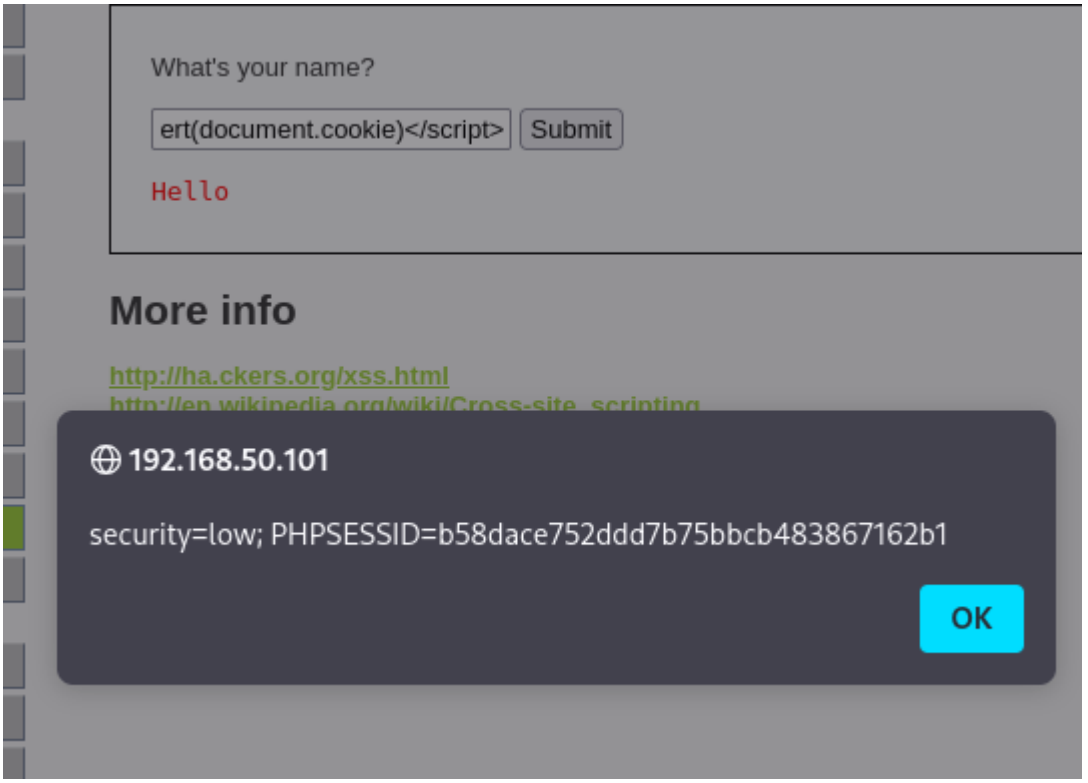
W13D4 - XSS Reflected e SQL Injection (Blind)

collegandoci alla DVWA e impostando il livello di security a LOW, facciamo le prove con XSS Reflected e SQL Injection.

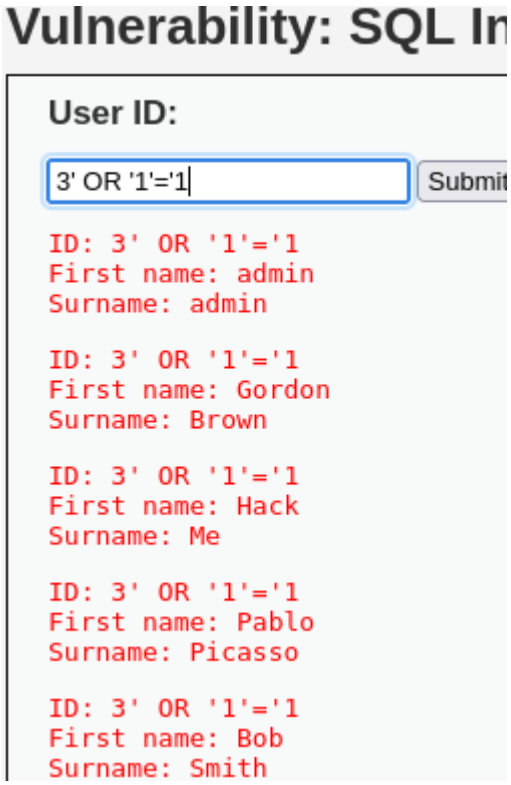
su XSS Reflected possiamo provare a scrivere World! e lui ci darà come risultato la parola World in corsivo

oppure scrivendo <script>alert(document.cookie)</script> ci farà apparire il pop up con i cookie del sito grazie al parametro document.cookie

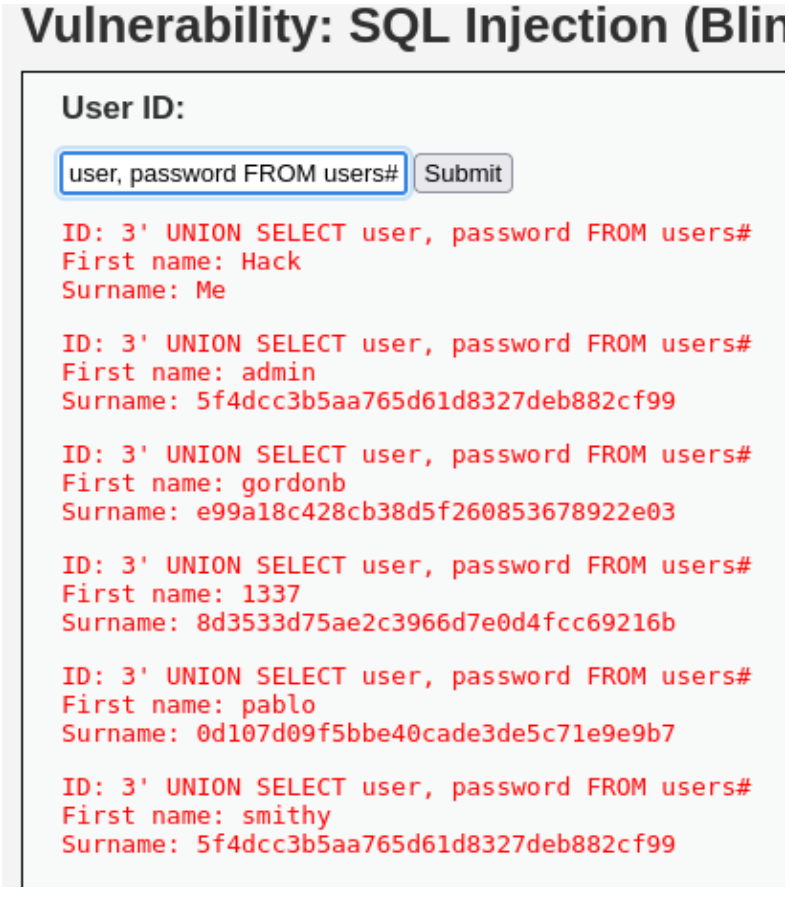


su SQL Injection se proviamo a inserire il testo come in figura ci darà come risultato tutti gli user che sono dentro la tabella, in questo caso la tabella users, questo perché scrivendo il

parametro OR 1=1 dirà sempre vero quindi non solo ci farà vedere l'UID 3 ma anche tutti gli altri.



si può notare una vulnerabilità con quest'ultimo, infatti se scriviamo la seguente riga come in figura sotto (3' UNION SELECT user, password FROM users#) # è il commento cosi da almeno non eseguire altre query oltre quello. Come risultato ci dà l'user e anche le loro



password. ci seleziona First name e Surname perché molto probabilmente la query precedente a UNION è SELECT First name, Surname FROM users WHERE ID = x (input da parte dell’utente)