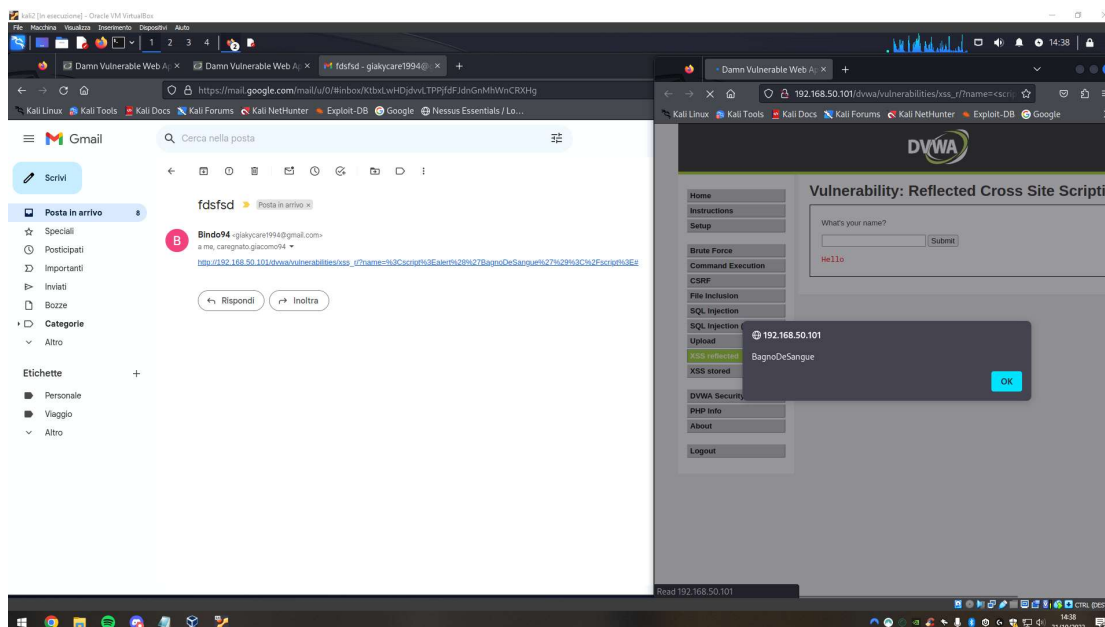
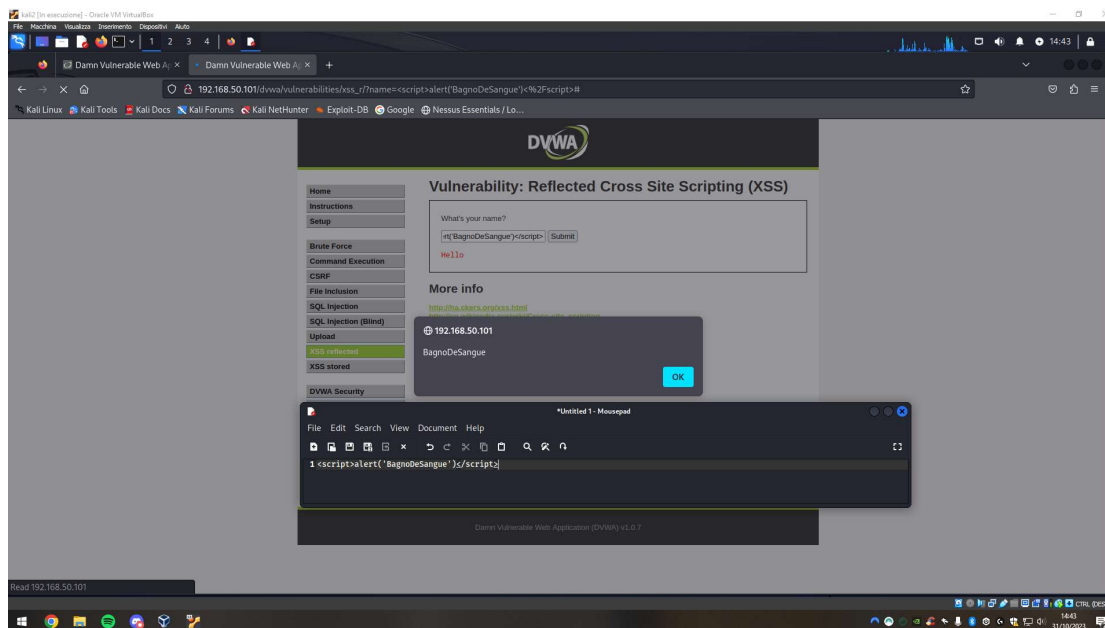


Exploit DVWA - XSS e SQL injection

Durante l'esercizio di oggi andremo a testare le vulnerabilità XSS e SQL injection.

Per il XSS reflected ho utilizzato lo script `<script>alert('BagnoDeSangue')</script>` che praticamente fa uscire un pop-up con sopra scritto il messaggio che vogliamo, poi ho copiato il link che si è creato e ho provato ad inviarmelo via mail ed aprirlo e il risultato lo vediamo nel secondo screen.



Come seconda cosa ho testato il SQL Injection utilizzando lo script.

`%' and 1=0 union select null,`

concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #

Il termine SQL injection indica esattamente di cosa si tratta: un'iniezione di codice nel linguaggio SQL. Infatti noi andremo a iniettare questo script dentro il database di DVWA per andare a ricavare tutte le informazioni che contiene come ID, nomi, cognomi e password.

