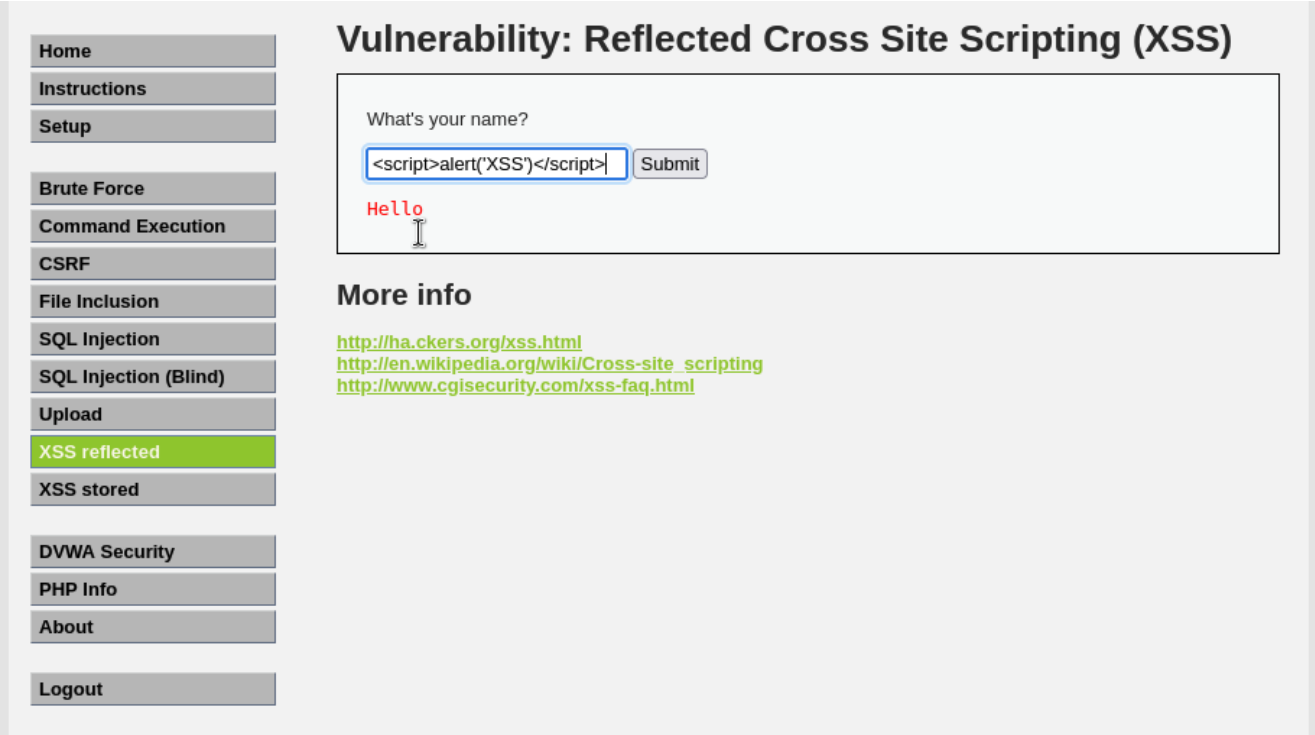
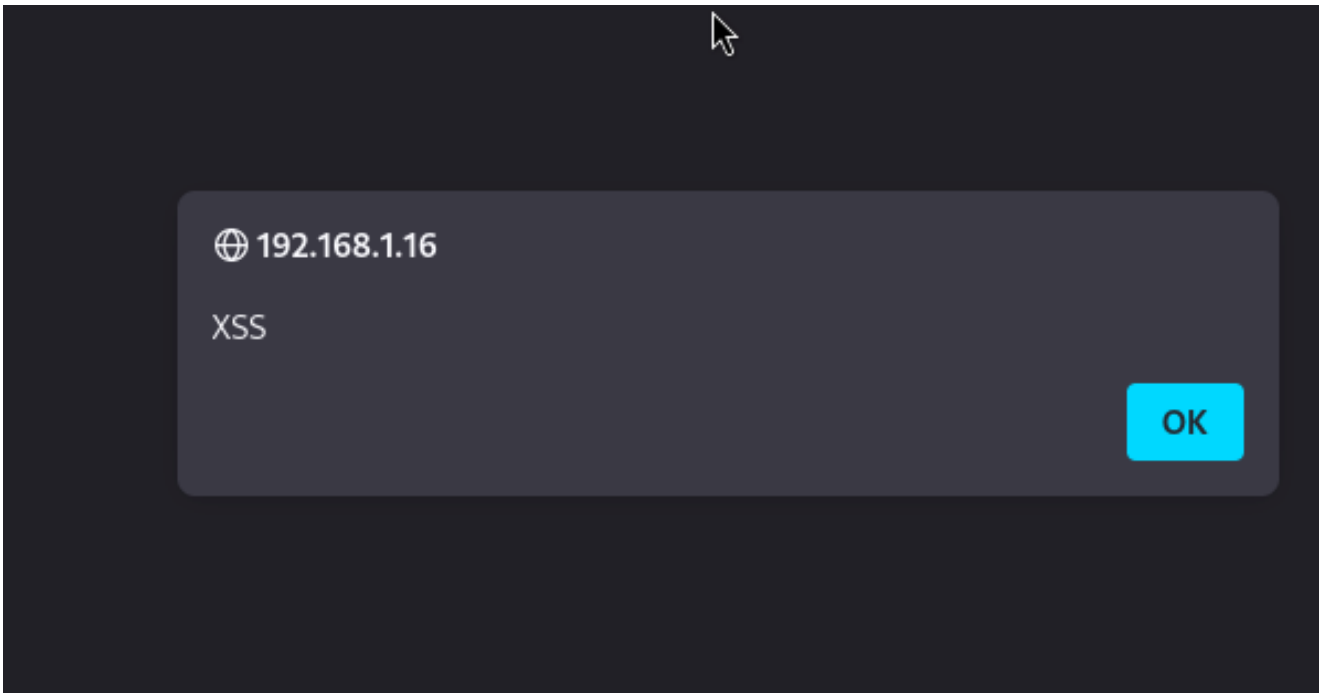
XSS – SQL INJECTION

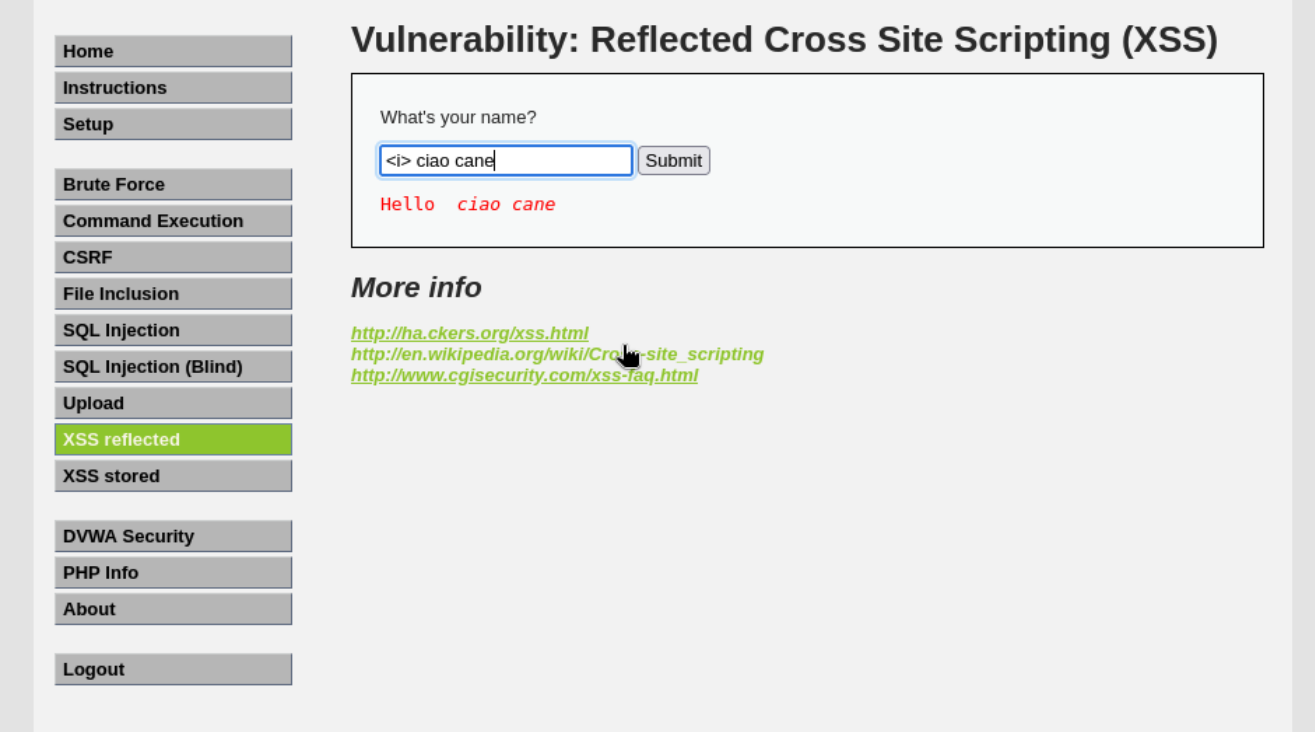
ALERT <script>alert('XSS')</script>



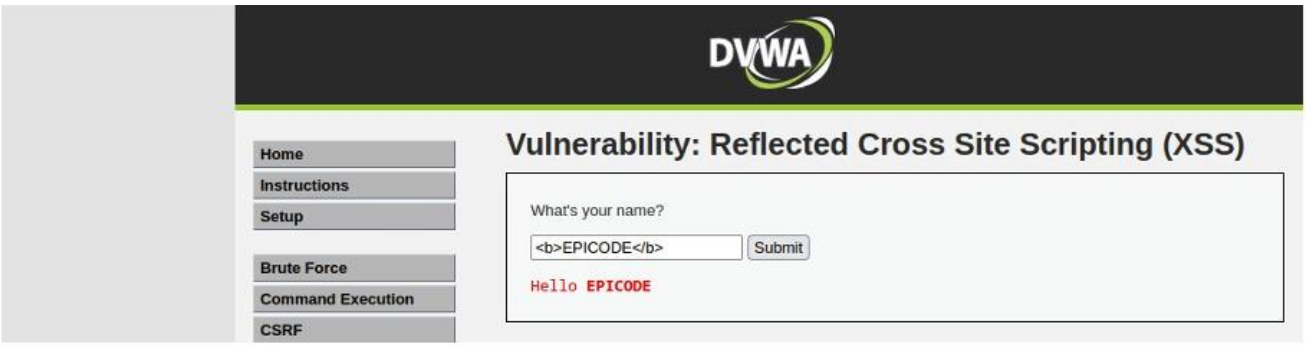
OUTPUT ALERT <script>alert('XSS')</script>



CORSIVO <i>Testo in corsivo<i>

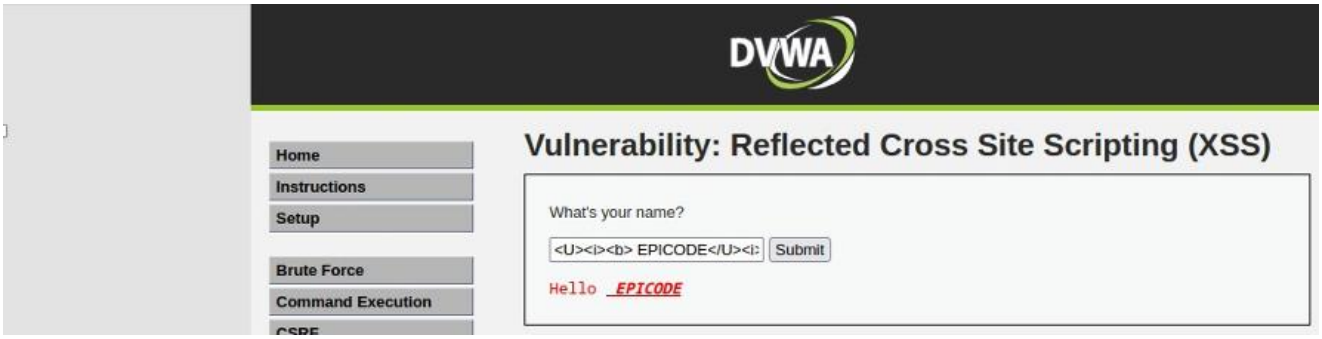


GRASSETTO <b>Testo in grassetto<b>

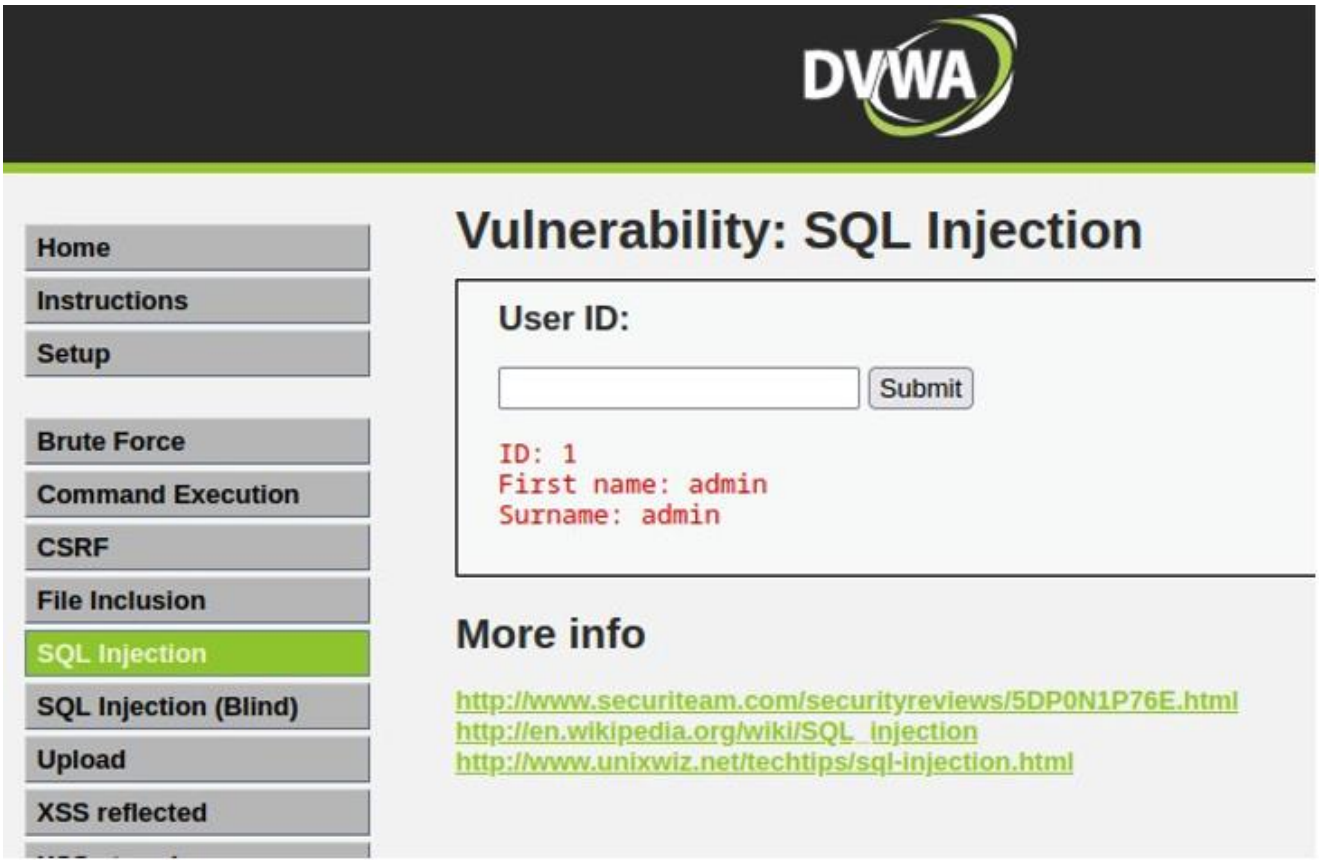


SOTTOLINEATO <U>Testo sottolineato<U>

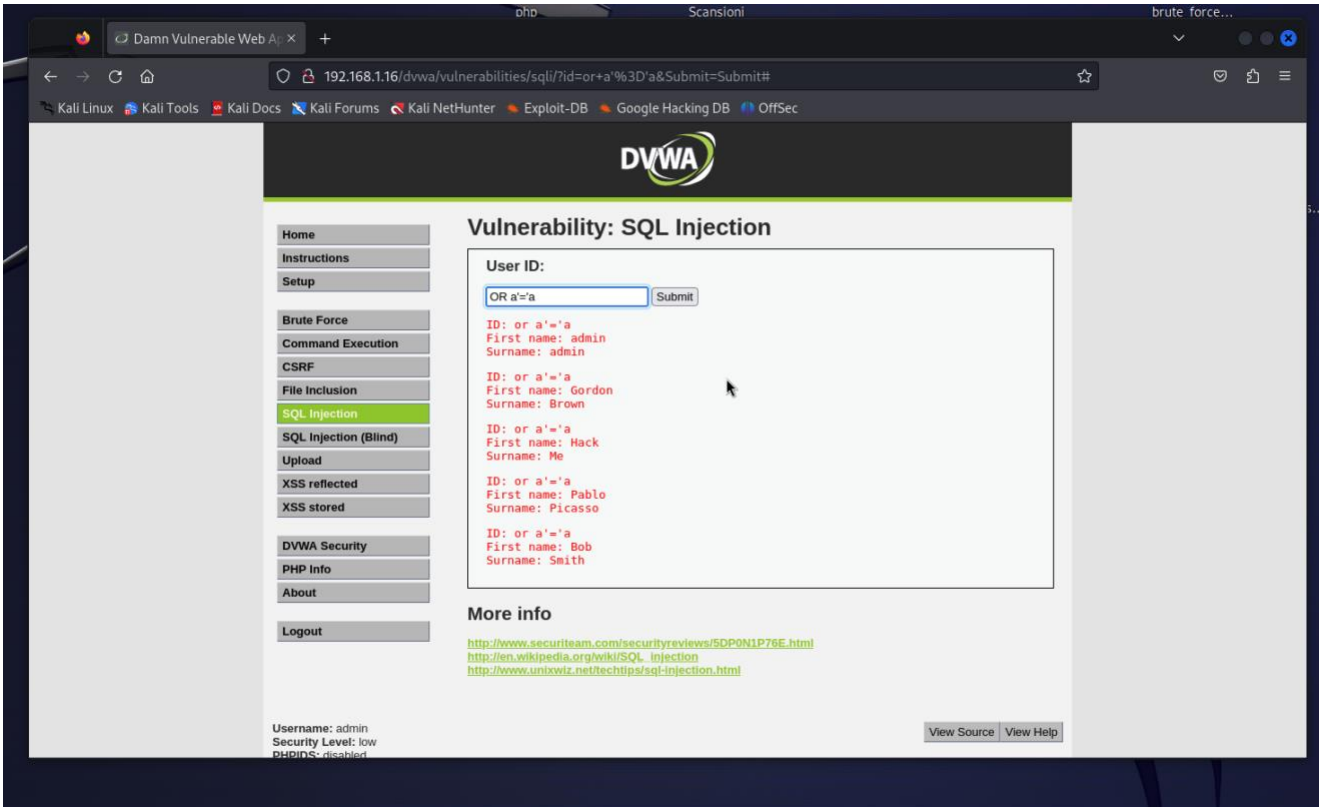
CORSIVO, GRASSETTO, SOTTOLINEATO



Ho avuto accesso a nome e cognome di un utente inserendo 1 nel campo User ID



Bypassata autenticazione tramite ' OR 'a'='a' – (poiché la condizione a=a è sempre vera, l'operatore OR restituirà sempre un risultato valido, motivo per cui sono riuscito ad accedere ad una nuova posizione che altrimenti sarebbe protetta).



%' or 0=0 union select null, user() #

- Tramite %’ ho indicato la fine di un’istruzione SQL, con 0=0 ho dato una condizione sempre vera, al fine di bypassare controlli di autenticazione.
- Con union ho combinato i risultati di due query;
- Tramite parametro sono venuto a conoscenza di quanti campi vengono selezionati dalla query vulnerabile;
- infine tramite parametro user ho listato per l’appunto tutti gli utenti presenti, reperendone nome e cognome.