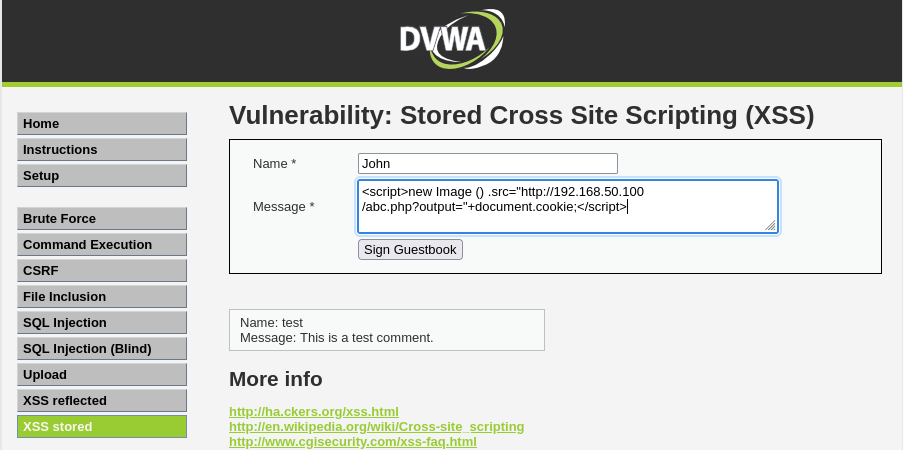
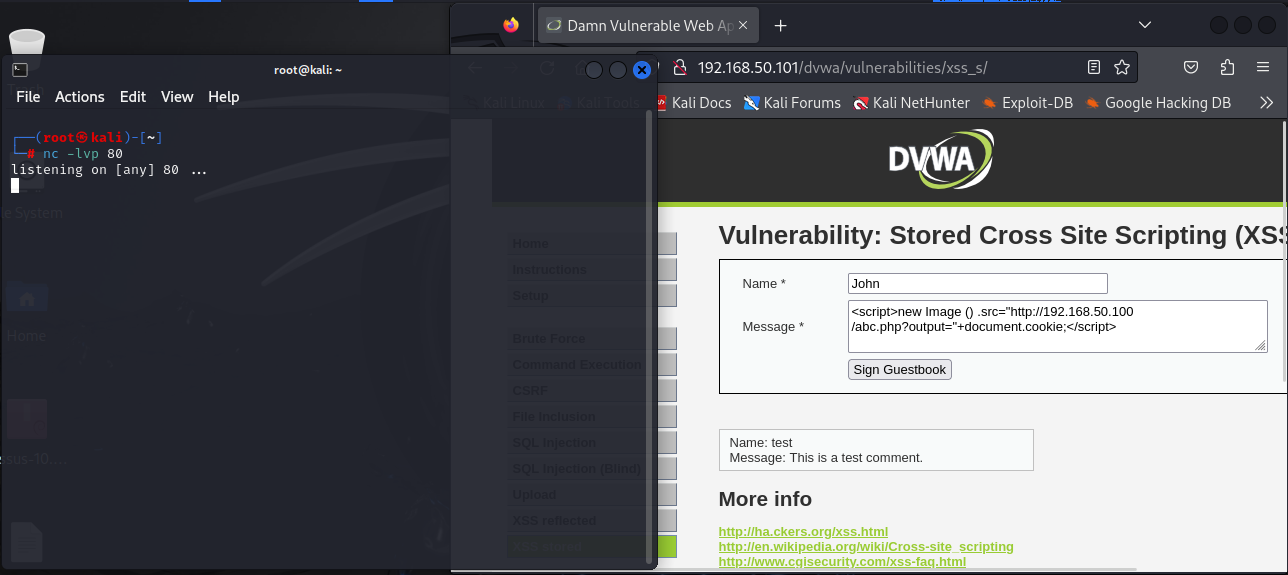
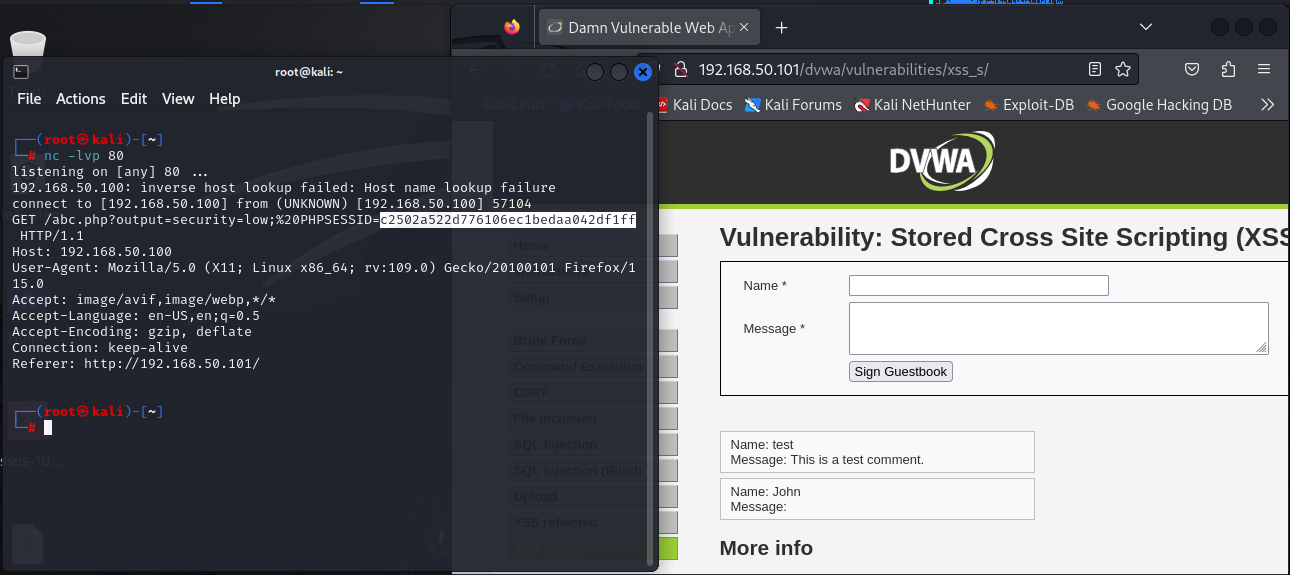
**XSS**

L’XSS è un tipo di vulnerabilità che sfrutta il mancato controllo di file di testo inviati da un attaccante per iniettare stringhe di codice malevole nel sito web visitato dalla vittima.

Nel nostro caso l’obiettivo è rubare i cookie di un ipotetico utente a cui inietteremo questo codice.

Nel livello di difficoltà basso della DVWA il messaggio viene ripulito solo di eventuali spazi ad inizio e fine quindi il nostro codice entrerà sempre nel sito.

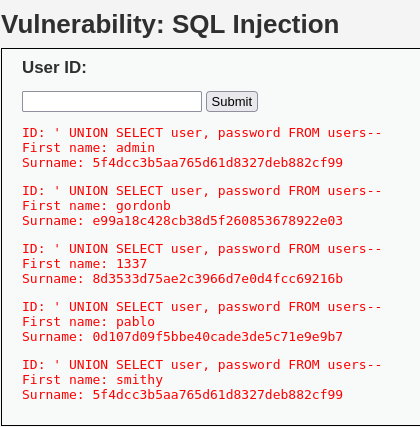
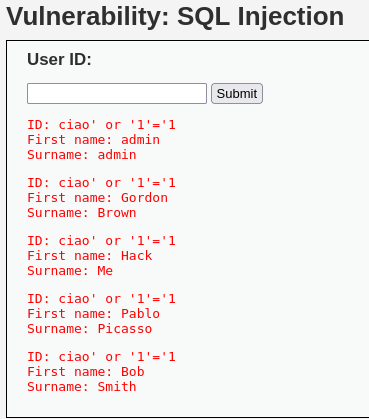
Il codice che andremo ad iniettare rimarrà permanentemente nel sito web a menoche venga rimosso manualmente quindi ogni volta che si accederà a questa pagina, anche il codice verrà eseguito. Il codice che per semplicità ho scritto in Javascript crea un’immagine che andrà al mio url di Kali linux.

Ci mettiamo in ascolto sulla porta 80 e dopo aver iniettato e ricaricato la pagina per far eseguire il codice, avremo a disposizione sul nostro terminale i cookie (evidenziati) che potranno essere in seguito immessi sul nostro browser per permetterci di entrare come admin senza conoscere password o user name. 

**SQL Injection**

SQL Injection è una vulnerabilità che permette all’attaccante di interferire con le query SQL in cui sono stati inseriti dati in modo poco sicuro. E’ una debolezza fortunatamente facile da risolvere ma se presente può causare seri danni perché iniettando codice nel server, l’attaccante può potenzialmente avere accesso a tutti i nomi e le password degli utenti presenti su quel sito.

Il sito ragiona per confronti, quando io fornisco un nome, lui lo confronta con tutti quelli che ha nella sua lista e poi, trovata una coincidenza e ci da una risposta giusta o sbagliata.

Il problema (nel nostro caso in cui non vi sono controlli sulle stringhe inserite) è che se noi forniamo una verità logica come ad esempio 1=1, essendo sempre gusta, il sito lo percepirà come un imput valido per ogni campo quindi ci fornirà tutti i dati presenti in quella colonna di database. 

Le password nel nostro caso sono cifrate con in codice Hash ma possono essere facilmente reperite essendo il codice Hash un codice universale.Q