Cuore Andrea

29-11-2022

XSS e SQL INJECTION

XSS DVWA:

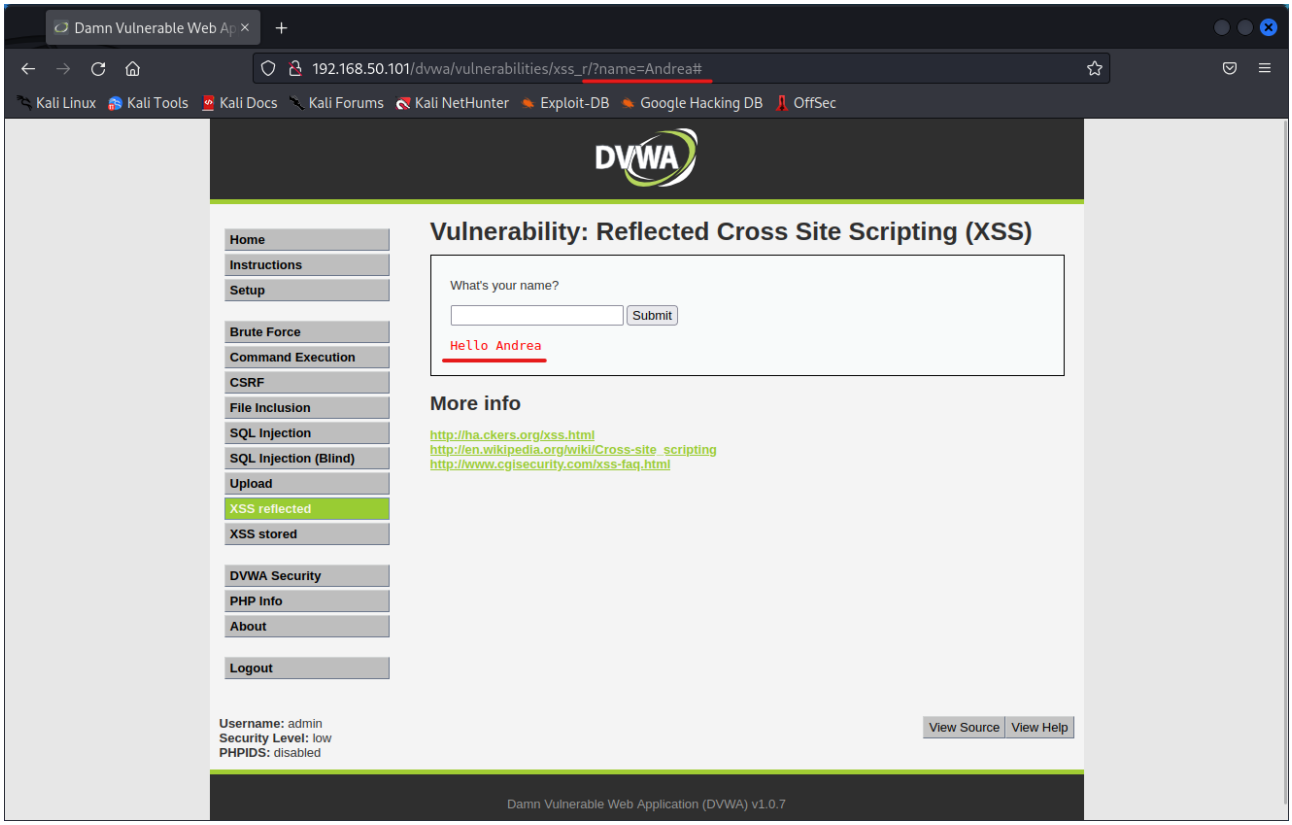
La task di oggi ci richiedeva di effettuare un attacco di XSS su DVWA (livello protezione Low).

L'attacco è stato eseguito nelle seguenti fasi:

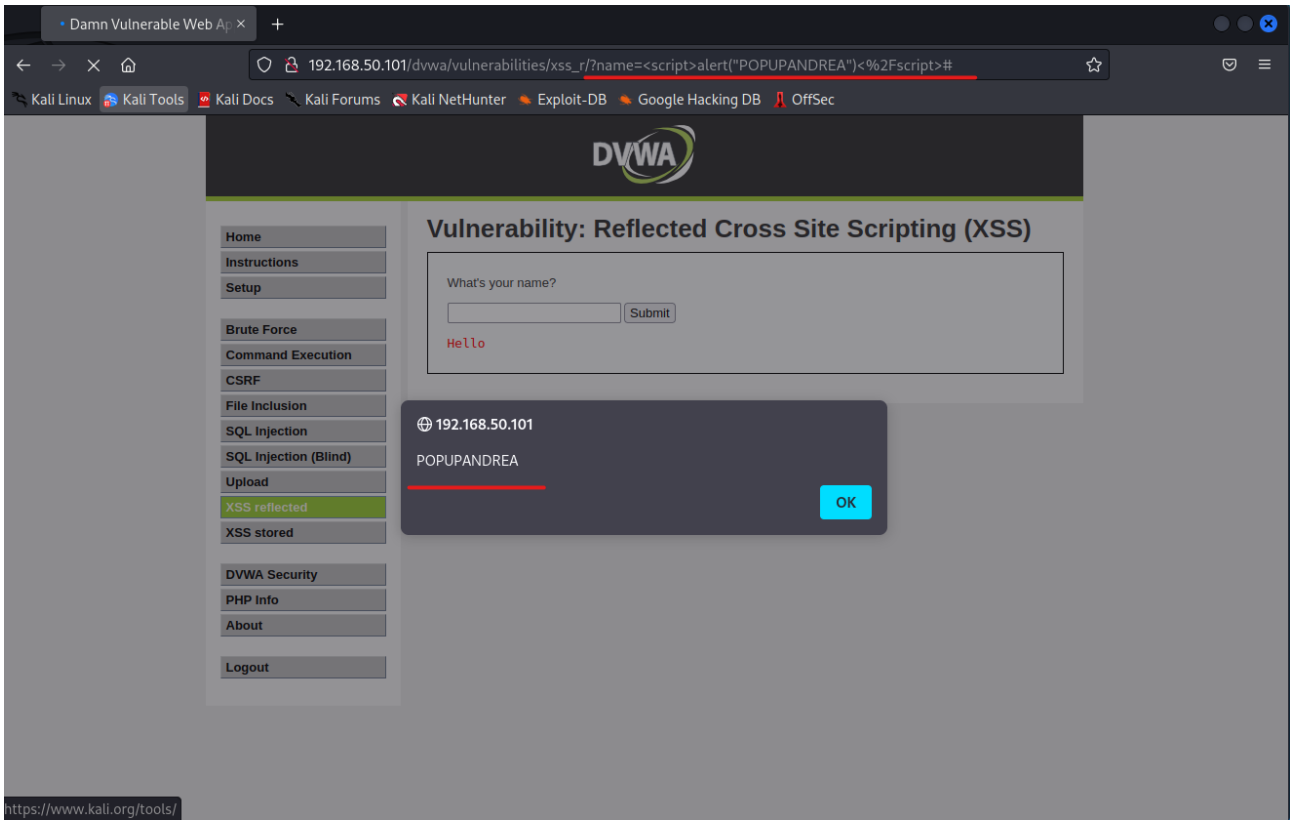
1) Controllo della presenza di vulnerabilità della pagina:
    a. Per effettuare questo tipo di controllo, una volta raggiunta la pagina da me interessata ho svolto 2 tipi di test: Il primo consiste nel monitorare l'URL a seguito di un input nel form presente, in questa fase vediamo che il nostro input viene riportato anche nella stringa URL, controllato ciò si passa alla fase due, ovvero inserire nel form, al posto del nostro nome, uno script che in questo caso ci fa apparire un pop-up
2) Fase di exploit:
    a. . Confermata la presenza di questi due "requisiti" si passa all'exploit vero e proprio, nel nostro caso un cookie grabbing, ovvero nel form andiamo ad inserire uno script che ci darà come risultato un pop-up con il cookie corrente.

Di seguito riportati gli screen delle varie fasi:

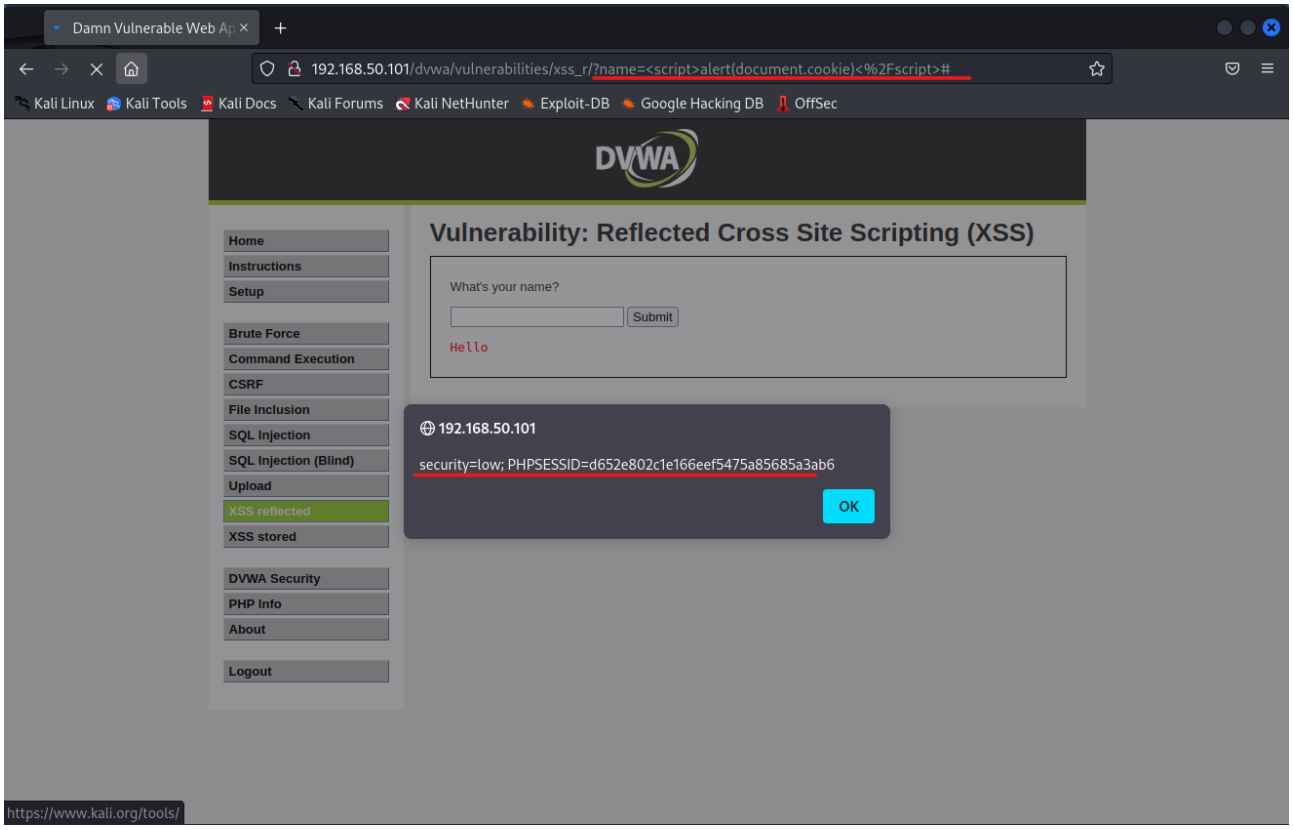
1)



2)



3)

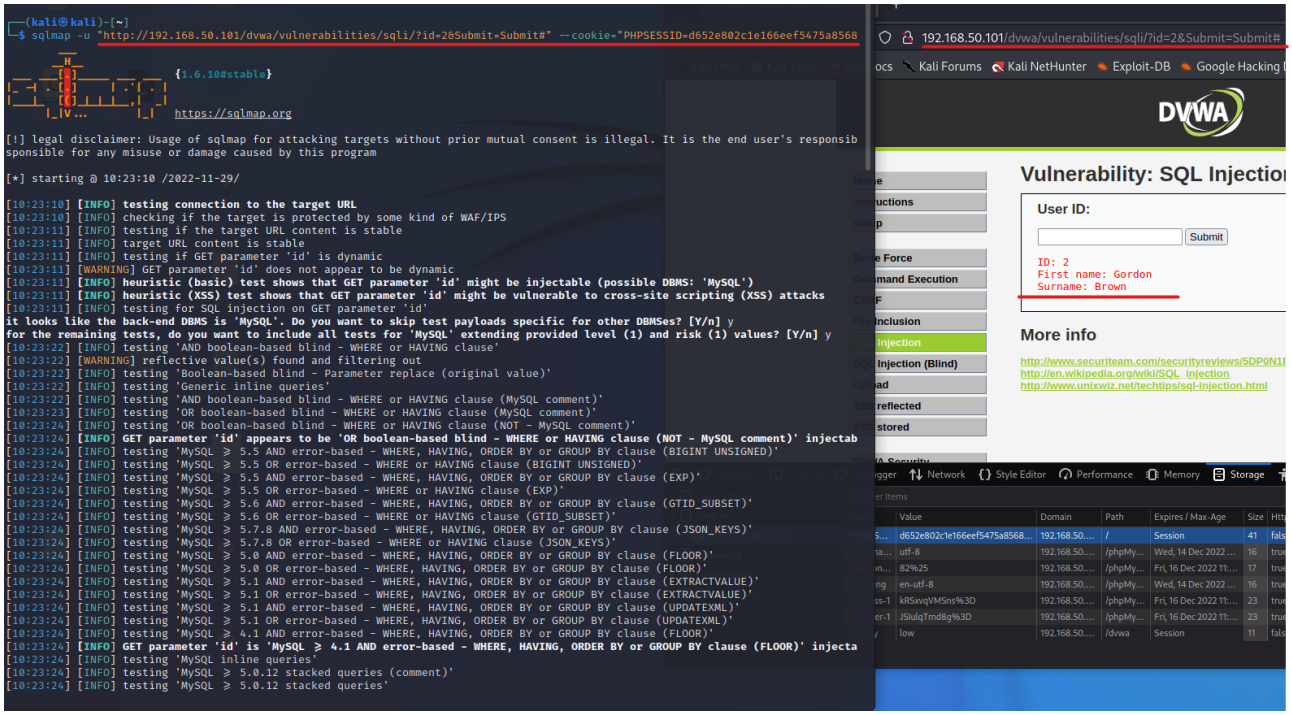


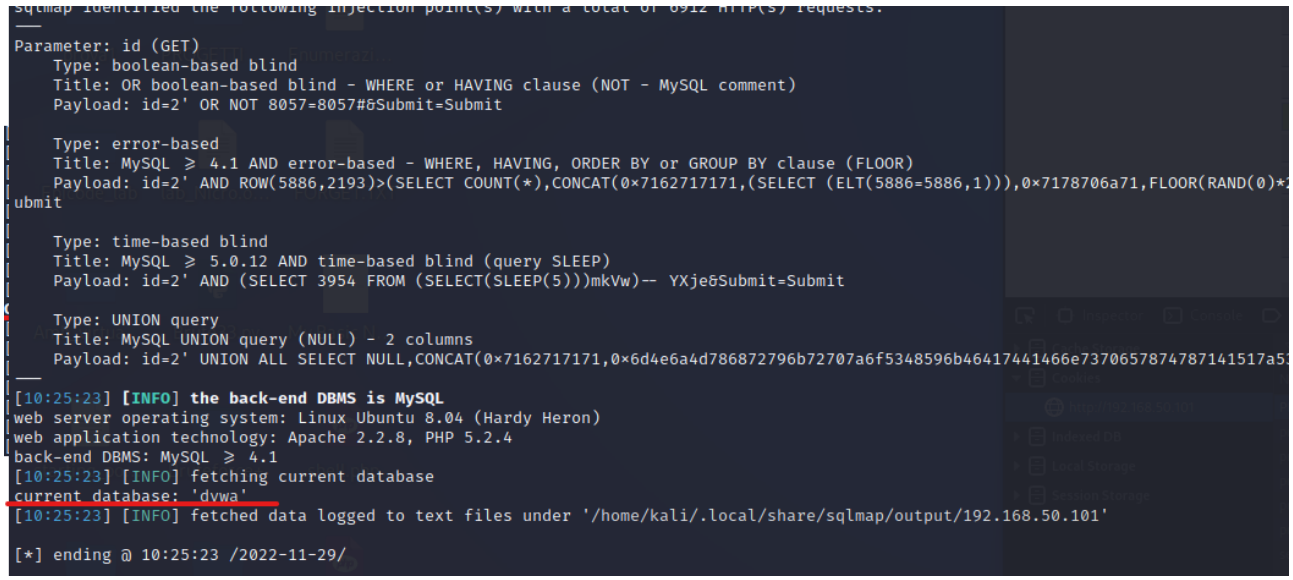
SQL INJECTION:

Per la fase di SQL Injection mi sono avvalso del tool SQLmap, anche qui ho diviso l'attacco in più parti.

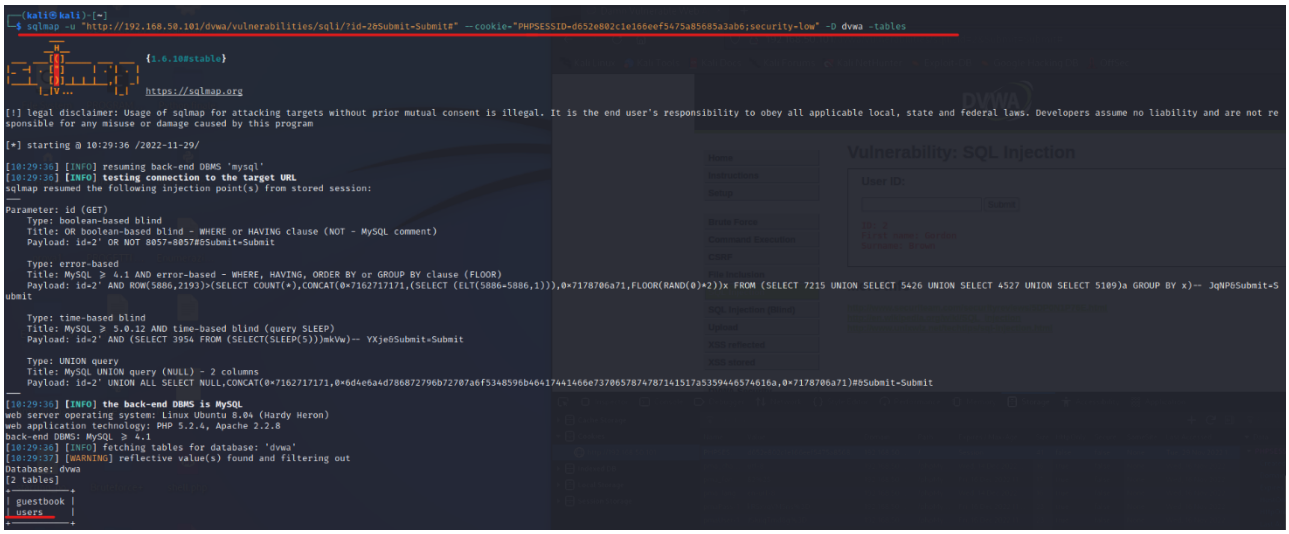
Nella prima fase ho inviato un ID utente nell'apposito form, per recuperare l'URL e rendere meno faticoso e più rapido il lavoro al nostro tool, successivamente ho recuperato l'id di sessione per evitare redirect alla pagina index.php.

Presi questi due componenti possiamo avviare SQLmap per trovare il database corrente che stiamo interrogando.





Una volta trovato il nostro database possiamo andare ad enumerare le "tables" presenti nello stesso.



Notiamo che vi sono 2 tables: Guestbook e user, ora che abbiamo tutti i parametri possiamo finalmente enumerare tutti gli utenti presenti nel database con gli switch:

- -D : equivalente al nome del database trovato inizialmente
- -T: che indica la tables sulla quale vogliamo lavorare

Dunque il comando finale sarà del tipo:

sqlmap -u “url” –cookie “cookie” -D “nome db” -T “tables che vogliamo utilizzare” –dump