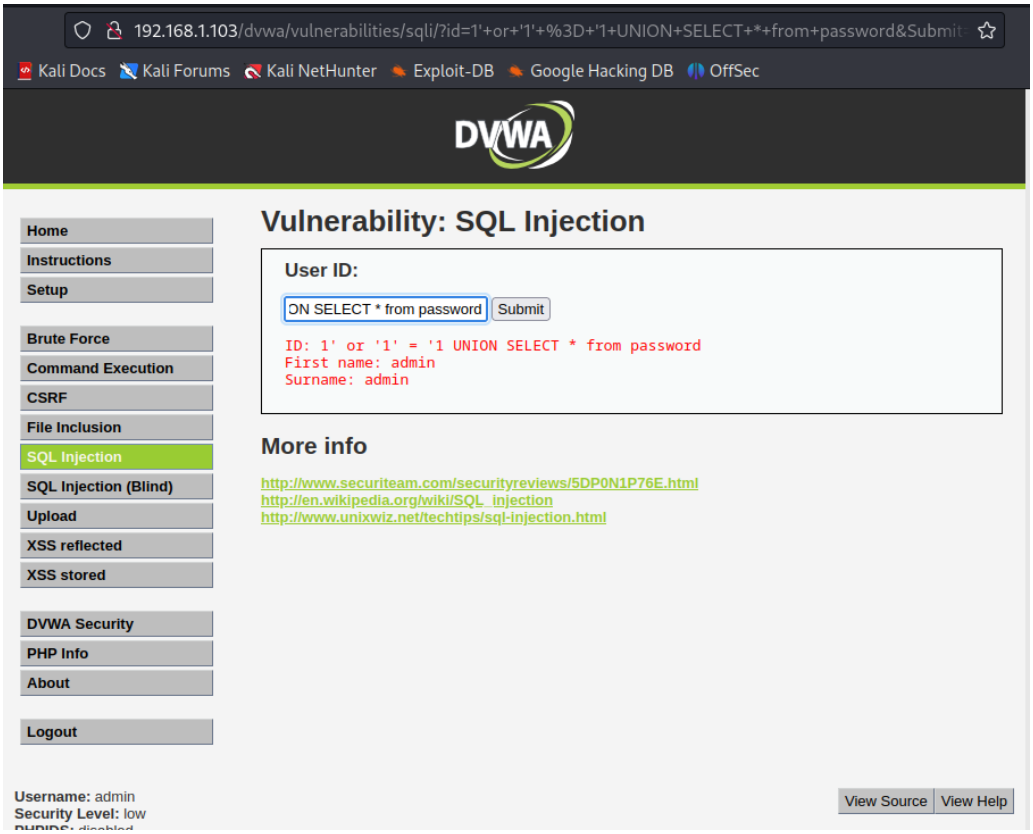
Un attacco SQL Injection permette ad un utente malintenzionato di prendere il controllo dei comandi SQL di una web app, ad esempio in questo caso ci ha permesso di avere a disposizione le credenziali degli utenti.

Inserendo l'input 1' or '1' = '1 oppure a' or 'a' = 'a creiamo una condizione sempre vera, questo ci permette di manipolare il comportamento di una query del database che ci restituisce così i risultati del campo utente

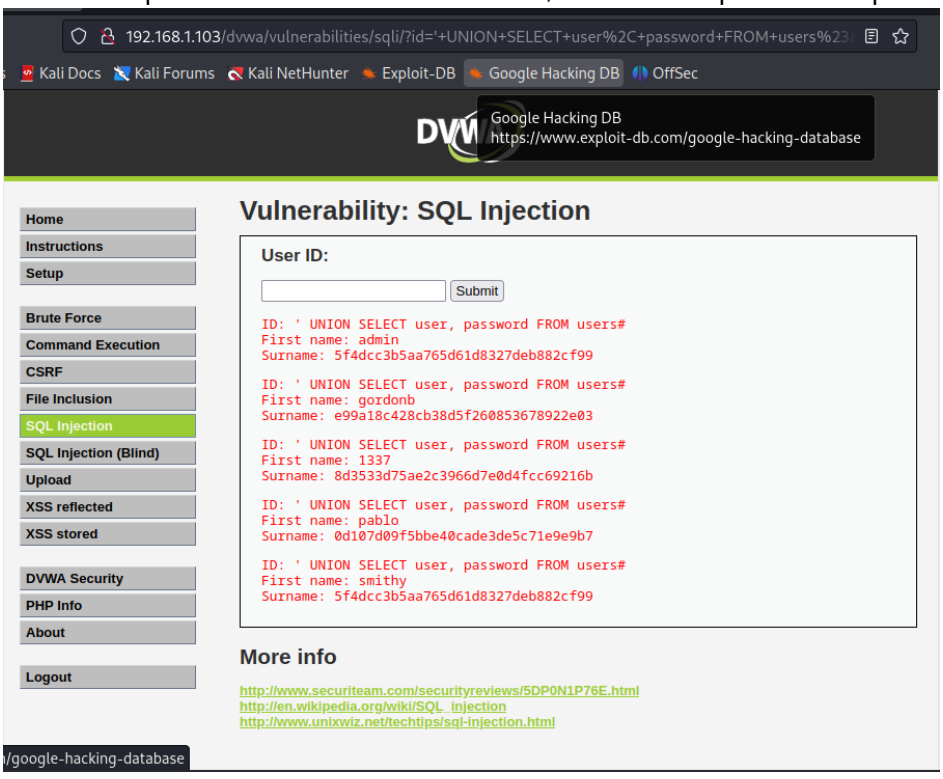




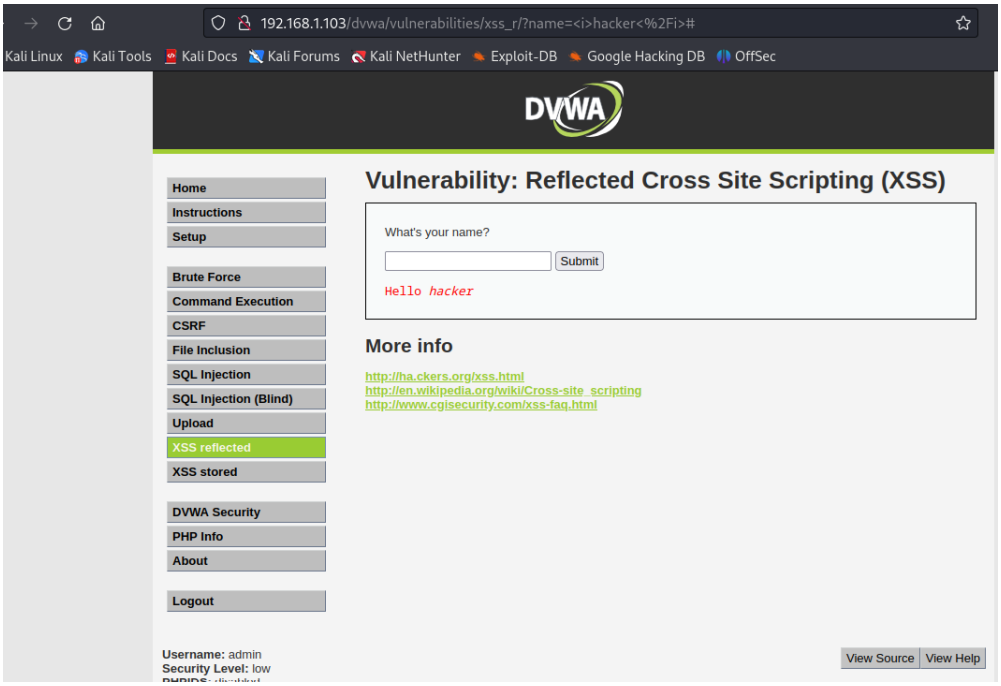
Successimvamente unendo due operatori logici con il comando UNION SELECT possiamo combinare più richieste. Ad esempio 1’ or ‘1’ = ‘1 UNION SELECT * from password, questo tipo di inserimento va a combinare due condizioni, dove la prima parte ('1' or '1'' = '1') è progettata per essere sempre vera e la seconda parte ('UNION SELECT * from password') cerca di eseguire una query SQL non autorizzata per recuperare dati dalla tabella "password".



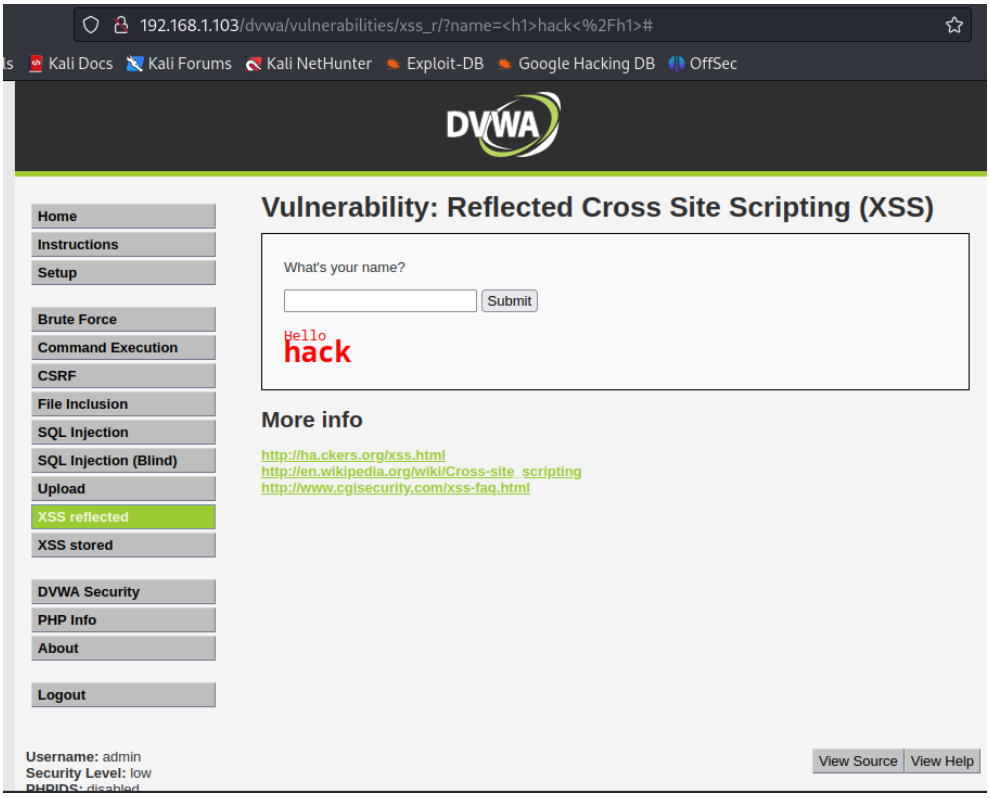
Possiamo unire anche più richieste nello stesso comando ad esempio per eseguire una query SQL che cerca di recuperare informazioni sugli utenti da una tabella chiamata users possiamo usare il comando: ' UNION SELECT user, password FROM users# Quindi cercando di combinare due query SQL: la prima parte dell'input (' UNION SELECT user, password FROM users#) è progettata per essere aggiunta alla query originale del sito web e recuperare dati dalla tabella "users", inclusi i campi "user" e "password".



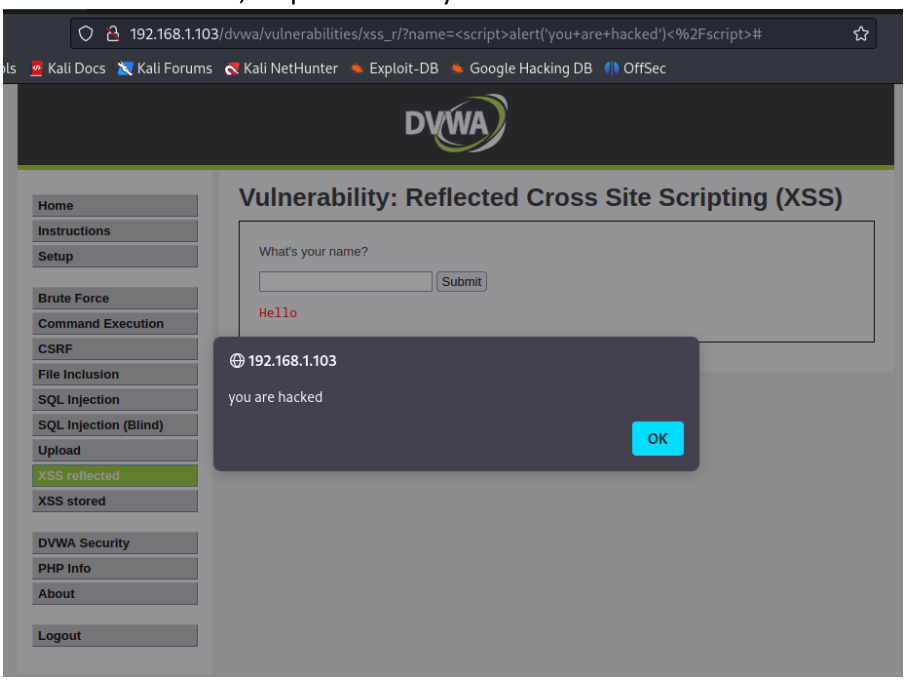
Un altro tipo di vulnerabilità è l'XSS riflesso in cui un attaccante è in grado di iniettare script malevoli (HTML o JavaScript) all'interno di una pagina web visualizzata da altri utenti. Questa vulnerabilità si verifica quando l'applicazione web prende dati forniti dall'utente e li restituisce nella pagina web senza una corretta sanitizzazione ovalidazione. In questo caso la sintassi da eseguire è hacker otterremo la stringa di testo in corsivo.



Invece con <h> hack </h> otteniamo una stringa in grassetto



Un altro modo di fruttare questa vulnerabilità è di inserire un alert che ci dà in output una finestra pop-up con il contenuto dell'alert, in questo caso "you are haked". Il codice da inserire è <script> alert('you are hacked')</script>



Un modo "utile" di usare l'xss riflesso è il recupero di cookies, con il codice <script> alert(document.cookie)</script> visualizzerà una finestra di avviso con il contenuto del cookie della pagina web. Gli attaccanti possono utilizzare questo tipo di attacco per rubare cookie di sessione o altre informazioni sensibili dagli utenti.