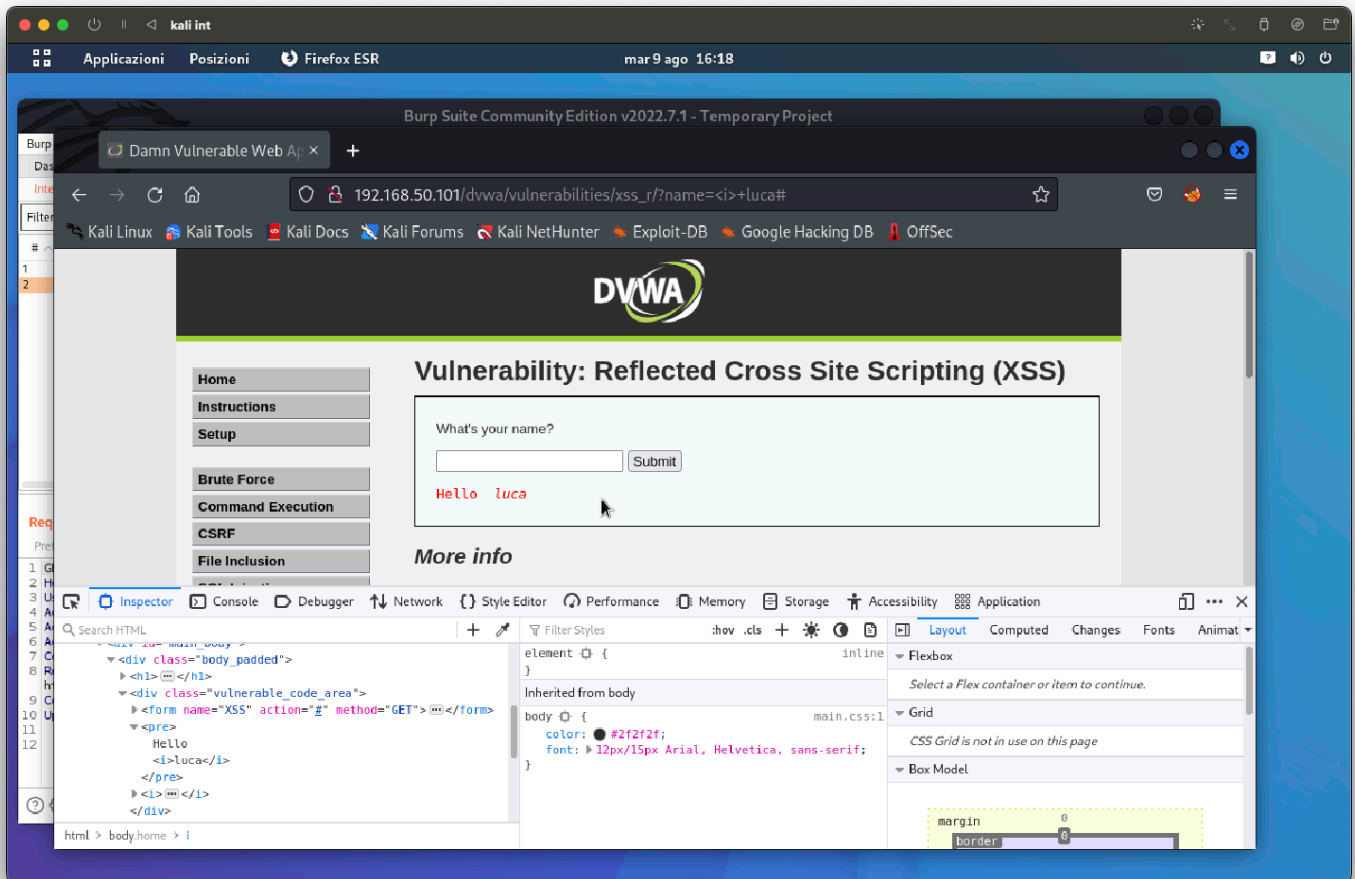
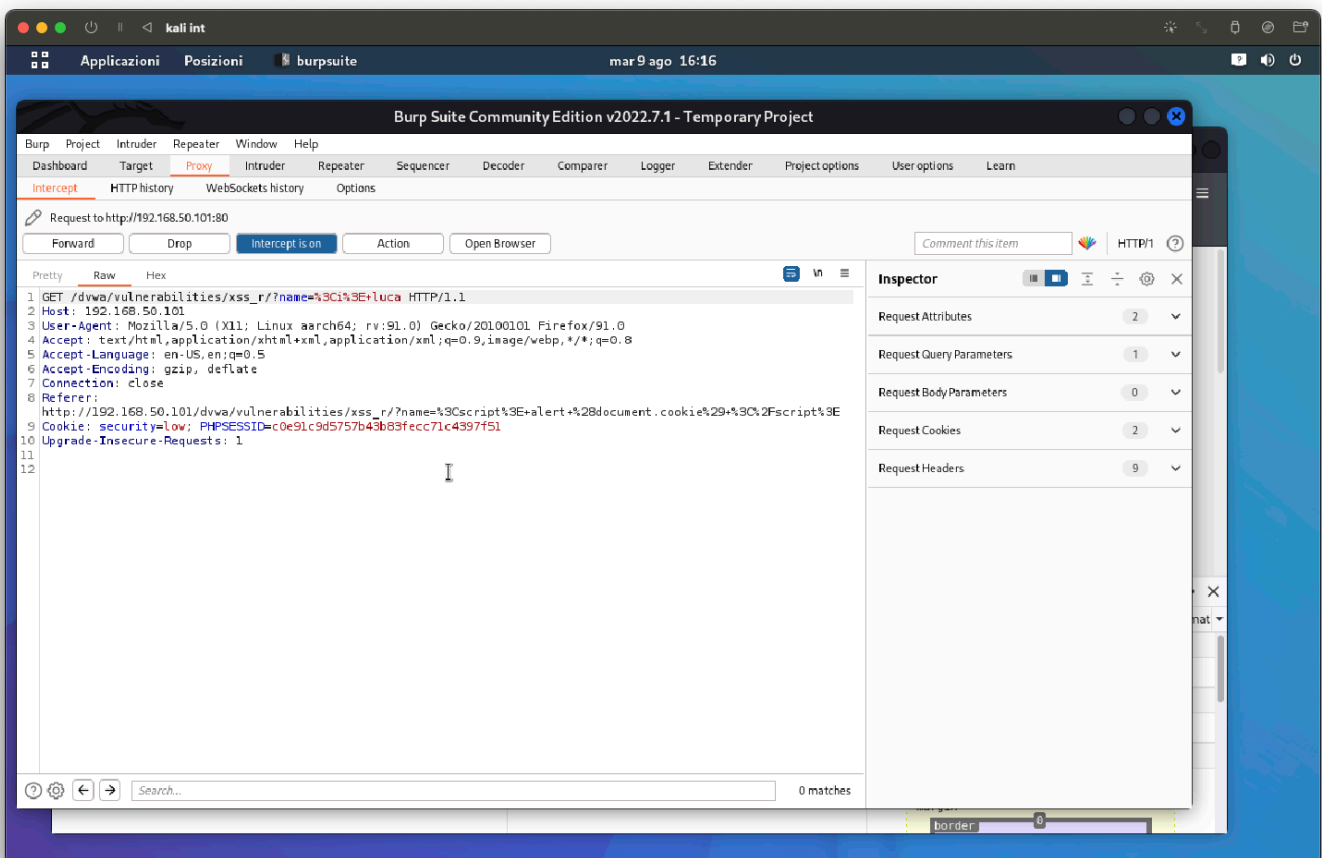


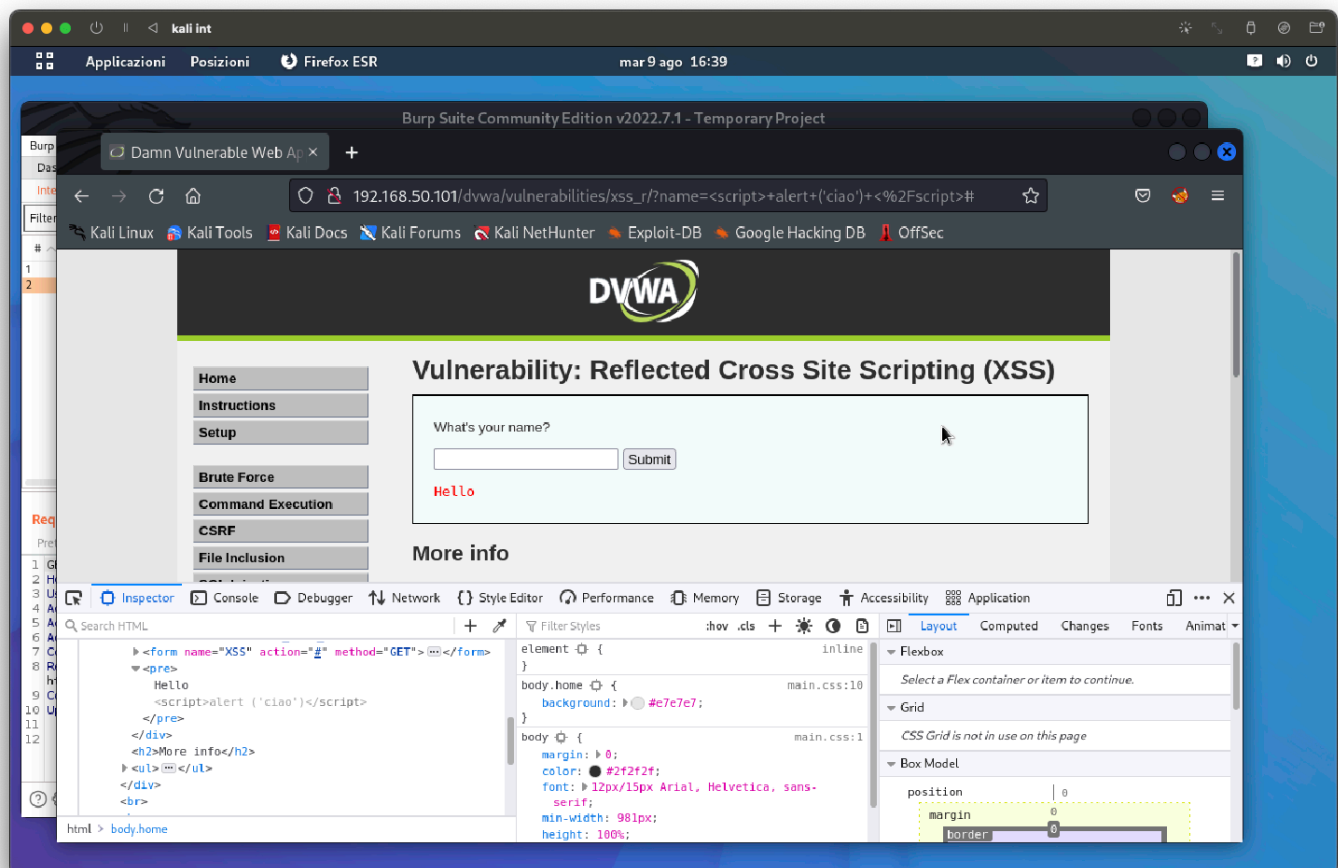
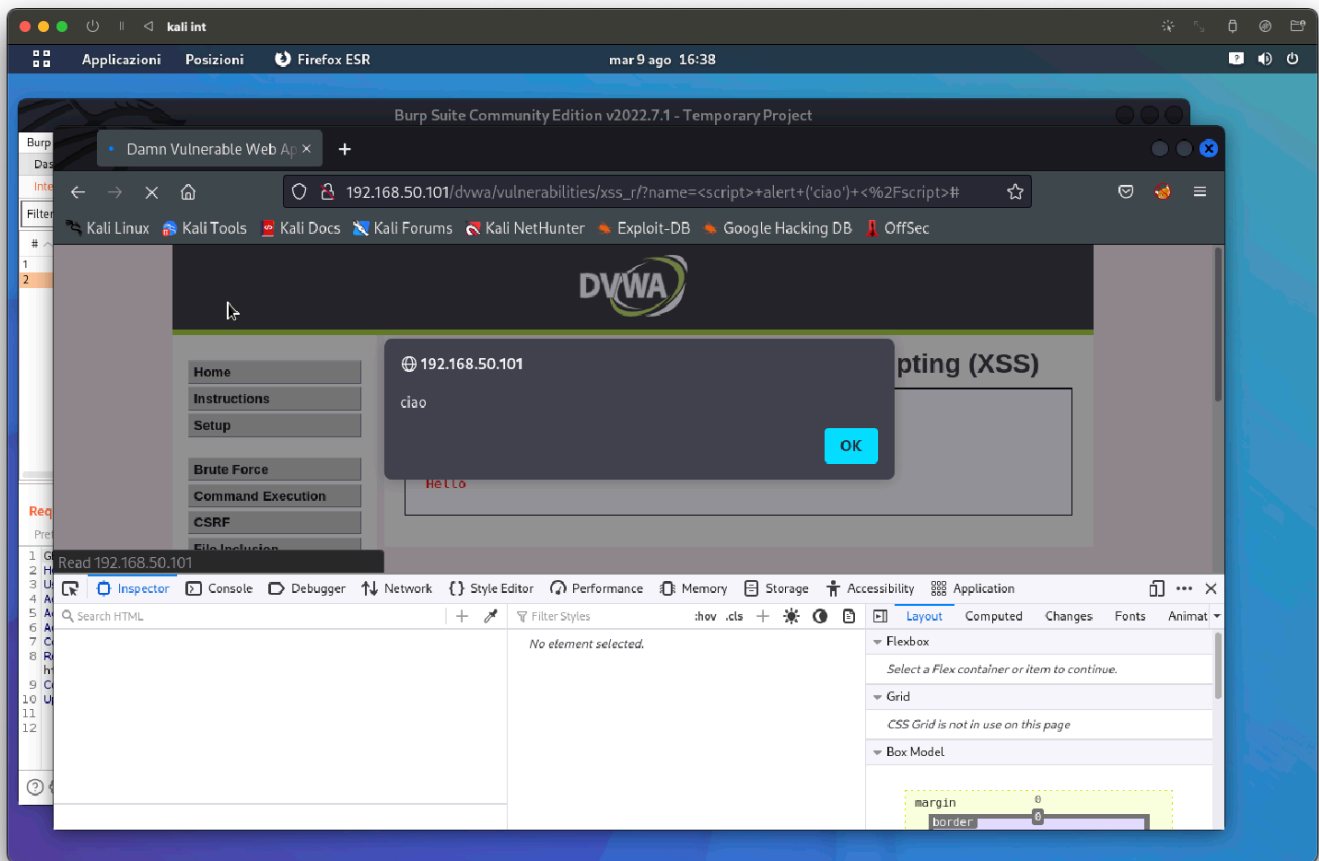
ATTACCO DI TIPO XSS SUL DVWA



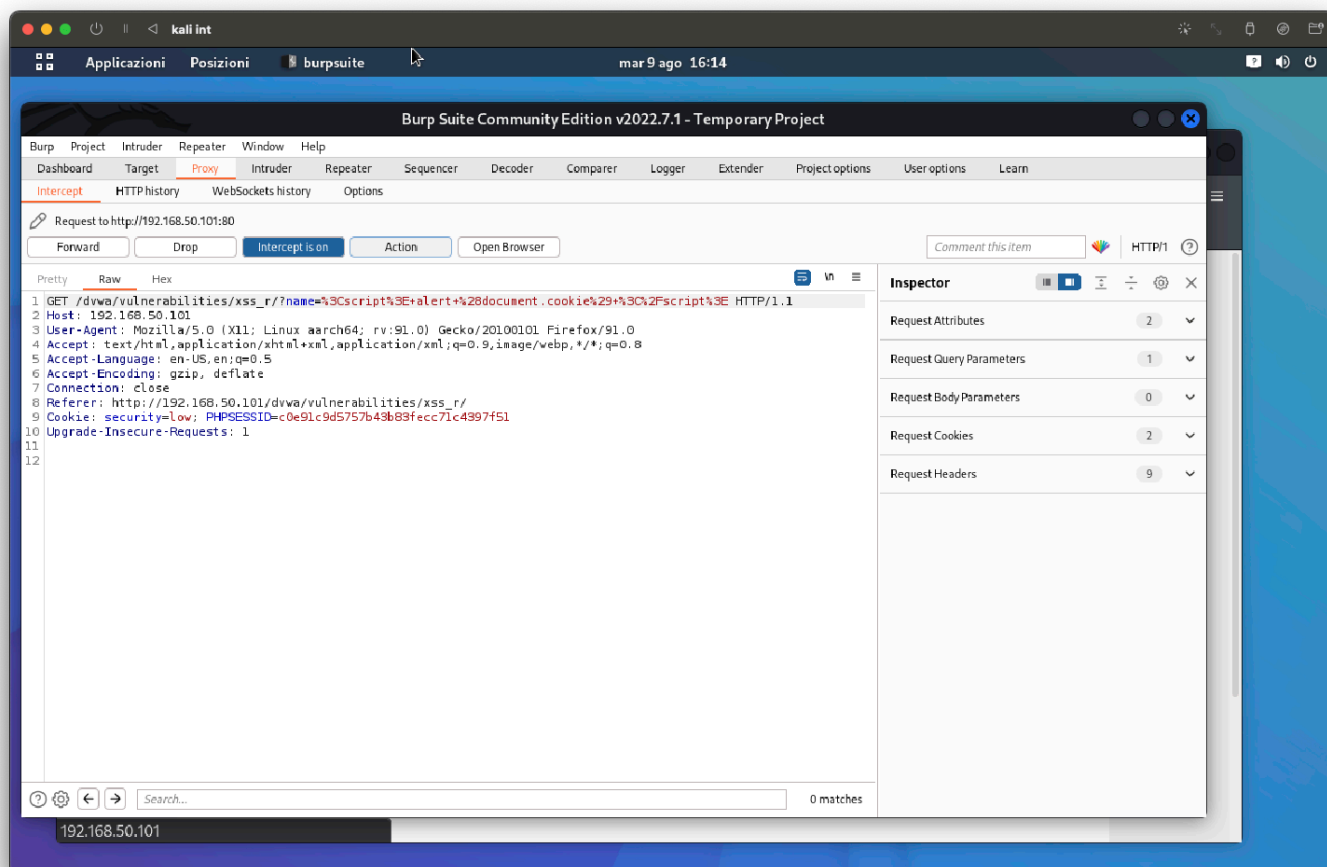
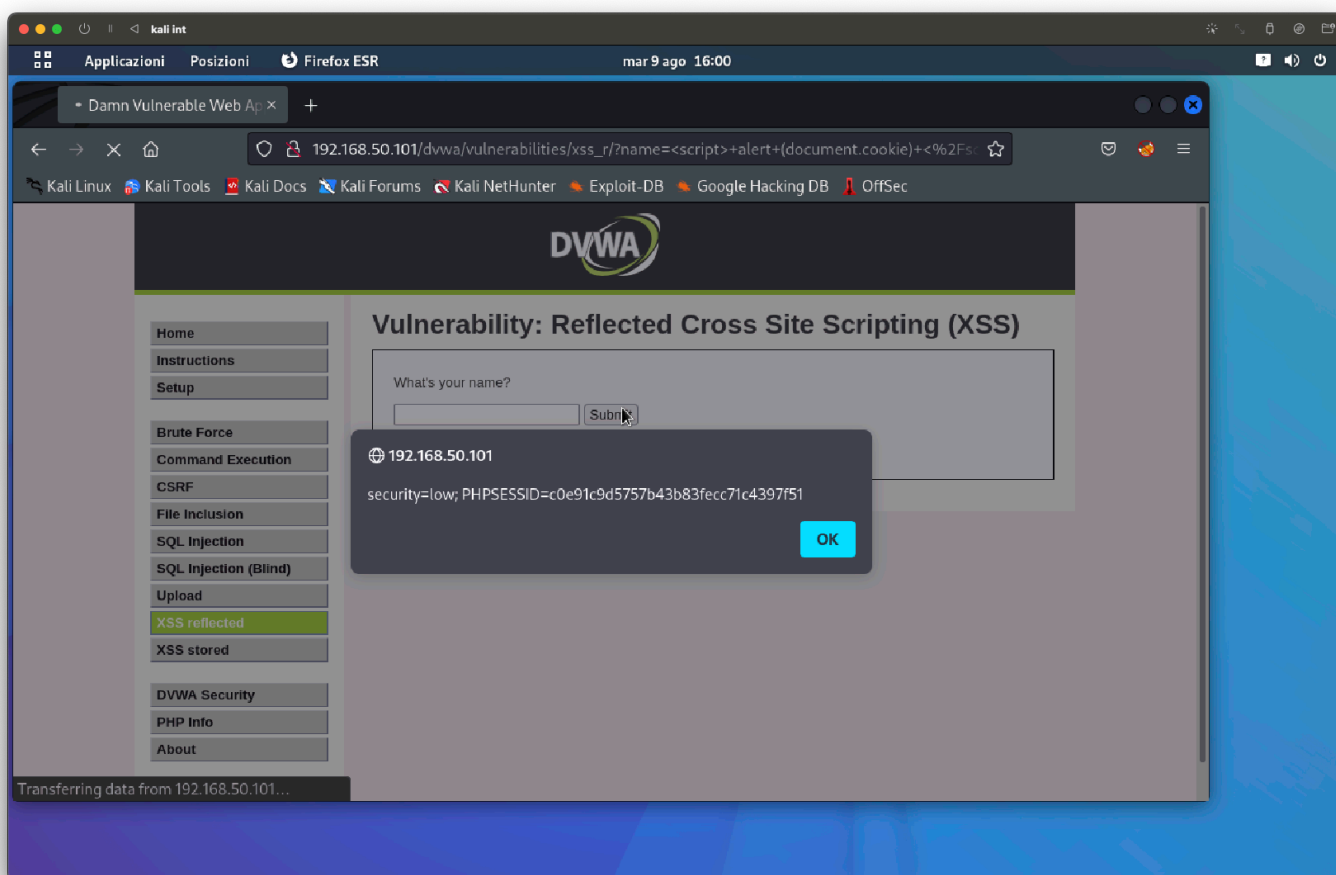
SIAMO ANDATI AD INSERIRE DEL CODICE HTML IN QUESTO CASO ABBIAMO INSERITO IL TAG `<i>` CHE STA PER ITALIC PER FARCI RESTITUIRE UNA STRINGA IN CORSIVO E COME POSSIAMO VEDERE DALLA FOTO SOPRA

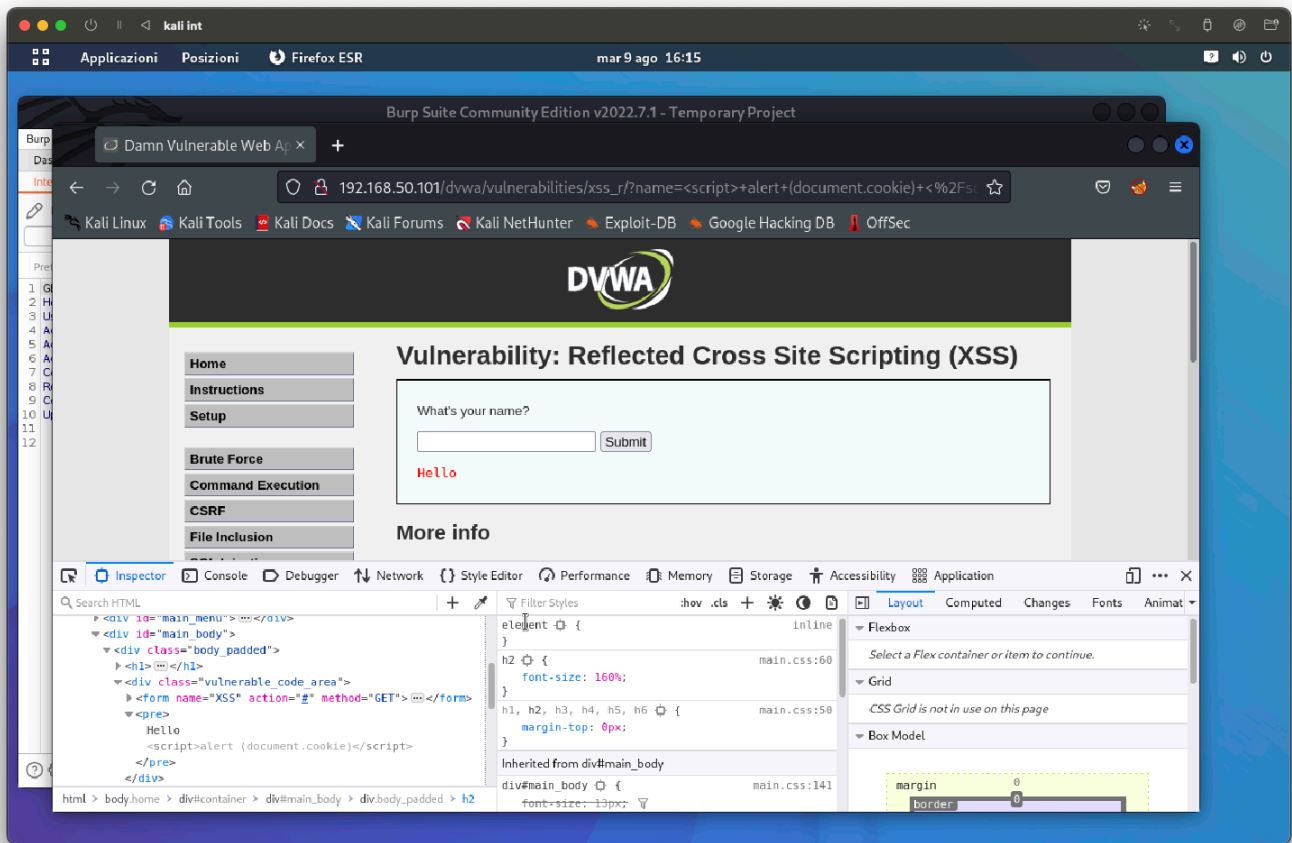


NELLA FOTO SOTTO INVECE SIAMO ANDATI AD INSERIRE UN CODICE HTML/JAVASCRIPT IN QUESTO CASO UN ALERT CON IL SEGUENTE CODICE `<SCRIPT>ALERT('XSS')</SCRIPT>` CHE COME SI PUO VEDERE DALLA FOTO SOTTO CI RESTITUISCE IL POP-UP

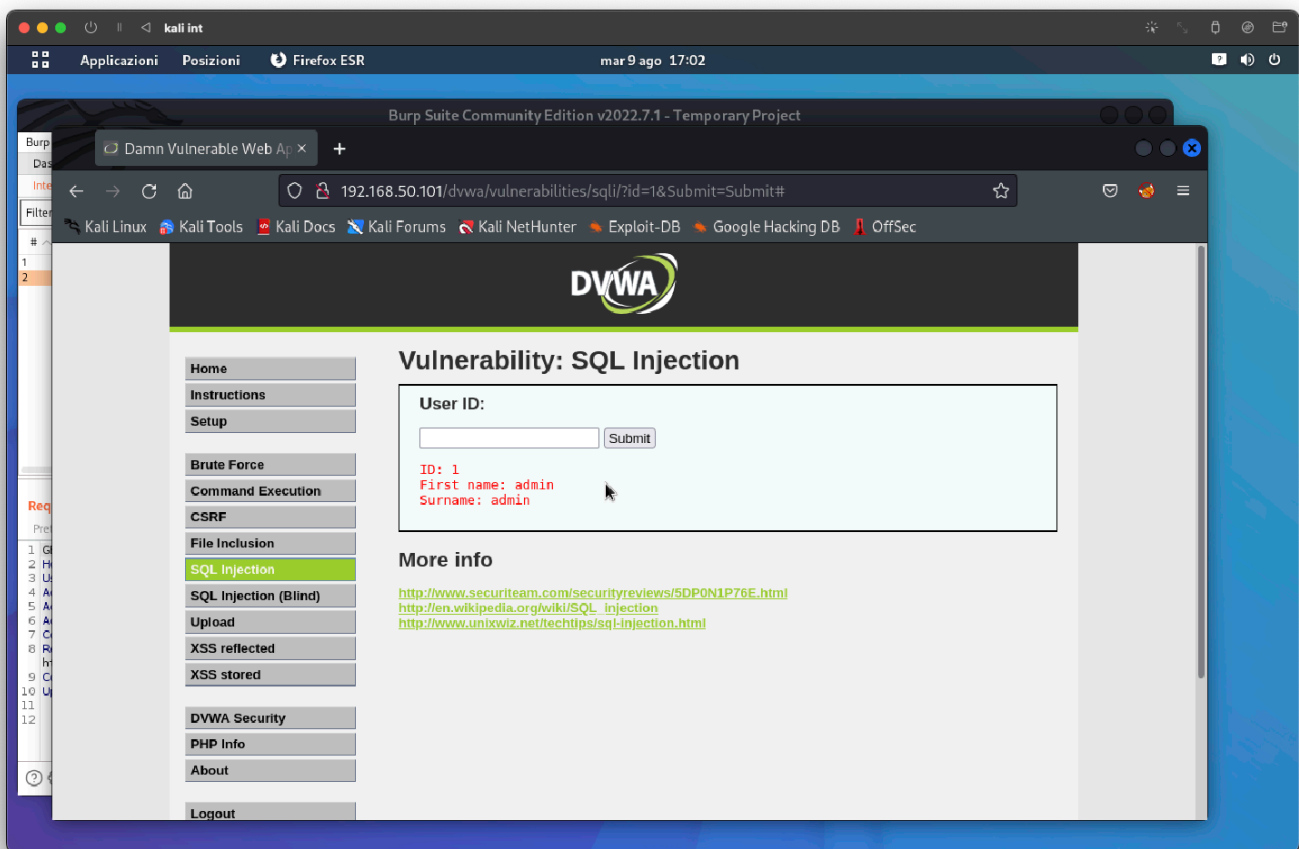


INSERENDO SEMPRE UN CODICE HTML/JAVASCRIPT, IN QUESTO CASO ABBIAMO USATO IL CODICE SEGUENTE `<SCRIPT>ALERT(DOCUMENT.COOKIE)</SCRIPT>` CHE CI RESTITUIRA UN POP-UP CONTENETE IL COOKIE DELLA SESSIONE

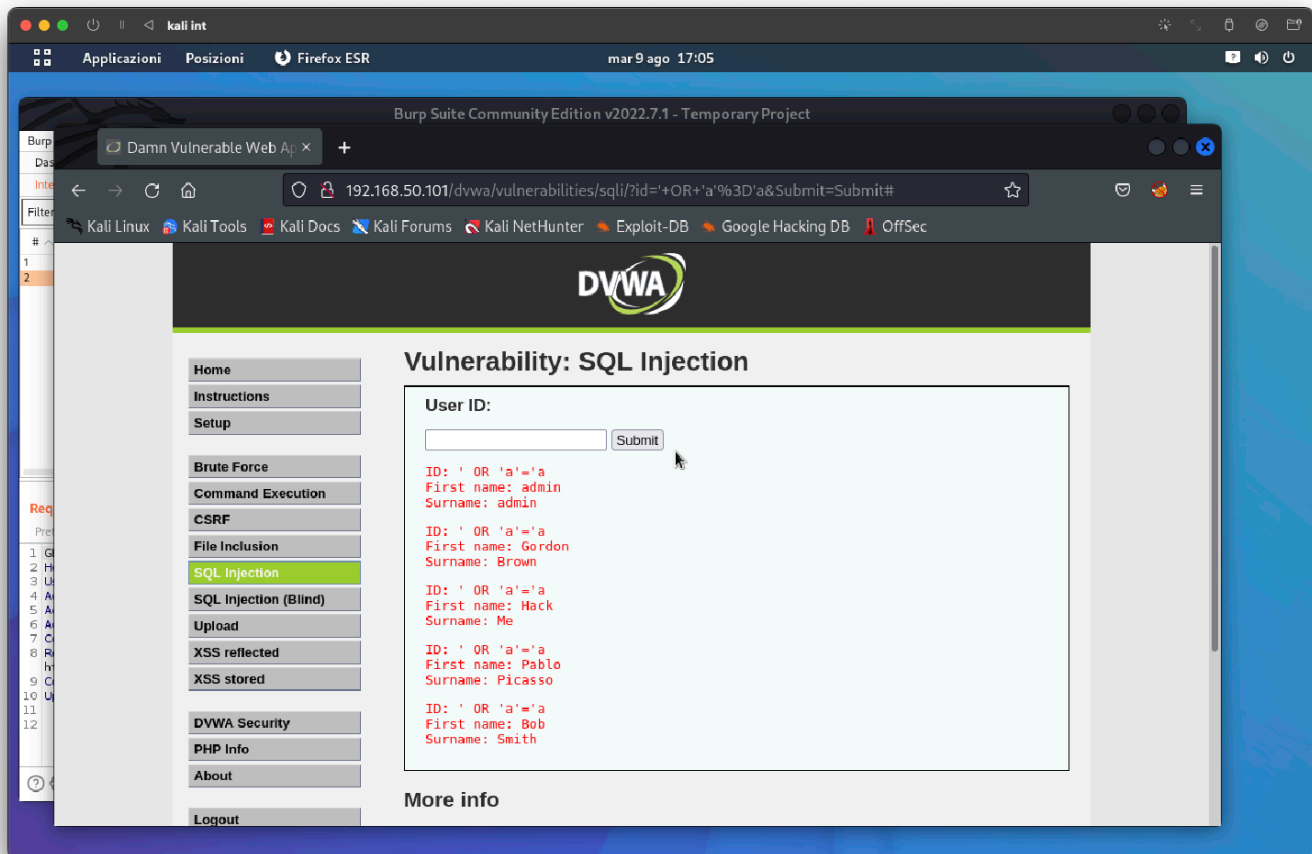




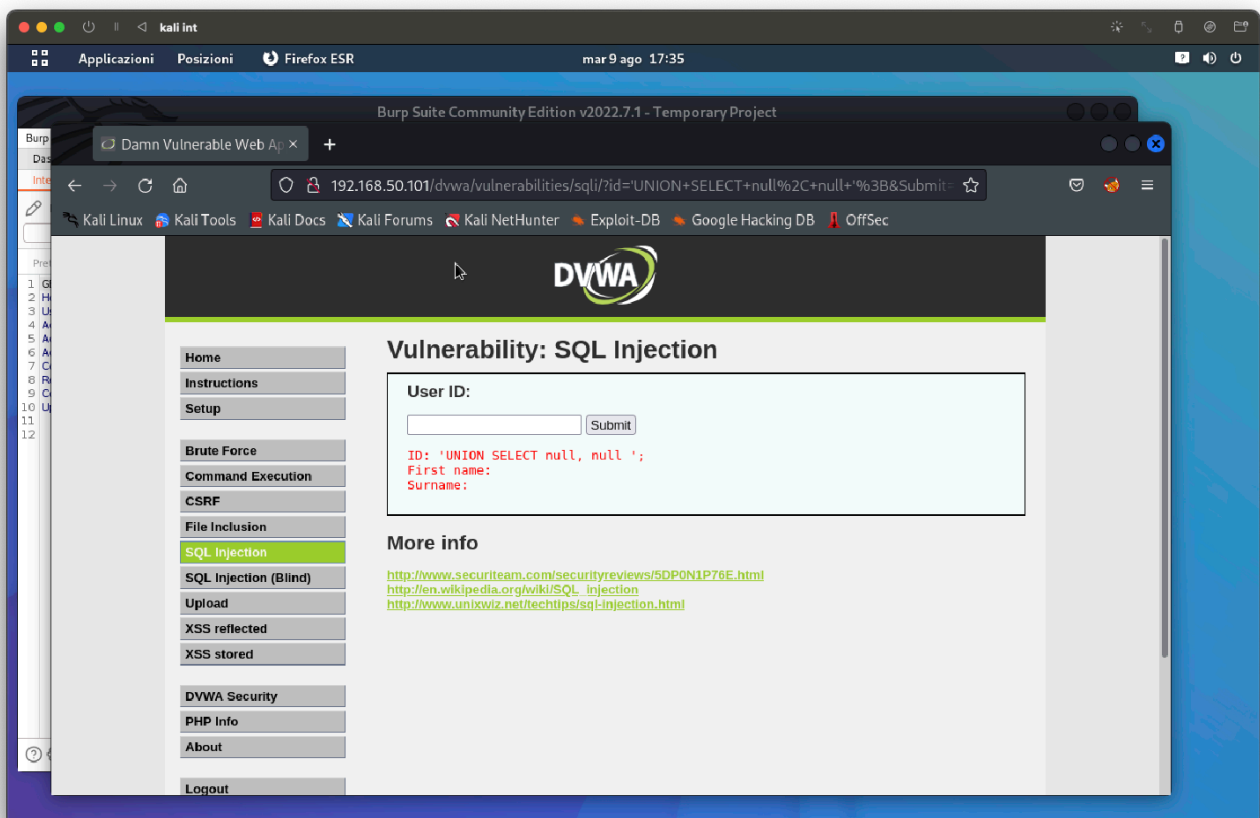
ATTACCO DI TIPO SQL INJECTION SULLA DVWA DI METASPLOITABLE



NELLA FOTO SOPRA METTENDO IL NUMERO DELL'USER ID CI HA RESTITUITO LE INFORMAZIONI RIGUARDANTI L'UTENTE CON ID 1



NEL SECONDO CASO ABBIAMO USATO UNA CONDIZIONE INSERENDO **OR 'A'='A'** QUESTO COMANDO CI RESTITUISCE UNA CONDIZIONE SEMPRE VERA E IN QUESTO CASO IL RISULTATO SARA LA LISTA DI TUTTI GLI UTENTI COME SI PUO NOTARE DALLA FOTO SOPRA



NEL TERZO CASO ABBIAMO USANDO IL COMANDO **UNION** PER UNIRE DUE RISULTATI NELLA FOTO SOPRA SIAMO ANDATI UNIRE I RISULTATI DEGLI UTENTI CON NULL INFATTI SI NOTA CHE NON CI SONO PIU LE INFORMAZIONI RIGUARDANTI GLI UTENTI

UN ALTRA PROVA CHE SONO ANDATO A FARE CERCANDO SU INTERNET SEMPRE CON IL COMANDO UNION SONO ANDATO AD INSERIRE AL POSTO DI NULL I SEGUENTI COMANDI **VERSION()** E **DATABASE()** CHE COME POSSIAMO VEDERE DALLA FOTO SOTTO CI RESTITUISCE LA VERSIONE E IL NOME DEL DATABASE

